Capacity, MSE and Secrecy Analysis of Linear Block Precoding for Distributed Antenna Systems in Multi-User Frequency-Selective Fading Channels

Toshiaki Koike-Akino, Andreas F. Molisch, *Fellow, IEEE*, Chunjie Duan, Zhifeng Tao, and Philip Orlik

Abstract—Block transmission with cyclic prefix is a promising technique to realize high-speed data rates in frequency-selective fading channels. Many popular linear precoding schemes, including orthogonal frequency-division multiplexing (OFDM), single-carrier (SC) block transmission, and time-reversal (TR), can be interpreted as such a block transmission. This paper presents a unified performance analysis that shows how the optimal precoding strategy depends on the optimization criterion such as capacity, mean-square error, and secrecy. We analyze three variants of TR methods (based on maximum-ratio combining, equal-gain combining and selective combining) and two-types of pre-equalization methods (zero-forcing and minimum mean-square error). As one application of our framework, we derive optimal precoding (i.e., OFDM with optimal power and phase control) in the presence of interference limitation for distributed antenna systems; we find that without power/phase control, OFDM does not have any capacity advantage over SC transmissions. When comparing SC and TR, we verify that for single-antenna systems in the high SNR regimes, SC has a capacity advantage; however, TR performs better in the low SNR regime. For distributed multiple-antenna systems, TR always provides higher capacity, and the capacity of TR can approach that of optimal precoders with a large number of distributed antennas. Furthermore, we make an analysis of secrecy capacity which shows how high-rate messages can be transmitted towards an intended user without being decoded by the other users from the viewpoint of information–theoretic security. We demonstrate that TR precoding can be the best candidate among the non-optimal precoders for achieving high secrecy capacity, while the optimal precoder offers a significant gain over those non-optimal precoders.

Index Terms—Distributed antenna systems, cooperative diversity, linear block precoding, frequency-selective fading, information-theoretic security.

I. INTRODUCTION

A S data rates are constantly increasing, wireless transmission systems require larger bandwidths, that makes them more susceptible to the effects of the frequency selectivity in the propagation channels [2]. Several transmission schemes are used for fourth-generation cellular and other advanced wireless communication systems to cope with this situation:

- Multi–carrier transmission, in particular orthogonal frequency-division multiplexing (OFDM), has been adopted for most high data-rate wireless standards, including WiMAX, WiFi (802.11a, g, n), and the downlink of the 3GPP LTE.
- Single-carrier (SC) block transmission, combined with frequency-domain equalizations, is used in situations where the transmitter can avoid high peak-to-average-power ratios, e.g., the uplink of 3GPP LTE.
- Time-reversal (TR) is another transmission technique that has gathered great interest in the past few years [3–16] since it has a potential to decrease effective channel length and to simplify the receiver construction.

All of the above techniques can be interpreted as linear block precoding schemes using cyclic prefix (CP); the choice of precoder determines whether OFDM, SC, or TR is used. While there are extensive literature dealing with each of those methods separately, there is — to the authors' best knowledge — no unified performance analysis, which makes a theoretical comparison amongst them.

Distributed antenna systems and base station (BS) cooperation [2], where spatially separated transmitters cooperate for transmission of signals, have recently gathered interest as a method for decreasing interference and enhancing throughput in cellular systems. In a simple, yet highly effective, scheme, the different BSs linearly weight the signals, so that they superpose in a desired way at the receiver. The combination of BS cooperation with block precoding is considered as the most promising method for high-speed, high-spectral efficiency communication in future cellular networks.

Analysis of interference–aware capacity can be of great importance for evaluating the advantage of cooperative communications. Increasing data rate for an intended inner-cell user while maintaining low interference to cell-edge users contributes directly to improving spectrum efficiency for cellular networks. In addition to the spectrum efficiency, there has been a rapid increase in demand of realizing secure radio communications to protect confidentiality and privacy in

recent years. Although some good cryptographic techniques have been used in practice, the existing ciphers strongly rely on computational complexity and can be broken by an eavesdropper with sufficiently powerful computers. In order to raise the security level, it is foreseen that physical-layer security based on information-theoretic perfect secrecy shall become a significant factor in the near future [17–21].

In this paper, we focus on a distributed base station cooperation technique and present a unified performance analysis for various types of linear block precoding schemes, including several types of TR schemes, OFDM, SC transmissions (or, unitary precoding), and pre-equalization schemes. For comparison, we derive the optimal precoder based on three different criteria: i) to maximize link capacity for optimal receivers, ii) to minimize mean-square error (MSE) for low-complexity minimum MSE (MMSE) receivers, and iii) to maximize secrecy capacity for secure communications. Multiple active receivers ("interference-exposed victim" or "eavesdropper") as well as multiple distributed transmitting antennas (namely, cooperative base stations) are taken into account. The chief contribution of this paper lies in to provide several examples for the usefulness of our framework, as summarized below.

- We derive an optimal precoding scheme, which requires modified water-filling for power allocation, in distributed-antenna multi-user systems.
- We show that at low SNRs, TR always performs better than SC. However, in the single-antenna case, SC provides higher capacity than TR at high SNRs if the cyclic prefix is long enough.
- We confirm that TR performs better than other non-optimal schemes when we exploit multiple distributed antennas for cooperative transmissions.
- We derive a scaling law which shows how the use of multiple antennas can increase the capacity of TR compared with that of SC.
- In addition, we analyze the secrecy capacity [17–21] to discuss information-theoretic security of various precoders for applications, in which confidential messages are transmitted to only one intended user without being eavesdropped by other users.

The remainder of the paper is organized as follows: Section II sets up the system model of distributed antenna multi-user communications, and presents the mathematical formulation of the most existing precoders. The performance measures of capacity, MSE, and secrecy are addressed as well. Section III derives the optimal precoder for different criteria among all the possible linear block precoders; subsequently Section IV derives a capacity scaling law which presents the impact of multiple antennas on the capacity advantage of TR over SC. Information-theoretic secrecy capacity for TR and SC precoders is discussed in Section V. The link capacity, MSE and secrecy capacity comparisons are followed by a summary and conclusions.

II. DISTRIBUTED ANTENNA SYSTEM WITH LINEAR BLOCK PRECODING

A. System Description

Fig. 1 shows the system model, in which we consider M distributed transmitters (or, cooperating base stations) and one intended receiver as well as $N-1$ unintended receivers (either "interference-exposed victims" or "legitimate eavesdroppers"), all of which are equipped with only one antenna. In this system, a cooperative diversity transmission technique is adopted amongst some neighboring base stations around mobile users. We focus on block transmissions, where one transmitting block consists of L information symbols and an $L_{\rm cp}$-symbol CP. We assume a block fading channel, in which the channel remains constant over the duration of a transmission block. The precoding for each cooperating transmitters is done based on the instantaneous channel impulse responses. We assume a simplified (tap-spaced) channel model with independent Rayleigh fading of each tap: Let $h_{n,m}(p) \in \mathbb{C}$ be the channel impulse response for $pT_{\rm s}$ delayed wave ($0 \leq p < P_{\rm ch}$) from the m-th transmitter to the n-th receiver for $1 \leq m \leq M$ and $1 \leq n \leq N$. Here, $T_{\rm s}$ is the symbol duration. Unless stated otherwise, we suppose that all the propagation delays and the distributed transmitter's asynchronous lags are absorbed by the CP length.

Through a backbone network, source data is distributed to all M transmitters. At each transmitter, the corresponding modulation data (or, codeword) $\boldsymbol{x} \in \mathbb{C}^{L \times 1}$ is multiplied with a block linear precoding matrix $\boldsymbol{P}_m \in \mathbb{C}^{L \times L}$. After padding with the CP, the precoded block is transmitted to the n-th receiver, which in turn discards the CP and obtains

$$\boldsymbol{y}_n = \sum_{m=1}^{M} \boldsymbol{H}_{n,m} \boldsymbol{P}_m \boldsymbol{x} + \boldsymbol{z}_n \triangleq \boldsymbol{\mathcal{H}}_n \boldsymbol{x} + \boldsymbol{z}_n, \qquad (1)$$

where $\boldsymbol{y}_n \in \mathbb{C}^{L \times 1}$, $\boldsymbol{H}_{n,m} \in \mathbb{C}^{L \times L}$, and $\boldsymbol{z}_n \in \mathbb{C}^{L \times 1}$ denote the received signal sequence, the (time domain) channel matrix, and the additive white Gaussian noise, respectively. The matrix $\boldsymbol{\mathcal{H}}_n = \sum_{m=1}^{M} \boldsymbol{H}_{n,m} \boldsymbol{P}_m \in \mathbb{C}^{L \times L}$ denotes the effective channel matrix which combines the precoded channels from all the cooperating transmitters to the n-th user. We assume unity-energy modulations $\mathbb{E}[\boldsymbol{x}\boldsymbol{x}^{\dagger}] = \boldsymbol{I}_L$, and $\mathbb{E}[\boldsymbol{z}_n\boldsymbol{z}_n^{\dagger}] = \sigma^2 \boldsymbol{I}_L$ with a noise variance of σ^2, where $\boldsymbol{I}_L$ denotes the L-dimensional identity matrix, and $[\cdot]^{\dagger}$ denotes the Hermitian transpose. For the simulation in Section VI, we make further assumptions about the channel statistics; namely that each delay tap is Rayleigh fading, the power delay profile exhibits a single exponential decay, and $\mathbb{E}[\boldsymbol{H}_{n,m}^{\dagger}\boldsymbol{H}_{n,m}] = \rho_{n,m}\boldsymbol{I}_L$ with $\rho_{n,m}$ being the the path loss between the m-th transmitter and the n-th user. The transmission power is controlled by the precoder $\boldsymbol{P}_m$. When we have $\mathrm{tr}[\boldsymbol{P}_m\boldsymbol{P}_m^{\dagger}] = LE_m$ where E_m is the transmission symbol energy at the m-th transmitter, the received signal-to-noise power ratio (SNR) at the n-th user becomes $(\sum E_m \rho_{n,m})/\sigma^2$. We put a transmission power constraint so that the transmission power does not exceed the maximum limit, $E_m \leq E_{\rm s}$, where $E_{\rm s}$ denotes the maximum allowable transmission energy per symbol. Without loss of generality, we suppose that the first user ($n = 1$) is the intended destination to receive the precoded message.
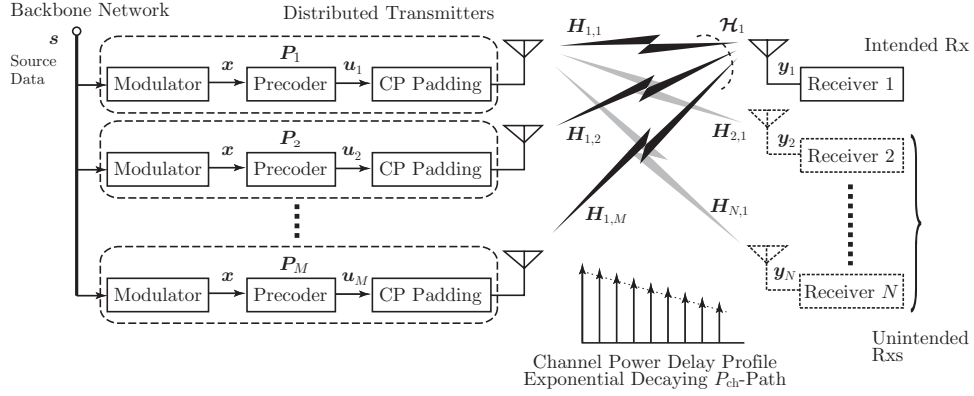
Fig. 1.   Distributed antenna systems with linear block precoding for multi-user frequency-selective fading channels.

With a sufficiently long CP, we can write the channel matrix in the cyclic Toeplitz matrix form:

$$\boldsymbol{H}_{n,m} = \sum_{p=0}^{P_{\text{ch}}-1} h_{n,m}(p)\boldsymbol{\Pi}^p, \qquad (2)$$

where $\boldsymbol{\Pi} \in \mathbb{Z}_2^{L \times L}$ being a cyclic shift matrix, defined as

$$\boldsymbol{\Pi} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \ddots & \ddots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}. \qquad (3)$$

Note that every column vector of the channel matrix $\boldsymbol{H}_{n,m}$ consists of the tapped delay line $[h_{n,m}(0), h_{n,m}(1), \ldots, h_{n,m}(P_{\text{ch}}-1)]$. The channel matrix $\boldsymbol{H}_{n,m}$ is related to the (diagonal) frequency-domain channel matrix $\boldsymbol{G}_{n,m} \in \mathbb{C}^{L \times L}$ as

$$\boldsymbol{H}_{n,m} = \boldsymbol{F}\boldsymbol{G}_{n,m}\boldsymbol{F}^\dagger, \qquad (4)$$

where the unitary matrix $\boldsymbol{F} \in \mathbb{C}^{L \times L}$ denotes the discrete Fourier transform (DFT), whose (k,l)-th entry is expressed as $\frac{1}{\sqrt{L}}\exp(-\jmath 2\pi kl/L)$.

B. Block Precoding Matrix

We now describe several block transmission schemes which include SC (or equivalently, unitary precoding), OFDM, three variants of TRs and two types of pre-equalization methods. Through appropriate choice of the precoder matrix $\boldsymbol{P}_m$, the signal model described above can represent all of those block transmission schemes.

1) Single-Carrier (SC) Unitary Block Transmission: The precoding matrix for the SC block transmission is given as

$$\boldsymbol{P}_m = \eta_m \boldsymbol{I}_L, \qquad (5)$$

where η_m denotes a normalization factor so that the resulting transmission symbol energy becomes E_m (i.e., $\eta_m = \sqrt{E_m}$ for this case). The above expression indicates that the SC transmission is one of the unitary precoding schemes, employing a specific unitary matrix $\boldsymbol{I}_L$,

2) Multi-Carrier OFDM Signalling: The precoding matrix for OFDM signalling is expressed as

$$\boldsymbol{P}_m = \boldsymbol{F}\boldsymbol{\Phi}_m, \qquad (6)$$

where a diagonal matrix $\boldsymbol{\Phi}_m \in \mathbb{C}^{L \times L}$ determines per-subcarrier power allocation at the m-th transmitter. It is well–known that optimal power allocation for one–to–one communications is generally obtained by water filling. If we cannot adopt such a power control (perfect channel state information is not available at the transmitter), we should generally use a constant power allocation: $\boldsymbol{\Phi}_m = \eta_m \boldsymbol{I}_L$, which makes the OFDM signalling one of the unitary precoding schemes because the DFT matrix $\boldsymbol{F}$ is a unitary matrix.

3) Time-Reversal (TR) Precoding: The original TR scheme [3–7] has the following precoding matrix:

$$\boldsymbol{P}_m = \eta_m \boldsymbol{H}_{1,m}^\dagger. \qquad (7)$$

Note that the normalization factor becomes $\eta_m = \sqrt{LE_m/\|\boldsymbol{H}_{1,m}\|^2}$ for this case in order to have $\text{tr}[\boldsymbol{P}_m\boldsymbol{P}_m^\dagger] = LE_m$. It means that the precoded block with the matrix $\boldsymbol{H}_{1,m}^\dagger$ is a filter output from the tapped delay line consisting of the channel response $[h_{1,m}^*(P_{\text{ch}}-1), \ldots, h_{1,m}^*(1), h_{1,m}^*(0)]$ which is the time-reversed version of the tapped delay line $[h_{1,m}(0), h_{1,m}(1), \ldots, h_{1,m}(P_{\text{ch}}-1)]$ for the original channel matrix $\boldsymbol{H}_{1,m}$. Because it is a kind of pre-equalization schemes based on maximum-ratio combining (MRC), we refer to it as MRC-TR.

In [8], a one-bit TR scheme is introduced, in which the precoder only controls the phase of the tapped delay line according to the channel response. Its precoding matrix is expressed as follows:

$$\boldsymbol{P}_m = \eta_m \Big(\sum_{p=0}^{P_{\text{ch}}-1} \frac{h_{1,m}(p)}{|h_{1,m}(p)|}\boldsymbol{\Pi}^p \Big)^\dagger \triangleq \eta_m \breve{\boldsymbol{H}}_{1,m}^\dagger, \qquad (8)$$

which only requires phase information of the channel impulse response. The matrix $\breve{\boldsymbol{H}}_{1,m} \in \mathbb{C}^{L \times L}$ denotes the phase-synchronized version of the channel matrix $\boldsymbol{H}_{1,m}$. Since this TR scheme performs in the same way as the pre-equalization based on equal-gain combining (EGC), we call it EGC-TR hereafter.

In a similar manner, we introduce a TR scheme based on selective B-branch combining (denoted by SLC-TR) as

follows:

$$\boldsymbol{P}_m = \eta_m \Big(\sum_{b=0}^{B-1} h_{1,m}(p_b) \boldsymbol{\Pi}^{p_b} \Big)^{\dagger}, \tag{9}$$

where p_b represents the path index whose channel strength $|h_{1,m}(p_b)|^2$ is the b-th largest one. It is a kind of the pre-rake method. In this paper, we use two-tap filter (i.e., $B = 2$) for simplicity.

4) Linear Pre-equalization: We consider pre-equalization schemes based on zero forcing (ZF) and MMSE criteria, whose precoder matrices are respectively expressed as follows:

$$\boldsymbol{P}_m = \eta_m \boldsymbol{H}_{1,m}^{\dagger} (\boldsymbol{H}_{1,m} \boldsymbol{H}_{1,m}^{\dagger})^{-1}, \tag{10}$$

$$\boldsymbol{P}_m = \eta_m \boldsymbol{H}_{1,m}^{\dagger} (\boldsymbol{H}_{1,m} \boldsymbol{H}_{1,m}^{\dagger} + \sigma^2 \boldsymbol{I}_L)^{-1}. \tag{11}$$

Here, the normalization factor η_m is appropriately set to have $\mathrm{tr}[\boldsymbol{P}_m \boldsymbol{P}_m^{\dagger}] = L E_m$. The ZF pre-equalization can achieve the inter-symbol interference (ISI) free environment. However, it can degrade the transmission power efficiency when the channel response exhibits deep fades. Therefore, the MMSE criterion which takes account of average distortion level at the receiver is generally better than the ZF pre-equalization.

C. Performance Measures: Capacity, MSE, and Secrecy

The main purpose of this paper is to compare various precoding schemes described above for distributed antenna systems. To compare them, we consider three types of performance measures: i) the achievable link capacity, ii) the achievable MSE performance, and iii) the achievable secrecy rate. The achievable link capacity is an important performance measure for optimal receiving algorithms, whereas the MSE performance is suited for MMSE low-complexity receivers. We discuss the achievable secrecy rate [17–21] from the view point of information–theoretic security, which qualifies the rate at which data can be securely sent to an intended receiver without being eavesdropped by the other receivers. Note that we can consider other performance measures such as peak-to-average power ratio, outage capacity, complexity, and error probability. Nevertheless, our unified analysis on capacity, MSE and secrecy still gives us useful insights into the fundamental characteristics for cooperative communications.

1) Capacity for Optimal Receiver: For an optimal receiver, the link capacity for the n-th user, for a particular channel realization, is given as

$$C_n = \frac{1}{L} \ln \det \Big(\boldsymbol{I}_L + \frac{1}{\sigma^2} \boldsymbol{\mathcal{H}}_n \boldsymbol{\mathcal{H}}_n^{\dagger} \Big), \tag{12}$$

which is normalized by the bandwidth of $1/T_s$. Here, we neglect the loss of spectral efficiency due to the CP. Note that the capacity equation can employ either time- or frequency-domain representations of the channel, since $\det(\boldsymbol{F}\boldsymbol{A}\boldsymbol{F}^{\dagger}) = \det(\boldsymbol{A})$. The Ergodic capacity is obtained by averaging the capacity for all the possible channel realizations.

2) MSE for MMSE Equalization: The MMSE linear equalization is known as a low-complexity algorithm especially when applied to the frequency-domain operations. The MMSE equalization achieves the following MSE at the n-th user:

$$\varepsilon_n = \frac{1}{L} \mathrm{tr} \Big[\Big(\boldsymbol{I}_L + \frac{1}{\sigma^2} \boldsymbol{\mathcal{H}}_n^{\dagger} \boldsymbol{\mathcal{H}}_n \Big)^{-1} \Big]. \tag{13}$$

It is known by Verdú's theorem [22] that the link capacity and MSE are closely related to each other. We should, however, note that a specific precoder which can achieve higher capacity does not always offer better MSE performance. This motivates us to evaluate different performance measures for comparing several precoders.

3) Secrecy Rate for Confidential Message Transmissions: As outlined in the literature studying information-theoretic security [17–21], we can transmit confidential data to a certain intended user without being decoded at the other unintended users, using Wyner's encoding strategy. The achievable rate is, however, decreased by the link capacity of unintended users for Gaussian channels; more specifically, the achievable secrecy rate is written as follows:

$$R_{\mathrm{S}} = \min_{n \in \{2,\ldots,N\}} \Big[C_1 - C_n \Big]_{+0}, \tag{14}$$

where $[x]_{+a} = \max(x, a)$. Basically, we require higher received SNR at the intended user than at the other eavesdropping users for secure communications.

III. OPTIMAL PRECODER

In this section, we derive optimal precoding which is designed according to three different criteria; to maximize link capacity, to minimize MSE, and to maximize secrecy rate. As we can see in the following, these optimal precoders are all based on OFDM signalling, while the optimal power allocation differs from each other.

A. Optimal Precoder for Maximizing Capacity

We first derive an optimal precoder which maximizes capacity constrained on the transmission power and the interference to victim receivers. The optimization problem is described as

$$\max_{\{\boldsymbol{P}_m\}} \quad \frac{1}{L} \ln \det \Big(\boldsymbol{I}_L + \frac{1}{\sigma^2} \boldsymbol{\mathcal{H}}_1 \boldsymbol{\mathcal{H}}_1^{\dagger} \Big), \tag{15}$$

$$\text{s.t.} \quad \frac{1}{LM} \sum_{m=1}^{M} \mathrm{tr} \Big[\boldsymbol{P}_m \boldsymbol{P}_m^{\dagger} \Big] \le E_{\mathrm{s}}, \tag{16}$$

$$\frac{1}{LM} \mathrm{tr} \Big[\boldsymbol{\mathcal{H}}_n \boldsymbol{\mathcal{H}}_n^{\dagger} \Big] \le E_{\mathrm{v}}, \quad \text{for all } 2 \le n \le N, \tag{17}$$

with E_{s} being the maximum symbol energy for transmission and E_{v} being the allowable interference energy at each unintended receivers. As shown in the detailed derivation in Appendix A, the solution is written in the form of $\boldsymbol{P}_m = \boldsymbol{F}\boldsymbol{\Phi}_m$. It indicates that the optimal precoder is OFDM with appropriate per-subcarrier power control even for multi-user distributed antenna systems.

Appendix A shows that we need to satisfy the following Karush-Kuhn-Tucker (KKT) condition:

$$\boldsymbol{H}_{1,m}^{\dagger} \boldsymbol{\mathcal{H}}_1 \Big(\sigma^2 \boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_1^{\dagger} \boldsymbol{\mathcal{H}}_1 \Big)^{-1} = \lambda_1 \boldsymbol{P}_m + \sum_{n=2}^{N} \lambda_n \boldsymbol{H}_{n,m}^{\dagger} \boldsymbol{\mathcal{H}}_n, \tag{18}$$

where λ_n are the Lagrangian multipliers. Note that the optimal power allocation is not given by the conventional water-filling for $N \ge 2$. Without interference limitation ($N = 1$), the

optimal power allocation of the i-th sub-carrier for the m-th antenna becomes

$$\Phi_m(i) = \sqrt{\left[\frac{1}{\lambda_1} - \frac{\sigma^2}{\|\boldsymbol{g}_1(i)\|^2}\right]_{+0}} \frac{G_{1,m}^*(i)}{\|\boldsymbol{g}_1(i)\|}, \qquad (19)$$

where $G_{n,m}(i)$ is the i-th diagonal entry of the frequency-domain channel matrix $\boldsymbol{G}_{n,m}$, and the vector $\boldsymbol{g}_n(i)$ is defined as $\boldsymbol{g}_n(i) = [G_{n,1}^*(i), G_{n,2}^*(i), \ldots, G_{n,M}^*(i)]^{\mathrm{T}}$. We can see that distributed antennas shall form the MRC diversity transmissions and use the conventional water filling power allocation for the single-user case $N = 1$.

B. Optimal Precoder for Minimizing MSE

In a similar way, the optimization problem to achieve minimal MSE, when the receiver uses MMSE equalizers, is described below

$$\min_{\{\boldsymbol{P}_m\}} \quad \frac{1}{L}\mathrm{tr}\left[\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-1}\right], \qquad (20)$$

$$\mathrm{s.t.} \quad \frac{1}{LM}\sum_{m=1}^{M}\mathrm{tr}\left[\boldsymbol{P}_m\boldsymbol{P}_m^\dagger\right] \le E_{\mathrm{s}}, \qquad (21)$$

$$\frac{1}{LM}\mathrm{tr}\left[\boldsymbol{\mathcal{H}}_n\boldsymbol{\mathcal{H}}_n^\dagger\right] \le E_{\mathrm{v}}, \quad \text{for all } 2 \le n \le N. \quad (22)$$

The derivation of optimal solution can be found in Appendix B, where we derive the following KKT condition:

$$\sigma^2\boldsymbol{H}_{1,m}^\dagger\boldsymbol{\mathcal{H}}_1\left(\sigma^2\boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-2} = \lambda_1\boldsymbol{P}_m + \sum_{n=2}^{N}\lambda_n\boldsymbol{H}_{n,m}^\dagger\boldsymbol{\mathcal{H}}_n. \qquad (23)$$

Its solution is expressed in the form of $\boldsymbol{P}_m = \boldsymbol{F}\boldsymbol{\Phi}_m$, which is also based on OFDM signalling. However, the optimal power allocation differs from the one for maximizing capacity because we have different KKT conditions. The optimal power allocation requires a modification from the conventional water filling for any arbitrary number of N, as shown in Appendix. For instance, the optimal power control is obtained as

$$\Phi_m(i) = \sqrt{\left[\sqrt{\frac{\sigma^2}{\lambda_1\|\boldsymbol{g}_1(i)\|^2}} - \frac{\sigma^2}{\|\boldsymbol{g}_1(i)\|^2}\right]_{+0}} \frac{G_{1,m}^*(i)}{\|\boldsymbol{g}_1(i)\|}, \quad (24)$$

for the single-user case $N = 1$.

C. Optimal Precoder for Maximizing Secrecy Rate

We write the optimization problem for maximizing achievable secrecy rate as follows:

$$\max_{\{\boldsymbol{P}_m\},R} \quad \frac{1}{L}\ln\det\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_1\boldsymbol{\mathcal{H}}_1^\dagger\right) - R, \qquad (25)$$

$$\mathrm{s.t.} \quad \frac{1}{LM}\sum_{m=1}^{M}\mathrm{tr}\left[\boldsymbol{P}_m\boldsymbol{P}_m^\dagger\right] \le E_{\mathrm{s}}, \qquad (26)$$

$$\frac{1}{L}\ln\det\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_n\boldsymbol{\mathcal{H}}_n^\dagger\right) \le R, \qquad (27)$$

for all $2 \le n \le N$. The optimization parameter R denotes the link capacity of the best eavesdropper amongst all the possible active unintended users.

Shown in Appendix C, the KKT condition is given by

$$\lambda_1\boldsymbol{P}_m = \boldsymbol{H}_{1,m}^\dagger\boldsymbol{\mathcal{H}}_1\left(\sigma^2\boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-1}$$
$$- \sum_{n=2}^{N}\lambda_n\boldsymbol{H}_{n,m}^\dagger\boldsymbol{\mathcal{H}}_n\left(\sigma^2\boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_n^\dagger\boldsymbol{\mathcal{H}}_n\right)^{-1}, \quad (28)$$

where $\sum_{n=2}^{N}\lambda_n = 1$. Again, its solution is given by OFDM signalling $\boldsymbol{P}_m = \boldsymbol{F}\boldsymbol{\Phi}_m$. In the Appendix, it is verified that the optimal precoding vector $\boldsymbol{\phi}(i) = [\Phi_1(i), \Phi_2(i), \ldots, \Phi_M(i)]^{\mathrm{T}}$ is a linear combination of MRC beamformers $\boldsymbol{g}_1(i), \boldsymbol{g}_2(i), \ldots, \boldsymbol{g}_N(i)$. As an example, for the two-user case ($N = 2$), we obtain the optimal precoder

$$\boldsymbol{\phi}(i) = \zeta(i)\left((\lambda_1 + \kappa(i))\boldsymbol{g}_1(i) - \kappa(i)\frac{\boldsymbol{g}_2^\dagger(i)\boldsymbol{g}_1(i)}{\|\boldsymbol{g}_2(i)\|^2}\boldsymbol{g}_2(i)\right), \qquad (29)$$

where $\kappa(i) = \|\boldsymbol{g}_2(i)\|^2 / \left(\sigma^2 + \lambda_1^2\zeta^2(i)|\boldsymbol{g}_2^\dagger(i)\boldsymbol{g}_1(i)|^2\right)$. The real–valued parameter $\zeta(i)$ is an amplitude control factor. Note that the optimum precoding described above is a combination of two beamforming vectors: one is the MRC beamformer to maximize the SNR at the intended user and the other is the nulling beamformer to minimize the SNR at the unintended user. The optimal precoder converges to the nulling beamformer in the high SNR regimes because $\lambda_1 \to 0$ for $\sigma^2 \to 0$.

IV. MRC-TR VERSUS SC: CAPACITY SCALING LAW

This section describes a scaling law which shows the capacity advantage of MRC-TR over SC with respect to the number of distributed antennas M. We confirm that the MRC-TR does not offer better performance than does the SC for the high SNR regime if we use only one transmitter. However, distributed multi-antenna systems enable the MRC-TR to outperform the SC. We derive the following scaling law:

- For high SNRs, the capacity gap between MRC-TR and SC asymptotically increases in a logarithmic manner as a function of M.
- For low SNRs, the capacity ratio between MRC-TR and SC has a linear increase with respect to M.

As well as the above-mentioned scaling law, we obtain a lower bound and an upper bound of the link capacity for the SC and the TR precoders.

A. Unitary Precoder and MRC-TR Precoder

The SC precoder ($\boldsymbol{P}_m = \eta_m\boldsymbol{I}_L$) provides the following capacity of

$$C_{1,\mathrm{SC}} = \frac{1}{L}\sum_{i=0}^{L-1}\ln\left(1 + \frac{1}{\sigma^2}\left|\sum_m \eta_m G_{1,m}(i)\right|^2\right). \qquad (30)$$

When each distributed transmitter has an identical transmission power, we can write $\eta_m^2 = E_{\mathrm{s}}$ for all $1 \le m \le M$. Note that any arbitrary unitary precoding (including OFDM without power control, i.e., $\boldsymbol{P}_m = \eta_m\boldsymbol{F}$) offers exactly the same capacity as the one given above. Hence, OFDM without per-subcarrier power/phase control has no advantage over the SC transmission.

In contrast, the MRC-TR precoder ($\boldsymbol{P}_m = \eta_m \boldsymbol{H}_{1,m}^\dagger$) gives the following capacity:

$$C_{1,\mathrm{TR}} = \frac{1}{L} \sum_{i=0}^{L-1} \ln\left(1 + \frac{1}{\sigma^2}\left(\sum_m \eta_m |G_{1,m}(i)|^2\right)^2\right). \quad (31)$$

For the case when the transmission power is identical for all the distributed antennas, we have $\eta_m^2 = E_s/\bar{\gamma}_m^2$ where $\bar{\gamma}_m^2 = \frac{1}{L}\sum_i |G_{1,m}(i)|^2$ is the average channel gain.

B. Asymptotic Capacity of Unitary and MRC-TR Precoders

For the purpose of analytical derivations, we assume that $G_{n,m}(i)$ has a complex Gaussian distribution $\mathcal{CN}(0, \rho_n)$ (i.e., Rayleigh fading with path loss $\rho_{n,m} = \rho_n$ for any n, m), the channel coherence bandwidth is much smaller than the considered system bandwidth, and $\bar{\gamma}_m^2 = \rho_1$ for large packet length. These assumptions imply that the probability distribution functions of $|\sum G_{1,m}(i)|^2/\rho_1$ and $\sum |G_{1,m}(i)|^2/\rho_1$ follow an exponential distribution with mean M and a chi-square distribution with $2M$ degrees of freedom, respectively.

Using the probability density functions of the channel gains, we can obtain the asymptotic capacity for the unitary precoder and the MRC-TR precoder for $L \longrightarrow \infty$ as follows:

$$C_{1,\mathrm{SC}} \longrightarrow \int_0^\infty \ln\left(1 + \frac{E_s\rho_1}{\sigma^2}t\right)\frac{1}{M}e^{-t/M}\mathrm{d}t, \quad (32)$$

$$C_{1,\mathrm{TR}} \longrightarrow \int_0^\infty \ln\left(1 + \frac{E_s\rho_1}{\sigma^2}t^2\right)\frac{t^{M-1}}{(M-1)!}e^{-t}\mathrm{d}t, \quad (33)$$

where we set an identical power allocation ($\eta_1 = \eta_2 = \cdots = \eta_M$) for each distributed antenna. It should be noted that the above integrals can be expressed by special functions using the Meijer's hypergeometric G-function. In order to obtain more useful insights into the impact of the number of distributed antennas M, we now approximate the integrals by well-known functions for the high SNR and low SNR regimes.

C. Capacity Scaling Law

1) High SNR Regime: In a high SNR regime such that $ME_s\rho_1/\sigma^2 \gg 1$, we can approximate $\ln(1 + t) \simeq \ln(t)$ for $|t| \gg 1$ and obtain

$$\begin{aligned} C_{1,\mathrm{SC}} &\simeq \int_0^\infty \ln\left(\frac{E_s\rho_1}{\sigma^2}t\right)\frac{1}{M}e^{-t/M}\mathrm{d}t \\ &= \ln\frac{ME_s\rho_1}{\sigma^2} - \gamma_\mathrm{E}, \end{aligned} \quad (34)$$

$$\begin{aligned} C_{1,\mathrm{TR}} &\simeq \int_0^\infty \ln\left(\frac{E_s\rho_1}{\sigma^2}t^2\right)\frac{t^{M-1}}{(M-1)!}e^{-t}\mathrm{d}t \\ &= 2\left(\sum_{m=1}^{M-1}\frac{1}{m} - \gamma_\mathrm{E}\right) + \ln\frac{E_s\rho_1}{\sigma^2}, \end{aligned} \quad (35)$$

where $\gamma_\mathrm{E} \simeq 0.58$ is the Euler's constant. Therefore, the capacity advantage of the MRC-TR precoder over the unitary precoder can be written in the following way:

$$\begin{aligned} C_{1,\mathrm{TR}} - C_{1,\mathrm{SC}} &\simeq 2\sum_{m=1}^{M-1}\frac{1}{m} - \left(\ln(M) + \gamma_\mathrm{E}\right) \\ &\simeq \ln(M-1) + \gamma_\mathrm{E}, \quad (M \gg 1), \end{aligned} \quad (36)$$

where the last approximation results from the fact that the harmonic number $\sum_m^{M-1} 1/m$ can be well approximated by $\frac{1}{2}\ln(M(M-1)) + \gamma_\mathrm{E}$ for large M.

From the derivation above, we can see that $C_{1,\mathrm{TR}} - C_{1,\mathrm{SC}} \simeq \ln(M-1) + \gamma_\mathrm{E}$ is logarithmically increased with M, which implies that a larger number of distributed antennas can take more advantage for the MRC-TR precoder compared to the unitary (SC) precoder. Note that $C_{1,\mathrm{SC}} > C_{1,\mathrm{TR}}$ by γ_E for $M = 1$, while otherwise $C_{1,\mathrm{SC}} < C_{1,\mathrm{TR}}$. Therefore, MRC-TR can be worse than SC by $\gamma_\mathrm{E}/\ln(2) \simeq 0.84$ bps/Hz for high SNR in the single antenna case. The opposite happens for the case in which multiple antennas are used: when $M = 2$, the achievable gain is $C_{1,\mathrm{TR}} - C_{1,\mathrm{SC}} \simeq (2 - \ln(2) - \gamma_\mathrm{E})/\ln(2) \simeq 1.05$ bps/Hz.

2) Low SNR Regime: For low SNRs ($ME_s\rho_1/\sigma^2 \ll 1$), approximating $\ln(1+t) \simeq t$ for $|t| \ll 1$, we obtain

$$C_{1,\mathrm{SC}} \simeq \int_0^\infty \frac{E_s\rho_1}{\sigma^2}t\frac{1}{M}e^{-t/M}\mathrm{d}t = \frac{ME_s\rho_1}{\sigma^2}, \quad (37)$$

$$C_{1,\mathrm{TR}} \simeq \int_0^\infty \frac{E_s\rho_1}{\sigma^2}t^2\frac{t^{M-1}}{(M-1)!}e^{-t}\mathrm{d}t = \frac{ME_s\rho_1}{\sigma^2}(M+1). \quad (38)$$

Note that the term of $ME_s\rho_1/\sigma^2$ is the received SNR at the intended user. Hence, the capacity ratio can be written as follows:

$$\frac{C_{1,\mathrm{TR}}}{C_{1,\mathrm{SC}}} \simeq M + 1. \quad (39)$$

It suggests that MRC-TR always offers better capacity than SC in the low SNR regimes, and the capacity ratio $C_{1,\mathrm{TR}}/C_{1,\mathrm{SC}} \simeq M+1$ can linearly increase with the number of distributed antennas M.

D. Lower and Upper Bounds of Asymptotic Capacity

The approximations of $\ln(1+t) \simeq \ln(t)$ for high SNR $t \gg 1$ and $\ln(1+t) \simeq t$ for low SNR $t \ll 1$ can be used for deriving lower and upper bounds of the link capacity as follows. Since $\ln(t) < \ln(1+t) \le t$ for any arbitrary $t \ge 0$, the approximated capacities for high SNRs given in (34) and (35) work as a lower bound of the link capacity, while the expressions in (37) and (38) can be used as the upper bound of the asymptotic link capacity $C_{1,\mathrm{SC}}$ and $C_{1,\mathrm{TR}}$, respectively. We can readily obtain a tighter upper bound by using Jensen's inequality for the concave function of $\ln(1+t)$ with respect to t. Consequently, we have the capacity bound as follows:

$$\ln\frac{ME_s\rho_1}{e^{\gamma_\mathrm{E}}\sigma^2} < C_{1,\mathrm{CS}} < \ln\left(1 + \frac{ME_s\rho_1}{\sigma^2}\right), \quad (40)$$

$$\ln\frac{(M-1)ME_s\rho_1}{\sigma^2} < C_{1,\mathrm{TR}} < \ln\left(1 + \frac{(M-1)ME_s\rho_1}{\sigma^2}\right), \quad (41)$$

where we used $\sum_{m=1}^{M-1} 1/m - \gamma_\mathrm{E} > \frac{1}{2}\ln(M(M-1))$ for $M \ge 1$. Those bounds are tight in particular for high SNRs.

V. SECRECY ANALYSIS OF MRC-TR AND SC

In this section, we develop a similar analysis which shows the secrecy advantage of the MRC-TR precoder over the unitary precoder. As shown in (14), the achievable secrecy rate

is the difference between the link capacity of the intended user and the link capacity of the best eavesdropping user. The link capacity at the n-th user, when we use the unitary precoder $\boldsymbol{P}_m = \eta_m \boldsymbol{I}_L$ and the MRC-TR precoder $\boldsymbol{P}_m = \eta_m \boldsymbol{H}_{1,m}^\dagger$, can be respectively written as

$$C_{n,\mathrm{SC}} = \frac{1}{L} \sum_{i=0}^{L-1} \ln\left(1 + \frac{1}{\sigma^2}\left|\sum_{m=1}^{M} \eta_m G_{n,m}(i)\right|^2\right), \qquad (42)$$

$$C_{n,\mathrm{TR}} = \frac{1}{L} \sum_{i=0}^{L-1} \ln\left(1 + \frac{1}{\sigma^2}\left|\sum_{m=1}^{M} \eta_m G_{n,m}(i)G_{1,m}^*(i)\right|^2\right). \qquad (43)$$

We derive an asymptotic behavior of those capacity, and obtain the corresponding secrecy rates.

A. Achievable Secrecy Rate of Unitary Precoder

Since the term of $\sum \eta_m G_{n,m}(i)$ in (42) follows the complex Gaussian distribution $\mathcal{CN}(0, M E_s \rho_n)$ for $\eta_m^2 = E_s$, we can obtain the asymptotic capacity for the eavesdropper in a manner similar to the previous section:

$$C_{n,\mathrm{SC}} \longrightarrow \int_0^\infty \ln\left(1 + \frac{E_s \rho_n}{\sigma^2} t\right) \frac{1}{M} e^{-t/M} \mathrm{d}t$$

$$\simeq \begin{cases} \ln \frac{M E_s \rho_n}{\sigma^2} - \gamma_\mathrm{E}, & \left(\frac{M E_s \rho_n}{\sigma^2} \gg 1\right), \\ \frac{M E_s \rho_n}{\sigma^2}, & \left(\frac{M E_s \rho_n}{\sigma^2} \ll 1\right). \end{cases} \qquad (44)$$

Correspondingly, we obtain the achievable secrecy rate of the unitary precoder as follows:

$$R_{\mathrm{S,SC}} = \left[C_{1,\mathrm{SC}} - \max_{n \in \{2,\ldots,N\}} C_{n,\mathrm{SC}} \right]_{+0}$$

$$\simeq \begin{cases} \left[\ln(\rho_1/\rho_{n'})\right]_{+0}, & (\text{High SNR}), \\ \frac{M E_s \rho_1}{\sigma^2}\left[1 - \rho_{n'}/\rho_1\right]_{+0}, & (\text{Low SNR}), \end{cases} \qquad (45)$$

where $n' = \arg\max_n \rho_n$. Given a certain SNR of $M E_s \rho_1/\sigma^2$, the secrecy rate cannot be improved by increasing the number of the distributed antennas M. Note that we cannot transmit any confidential data if the path loss of the intended user is larger than the best eavesdropper, i.e., for $\rho_1 \leq \rho_{n'}$.

B. Achievable Secrecy Rate of MRC-TR Precoder

The term of $\sum G_{n,m}(i)G_{1,m}^*(i)$ in (43) is no longer the chi-square distribution. From [23], the probability density function for the squared sum of products of independent Rayleigh signals are expressed as

$$f_V(v) = \frac{2}{\sqrt{\pi}} \frac{v^{(2M-3)/4}}{(M-1)!} K_{M-1/2}(2\sqrt{v}), \qquad (46)$$

for $v \geq 0$, where $K_n(x)$ is the modified Bessel function of the n-th order. The probability density function of $|\sum_{m=1}^{M} G_{n,m}(i)G_{1,m}(i)|^2/\rho_1\rho_n$ is then given by taking the convolution of $f_V(v)$. Using $f_V(v)$, we can write

$$C_{n,\mathrm{TR}} \longrightarrow \int_0^\infty \int_0^\infty \ln\left(1 + \frac{E_s \rho_n}{\sigma^2}(u+v)\right) f_V(u)f_V(v) \mathrm{d}u\mathrm{d}v, \qquad (47)$$

where u and v correspond to the squared real- and imaginary-parts of $\sum G_{n,m}(i)G_{1,m}^*(i)/\sqrt{\rho_1\rho_n}$.

1) High SNR Regimes: For high SNR regimes such that $\ln(1+t) \simeq \ln(t)$, we have the lower bound of the link capacity of the n-th eavesdropping user as follows:

$$C_{n,\mathrm{TR}} \simeq \int_0^\infty \int_0^\infty \ln\left(\frac{E_s \rho_n}{\sigma^2}(u+v)\right) f_V(u)f_V(v) \mathrm{d}u\mathrm{d}v$$

$$\geq \int_0^\infty \int_0^\infty \ln\left(\frac{E_s \rho_n}{\sigma^2} 2\sqrt{uv}\right) f_V(u)f_V(v) \mathrm{d}u\mathrm{d}v$$

$$= \ln\left(\frac{2E_s \rho_n}{\sigma^2}\right) - \ln(4) - 2\gamma_\mathrm{E} + \sum_{m=1}^{M-1} \frac{1}{m}$$

$$\geq \ln\left(\frac{(M-1)E_s \rho_n}{2e^{\gamma_\mathrm{E}}\sigma^2}\right). \qquad (M \gg 1) \qquad (48)$$

We used $u + v \geq 2\sqrt{uv}$ for any $u, v \geq 0$.

From the fact that the function of $\ln(u+v)$ is concave in terms of both u and v, an upper bound of the link capacity of the n-th eavesdropper is obtained by Jensen's inequality as follows:

$$C_{n,\mathrm{TR}} \simeq \mathbb{E}_{u,v}\left[\ln\left(\frac{E_s \rho_n}{\sigma^2}(u+v)\right)\right]$$

$$\leq \ln\left(\frac{E_s \rho_n}{\sigma^2}(\mathbb{E}[u] + \mathbb{E}[v])\right) = \ln\left(\frac{M E_s \rho_n}{\sigma^2}\right). \quad (49)$$

From the lower bound in (48) and the upper bound in (49), the link capacity of the eavesdropper for high SNR cases can be approximated as

$$C_{n,\mathrm{TR}} \simeq \ln\left(\frac{(M-1)E_s \rho_n}{\beta\sigma^2}\right), \qquad (50)$$

where β is a constant value which lies in

$$\frac{M-1}{M} \leq \beta \leq 2e^{\gamma_\mathrm{E}} \simeq 3.56. \qquad (51)$$

Using this expression, the secrecy rate for high SNR regimes is written as

$$R_{\mathrm{S,TR}} = [C_{1,\mathrm{TR}} - C_{n',\mathrm{TR}}]_{+0}$$

$$\simeq \left[\ln\frac{(M-1)M E_s \rho_1}{\sigma^2} - \ln\frac{(M-1)E_s \rho_{n'}}{\beta\sigma^2}\right]_{+0}$$

$$= \left[\ln\frac{M\beta\rho_1}{\rho_{n'}}\right]_{+0}. \qquad (52)$$

It suggests that the achievable secrecy rate of the MRC-TR precoder is improved by increasing the number of distributed antennas M in a logarithmic manner. However, increasing the transmission power E_s does not contribute to improving the secrecy rate. The ratio of path loss $\rho_1/\rho_{n'}$ dominates the secrecy in high SNR cases. This behavior can be explained by the fact that increasing power benefits both intended receiver and eavesdropper equally, while increasing the number of transmit antennas improves the spatial focusing of the signal.

2) Low SNR Regimes: For low SNRs such that $\ln(1+t) \simeq t$, we can approximate

$$C_{n,\mathrm{TR}} \simeq \int_0^\infty \int_0^\infty \frac{E_s \rho_n}{\sigma^2}(u+v)f_V(u)f_V(v)\mathrm{d}u\mathrm{d}v = \frac{M E_s \rho_n}{\sigma^2}. \qquad (53)$$

Hence, the secrecy rate for low SNR regimes is written as

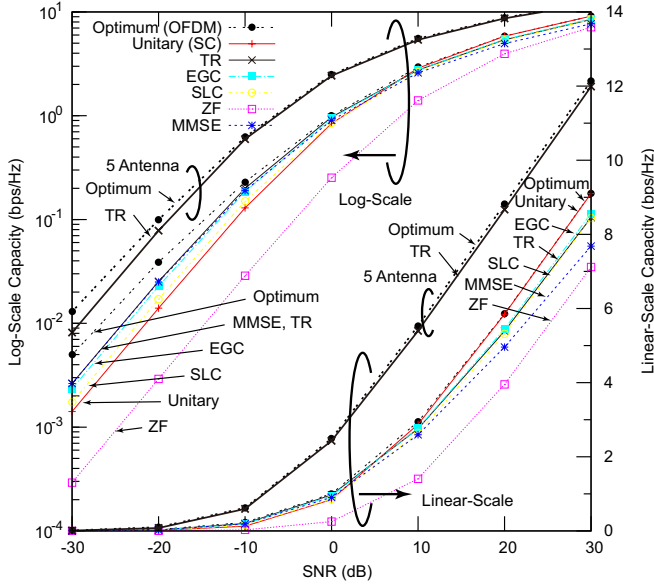$$R_{\mathrm{S,TR}} \simeq \frac{M E_s \rho_1}{\sigma^2}(M+1)\left[1 - \frac{\rho_{n'}}{(M+1)\rho_1}\right]_{+0}. \qquad (54)$$

Fig. 2.   Link capacity as a function of SNR in 1.0 dB decaying 16-path Rayleigh fading ($M = 1$ and $M = 5$).

Fig. 3.   Link capacity versus the number of distributed antennas in 1.0 dB decaying 16-path Rayleigh fading (± 30 dB SNR).

It implies that we can transmit a secret data even if the path loss of the intended user is larger than that of the eavesdropper, i.e., $\rho_1 \leq \rho_{n'}$. More importantly, the achievable secrecy rate of the TR precoder can linearly increase according to the number of distributed antennas M, and it converges to the channel capacity, more specifically, $\lim_{M \to \infty} R_{\text{S,TR}} = C_{1,\text{TR}}$.

VI. CAPACITY, MSE AND SECRECY COMPARISONS

A. Simulation Parameter

For the simulations, we assume that the channel is frequency-selective Rayleigh fading with $P_{\text{ch}} = 16$ sample-spaced paths whose power delay profile is exponentially decreasing with increased delay by 1 dB each. We use a transmission block with $L = 512$ symbols. Unless stated otherwise, we use a cyclic prefix with $L_{\text{cp}} = 16$ to achieve inter-block interference free environment. We define the received SNR of the n-th user by $M E_s \rho_n / \sigma^2$. We evaluate the performance for the case of the identical path loss $\rho_1 = \rho_2 = \cdots = \rho_N$, unless stated otherwise. The optimal precoder with OFDM signalling requires full channel state information even at the other cooperating base stations, whereas the non-optimal precoders used in this paper are allowed to exploit only the local channel state information available at each base station; this might be more practical for many applications.

B. Capacity Comparison

Table I lists capacity comparisons among the several types of precoding schemes that we presented in Section II-B, according to the instantaneous channel realization. The transmission energy η_m^2 is constrained by the maximum symbol energy E_s and the allowable interference energy E_v as in (16) and (17).

Fig. 2 shows (log-scaled and linear-scaled) Ergodic capacity versus the received SNR, $M E_s \rho_1 / \sigma^2$, of various precoding schemes for the case when there is no interference limitation,
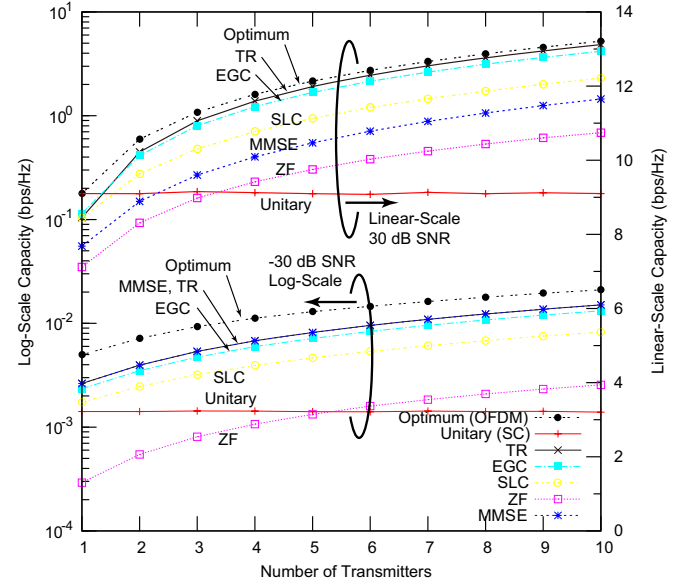
i.e. $E_v = \infty$. Log-scaled curves present focus on low SNR regimes, while linear-scaled curves are for high SNR regimes. From Fig. 2, one can see that the TR schemes are better than pre-equalization schemes, whereas those are worse than SC by approximately 0.8 bps/Hz for high SNR as we discussed in Section IV. The OFDM with optimal power allocation has no visible advantage over SC. However, OFDM outperforms SC for low SNR. In the low SNR regimes, TR can offer twice as high capacity as SC. Note that the use of multiple antennas ($M = 5$) can significantly improve the capacity. For that case, the performance gap between the optimal precoding and the MRC-TR precoding becomes very small.

In Fig. 3, we show the impact of the number of distributed antennas M on the link capacity for an SNR of ± 30 dB. We can see that the unitary precoder (SC and OFDM without power control) cannot enjoy any benefit even if we increase the number of distributed antennas. For low SNR, TR offers the capacity comparable to the one achieved by MMSE, and TR is always better than the unitary precoding. Note that the simulation result of capacity ratio $C_{\text{TR}} / C_{\text{SC}}$ completely matches the scaling law of $1 + M$ which is derived in Section IV. For high SNR, TR is worse than SC by 0.8 bps/Hz when $M = 1$, whereas it outperforms SC with multiple transmitters. Moreover, the TR can approach the optimal precoder (OFDM with optimal power control) for large M. The simulated capacity advantage of $C_{\text{TR}} - C_{\text{SC}}$ perfectly agrees with the scaling law of $2 \sum_{m=1}^{M-1} 1/m - (\gamma_{\text{E}} + \ln(M))$.

C. MSE Comparison

In Fig. 4, we plot the MSE curves with no interference limitation as a function of the number of transmitters M at an SNR of 0 dB and 30 dB. At high SNR, the original MRC-TR scheme has the worst performance in MSE among these precoding schemes for $M = 1$, whereas it can outperform all the other non-optimal precoders when $M \geq 3$. The

TABLE I
CAPACITY COMPARISON AMONG VARIOUS TYPES OF LINEAR BLOCK PRECODING

| Precoding Scheme	Capacity C	Energy limitation η_m^2
Optimum (OFDM)	$\frac{1}{L}\sum \ln\left(1 + \frac{1}{\sigma^2}|\Psi_1(i)|^2\right)$	$|\Psi_1(i)|^2$ is given by modified water filling in (65)
Unitary (SC)	$\frac{1}{L}\sum \ln\left(1 + \frac{1}{\sigma^2}|\sum \eta_m G_{1,m}(i)|^2\right)$	$\frac{1}{M}\sum \eta_m^2 \leq E_{\mathrm{s}},\ \frac{1}{ML}\sum|\sum \eta_m G_{n,m}(i)|^2 \leq E_{\mathrm{v}}$
MRC-TR	$\frac{1}{L}\sum \ln\left(1 + \frac{1}{\sigma^2}\left(\sum \eta_m |G_{1,m}(i)|^2\right)^2\right)$	$\frac{1}{ML}\sum \eta_m^2 \sum |G_{1,m}(i)|^2 \leq E_{\mathrm{s}},\ \frac{1}{ML}\sum|\sum \eta_m G_{n,m}(i)G_{1,m}^*(i)|^2 \leq E_{\mathrm{v}}$
EGC-TR, SLC-TR	$\frac{1}{L}\sum \ln\left(1 + \frac{1}{\sigma^2}|\sum \eta_m G_{1,m}(i)\breve{G}_{1,m}(i)|^2\right)$	$\frac{1}{ML}\sum \eta_m^2 \sum |\breve{G}_{1,m}(i)|^2 \leq E_{\mathrm{s}},\ \frac{1}{ML}\sum|\sum \eta_m G_{n,m}(i)\breve{G}_{1,m}(i)|^2 \leq E_{\mathrm{v}}$
ZF	$\ln\left(1 + \frac{1}{\sigma^2}\left(\sum \eta_m\right)^2\right)$	$\frac{1}{ML}\sum \eta_m^2 \sum \frac{1}{|G_{1,m}(i)|^2} \leq E_{\mathrm{s}},\ \frac{1}{ML}\sum|\sum \eta_m \frac{G_{n,m}(i)G_{1,m}^*(i)}{|G_{1,m}(i)|^2}|^2 \leq E_{\mathrm{v}}$
MMSE	$\frac{1}{L}\sum \ln\left(1 + \frac{1}{\sigma^2}\left(\sum \eta_m \frac{|G_{1,m}(i)|^2}{|G_{1,m}(i)|^2+\sigma^2}\right)^2\right)$	$\frac{1}{ML}\sum \eta_m^2 \sum \frac{|G_{1,m}(i)|^2}{(|G_{1,m}(i)|^2+\sigma^2)^2} \leq E_{\mathrm{s}},\ \frac{1}{ML}\sum|\sum \eta_m \frac{G_{n,m}(i)G_{1,m}^*(i)}{|G_{1,m}(i)|^2+\sigma^2}|^2 \leq E_{\mathrm{v}}$
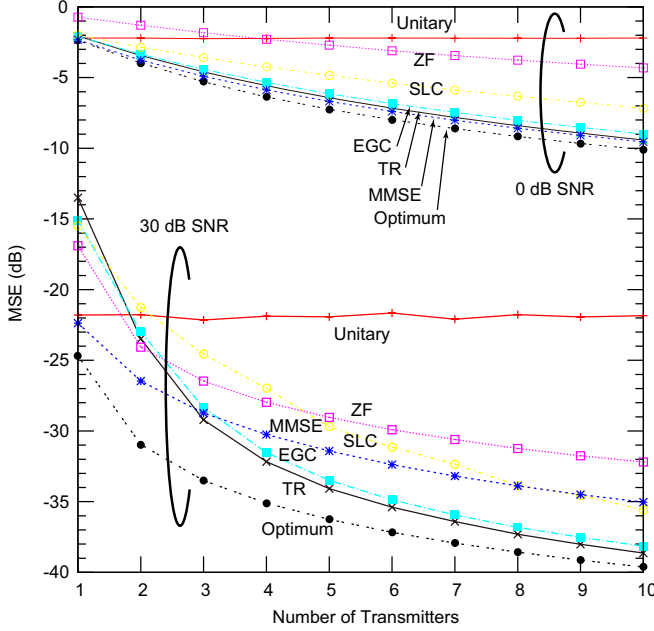
Fig. 4. MSE versus the number of transmitters in 1.0 dB decaying 16-path Rayleigh fading (0 dB and 30 dB SNR).
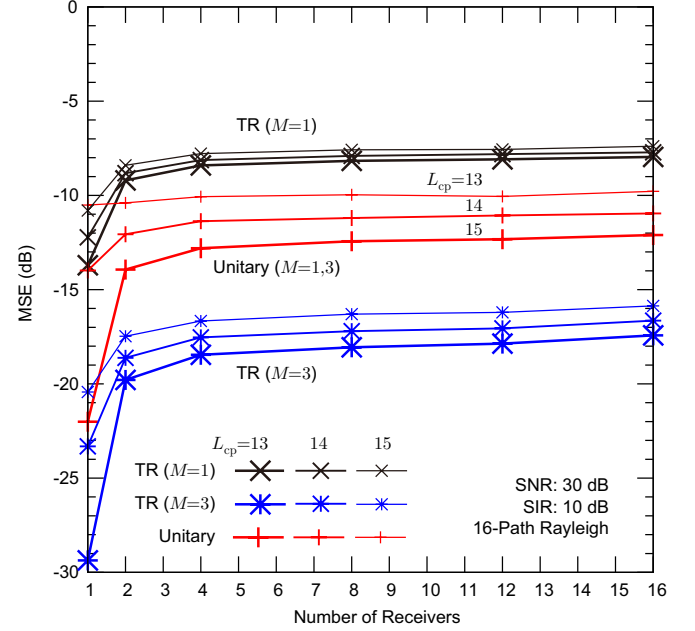

Fig. 5. MSE versus the number of receivers in 1.0 dB decaying 16-path Rayleigh fading (30 dB SNR, 10 dB SIR, $M \in \{1,3\}$, $L_{\mathrm{cp}} \in \{13, 14, 15\}$).

MSE performance of TR can converge to that of the optimal precoder. The MMSE precoding can offer the minimum MSE performance among the non-optimal precoders for low SNR regimes, while it cannot achieve good MSE performance in high SNR regimes for a large number of cooperating base stations ($M \geq 3$). It is because we do not allow the use of full channel state information over all the distributed antennas.

In Fig. 5, we evaluate MSE versus the number of active receivers N for a signal-to-interference ratio (SIR) of $E_{\mathrm{s}}/E_{\mathrm{v}} = 10$ dB and an SNR of $ME_{\mathrm{s}}\rho_1/\sigma^2 = 30$ dB. Here, we use $M = 1$ or $M = 3$ base stations to compare the unitary precoding and the MRC-TR precoding. Due to the interference limitation, the MSE can be degraded when $N > 1$. However, the MSE degradation can be saturated for more-than four antennas. In this figure, we also present the MSE curves when the cyclic prefix length is not sufficient to avoid inter-symbol interference, i.e., $L_{\mathrm{cp}} < 15$. We can see that the decrease of the cyclic prefix length can degrade MSE especially for the unitary (SC) precoder. Note that the TR is more robust than the SC for insufficient CP lengths because the TR can shorten the effective channel delay spread.

D. Secrecy Comparison

In Table II, we list achievable secrecy capacity comparisons for various precoding schemes, according to the instantaneous channel realization. Through the simulation taking average over the possible channel realizations, we show the average secrecy rate performance in Fig. 6 as a function of SNR for $M = 5$ base stations and $N = 2$ active users. For low SNR regimes, the secrecy capacity is almost comparable to the link capacity, as discussed in Section V. In contrast, for high SNR regimes, all the non-optimal precoders suffer from a significant performance degradation compared to the optimal precoding. This results from the fact that the optimal precoder exploits the channel state information at all the distributed base stations to make a nulling beamform vector for the eavesdropping user. Note that while it may be practical for a cellular system to have channel state information of all the legitimate users available, in most practical cases the transmitters do no know the channel to the eavesdroppers - in particular if the eavesdroppers are clandestine. As addressed in Section V, it is confirmed that the increase of SNR does not contribute to improving secrecy rate for the non-optimal precoder in the high SNR regimes. Note that among the non-optimal precoders, the MRC-TR precoding offers the best secrecy rate.

TABLE II
ACHIEVABLE SECRECY RATE COMPARISON AMONG VARIOUS TYPES OF LINEAR BLOCK PRECODING

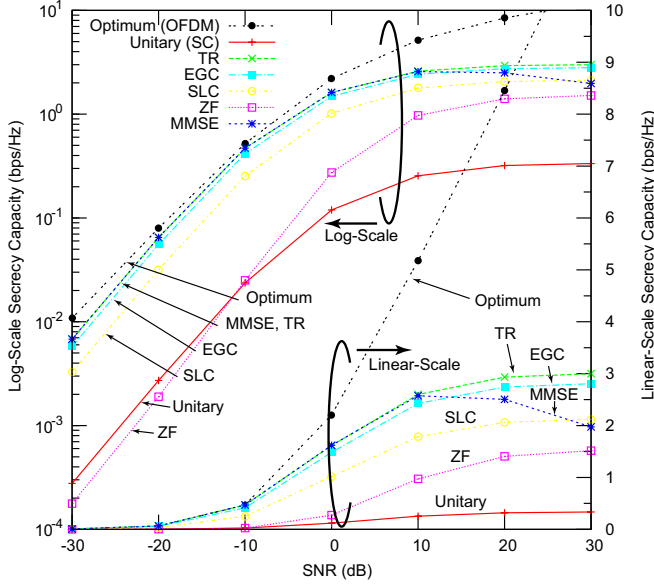| Precoding Scheme	Achievable Secrecy Rate R_S	Energy limitation η_m^2
Optimum (OFDM)	$\frac{1}{L}\sum \ln\big(\sigma^2+\vert\Psi_1(i)\vert^2\big)/\big(\sigma^2+\vert\Psi_{n'}(i)\vert^2\big)$	$\vert\Psi_1(i)\vert^2$ and $\vert\Psi_{n'}(i)\vert^2$ are given in (80)
Unitary (SC)	$\frac{1}{L}\sum \ln\big(\sigma^2+\vert\sum\eta_m G_{1,m}(i)\vert^2\big)/\big(\sigma^2+\vert\sum\eta_m G_{n',m}(i)\vert^2\big)$	$\frac{1}{M}\sum\eta_m^2 \le E_s$
MRC-TR	$\frac{1}{L}\sum \ln\big(\sigma^2+(\sum\eta_m\vert G_{1,m}(i)\vert^2)^2\big)/\big(\sigma^2+\vert\sum\eta_m G_{n',m}(i)G_{1,m}^*(i)\vert^2\big)$	$\frac{1}{ML}\sum\eta_m^2\sum\vert G_{1,m}(i)\vert^2 \le E_s$
EGC-TR, SLC-TR	$\frac{1}{L}\sum \ln\big(\sigma^2+\vert\sum\eta_m G_{1,m}(i)\breve{G}_{1,m}(i)\vert^2\big)/\big(\sigma^2+\vert\sum\eta_m G_{n',m}(i)\breve{G}_{1,m}(i)\vert^2\big)$	$\frac{1}{ML}\sum\eta_m^2\sum\vert\breve{G}_{1,m}(i)\vert^2 \le E_s$
ZF	$\ln\big(1+\frac{1}{\sigma^2}(\sum\eta_m)^2\big)-\frac{1}{L}\sum\ln\big(1+\frac{1}{\sigma^2}\vert\sum\eta_m G_{n',m}(i)/G_{1,m}(i)\vert^2\big)$	$\frac{1}{ML}\sum\eta_m^2\sum\frac{1}{\vert G_{1,m}(i)\vert^2} \le E_s$
MMSE	$\frac{1}{L}\sum\ln\big(\sigma^2+(\sum\eta_m\frac{\vert G_{1,m}(i)\vert^2}{\vert G_{1,m}(i)\vert^2+\sigma^2})^2\big)/\big(\sigma^2+\vert\sum\eta_m\frac{G_{n',m}(i)G_{1,m}^*(i)}{\vert G_{1,m}(i)\vert^2+\sigma^2}\vert^2\big)$	$\frac{1}{ML}\sum\eta_m^2\sum\frac{\vert G_{1,m}(i)\vert^2}{(\vert G_{1,m}(i)\vert^2+\sigma^2)^2} \le E_s$

Fig. 6. Achievable secrecy rate as a function of SNR in 1.0 dB decaying 16-path Rayleigh fading ($M=5$, $N=2$, $\rho_1=\rho_2$).

secrecy capacity among the non-optimal precoders. Although its secrecy capacity is much lower than the optimal one, the TR scheme can be the best candidate for practical precoding because it requires no channel state information of eavesdroppers. Moreover, the asymptotic analysis of the achievable secrecy rate verified that TR achieves secrecy capacity comparable to the channel capacity in the low SNR regimes and for the case where we can use a large number of cooperative base stations.

Capacity, MSE, and physical-layer security are, of course, not the only relevant parameters for the selection of a transmission scheme. For example, SC generally provides lower peak-to-average power ratio for transmissions, making it easier to build suitable power amplifiers; TR provides channel shortening which can decrease the required length of the CP, and also allows to shift complexity from the receiver to the transmitter, which is often desirable. Another measure which aggregates multi-variate performance may be attractive to see overall system performance in multi-user networks. Nevertheless, our unified evaluation methodology still allows us to gain new insights into the most fundamental characteristics of a very important class of high-speed digital transmission schemes.

VII. SUMMARY

In this paper, we investigated the capacity, MSE, and secrecy rate achieved by several linear block precoding schemes. We derived an optimal precoding scheme (OFDM with optimal power and phase control) in the presence of interference limitation and multiple distributed antennas. We confirmed that OFDM with optimal power control has advantages over the SC block transmission in capacity only in the low SNR regime, and in MSE for high SNR. For single antenna systems, the TR precoding has a capacity loss of approximately 0.8 bps/Hz over SC for high SNR, while it offers double the capacity of SC for a low SNR. We derived a capacity scaling law which shows how the number of cooperative transmitters can increase the capacity: The capacity difference between TR and SC has a logarithmic increase with the number of transmitters for high SNR, and the capacity ratio has a linear increase for low SNR. In distributed antenna systems, TR gives a high capacity which is close to the one achieved by the optimal precoder.

To evaluate physical-layer security level, we compared secrecy capacity achieved by different precoding schemes. The optimal precoder that was derived in this paper can achieve high secrecy capacity because multiple cooperative base stations can beamform to null the radio waves for some eavesdroppers. The TR precoder can offer the highest

APPENDIX

A. Optimal Precoder for Maximizing Link Capacity

Here we derive the optimal precoder which maximizes the link capacity with constraints of transmission power and interference level, as defined in (15), (16) and (17). We use the Lagrange multipliers method to optimize precoding. The Lagrangian utility function to be optimized is written as

$$\mathcal{L} = \ln\det\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_1\boldsymbol{\mathcal{H}}_1^\dagger\right)$$
$$- \lambda_1\left(\sum_{m=1}^M \text{tr}\left[\boldsymbol{P}_m\boldsymbol{P}_m^\dagger\right] - LME_s\right)$$
$$- \sum_{n=2}^N \lambda_n\left(\sum_{m=1}^M \text{tr}\left[\boldsymbol{\mathcal{H}}_n\boldsymbol{\mathcal{H}}_n^\dagger\right] - LME_v\right). \quad (55)$$

Taking the derivative with respect to $\boldsymbol{P}_m^*$, we obtain the KKT condition for stationary points, as follows:

$$\boldsymbol{H}_{1,m}^\dagger\boldsymbol{\mathcal{H}}_1\left(\sigma^2\boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-1} = \lambda_1\boldsymbol{P}_m + \sum_{n=2}^N \lambda_n\boldsymbol{H}_{n,m}^\dagger\boldsymbol{\mathcal{H}}_n,$$
$$(56)$$

where λ_n are the Lagrangian multipliers. It can be found that the solution is written in the form of $\boldsymbol{P}_m = \boldsymbol{F}\boldsymbol{\Phi}_m$, i.e., OFDM signalling.

Let $G_{n,m}(i)$ and $\Phi_m(i)$ be the i-th diagonal element of the frequency-domain channel matrix $\boldsymbol{G}_{m,n}$ and the power allocation matrix $\boldsymbol{\Phi}_m$, respectively. When we define

$$\Psi_n(i) = \sum_{m=1}^{M} G_{n,m}(i)\Phi_m(i), \tag{57}$$

we can rewrite the KKT condition for each diagonal entry as

$$\frac{G_{1,m}^*(i)\Psi_1(i)}{\sigma^2 + |\Psi_1(i)|^2} = \lambda_1 \Phi_m(i) + \sum_{n=2}^{N} \lambda_n G_{n,m}^*(i)\Psi_n(i), \tag{58}$$

where $\boldsymbol{H}_{n,m} = \boldsymbol{F}\boldsymbol{G}_{n,m}\boldsymbol{F}^\dagger$ and $\boldsymbol{\mathcal{H}}_n = \boldsymbol{F}\sum_m \boldsymbol{G}_{n,m}\boldsymbol{\Phi}_m$ are used. Stacking the KKT conditions for all $m \in \{1,\ldots,M\}$ into a column vector yields

$$\frac{\Psi_1(i)}{\sigma^2 + |\Psi_1(i)|^2}\boldsymbol{g}_1(i) = \boldsymbol{\Theta}(i)\boldsymbol{\phi}(i), \tag{59}$$

where

$$\boldsymbol{\Theta}(i) = \lambda_1 \boldsymbol{I}_M + \boldsymbol{G}^\dagger(i)\boldsymbol{\Lambda}\boldsymbol{G}(i), \tag{60}$$

$$\boldsymbol{g}_n(i) = \begin{bmatrix} G_{n,1}^*(i) \\ \vdots \\ G_{n,M}^*(i) \end{bmatrix}, \quad \boldsymbol{\phi}(i) = \begin{bmatrix} \Phi_1(i) \\ \vdots \\ \Phi_M(i) \end{bmatrix}, \tag{61}$$

$$\boldsymbol{G}(i) = \begin{bmatrix} \boldsymbol{g}_1(i) & \boldsymbol{g}_2(i) & \cdots & \boldsymbol{g}_N(i) \end{bmatrix}^\dagger, \tag{62}$$

$$\boldsymbol{\Lambda} = \mathrm{diag}\,(0, \lambda_2, \ldots, \lambda_N). \tag{63}$$

Hence, we obtain the solution of optimal power control as

$$\boldsymbol{\phi}(i) = \frac{\Psi_1(i)}{\sigma^2 + |\Psi_1(i)|^2}\boldsymbol{\Theta}^-(i)\boldsymbol{g}_1(i), \tag{64}$$

where $[\cdot]^-$ denotes the pseudo inverse.

Since $\Psi_1(i) = \boldsymbol{g}_1^\dagger(i)\boldsymbol{\phi}(i)$, the optimal $\Psi_1(i)$ must fulfil

$$|\Psi_1(i)|^2 = [\xi(i) - \sigma^2]_{+0}, \tag{65}$$

where $\xi(i) = \boldsymbol{g}_1^\dagger(i)\boldsymbol{\Theta}^-(i)\boldsymbol{g}_1(i)$. The Lagrangian multipliers λ_n are chosen for satisfying (16) and (17). Note that this optimal power control is not given by the conventional water filling unless $\lambda_n = 0$ for all $2 \le n \le N$, i.e., there is no interference limitation (17). Without interference limitation, the m-th entry of the optimal power allocation in (64) reduces to

$$\Phi_m(i) = \sqrt{\left[\frac{1}{\lambda_1} - \frac{\sigma^2}{\|\boldsymbol{g}_1(i)\|^2}\right]_{+0}}\frac{G_{1,m}^*(i)}{\|\boldsymbol{g}_1(i)\|}, \tag{66}$$

which means that distributed antennas should form the MRC diversity transmissions and use the conventional water filling for power allocation.

With the optimal precoder, the maximized capacity is expressed as

$$C_1 = \frac{1}{L}\sum_{i=0}^{L-1}\ln\left(1 + \frac{1}{\sigma^2}|\Psi_1(i)|^2\right) = \frac{1}{L}\sum_{i=0}^{L-1}\left[\ln\left(\frac{\xi(i)}{\sigma^2}\right)\right]_{+0}.$$

B. Optimal Precoder for Minimizing MSE

The Lagrangian utility function to be optimized for minimizing the MSE is written as

$$\mathcal{L} = -\mathrm{tr}\left[\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-1}\right]$$
$$- \lambda_1\left(\sum_{m=1}^{M}\mathrm{tr}\left[\boldsymbol{P}_m\boldsymbol{P}_m^\dagger\right] - LME_s\right)$$
$$- \sum_{n=2}^{N}\lambda_n\left(\sum_{m=1}^{M}\mathrm{tr}\left[\boldsymbol{\mathcal{H}}_n\boldsymbol{\mathcal{H}}_n^\dagger\right] - LME_v\right). \tag{67}$$

Taking the derivative in terms of $\boldsymbol{P}_m^*$ yields

$$\frac{\partial\mathcal{L}}{\partial\boldsymbol{P}_m^*} = \frac{1}{\sigma^2}\boldsymbol{H}_{1,m}^\dagger\boldsymbol{\mathcal{H}}_1\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-2}$$
$$- \lambda_1\boldsymbol{P}_m - \sum_{n=2}^{N}\lambda_n\boldsymbol{H}_{n,m}^\dagger\boldsymbol{\mathcal{H}}_n. \tag{68}$$

Zeroing the above expression gives the KKT conditions. Its solution is also based on OFDM signalling. However, the optimal power allocation differs from the one for maximizing capacity; it is given as follows:

$$\boldsymbol{\phi}(i) = \frac{\sigma^2\Psi_1(i)}{\left(\sigma^2 + |\Psi_1(i)|^2\right)^2}\boldsymbol{\Theta}^-(i)\boldsymbol{g}_1(i), \tag{69}$$

where $\Psi_1(i)$ must fulfil

$$|\Phi_1(i)|^2 = \left[\sqrt{\sigma^2\xi(i)} - \sigma^2\right]_{+0}. \tag{70}$$

It requires a modification from conventional water filling. Without interference limitation ($\lambda_n = 0$ for all $2 \le n \le N$), the m-th element of the optimal power in (69) reduces to

$$\Phi_m(i) = \sqrt{\left[\sqrt{\frac{\sigma^2}{\lambda_1\|\boldsymbol{g}_1(i)\|^2}} - \frac{\sigma^2}{\|\boldsymbol{g}_1(i)\|^2}\right]_{+0}}\frac{G_{1,m}^*(i)}{\|\boldsymbol{g}_1(i)\|}. \tag{71}$$

With the optimal precoder, the minimized MSE is written as

$$\varepsilon_1 = \frac{1}{L}\sum_{i=0}^{L-1}\left(1 + \frac{1}{\sigma^2}|\Psi_1(i)|^2\right)^{-1} = \frac{1}{L}\sum_{i=0}^{L-1}\left(\left[\frac{\xi(i)}{\sigma^2}\right]_{+1}\right)^{-\frac{1}{2}}.$$

C. Optimal Precoder for Maximizing Secrecy Rate

The Lagrangian utility function for maximizing the secrecy rate can be expressed as

$$\mathcal{L} = \ln\det\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_1\boldsymbol{\mathcal{H}}_1^\dagger\right) - LR$$
$$- \lambda_1\left(\sum_{m=1}^{M}\mathrm{tr}\left[\boldsymbol{P}_m\boldsymbol{P}_m^\dagger\right] - LME_s\right)$$
$$- \sum_{n=2}^{N}\lambda_n\left(\ln\det\left(\boldsymbol{I}_L + \frac{1}{\sigma^2}\boldsymbol{\mathcal{H}}_n\boldsymbol{\mathcal{H}}_n^\dagger\right) - LR\right). \tag{72}$$

Taking the derivative in terms of $\boldsymbol{P}_m^*$ yields the KKT condition:

$$\frac{\partial\mathcal{L}}{\partial\boldsymbol{P}_m^*} = \boldsymbol{H}_{1,m}^\dagger\boldsymbol{\mathcal{H}}_1\left(\sigma^2\boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_1^\dagger\boldsymbol{\mathcal{H}}_1\right)^{-1} - \lambda_1\boldsymbol{P}_m$$
$$- \sum_{n=2}^{N}\lambda_n\boldsymbol{H}_{n,m}^\dagger\boldsymbol{\mathcal{H}}_n\left(\sigma^2\boldsymbol{I}_L + \boldsymbol{\mathcal{H}}_n^\dagger\boldsymbol{\mathcal{H}}_n\right)^{-1} = \boldsymbol{0}. \tag{73}$$

Meanwhile, the derivative of $\mathcal{L}$ with respect to R gives the KKT condition of

$$\sum_{n=2}^{N} \lambda_n = 1. \tag{74}$$

The optimal precoder is the OFDM signalling in the form of $\boldsymbol{P}_m = \boldsymbol{F}\boldsymbol{\Phi}_m$. With $\boldsymbol{g}_n(i)$ and $\boldsymbol{\phi}(i)$, we can rewrite the KKT condition per sub-carrier as follow:

$$\lambda_1 \boldsymbol{\phi}(i) =$$
$$\underbrace{\left(\frac{\boldsymbol{g}_1(i)\boldsymbol{g}_1^{\dagger}(i)}{\sigma^2 + |\boldsymbol{g}_1^{\dagger}(i)\boldsymbol{\phi}(i)|^2} - \sum_{n=2}^{N} \lambda_n \frac{\boldsymbol{g}_n(i)\boldsymbol{g}_n^{\dagger}(i)}{\sigma^2 + |\boldsymbol{g}_n^{\dagger}(i)\boldsymbol{\phi}(i)|^2} \right)}_{\boldsymbol{\Omega}(i)} \boldsymbol{\phi}(i). \tag{75}$$

It implies that the Lagrange multiplier λ_1 and the precoding vector $\boldsymbol{\phi}(i)$ shall be the eigenvalue and the associated eigenvector of a matrix $\boldsymbol{\Omega}(i) \in \mathbb{C}^{M \times M}$. It means that the optimal precoder controls $\boldsymbol{\Omega}(i)$ to have the identical eigenvalue over all the sub-carrier for $i = 1, 2, \ldots, L$.

It is obvious that the eigenvector $\boldsymbol{\phi}(i)$ can be expressed as a linear combination of $\boldsymbol{g}_1(i), \ldots, \boldsymbol{g}_N(i)$. For a specific case of $N = 2$ and $M \geq N$ given a non-zero eigenvalue λ_1, the associated eigenvector becomes

$$\boldsymbol{\phi}(i) = \zeta(i)\big(\lambda_1 \boldsymbol{\phi}_1(i) + \kappa(i)\boldsymbol{\phi}_2(i)\big), \tag{76}$$

where

$$\kappa(i) = \frac{\|\boldsymbol{g}_2(i)\|^2}{\sigma^2 + \lambda_1^2 \zeta^2(i)|\boldsymbol{g}_2^{\dagger}(i)\boldsymbol{g}_1(i)|^2}, \tag{77}$$

$$\boldsymbol{\phi}_1(i) = \boldsymbol{g}_1(i), \tag{78}$$

$$\boldsymbol{\phi}_2(i) = \left(\boldsymbol{I}_M - \frac{\boldsymbol{g}_2(i)\boldsymbol{g}_2^{\dagger}(i)}{\|\boldsymbol{g}_2(i)\|^2} \right) \boldsymbol{g}_1(i). \tag{79}$$

The real–valued parameter $\zeta(i)$ is an amplitude control factor. It should be noted that $\boldsymbol{\phi}_1(i)$ is the MRC beamforming vector to maximize the SNR at the intended user, whereas $\boldsymbol{\phi}_2(i)$ is one of nulling beamformers to minimize the SNR at the unintended user. It can be seen that the optimal precoder is an appropriate mixture of the MRC beamformer and the nulling beamformers even for the generalized case of $N \geq 2$.

Multiplying $\boldsymbol{\phi}^{\dagger}(i)$ from the left of the KKT condition (75), we have

$$\lambda_1 \|\boldsymbol{\phi}(i)\|^2 = \frac{|\Psi_1(i)|^2}{\sigma^2 + |\Psi_1(i)|^2} - \sum_{n=2}^{N} \lambda_n \frac{|\Psi_n(i)|^2}{\sigma^2 + |\Psi_n(i)|^2}, \tag{80}$$

where $\lambda_1 \|\boldsymbol{\phi}(i)\|^2 \geq 0$. The Lagrange multiplier λ_1 must be satisfied with

$$\lambda_1 \geq \frac{\sigma^2}{LME_{\text{s}}} \sum_{i=0}^{L-1} \left(\sum_{n=2}^{N} \lambda_n \frac{1}{\sigma^2 + |\Psi_n(i)|^2} - \frac{1}{\sigma^2 + |\Psi_1(i)|^2} \right). \tag{81}$$

Using the optimal power allocation $\boldsymbol{\phi}(i)$ and the corresponding channel gains $|\Psi_n(i)|^2$, the optimized secrecy rate is written as

$$R_{\text{S}} = \frac{1}{L} \sum_{i=0}^{L-1} \ln \frac{\sigma^2 + |\Psi_1(i)|^2}{\sigma^2 + |\Psi_{n'}(i)|^2}, \tag{82}$$

where n' is the user index whose link capacity is the maximum over all the possible eavesdropping receivers.

REFERENCES

[1] T. Koike, A. F. Molisch, Z. Tao, P. Orlik, and T. Kuze, "Unified analysis of linear block precoding for distributed antenna systems," in *Proc. IEEE GLOBECOM*, Nov. 2009.

[2] A. F. Molisch, *Wireless Communications*. John Wiley & Sons, 2005.

[3] P. Kyritsi, G. Papanicolaou, P. Eggers, and A. Oprea, "Time reversal techniques for wireless communications," in *Proc. IEEE VTC-Fall*, Sep. 2004, pp. 47–51.

[4] J. M. F. Moura and Y. Jin, "Detection by time reversal: single antenna," *IEEE Trans. Signal Process.*, vol. 51, no. 1, pp. 187–201, Jan. 2007.

[5] D. D. Stancil, A. G. Cepni, B. E. Henty, Y. Jiang, Y. Jin, J.-G. Zhu, and J. M. F. Moura, "Super-resolution focusing and nulling in rich multipath environments using time-reversal techniques," in *Proc. IEEE ICEAA*, Apr. 2005.

[6] G. Ding, D. Wang, and Z. Chen, "Performance evaluation of two kinds of precoding joint with MMSE equalization in DS-UWB," in *Proc. ChinaCom*, Oct. 2006, pp. 1–5.

[7] P. Kyritsi, G. Papanicolaou, P. Eggers, and A. Oprea, "MISO time reversal and delay-spread compression for FWA channels at 5 GHz," *IEEE Antennas Wireless Propagat. Lett.*, vol. 3, pp. 96–99, 2004.

[8] H. T. Nguyen, "On the performance of one bit time reversal for multi-user wireless communications," in *Proc. IEEE ISWCS*, 2007, pp. 672–676.

[9] H. T. Nguyen, P. Kyritsi, and P. C. F. Eggers, "Time reversal technique for multi-user wireless communication with single tap receiver," in *Proc. IST Mobile Wireless Commun. Summit*, July 2007.

[10] P. Kyritsi, P. Stoica, G. Papanicolaou, P. Eggers, and A. Oprea, "Time reversal and zero-forcing equalization for fixed wireless access channels," in *Proc. Asilomar Conf.*, Oct. 2005, pp. 1297–1301.

[11] H. T. Nguyen, J. B. Andersen, G. F. Pedersen, P. Kyritsi, and P. C. F. Eggers, "Time reversal in wireless communications: a measurement-based investigation," *IEEE Trans. Wireless Commun.*, vol. 5, no. 8, pp. 2242–2252, Aug. 2006.

[12] H. T. Nguyen, J. B. Andersen, and G. F. Pedersen, "The potential use of time reversal techniques in multiple element antenna systems," *IEEE Commun. Lett.*, vol. 9, no. 1, pp. 40–42, Jan. 2005.

[13] Y. Jin, Y. Jiang, and J. M. F. Moura, "Multiple antenna time reversal transmission in ultra-wideband communications," in *Proc. IEEE GLOBECOM*, Nov. 2007.

[14] R. C. Qiu, C. J. Zhou, N. Guo, and J. Q. Zhang, "Time reversal with MISO for ultrawideband communications: experimental results," *IEEE Trans. Wireless Propagat. Lett.*, vol. 5, pp. 269–273, 2006.

[15] C. Zhou, N. Guo, and R. C. Qiu, "Experimental results on multiple-input single-output (MISO) time reversal for UWB systems in an office environment," in *Proc. IEEE MILCOM*, 2007.

[16] H. T. Nguyen, I. Z. Kovács, and P. C. F. Eggers, "A time reversal transmission approach for multiuser UWB communications," *IEEE Trans. Antennas Propagat.*, vol. 54, no. 11, pp. 3216–3224, Nov. 2006.

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

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

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

[20] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 572–578, May 1989.

[21] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channels with multiple eavesdroppers," in *Proc. IEEE ISIT*, June 2007.

[22] A. M. Tulino and S. Verdú, "Random matrices and wireless communications," *Foundations Trends Commun. Inf. Theory*, vol. 1, no. 1, June 2004.

[23] M. K. Simon, *Probability Distributions Involving Gaussian Random Variables: A Handbook for Engineers and Scientists*. Springer, 2006.

Toshiaki Koike-Akino received the B.S. degree in electrical and electronics engineering, and the M.S. and Ph.D. degrees in communications and computer engineering, from Kyoto University in 2002, 2003, and 2005, respectively. Since 2006, he has been a postdoctoral researcher at Harvard University, and concurrently has been a visiting researcher at Mitsubishi Electric Research Laboratories (MERL) since 2010. His research interests include digital signal processing for cooperative communications. He has served as a TPC member of IEEE PIMRC 2009, GLOBECOM 2010, ICC 2011, and VTC 2011. He received the YRP Encouragement Award 2005, the 21st TELECOM System Technology Award, the 2008 Ericsson Young Scientist Award, the IEEE GLOBECOM'08 Best Paper Award in the Wireless Communications Symposium, the 24th TELECOM System Technology Encouragement Award, and the IEEE GLOBECOM'09 Best Paper Award in the Wireless Communications Symposium.

Andreas F. Molisch received the Dipl. Ing., Dr. techn., and habilitation degrees from the Technical University Vienna (Austria) in 1990, 1994, and 1999, respectively. From 1991 to 2000, he was with TU Vienna, becoming an Associate Professor there in 1999. From 2000–2002, he was with the Wireless Systems Research Department at AT&T (Bell) Laboratories Research in Middletown, NJ. From 2002–2008, he was with Mitsubishi Electric Research Labs, Cambridge, MA, USA, most recently as a Distinguished Member of Technical Staff and Chief Wireless Standards Architect. Concurrently, he was Professor and Chairholder for radio systems at Lund University, Sweden. Since 2009, he is a Professor of electrical engineering at the University of Southern California, Los Angeles, CA, USA.

He has done research in the areas of SAW filters, radiative transfer in atomic vapors, atomic line filters, smart antennas, and wideband systems. His current research interests are measurement and modeling of mobile radio channels, UWB, cooperative communications, and MIMO systems. He has authored, co-authored, or edited four books (among them the textbook *Wireless Communications*, Wiley-IEEE Press), eleven book chapters, some 130 journal papers, and numerous conference contributions, as well as more than 70 patents and 60 standards contributions.

He is Area Editor for Antennas and Propagation of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and co-editor of special issues of several journals. He has been a member of numerous TPCs, vice chair of the TPC of VTC 2005 spring, general chair of ICUWB 2006, TPC co-chair of the wireless symposium of GLOBECOM 2007, TPC chair of Chinacom2007, and general chair of Chinacom 2008, TPC chair of the Communications Theory Workshop 2009, TPC vicechair of VTC 2010 spring, and workshop co-chair of ICC 2010. He has participated in the European research initiatives "COST 231," "COST 259," and "COST273," where he was chairman of the MIMO channel working group; he was also chairman of the IEEE 802.15.4a channel model standardization group. From 2005–2008, he was chairman of Commission C (signals and systems) of URSI (International Union of Radio Scientists), and since 2009, he is the Chair of the Radio Communications Committee of the IEEE Communications Society. He is a Fellow of the IEEE, a Fellow of the IET, an IEEE Distinguished Lecturer, and recipient of several awards.

Chunjie Duan received his B.Sc. from Tsinghua University, Beijing, China, the M.Sc. from Colorado State University, and the Ph.D. from the University of Colorado at Boulder, all in electrical engineering. He worked at Alcatel Bell Telephone as a system engineer from 1993 to 1996. From 1998 to 2004, he was with Qualcomm Inc's Infrastructure Division, which later became Ericsson Wireless Communications, as a senior engineer in CDMA systems and hardware design. Since 2004, he has been with Mitsubishi Electric Research Laboratories in Cambridge, Massachusetts, where he is currently a Senior Principal Technical Staff. His research interests are in physical layer design and signal processing in wireless and optical communications, as well as hardware implementations.

Philip Orlik received the B.E. degree in 1994 and the M.S. degree in 1997, both from the State University of New York at Stony Brook. In 1999, he earned his Ph.D. in electrical engineering, also from SUNY Stony Brook. He is currently a Senior Technical Staff member at Mitsubishi Electric Research Laboratories Inc. in Cambridge, MA. His primary research focus is on advanced wireless and mobile cellular communications, sensor networks, ad hoc networking, and UWB. Other research interests include vehicular/car-to-car communications, mobility modeling, performance analysis, and queuing theory.