COMBINING DIRTY-PAPER CODING AND ARTIFICIAL NOISE FOR SECRECY

Bo Wang[*]*, Pengcheng Mu*[*]*, Chao Wang*[*]*, Weile Zhang*[*]*, Hui-Ming Wang*[*] *and Bobin Yao*[†]

[*]School of Electron. & Inform. Eng., Xi'an Jiaotong University, Xi'an, China 710049
[†]School of Electron. & Control Eng., Chang'an University, Xi'an, China, 710064

ABSTRACT

This paper studies the dirty-paper coding (DPC) based secure transmission in a multiuser broadcast channel. Since the encoding order of DPC determines which information-bearing signals must be treated as noise by potential eavesdroppers, adopting DPC enables the accurate characterization of the intrinsic secrecy as well as secrecy outage of multiuser broadcasting. Furthermore, the information-bearing signals can be designed to provide secrecy in addition to supporting normal (unclassified) transmission. To show this, we consider the scenario where one user requests secure transmission and the other users request normal transmission, and propose a hybrid secure transmission scheme which combines zero-forcing DPC and artificial noise (AN). By solving the secrecy rate maximization problem under constraints on the secrecy outage probability and the normal communication rates, we find that in addition to supporting the normal transmission, the proposed scheme has the potential to achieve a secrecy rate close to that of the traditional AN-based beamforming.

***Index Terms*—** Physical layer security, broadcast channel, dirty-paper coding, secrecy outage, artificial noise.

1. INTRODUCTION

In this paper we consider the physical layer security in a wiretap broadcast channel (BC) where a multi-antenna transmitter sends independent messages to multiple users in the presence of an external eavesdropper. In this scenario, the received signal of the eavesdropper contains the messages intended for different users. When the eavesdropper tries to decode one message, the other messages act as interference and make the decoding more difficult to succeed. Hence, such multiuser broadcasting provides some *intrinsic secrecy* [1].

In reality, the eavesdropper's channel state information (CSI) is usually unavailable. In this case, the intrinsic secrecy as well as the eavesdropper's decoding ability is hard to characterize. To bypass this problem, an optimistic assumption often adopted in existing works (see e.g. [2]) is that, to decode the message for one user, the eavesdropper always treats the signals for the other users as noise. This assumption overestimates the intrinsic secrecy and the resultant secrecy rates are usually not achievable. Another assumption often adopted (see e.g. [3]) is that, the interference from unintended messages can be completely cancelled. This pessimistic assumption ignores the intrinsic secrecy and leads to conservative secrecy rates. In fact, the key to accurately characterizing the intrinsic secrecy of multiuser broadcasting is the dirty-paper coding (DPC) [4] which achieves the underlying secrecy capacity region [5, 6]. It is shown in [5, 6] that, if the transmitter adopts DPC, then he accurately knows which signals must be regarded as noise and which must be regarded as perfectly cancelled, irrespective of the eavesdropper's CSI. Therefore, the secrecy of some messages can be protected by the others, and this secrecy rate is accurate and achievable in theory. Compared with the traditional artificial noise (AN) based secure transmission scheme [7], such DPC-based scheme has higher power efficiency since it uses information-bearing signals as artificial interference.

In this paper, we assume the eavesdropper's CSI is unavailable and choose secrecy outage as the secrecy metric. We show that adopting DPC enables the accurate characterization of secrecy outage in the wiretap BC. Such characterization incorporates the intrinsic secrecy of multiuser broadcasting and is not seen in existing works. Furthermore, since the information-bearing signals can provide intrinsic secrecy, they can be designed to support secure transmission and normal (unclassified) transmission simultaneously. To show this, we consider the scenario where one user requests secure transmission and the other users request normal transmission, and study the secrecy rate maximization problem under constraints on the secrecy outage probability (SOP) and the normal communication rates. To simplify the problem, we propose a hybrid secure transmission scheme which combines zero-forcing dirty-paper coding (ZF-DPC) [8] and AN. The use of ZF-DPC in physical layer security is rarely studied in existing works, while in this paper we show that the orthogonal structure of ZF-DPC can lead to a closed-form SOP and the global optimal solution to the considered problem. Simulation results show that the proposed scheme can achieve a rather good secrecy rate in addition to supporting the normal transmission. Furthermore, the obtained solution also provides useful insights into the transmission design.

This work is supported in part by the NSFC (No. 61071125, 61172092, and 61172093), and the Foundation for Innovative Research Groups of the NSFC (No. 61221063).

2. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a multiple-input single-output (MISO) wiretap BC with an N-antenna transmitter, Alice, M single-antenna legitimate receivers, Bob-1, Bob-2, ..., Bob-M, and a single-antenna eavesdropper, Eve. When Alice transmits $\mathbf{x} \in \mathbb{C}^N$, the received signals of Bob-m and Eve are, respectively,

$$y_m = \mathbf{h}_m^{\mathrm{H}}\mathbf{x} + n_m, \quad m = 1, 2, \ldots, M \tag{1}$$

$$y_{\mathrm{E}} = \mathbf{h}_{\mathrm{E}}^{\mathrm{H}}\mathbf{x} + n_{\mathrm{E}}, \tag{2}$$

where $\mathbf{h}_m, \mathbf{h}_{\mathrm{E}} \in \mathbb{C}^N$ denote the channels from Alice to Bob-m and Eve, respectively, and n_m and n_{E} are the receiver noises and assumed to be independent $\mathcal{CN}(0,1)$ variables.

To send independent messages to each user, the broadcast signal $\mathbf{x}$ can be decomposed as $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2 + \cdots + \mathbf{x}_M$, where $\mathbf{x}_m \sim \mathcal{CN}(\mathbf{0}, \mathbf{K}_m)$ is the signal intended for Bob-m. The secrecy capacity region of the underlying multiple-input multiple-output (MIMO) wiretap BC is established in [5, 6] where the secrecy is achieved by combining DPC [4, 8] and random binning. Let the encoding order of DPC be from 1 to M, then the achievable secrecy rate of Bob-m is given by

$$R_{\mathrm{s},m} \leq \left\{\log\left(1+\gamma_m\right) - \log\left(1+\gamma_{\mathrm{E},m}\right)\right\}^+, \tag{3}$$

for $m = 1, 2, \ldots, M$, where $\{\cdot\}^+$ stands for $\max\{\cdot, 0\}$,

$$\gamma_m = \frac{\mathbf{h}_m^{\mathrm{H}}\mathbf{K}_m\mathbf{h}_m}{\mathbf{h}_m^{\mathrm{H}}\left(\sum_{i=m+1}^{M}\mathbf{K}_i\right)\mathbf{h}_m + 1}, \tag{4}$$

is the equivalent signal-to-noise ratio (SNR) of Bob-m, and

$$\gamma_{\mathrm{E},m} = \frac{\mathbf{h}_{\mathrm{E}}^{\mathrm{H}}\mathbf{K}_m\mathbf{h}_{\mathrm{E}}}{\mathbf{h}_{\mathrm{E}}^{\mathrm{H}}\left(\sum_{i=m+1}^{M}\mathbf{K}_i\right)\mathbf{h}_{\mathrm{E}} + 1}, \tag{5}$$

is Eve's equivalent SNR when she tries to decode the message for Bob-m. From (4) and (5) we see that, as an effect of DPC, both Bob-m and Eve should treat $\sum_{i=1}^{m-1}\mathbf{x}_i$ as perfectly cancelled and $\sum_{i=m+1}^{M}\mathbf{x}_i$ as noise. In other words, later encoded messages can provide intrinsic secrecy for earlier encoded users.

In this paper, we assume the CSI concerning the legitimate parties ($\{\mathbf{h}_m\}$) is publicly known, while the CSI of Eve ($\mathbf{h}_{\mathrm{E}}$) is only known by herself. Furthermore, we assume $\mathbf{h}_{\mathrm{E}} \sim \mathcal{CN}(\mathbf{0}, \Gamma_{\mathrm{E}}\mathbf{I}_N)$. Under this assumption, (3) cannot give an achievable secrecy rate and we choose secrecy outage [9] as the secrecy metric, which refers to the situation when (3) is violated and perfect secrecy is compromised. Therefore the secrecy outage probability (SOP) of Bob-m is defined by

$$p_{\mathrm{so},m} \triangleq \Pr\left\{\log\left(1+\gamma_{\mathrm{E},m}\right) > \log\left(1+\gamma_m\right) - R_{\mathrm{s},m}\right\}, \tag{6}$$

where $R_{\mathrm{s},m}$ denotes the actually used secrecy rate of Bob-m.

In the following, we consider the scenario where one of the users (the secret Bob) requests secure transmission and the others (the normal Bobs) request normal transmission. Supposing Alice must support the communication rates required by the normal Bobs, the information-bearing signals for those users provide some intrinsic secrecy. We are interested in how much this intrinsic secrecy can be converted into the achievable secrecy rate of the secret Bob under an SOP constraint. To enable more intrinsic secrecy, we encode the secret message in the first place. Then all the other signals must be regarded as noise when Eve tries to decode the secret message, and we can deliberately design these signals to improve secrecy. Based on this point of view, we assume the secret Bob is Bob-1, and the encoding order is from 1 to M. The secrecy rate maximization problem is formulated as follows:

$$\max_{\{\mathbf{K}_m\}, R_{\mathrm{s},1}} \quad R_{\mathrm{s},1} \tag{7a}$$

$$\text{s.t.} \quad p_{\mathrm{so},1} \leq \varepsilon, \tag{7b}$$

$$\log\left(1+\gamma_m\right) \geq R_{\mathrm{b},m},\ m = 2, 3, \ldots, M, \tag{7c}$$

$$\mathrm{Tr}\left(\sum_{m=1}^{M}\mathbf{K}_m\right) \leq P, \tag{7d}$$

$$\mathbf{K}_m \succeq \mathbf{0},\ m = 1, 2, \ldots, M, \tag{7e}$$

where (7b) is the SOP constraint and $\varepsilon \in (0,1)$ is the required SOP, (7c) represents the constraints on the normal communication rates and $R_{\mathrm{b},m}$ is the rate required by Bob-m, (7d) is the power constraint and P is the power budget of Alice, and (7e) ensures that $\mathbf{K}_m$'s are valid covariance matrices.

3. HYBRID SECURE TRANSMISSION SCHEME

To simplify the optimization problem (7) and maintain performance, we propose a hybrid secure transmission scheme which combines ZF-DPC [8] and AN. The merit of ZF-DPC is that it can completely cancel the inter-user interference by combining DPC and (partial) zero-forcing beamforming, and its orthogonal structure is also compatible with AN.

To enable the proposed scheme, we assume $M \leq N$, and the channel matrix $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_M]^{\mathrm{H}}$ admits the QR decomposition $\mathbf{H} = \mathbf{G}\mathbf{U}_{\mathrm{s}}^{\mathrm{H}}$ where $\mathbf{G}$ is an $M \times M$ lower triangular matrix with diagonal entries $[\mathbf{G}]_{m,m} = \sqrt{g_m} \geq 0$ and $\mathbf{U}_{\mathrm{s}} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_M]$ is an $N \times M$ sub-unitary matrix. The hybrid transmit signal contains M information-bearing signals and $(N-M)$ additional AN signals:

$$\mathbf{x} = \mathbf{W}\mathbf{s} \tag{8}$$

where $\mathbf{s} = [s_1, s_2, \ldots, s_M, v_{M+1}, v_{M+2}, \ldots, v_N]^{\mathrm{T}}$ with $s_m \sim \mathcal{CN}(0,1)$ being the information-bearing signal for Bob-m and $v_n \sim \mathcal{CN}(0,1)$ the AN signal in the n-th direction. The beamforming matrix $\mathbf{W}$ takes the form of

$$\mathbf{W} = \mathbf{U}\mathrm{diag}\left(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_N}\right), \tag{9}$$

where $\mathrm{diag}(\cdot)$ denotes a diagonal matrix with the corresponding diagonal elements, p_n denotes the power allocated to the n-th direction and $\mathbf{U} = [\mathbf{U}_{\mathrm{s}}, \mathbf{u}_{M+1}, \mathbf{u}_{M+2}, \ldots, \mathbf{u}_N]$ is

an $N \times N$ unitary matrix. In other words, the information-bearing signals and AN signals are transmitted in N orthogonal directions, and the covariance matrix for each signal takes the unified expression

$$\mathbf{K}_n = p_n \mathbf{u}_n \mathbf{u}_n^{\mathrm{H}}, \quad n = 1, 2, \ldots, N. \tag{10}$$

Substituting (10) and $\mathbf{H} = \mathbf{G}\mathbf{U}_{\mathrm{s}}^{\mathrm{H}}$ into (4) and (5), we find that the equivalent SNR of Bob-m is simplified as $\gamma_m = g_m p_m$ (the AN signals do not affect Bobs since they are distributed in the null space of $\mathbf{H}$), and that of Eve becomes

$$\gamma_{\mathrm{E},1} = \frac{\left|\mathbf{h}_{\mathrm{E}}^{\mathrm{H}} \mathbf{u}_1\right|^2 p_1}{\sum_{n=2}^{N} \left|\mathbf{h}_{\mathrm{E}}^{\mathrm{H}} \mathbf{u}_i\right|^2 p_n + 1}. \tag{11}$$

Based on the above results, the secrecy rate maximization problem (7) can be simplified as the following power allocation problem:

$$\max_{\{p_n\}, z \geq 0} \quad R_{\mathrm{s},1} = \log\left(1 + g_1 p_1\right) - \log(1 + z) \tag{12a}$$

$$\text{s.t.} \quad \Pr\left\{ \frac{\left|\mathbf{h}_{\mathrm{E}}^{\mathrm{H}} \mathbf{u}_1\right|^2 p_1}{\sum_{n=2}^{N} \left|\mathbf{h}_{\mathrm{E}}^{\mathrm{H}} \mathbf{u}_n\right|^2 p_n + 1} > z \right\} \leq \varepsilon, \tag{12b}$$

$$p_m \geq q_m, \quad m = 2, 3, \ldots, M, \tag{12c}$$

$$\textstyle\sum_{n=1}^{N} p_n \leq P, \tag{12d}$$

$$p_n \geq 0, \quad n = 1, 2, \ldots, N, \tag{12e}$$

where $\log(1+z)$ denotes the rate redundancy used to confuse Eve, and $q_m = (2^{R_{\mathrm{b},m}} - 1)/g_m$ corresponds to the required communication rate of Bob-m.

Remark 1. We note that (12) is similar to the optimization of AN-based beamforming. Here the information-bearing signals together with AN signals act as interference and provided secrecy. However, (12c) indicates that the information-bearing signals should also support the normal transmission.

4. EFFICIENT ALGORITHM

The biggest challenge in solving (12) lies in the SOP constraint (12b). Nevertheless, thanks to the orthogonal structure (9), the constraint (12b) can be rewritten as [10]:

$$\text{(12b)} \Leftrightarrow \exp\left(-\frac{z}{\Gamma_{\mathrm{E}} p_1}\right) \prod_{n=2}^{N} \left(1 + \frac{z p_n}{p_1}\right)^{-1} \leq \varepsilon. \tag{13}$$

Introducing $w = z/p_1$, now we can reformulate (12) as:

$$\max_{\{p_n\}, w} \quad R_{s,1} = \log\left(1 + g_1 p_1\right) - \log(1 + w p_1) \tag{14a}$$

$$\text{s.t.} \quad w/\Gamma_{\mathrm{E}} + \textstyle\sum_{n=2}^{N} \ln\left(1 + w p_n\right) \geq \ln(\varepsilon^{-1}), \tag{14b}$$

$$\text{(12c), (12d), (12e)}, \tag{14c}$$

where (14b) is transformed from (12b) using (13).

As stated before, if we ignore (12c), then (14) becomes the AN-based secrecy rate maximization problem which has been well studied in existing works [11, 12]. It is known that allocating the power uniformly among $p_2, p_3, \ldots, p_N$ is optimal in terms of secrecy [11]. In the following, we will show that the power allocation among $p_2, p_3, \ldots, p_N$ is still clear when both secure and normal transmission are taken into consideration. To this end, we decompose (14) as

$$\max_{p_1 \geq 0} R\left(p_1\right) = \log\left(1 + g_1 p_1\right) - \log(1 + w\left(p_1\right) p_1), \tag{15}$$

where $w(p_1)$ is the optimal objective value of the optimization problem with a fixed p_1:

$$w\left(p_1\right) = \min_{\mathbf{p}, w} \quad w \tag{16a}$$

$$\text{s.t.} \quad \text{(14b), (12d)}, \tag{16b}$$

$$p_n \geq q_n, \quad n = 2, 3, \ldots, N, \tag{16c}$$

where $\mathbf{p}$ denotes $[p_2, p_3, \ldots, p_N]$ and

$$q_n = \begin{cases} (2^{R_{\mathrm{b},n}} - 1)/g_n, & n = 2, 3, \ldots, M, \\ 0, & n = M+1, M+2, \ldots, N. \end{cases} \tag{17}$$

To present the solution to the inner optimization problem (16) concisely, we need to rearrange q_n's such that these thresholds are in ascending order. Without loss of generality, we assume the rearranged q_n's are still denoted by $[q_2, q_3, \ldots, q_N]$ and p_n now corresponds to the rearranged q_n. The following proposition characterizes the global optimal solution to (16), which is denoted by w^* and $\mathbf{p}^* = [p_2^*, p_3^*, \ldots, p_N^*]$.

Proposition 1. *Define*

$$\Delta p \triangleq P - p_1 - \textstyle\sum_{n=2}^{N} q_n, \tag{18}$$

$$q_{\mathrm{s}}\left(n\right) \triangleq \left(n-1\right) q_n - \textstyle\sum_{i=2}^{n} q_i, \ n = 2, 3, \ldots, N, \tag{19}$$

$$F\left(\mathbf{p}, w\right) \triangleq w/\Gamma_{\mathrm{E}} + \textstyle\sum_{n=2}^{N} \ln\left(1 + w p_n\right) - \ln(\varepsilon^{-1}). \tag{20}$$

The problem (16) *is feasible iff* $\Delta p \geq 0$. *When* (16) *is feasible,* $\mathbf{p}^*$ *is given by*

$$p_n^* = \begin{cases} \dfrac{\Delta p - q_{\mathrm{s}}(n^*)}{n^* - 1} + q_{n^*}, & n = 2, 3, \ldots, n^*, \\ q_n, & n = n^*+1, n^*+2, \ldots, N, \end{cases} \tag{21}$$

where $n^* \in \{2, 3, \ldots, N\}$ *is the maximum integer that satisfies* $\Delta p \geq q_{\mathrm{s}}(n^*)$, *and* w^* *is the root of* $F\left(\mathbf{p}^*, w\right) = 0$.

Sketch of the proof. Constraints (12d) and (16c) indicate that (16) is feasible iff $\Delta p \geq 0$. Since $F(\mathbf{p}, w)$ is increasing in w, (14b) indicates that w^* should satisfy $F(\mathbf{p}, w^*) = 0$. Then we note that $F(\mathbf{p}, w)$ is a Schur-concave function of $\mathbf{p}$ [13], and $\mathbf{p}^*$ given by (21) is majorized by any other feasible $\mathbf{p} \neq \mathbf{p}^*$ (cf. Fig. 1). Therefore $F(\mathbf{p}, w) \leq F(\mathbf{p}^*, w)$ and the root of $F(\mathbf{p}^*, w) = 0$ gives the minimum w. □

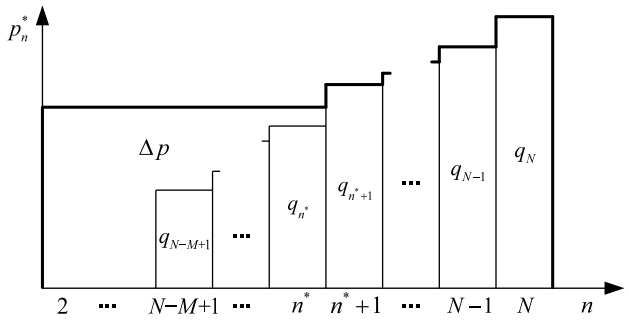

Fig. 1. The optimal power allocation among $p_2, p_3, \ldots, p_N$.

Remark 2. The optimal power allocation (21) is illustrated in Fig. 1 and it can be interpreted as follows. Allocating at least q_n to the n-th direction is necessary to support the required communication rate. Then Δp, the redundant power, is allocated to make the whole allocation as uniform as possible, which is consistent with the design of AN.

For the outer one-variable optimization problem (15), it is clear from Proposition 1 that the feasible range of p_1 is $[0, p_{\max}]$ with $p_{\max} \triangleq P - \sum_{n=2}^{N} q_n$. We have the following conclusion regarding the objective function of (15):

Proposition 2. *$R(p_1)$ is quasi-concave in p_1.*

Sketch of the proof. Using the techniques presented in [12] we can prove the following properties of $w(p_1)$ (the detailed proof is omitted due to space limitation).

Lemma 1. *(i) $w'(p_1)$ is continuous and $w'(p_1) > 0$. (ii) $w''(p_1) > 0$ when $w'(p_1)$ is differentiable.*

Lemma 1 implies that $w(p_1)$ is convex in p_1. Then $R(p_1) = \log(1 + g_1 p_1) - \log(1 + w(p_1)p_1)$ can be viewed as a composition of a monotonic function $\log(\cdot)$ and a concave-over-convex function $\frac{1+g_1 p_1}{1+w(p_1)p_1}$, and its quasi-concavity can be established according to [14, Example 3.38]. □

According to Proposition 2, the objective function $R(p_1)$ is either monotonic or has a unique maximum on $(0, p_{\max})$, which can be distinguished by checking $R'(0)$ and $R'(p_{\max})$. For the latter case, the maximum is achieved at the root of $R'(p_1) = 0$ which can be located using the bisection search. Note that $R'(p_1)$ is given by

$$R'(p_1) = \frac{1}{\ln 2}\left[\frac{g_1}{1+g_1 p_1} - \frac{w'(p_1)\,p_1 + w(p_1)}{1 + w(p_1)\,p_1}\right], \quad (22)$$

and $w'(p_1)$ is given by

$$w' = \frac{w}{1 + w p_{n^*}} \Big/ \left(\frac{1}{\Gamma_{\mathrm{E}}} + \sum_{n=2}^{N} \frac{p_n^*}{1 + w p_n^*}\right). \quad (23)$$

With the help of Proposition 1 and Proposition 2, we conclude that (14) can be efficiently solved to global optimality via (15) and (16).

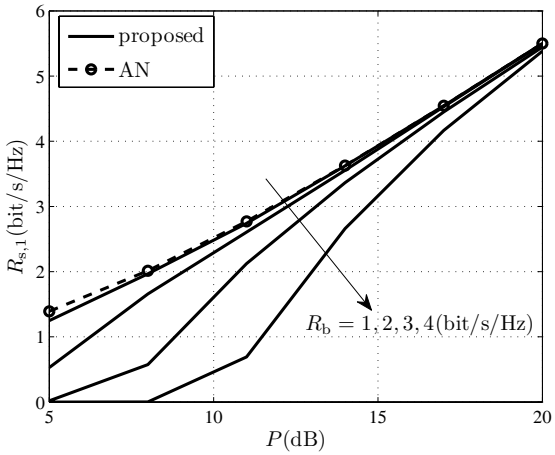

Fig. 2. Secrecy rate versus available power.

5. SIMULATION RESULTS AND CONCLUSIONS

Fig. 2 illustrates the average achievable secrecy rate of the proposed scheme in comparison with that of the traditional AN-based beamforming. The parameters are set as $N = 4$, $M = 3$, $\Gamma_{\mathrm{E}} = 1$, $\varepsilon = 0.1$, and $R_{\mathrm{b},2} = R_{\mathrm{b},3} \triangleq R_{\mathrm{b}} \in \{1, 2, 3, 4 \text{ (bit/s/Hz)}\}$. The results are averaged over 100 realizations of the legitimate channel matrix $\mathbf{H}$, whose elements are independently generated $\mathcal{CN}(0, 1)$ variables. As shown in the figure, the secrecy rate of the proposed scheme is upper bounded by that of the AN scheme, and the performance gap enlarges when P decreases or R_{b} increases. This is because our scheme supports normal transmission in addition to secure transmission. When P is small or R_{b} is great, most of the power will be allocated in favor of normal transmission, which makes the power allocated to Bob-1 limited and that to the other users and AN non-uniform. Nevertheless, the secrecy performance of the proposed schemes converges to that of the AN scheme when P is great enough, which indicates that the required normal communication rates are satisfied by the optimal power allocation of the AN scheme.

In this paper we have studied the DPC-based secure transmission in a multiuser BC. With DPC, we can accurately characterize the intrinsic secrecy as well as secrecy outage of multiuser broadcasting, and use the information-bearing signals as interference to provide secrecy. To further show the performance of the DPC-based scheme, we consider the scenario where one user requests secure transmission and the other users request normal transmission, and propose a hybrid secure transmission scheme which combines ZF-DPC and AN. Simulation results confirm that, in addition to supporting the normal transmission, the secrecy rate achieved by the proposed scheme can be close to that of the traditional AN-based beamforming where only the secure transmission of one user is supported.

6. REFERENCES

[1] 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.

[2] M. F. Hanif, L.-N. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Trans. Signal Process.*, vol. 62, no. 14, pp. 3536–3551, Jul. 2014.

[3] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[4] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.

[5] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[6] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2673–2682, May 2013.

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

[8] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691–1706, Jul. 2003.

[9] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE International Symposium on Information Theory (ISIT'2006)*, Jul. 2006, pp. 356–360.

[10] Hongsheng Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

[11] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[12] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18–21, Jan. 2015.

[13] Albert W Marshall, Ingram Olkin, and Barry C Arnold, *Inequalities: Theory of Majorization and Its Applications*, Springer-Verlag New York, second edition, 2011.

[14] Stephen Boyd and Lieven Vandenberghe, *Convex Optimaziation*, Cambridge University Press, 2004.