Resource Allocation for a Massive MIMO Relay Aided Secure Communication

Jian Chen, Xiaoming Chen, *Senior Member, IEEE*, Wolfgang H. Gerstacker, *Senior Member, IEEE*, and Derrick Wing Kwan Ng, *Member, IEEE*

***Abstract*— In this paper, we address the problem of joint power and time allocation for secure communications in a decode-and-forward massive multiple-input multiple-output (M-MIMO) relaying system in the presence of a passive eavesdropper. We apply the M-MIMO relaying technique to enhance the secrecy performance under very practical and adverse conditions, i.e., no availability of instantaneous eavesdropper channel state information (CSI) and only imperfect instantaneous legitimate CSI. We first provide a performance analysis of secrecy outage capacity, which reveals the minimum required number of relay antennas for achieving a positive secrecy outage capacity. Then, we propose an optimization framework to jointly optimize source transmit power, relay transmit power, and transmission time in each hop, with the goal of maximizing the secrecy outage capacity. Although the secrecy outage capacity is not a concave function with respect to the optimization variables, we show that it can be maximized by first maximizing over some of the variables, and then maximizing over the rest. To this end, we first derive a closed-form solution of optimal relay transmit power, afterward obtain that of optimal source transmit power, and then derive the optimal ratio of the first-hop duration to a complete transmission time. Moreover, several important system design insights are provided through asymptotic performance analysis. Finally, simulation results validate the effectiveness of the proposed joint resource allocation scheme.**

***Index Terms*— Physical layer security, massive MIMO, DF relaying protocol, resource allocation.**

I. Introduction

SECURE communication over wireless channels is always a critical issue due to the broadcast nature of the wireless medium. Traditionally, secure communication is guaranteed by high-layer encryption [1]. However, the secrecy provided by the commonly used encryption technique is threatened by the rapid development of the computing devices, such as quantum computers. Additionally, the encryption technique requires a secure channel for the exchange of a private key, which may be impractical in mobile and ad-hoc wireless networks. Inspired by seminal works of Shannon [2] and Wyner [3], it is found that perfectly secure communication can be realized only by exploiting physical layer techniques, namely physical layer security (PHY-security). The crux of physical layer security is to exploit the physical characteristics of wireless channels, i.e., fading, noise and interference, so as to maximize the rate difference between the main channel and the wiretap channel, namely secrecy rate [4]–[6].

Wyner showed that when the eavesdropper channel is a degraded version of the legitimate channel, an achievable positive secrecy rate exists. However, the feasibility of PHY-security in traditional single-antenna systems may be hampered by channel condition. For instance, if the eavesdropper channel is more capable than the legitimate channel, a zero secrecy rate might result [7]. In contrast, multiple-antenna system can handle the secrecy problem in communication networks more efficiently via spatial beamforming, which has been confirmed by extensive researches [8]–[12] and references thierein. The authors in [13] characterized the optimal spatial beamformer in terms of a generalized eigenvector for a point-to-point multiple-antenna system where the transmitter and the eavesdropper are equipped with multiple antennas and the intended receiver has a single antenna. Furthermore, in the case of a multiple-antenna eavesdropper, a computable characterization of the spatial beamformer was established as the saddle point solution to a minimax problem in multiple-input multiple-output (MIMO) wiretap channel in [14]. It is shown that multiple-antenna techniques can effectively improve the secrecy rate by exploiting spatial degrees of freedom. Moreover, as an important security-enhancing technique, cooperative relaying has also received considerable attention [15]–[17]. The authors in [18] provided a detailed analysis of various secure cooperative schemes, i.e., decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ), for a relay aided communication system in the presence of one or more eavesdroppers. The use of a relay might shorten the communication distance, and thus improve the secrecy rate. Besides, the relay can confuse the eavesdropper by sending artificial noise (AN) for assisting the secure transmission from the source to the legitimate destination [19].

Manuscript received December 3, 2015; revised March 16, 2016; accepted April 1, 2016. Date of publication April 7, 2016; date of current version May 4, 2016. This work was supported in part by the Natural Science Foundation of China under Grant 61301102, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20130820, and in part by the Doctoral Fund of Ministry of Education of China under Grant 20123218120022. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Lifeng Lai.

J. Chen and X. Chen are with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China, and also with the Institute for Digital Communications, University of Erlangen-Nürnberg, Erlangen 91058, Germany (e-mail: chenjian04@nuaa.edu.cn; chenxiaoming@nuaa.edu.cn).

W. H. Gerstacker is with the Institute for Digital Communications, University of Erlangen-Nürnberg, Erlangen 91058, Germany (e-mail: wolfgang.gerstacker@fau.de).

D. W. K. Ng is with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW 2052, Australia (e-mail: wingn@ece.ubc.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2016.2551685

To further improve the secrecy performance, multiple-antenna techniques and cooperative relaying techniques can be combined in secure communication systems [20]. In [21] and [22], optimal beamforming schemes for a multiple-antenna relay in two-hop secure communications based on AF and DF relaying protocols were presented, respectively. It is worth pointing out that the optimal beamforming schemes rely on the perfect knowledge of both the legitimate channel and the eavesdropper channel. However, in practice, the instantaneous eavesdropper CSI may be imperfect or even unavailable, since the eavesdropper is usually passive and well hidden. Therefore, robust secure beamforming combined with AN was proposed to maximize the worst-case secrecy rate in presence of imperfect eavesdropper CSI [23]. Furthermore, if there is no instantaneous eavesdropper channel state information (CSI), a joint beamforming and jamming scheme can be employed according to [24]. Specifically, the AN is transmitted in the null space of the legitimate channel, so as to confuse the eavesdropper while avoiding interference to the legitimate destination [25], [26]. In practice, instantaneous legitimate CSI at the transmitter is often imperfect due to channel estimation errors or limited CSI feedback [27]. In this case, the AN will also interfere with the legitimate signal resulting in a loss of secrecy rate. Thus, it is necessary to introduce new MIMO relaying techniques to effectively enhance wireless security under very practical and adverse assumptions, i.e., no instantaneous eavesdropper CSI and imperfect instantaneous legitimate CSI. Recently, it is found that massive MIMO (M-MIMO) can produce high-resolution spatial beams, and thus information leakage to an unintended user is expected to be negligible [28]–[30]. In [31] and [32], M-MIMO techniques were applied to secure relaying systems without instantaneous eavesdropper CSI and with imperfect instantaneous legitimate CSI. It was shown that even in a very adverse environment, such as short-distance interception, the secrecy performance can be improved significantly by M-MIMO techniques.

To guarantee secure relaying communications, there are a variety of available physical layer resources, i.e., antenna, time, and power. Through resource allocation, it is expected that the secrecy performance can be further improved [33]. However, resource allocation in secure relaying communications might affect the signal quality at both the legitimate destination and the eavesdropper. Thus, it is not a trivial task to carry out optimal resource allocation. In [34], the transmit powers at the source and the relay were jointly optimized, so as to maximize the secrecy outage capacity in DF secure relay networks without instantaneous eavesdropper CSI and with imperfect instantaneous legitimate CSI. Moreover, for secure relaying systems, it is necessary to allocate time between the first and the second hops optimally for a given duration of a complete transmission from the source to the destination. Considering cooperative relaying in secure cognitive radio networks, the optimal joint time and power allocation was derived in [35] for maximizing the secrecy rate. In [36], optimal relay power allocation schemes were proposed in DF M-MIMO secure relaying systems for maximizing the secrecy outage capacity and minimizing the interception probability, respectively. To the best of authors' knowledge, joint time and power allocation in DF M-MIMO secure relaying systems under practical conditions is still an open issue. In this paper, we focus on the analysis and design of a joint time and power allocation scheme for a DF M-MIMO secure relaying system in the sense of maximizing the secrecy outage capacity. The contributions of this paper are as follows:

1) We provide a performance analysis in terms of secrecy outage capacity for a DF M-MIMO secure relaying system without instantaneous eavesdropper CSI and under imperfect instantaneous legitimate CSI. Our results reveal the requirement on the minimum number of relay antennas for achieving a positive secrecy outage capacity.
2) We propose a joint source transmit power, relay transmit power, and time allocation scheme through maximizing the secrecy outage capacity. We obtain closed-form solutions of optimal power allocation at the source and the relay, and derive the optimal time allocation for the two-hop communication by using the Lagrange multiplier method. Simulation results show that the proposed scheme can achieve the same performance as the optimal resource allocation scheme based on a three-dimensional exhaustive search, and has a significant performance gain over fixed resource allocation schemes.
3) We find that full power transmission at the source is always optimal for maximizing the secrecy outage capacity, despite the non-convexity of the considered problem. Moreover, given a maximum transmit power constraint at the relay, the secrecy outage capacity is saturated when the maximum available source power is sufficiently large. Similarly, for a given maximum power constraint at the source, the secrecy outage capacity is also saturated as the maximum available relay power increases.

The remainder of this paper is organized as follows. A two-hop DF M-MIMO secure relaying system model is introduced in Section II. In Section III, we propose a joint power and time allocation scheme for maximizing the secrecy outage capacity. In Section IV, we present some simulation results to validate the effectiveness of the proposed scheme. Finally, we conclude the paper in Section V.

Notation: Bold upper (or lower) case letters are used to denote matrices (or column vectors), $(\cdot)^H$ is to denote conjugate transpose, $E[\cdot]$ is used to denote expectation, $\|\cdot\|$ is to denote the L_2 norm of a vector, $|\cdot|$ denotes the absolute value, $(a)^+$ denotes the operation $\max(a, 0)$, $f^{'}(x)$ and $f^{''}(x)$ denote the first and second derivative of $f(x)$ with respect to x, and $\sim$ is used to denote the equality in distribution. The acronym "i.i.d." means "independent and identically distributed", "pdf" means "probability density function", and "cdf" stands for "cumulative distribution function".

II. System Model

We consider a device-to-device (D2D) communication over a relay in Beyond 4th Generation (B4G) systems, as depicted in Fig. 1. A source sends a message to a legitimate destination with the aid of a relay, while an eavesdropper intends to intercept the message. We assume that the relay is fixed

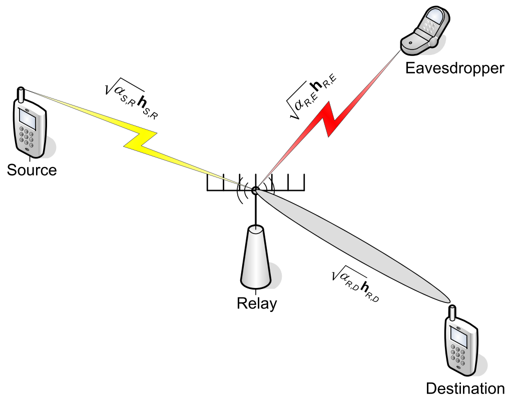

$\sqrt{\alpha_{S,R}}\mathbf{h}_{S,R}$
$\sqrt{\alpha_{R,E}}\mathbf{h}_{R,E}$
Eavesdropper
Source
Relay
$\sqrt{\alpha_{R,D}}\mathbf{h}_{R,D}$
Destination

Fig. 1. A DF M-MIMO secure relaying system.

and equipped with a massive antenna array, which is a key technology in B4G systems. According to [37], a massive antenna array in B4G systems typically will comprise $N_R \geq 64$ antennas. The other nodes are equipped with a single antenna each due to the size limitation of mobile devices. Besides, the eavesdropper may be an idle destination or pretends to be a legitimate receiver, such that it also employs a single antenna. Due to a long propagation distance, the direct transmission from the source to the legitimate destination does not exist. The relay works in a half-duplex mode, which means a complete transmission requires two orthogonal time slots. Specifically, the source sends the signal to the relay in the first time slot, and then the relay forwards the decoded signal to the legitimate destination in the second time slot. In this paper, it is assumed that the time duration of a two-hop transmission is T fixedly, and the transmission duration of the first hop is θT with $0 < \theta < 1$. In practice, the relay is far away from the source, such that it is difficult for the single-antenna eavesdropper to overhear both the source and the relay due to a long distance. Moreover, if the eavesdropper is an idle destination, it is close to the relay, but not to the source. Thus, following the previous related works [16], [38], we also assume that the eavesdropper only monitors the transmission from the relay to the destination.

We use $\sqrt{\alpha_{S,R}}\mathbf{h}_{S,R}$, $\sqrt{\alpha_{R,D}}\mathbf{h}_{R,D}$, and $\sqrt{\alpha_{R,E}}\mathbf{h}_{R,E}$ to represent the channels from the source to the relay, the relay to the destination, and the relay to the eavesdropper respectively, where $\alpha_{S,R}$, $\alpha_{R,D}$, and $\alpha_{R,E}$ are the distance-dependent path losses, and $\mathbf{h}_{S,R}$, $\mathbf{h}_{R,D}$, and $\mathbf{h}_{R,E}$ are N_R-dimensional channel small-scale fading vectors with independent and identically distributed (i.i.d.) zero mean and unit variance complex Gaussian entries. It is assumed that the channels remain constant during a time slot T and change independently over slots. Thus, the received signal at the relay in the first time slot can be expressed as

$$\mathbf{y}_R = \sqrt{P_S \alpha_{S,R}}\mathbf{h}_{S,R} s + \mathbf{n}_R, \tag{1}$$

where s is the Gaussian distributed transmit signal with a unit power, P_S is the transmit power at the source, and $\mathbf{n}_R$ is the additive white Gaussian noise (AWGN) vector with covariance matrix $\mathbf{I}_{N_R}$ at the relay. We assume that the relay has perfect instantaneous CSI about $\mathbf{h}_{S,R}$ through channel estimation based on pilots. Since maximum ratio combining (MRC) can achieve an asymptotically optimal performance in M-MIMO systems with a low complexity [39], the relay employs this reception scheme to recover the information from the source. Thus, the received signal after MRC becomes

$$\hat{y}_R = \sqrt{P_S \alpha_{S,R}}\frac{\mathbf{h}_{S,R}^H}{\|\mathbf{h}_{S,R}\|}\mathbf{h}_{S,R} s + \frac{\mathbf{h}_{S,R}^H}{\|\mathbf{h}_{S,R}\|}\mathbf{n}_R. \tag{2}$$

During the second time slot, the relay forwards the re-encoded Gaussian distributed signal $\hat{s}$ of unit norm using maximum ratio transmission (MRT) due to its low complexity and good performance in M-MIMO systems. We assume that the relay only has partial CSI about $\mathbf{h}_{R,D}$. This is because the estimation of $\mathbf{h}_{R,D}$ is commonly performed by making use of channel reciprocity in time division duplex (TDD) systems. However, due to duplexing and decoding delay, the resulting estimated CSI at the relay is usually imperfect [40]. In this case, the relation between the estimated CSI $\hat{\mathbf{h}}_{R,D}$ and the actual CSI $\mathbf{h}_{R,D}$ is given by

$$\mathbf{h}_{R,D} = \sqrt{\rho}\hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho}\mathbf{e}, \tag{3}$$

where $\mathbf{e}$ is the error noise vector with i.i.d., zero mean, and unit variance complex Gaussian entries, and is independent of $\hat{\mathbf{h}}_{R,D}$. $0 \leq \rho \leq 1$ is the correlation coefficient between $\hat{\mathbf{h}}_{R,D}$ and $\mathbf{h}_{R,D}$, which depends on delay duration and velocity of the destination [40]. Thus, the received signals at the destination and the eavesdropper are given by

$$y_D = \sqrt{P_R \alpha_{R,D}}\mathbf{h}_{R,D}^H \mathbf{r} + n_D, \tag{4}$$

and

$$y_E = \sqrt{P_R \alpha_{R,E}}\mathbf{h}_{R,E}^H \mathbf{r} + n_E, \tag{5}$$

respectively, where P_R is the transmit power of the relay, and $\mathbf{r} = \mathbf{v}_R \hat{s}$ is the forwarded signal with $\mathbf{v}_R = \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}$ being an MRT beamformer. n_D and n_E are AWGNs with unit variance at the destination and the eavesdropper, respectively.

Since the eavesdropper is usually passive and keeps silent, instantaneous CSI about $\mathbf{h}_{R,E}$ is unavailable at the relay. In this paper, we assume that the relay only has statistical knowledge about the channel from the relay to the eavesdropper, such as $\alpha_{R,E}$. This is reasonable because if the eavesdropper is an idle destination, the relay may obtain the position information. In the case of no instantaneous eavesdropper CSI, it is impossible to guarantee that the selected transmission rate is not greater than the secrecy capacity over fading channels. To evaluate the wireless security, we adopt secrecy outage capacity as a performance metric, which is defined as the maximum transmission rate such that the probability that the selected transmission rate is greater than the secrecy capacity is smaller than a given value [41]. Mathematically, it can be obtained from the condition

$$P_r(R_{soc} > C_D - C_E) = \varepsilon, \tag{6}$$

where C_D and C_E are the legitimate and eavesdropper channel capacities, respectively. ε is the maximum tolerable outage probability associated to a secrecy outage capacity R_{soc}.

III. Joint Power and Time Allocation

In this section, we first analyze the secrecy outage capacity for the considered DF M-MIMO secure relaying system under the situation of no instantaneous eavesdropper CSI and imperfect instantaneous legitimate CSI. Then, we reveal the condition for achieving a positive secrecy outage capacity. Finally, we propose a joint power and time allocation scheme for maximizing the secrecy outage capacity.

A. Some Primary Results on Very Long Random Vectors

In this paper, we consider a M-MIMO relaying system, and thus the channels can be modeled by very long random vectors. During the analysis, we will use some primary results on very long random vectors. Prior to performance analysis, we first introduce these useful results.

Let $\mathbf{p} \triangleq [p_1 \dots p_n]^T$ and $\mathbf{q} \triangleq [q_1 \dots q_n]^T$ be mutually independent $n \times 1$ vectors whose elements are i.i.d. zero mean random variables with variances σ_p^2 and σ_q^2, respectively. Then, as $n \to \infty$, the very long random vectors $\mathbf{p}$ and $\mathbf{q}$ have the following properties [42]:

A: According to the law of large numbers, we have

$$\frac{1}{n}\mathbf{p}^H\mathbf{p} \overset{a.s.}{\to} \sigma_p^2, \tag{7}$$

where $\overset{a.s.}{\to}$ denotes the almost sure convergence.

B: According to the Lindeberg-Lévy central limit theorem, we have

$$\frac{1}{\sqrt{n}}\mathbf{p}^H\mathbf{q} \overset{d}{\to} \mathcal{CN}(0, \sigma_p^2\sigma_q^2), \tag{8}$$

where $\overset{d.}{\to}$ denotes convergence in distribution.

B. Secrecy Outage Capacity

In this section, we focus on the analysis of secrecy outage capacity in the considered DF M-MIMO secure relaying system. Based on the received signal after performing MRC at the relay in (2), the channel capacity between the source to the relay can be written as

$$C_{S,R} = \theta \log_2(1 + \gamma_R), \tag{9}$$

where $\gamma_R = P_S \alpha_{S,R} \|\mathbf{h}_{S,R}\|^2$ is the received signal-to-noise ratio (SNR) at the relay. Similarly, according to (4) and (5), channel capacities from the relay to the destination and from the relay and the eavesdropper are given by

$$C_{R,D} = (1-\theta)\log_2(1+\gamma_D), \tag{10}$$

and

$$C_{R,E} = (1-\theta)\log_2(1+\gamma_E), \tag{11}$$

respectively, where $\gamma_D = P_R \alpha_{R,D} \left| \mathbf{h}_{R,D}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2$ and $\gamma_E = P_R \alpha_{R,E} \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2$ are SNRs at the destination and the eavesdropper, respectively.

According to the property of a two-hop DF relaying system, the legitimate and the eavesdropper channel capacities can be computed as

$$C_D = \min(C_{S,R}, C_{R,D}), \tag{12}$$

and

$$C_E = \min(C_{S,R}, C_{R,E}), \tag{13}$$

respectively.

Then, for the secrecy outage capacity in such a DF M-MIMO secure relaying system without instantaneous eavesdropper CSI and with imperfect instantaneous legitimate CSI, we have the following theorem:

Theorem 1: Given a maximum tolerable outage probability ε, the secrecy outage capacity can be tightly approximated as $R_{soc}(P_R, P_S, \theta) = \min\big(\theta \log_2(1 + P_S\alpha_{S,R}N_R), (1-\theta)\log_2(1+P_R\alpha_{R,D}\rho N_R)\big) - (1-\theta)\log_2(1-P_R\alpha_{R,E}\ln\varepsilon)$, if the number of relay antennas is sufficiently large.

Proof: Please refer to Appendix A. ■

From Theorem 1, it is known that the secrecy outage capacity is an increasing function of the number of relay antennas for a given outage probability requirement. Thus, it is possible to improve the secrecy outage capacity by adding relay antennas. In the sequel, we further analyze the effect of N_R on the secrecy performance. For notational simplicity, we let $\alpha_{S,R}N_R = A$, $\alpha_{R,D}\rho N_R = B$, $-\alpha_{R,E}\ln\varepsilon = B \cdot r_l$, where $r_l = -\frac{\alpha_{R,E}\ln\varepsilon}{\alpha_{R,D}\rho N_R}$. Then, the secrecy outage capacity can be rewritten as (14), as shown at the bottom of this page.

Note that the secrecy outage capacity may be negative from a pure mathematical view. Now, we find the condition for achieving a positive secrecy outage capacity. Observing the above secrecy outage capacity, we get the following proposition:

Proposition 1: Only if $0 < r_l < 1$, the secrecy outage capacity in such a DF M-MIMO secure relaying system in presence of imperfect CSI is positive.

Proof: Please refer to Appendix B. ■

From Proposition 1, it is known that if $r_l \geq 1$, the positive secrecy outage capacity does not exist despite the values of P_R, P_S, and θ. Thus, $0 < r_l < 1$ is the premise for power and time allocation in the considered DF M-MIMO secure relaying system. Given channel conditions and a secrecy outage probability requirement, there exists a minimum required number of antennas at the relay in order to fulfill the condition $0 < r_l < 1$. Then, we have the following proposition:

Proposition 2: In order to achieve a positive secrecy outage capacity, the number of antennas at the relay, N_R, must be larger than $-\frac{\alpha_{R,E}\ln\varepsilon}{\rho\alpha_{R,D}}$.

$$R_{soc}(P_R, P_S, \theta) = \begin{cases} (1-\theta)\log_2(1+P_RB) - (1-\theta)\log_2(1+P_RBr_l), & P_R \leq \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B} \\ \theta\log_2(1+P_SA) - (1-\theta)\log_2(1+P_RBr_l), & P_R \geq \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B} \end{cases} \tag{14}$$

Proof: According to the definition of $r_l = -\frac{\alpha_{R,E} \ln \varepsilon}{\rho \alpha_{R,D} N_R}$, $0 < r_l < 1$ is equivalent to $N_R > -\frac{\alpha_{R,E} \ln \varepsilon}{\rho \alpha_{R,D}}$. ■

Note that the more stringent the secrecy outage probability requirement is, the large the required minimum number of relay antennas is. However, for any non-zero secrecy outage probability tolerance, i.e., $0 < r_l < 1$ can always satisfy by deploying more relay antennas, which is an advantage of the considered M-MIMO relaying system. As a result, in what follows, we only consider the case of $0 < r_l < 1$ for the design of resource allocation.

C. Joint Power and Time Allocation

Intuitively, both power and time are scarce and critical resources in wireless communication systems. Especially for secure communication, an inappropriate resource allocation may not only waste the resource, but may also degrade the secrecy performance. This is because resource allocation will affect the performance of both the legitimate channel and the eavesdropper channel simultaneously. Thus, it is necessary to jointly optimize power and time for maximizing the secrecy outage capacity.

In general, joint power and time allocation in the considered DF M-MIMO secure relaying system can be formulated as the following optimization problem:

$$J_1: \max_{P_R, P_S, \theta} \; R_{soc}(P_R, P_S, \theta) \tag{15}$$

$$\text{s.t. } P_R \le P_{R,\max} \tag{16}$$

$$P_S \le P_{S,\max} \tag{17}$$

$$0 < \theta < 1, \tag{18}$$

where $P_{S,\max}$ and $P_{R,\max}$ are the maximum transmit power budgets at the source and the relay, respectively. Unfortunately, the objective function (15) in J_1 is not a convex function with respect to P_S, P_R, and θ, and thus it is difficult to obtain the optimal solution directly. To address this challenging problem, we apply the following property $\inf_{x,y} f(x, y) = \inf_x \tilde{f}(x)$, where $\tilde{f}(x) = \inf_y f(x, y)$ [43]. In other words, we can always minimize a function by first minimizing over some of the variables, and then minimizing over the remaining ones. This simple and general principle can be used to transform a difficult problem into solvable equivalent forms. Hence, to solve the non-convex optimization problem J_1, we can apply this principle twice. Specifically, we first maximize the objective function by maximizing over P_R, then over P_S, and finally solve an equivalent optimization problem related to θ.

1) Maximization Over P_R: By using the property mentioned above, we first maximize the objective function in (15) over P_R for given P_S and θ, which can be formulated as

$$H_1: \; R_1(P_S, \theta) = \max_{P_R} \; R_{soc}(P_R, P_S, \theta) \quad \text{s.t. } P_R \le P_{R,\max}. \tag{19}$$

In the sequel, we focus on getting a closed-form expression of optimal power at the relay, $P_R^\star$, and the corresponding maximum value of the objective function $R_1(P_R, \theta)$. By solving the optimization problem H_1, we have the following theorem about the closed-form expression of $P_R^\star$ and $R_1(P_S, \theta)$:

Theorem 2: The optimal power at the relay is $P_R^\star = \min\left(\frac{(1+P_S A)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}\right)$, and the corresponding maximum secrecy outage capacity is given by $R_1(P_S, \theta) = (1-\theta) \log_2\left(1 + \min\left(\frac{(1+P_S A)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}\right) B\right) - (1-\theta) \log_2\left(1 + \min\left(\frac{(1+P_S A)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}\right) B r_l\right)$.

Proof: Please refer to Appendix B. ■

Remark: It is found that if instantaneous eavesdropper CSI is unavailable, it is optimal for the DF secure relaying system to let the two hops have the same channel capacity, resulting in $P_R^\star = \min\left(\frac{(1+P_S A)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}\right)$, see Appendix B. Moreover, it is proved that the optimal relay transmit power is an increasing function of source transmit power. Then, we can obtain the following proposition:

Proposition 3: If the maximum available source transmit power is sufficiently large, then the maximum secrecy outage capacity will be saturated with respect to source transmit power. The saturated secrecy outage capacity is upper bounded by $R_1^{upper}(P_S, \theta) = (1-\theta) \log_2\left(1 + P_{R,\max} B\right) - (1-\theta) \log_2\left(1 + P_{R,\max} B r_l\right)$, which is independent of P_S and is an increasing function of $P_{R,\max}$.

Proof: If $P_{S,\max}$ is large enough, we always have $P_R^\star = \min\left(\frac{(1+P_S A)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}\right) = P_{R,\max}$, which is a constant. In this case, the maximum secrecy outage capacity is independent of P_S, and the corresponding saturated value is equal to $R_1^{upper}(P_S, \theta) = R_1(P_{R,\max}, \theta)$. ■

2) Maximization Over P_S: Based on the Theorem 2, the optimization problem J_1 is equivalent to

$$J_2: \max_{P_S, \theta} \; R_1(P_S, \theta) \quad \text{s.t. } P_S \le P_{S,\max}, \quad 0 < \theta < 1. \tag{20}$$

Using the above mentioned property again, we first maximize the objective function in (20) over P_S for a given θ. Thus, the optimization problem is transformed as

$$H_2: \; R_2(\theta) = \max_{P_S} \; R_1(P_S, \theta) \quad \text{s.t. } P_S \le P_{S,\max}. \tag{21}$$

By solving the above optimization problem, we get the following theorem:

Theorem 3: The optimal transmit power at the source from the perspectives of maximizing the secrecy outage capacity and minimizing the energy consumption is $P_S^\star = \min\left(P_{S,\max}, \frac{(P_{R,\max} B+1)^{\frac{1-\theta}{\theta}}-1}{A}\right)$, and the corresponding maximum secrecy outage capacity is given by $R_2(\theta) = \min\left((1-\theta) \log_2\left(1 + P_{R,\max} B\right) - (1-\theta) \log_2\left(1 + P_{R,\max} B r_l\right), \theta \log_2\left(1 + P_{S,\max} A\right) - (1-\theta) \log_2\left(1 + ((1 + P_{S,\max} A)^{\frac{\theta}{1-\theta}} - 1) r_l\right)\right)$.

Proof: Please refer to Appendix C. ■

Remark: It is found that the optimal source transmit power at the source is not unique in the sense of maximizing the secrecy outage capacity. However, $P_{S,\max}$ is always an optimal power. This is because increasing P_S does not degrade the secrecy performance since the eavesdropper only monitors the transmission from the relay to the destination. Then, from the perspective of reducing the computational complexity of the resource allocation algorithm, it is also likely to take $P_{S,\max}$ as the optimal source transmit power. Similarly, for the case of a large relay transmit power constraint, we can get the following proposition:

Proposition 4: If the maximum available relay transmit power is sufficiently large, then the maximum secrecy outage capacity will be saturated with respect to relay transmit power. The saturated secrecy outage capacity is upper bounded by $R_2^{upper}(\theta) = \theta \log_2\left(1 + P_{S,\max}A\right) - (1-\theta)\log_2\left(1 + \left((1 + P_{S,\max}A)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right)$, which is independent of P_R.

Proof: If $P_{R,\max}$ is large enough, we always have $P_S^\star = \min\left(P_{S,\max}, \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}\right) = P_{S,\max}$, which is a constant. Thus, the maximum secrecy outage capacity is saturated, and the corresponding saturated value is $R_2^{upper}(\theta) = \theta\log_2\left(1 + P_{S,\max}A\right) - (1-\theta)\log_2\left(1 + \left((1 + P_{S,\max}A)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right)$, which is independent of $P_{R,\max}$. ■

3) Maximization Over θ: Based on Theorem 2 and 3, we transform the original problem J_1 with three optimization variables P_S, P_R, and θ to a problem with only one optimization variable θ, which is equivalent to J_3 as below. Thus, we focus on getting an optimal solution of J_3 in this subsection.

$$\begin{aligned} J_3 :\ & \max_{\theta}\ R_2(\theta) \\ & \text{s.t. } 0 < \theta < 1. \end{aligned} \tag{22}$$

We first consider the case of $\theta \geq \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}$ or equivalently $P_{S,\max} \geq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$. In this context, the objective function can be reduced as $R_2(\theta) = \min\Big((1-\theta)\log_2\left(1 + P_{R,\max}B\right) - (1-\theta)\log_2\left(1 + P_{R,\max}Br_l\right), \theta\log_2\left(1 + P_{S,\max}A\right) - (1-\theta)\log_2\left(1 + \left((1 + P_{S,\max}A)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right)\Big) = (1-\theta)\log_2\left(1 + P_{R,\max}B\right) - (1-\theta)\log_2\left(1 + P_{R,\max}Br_l\right)$. Hence, J_3 is simplified as G_1 when $\theta \geq \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}$

$$\begin{aligned} G_1 :\ & \max_{\theta}\ (1-\theta)\log_2\left(1 + P_{R,\max}B\right) \\ & \qquad - (1-\theta)\log_2\left(1 + P_{R,\max}Br_l\right) \\ & \text{s.t. } \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1} \leq \theta < 1. \end{aligned} \tag{23}$$

Apparently, G_1 is a decreasing function of θ, thus it is easy to derive the optimal solution as $\theta_1^\star = \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}$, and the corresponding maximum value of the objective function is $\frac{\ln(P_{S,\max}A+1)}{\ln(P_{S,\max}A+1)+\ln(P_{R,\max}B+1)}\left(\log_2\left(1 + P_{R,\max}B\right) - \log_2\left(1 + P_{R,\max}Br_l\right)\right)$.

Otherwise, if $\theta \leq \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}$ or equivalently $P_{S,\max} \leq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$, the objective function in J_3 is reduced as $\theta\log_2\left(1 + P_{S,\max}A\right) - (1-\theta)\log_2\left(1 + \left((1 + P_{S,\max}A)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right)$. Therefore, J_3 is equivalent to

$$G_2 :\ \max_{\theta}\ R_3(\theta) \tag{24}$$

$$\text{s.t. } \theta \leq \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}, \tag{25}$$

where $R_3(\theta) = \theta\log_2\left(1 + P_{S,\max}A\right) - (1-\theta)\log_2\left(1 + \left((1 + P_{S,\max}A)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right)$. Checking the convexity of $R_3(\theta)$, we have the following theorem:

Lemma 1: The objective function of G_2, $R_3(\theta)$, is a concave function with respect to θ, when $\theta \leq \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}$.

Proof: Please refer to Appendix D. ■

According to the Lemma 1, G_2 is a convex optimization problem, such that it can be solved by the Lagrange multiplier method. Therefore, we first construct the Lagrange dual function as follows

$$\begin{aligned} \mathcal{L}(\theta, \mu) = \theta W &\log_2\left(1 + P_{S,\max}A\right) \\ & - (1-\theta)W\log_2\left(1 + \left((1 + P_{S,\max}A)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right) \\ & - \mu\left(\theta - \frac{1}{\frac{\ln(P_{S,\max}A+1)}{\ln(P_{R,\max}B+1)}+1}\right), \end{aligned} \tag{26}$$

where $\mu \geq 0$ is the Lagrange multiplier associated to the constraint (25). Hence, the dual problem of G_2 is given by

$$\min_{\mu}\max_{\theta} \mathcal{L}(\theta, \mu). \tag{27}$$

For a given μ, the optimal θ can be derived by solving the following Karush-Kuhn-Tucker (KKT) condition [43]:

$$\begin{aligned} \frac{\partial \mathcal{L}(\theta, \mu)}{\partial \theta} &= \frac{\partial R_3(\theta)}{\partial \theta} - \mu \\ &= 0. \end{aligned} \tag{28}$$

Furthermore, for a given θ, μ can be updated iteratively by the gradient method, which is given by

$$\mu(n+1) = \left[\mu(n) - \triangle_\mu\left(\frac{1}{\frac{\lg(P_{S,\max}A+1)}{\lg(P_{R,\max}B+1)}+1} - \theta\right)\right]^+, \tag{29}$$

where n is an iteration index, $\triangle_\mu$ is a positive iteration step size, and $[a]^+$ denotes the operation $\max(a, 0)$. Through iteration, it is possible to get the optimal solution $\theta_2^\star$. Note that $\theta_1^\star$ is in the feasible set of G_2, such that $\theta^\star = \theta_2^\star$ is the optimal solution of the optimization problem J_3.

In summary, we propose an iteration algorithm as follows to jointly allocate source transmit power, relay transmit power, and time ratio for the considered DF M-MIMO secure relaying system:

Algorithm 1 Joint Power and Time Allocation Algorithm

```
1) Initialize the system parameters $\alpha_{S,R}$, $\alpha_{R,D}$, $\alpha_{R,E}$, $P_{S,\max}$, $P_{R,\max}$, $\varepsilon$, $N_R$, $\rho$, and given a maximum tolerance $\delta$ and a positive iteration step $\triangle_\mu$. Let $n = 1$, $\mu = 0$, and $\theta(0) = 0.5$.
2) Solve equation (28) for achieving $\theta(n)$.
3) Update $\mu(n)$ according to equation (29).
4) If $|R_3(\theta(n)) - R_3(\theta(n-1))| < \delta$, then return $\theta^\star = \theta(n)$.
   Otherwise, let $n = n + 1$ and go to 2).
5) Compute $P_S^\star = \min\left(P_{S,\max}, \frac{(P_{R,\max}B+1)^{\frac{1-\theta^\star}{\theta^\star}}-1}{A}\right)$, and then
   get $P_R^\star = \min\left(\frac{(1+P_S^\star A)^{\frac{\theta^\star}{1-\theta^\star}}-1}{B}, P_{R,\max}\right)$.
```

Remark: Note that the solutions of these three variables P_S, P_R, and θ are coupled with each other. Thus, the proposed joint power and time allocation scheme can effectively improve the secrecy outage capacity compared to fixed resource allocation and separated resource allocation schemes.

IV. Simulation Results

To examine the effectiveness of the proposed joint power and time allocation scheme for a DF M-MIMO secure relaying system, we present several simulation results in the following scenario: we set $N_R = 100$, $\rho = 0.9$, $\varepsilon = 0.05$, and $P_{S,\max} = P_{R,\max} = 10$ dB, unless further specified. Additionally, for the sake of calculational simplicity, we normalize the path loss as $\alpha_{S,R} = 1$, and use $\alpha_{R,D}$ and $\alpha_{R,E}$ to denote the relative path loss. For instance, $\alpha_{R,E} > \alpha_{R,D}$ means that the eavesdropper is closer to the relay than the legitimate destination. Note that all simulation results are obtained through Monte-Carlo simulations by averaging over 10000 channel realizations.

In simulations, we use JPTA to denote the proposed joint power and time allocation scheme. Moreover, we compare the performance of the proposed scheme with the following baseline schemes: optimal power and time allocation scheme (OPTA), degraded power and time allocation scheme (DPTA), power allocation scheme with fixed time (PAFT), time allocation scheme with fixed power (TAFP), and fixed power and time allocation scheme (FPTA). Specifically, OPTA optimally allocates transmit powers and time ratio through a three-dimensional exhaustive search, DPTA jointly optimizes source transmit power and time ratio with a fixed relay transmit power or relay transmit power and time ratio with a fixed source transmit power by maximizing the secrecy outage capacity. PAFT jointly optimizes source and relay transmit powers by maximizing the secrecy outage capacity with a fixed time ratio, TAFP optimizes the time ratio with fixed source and relay transmit powers, and FPTA adopts fixed source transmit power, relay transmit power and time ratio regardless of the system parameters.

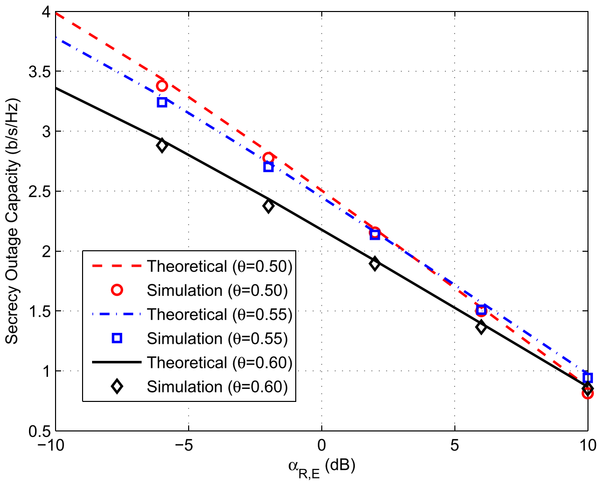


Fig. 2. Comparison of theoretical and simulation results with different values of θ.

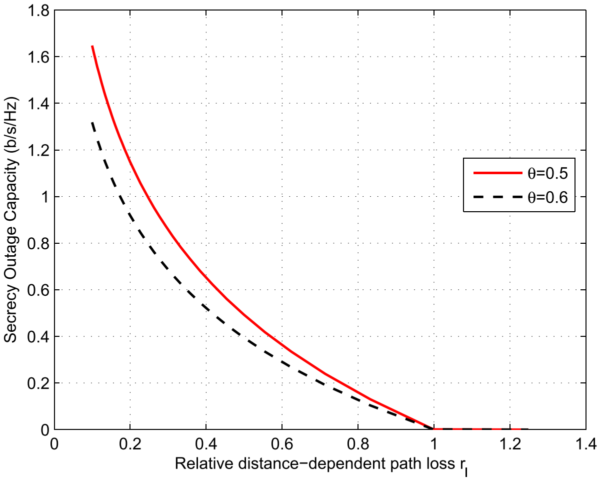


Fig. 3. The effect of relative distance-dependent path loss r_l.

First, we verify the accuracy of the derived theoretical expression of secrecy outage capacity with $P_S = P_R = 10$ dB, and $\alpha_{R,D} = 1.5$. As seen in Fig. 2, the theoretical results are well consistent with the simulations in the whole $\alpha_{R,E}$ region with different values of θ, which proves the accuracy of the derived approximation in Theorem 1. For a given θ, as $\alpha_{R,E}$ increases, the secrecy outage capacity decreases accordingly. This is because the interception ability of the eavesdropper enhances when the distance between the eavesdropper and the relay becomes small. Additionally, it is found from Fig. 2 that the curve with $\theta = 0.50$ is above the others in the small $\alpha_{R,E}$ region, while in the large θ region, the curve with $\theta = 0.55$ is above the others. Thus, it is necessary to allocate the time resource between the two hops for maximizing the secrecy outage capacity.

Second, we check the effect of relative distance-dependent path loss r_l on the secrecy outage capacity with $P_S = P_R = 10$ dB, and $\alpha_{R,D} = 1.5$. As claimed in the Proposition 1, only when $0 < r_l < 1$, the secrecy outage capacity is positive, c.f. Fig. 3. Note that all secrecy outage capacities with different values of θ become zero from the

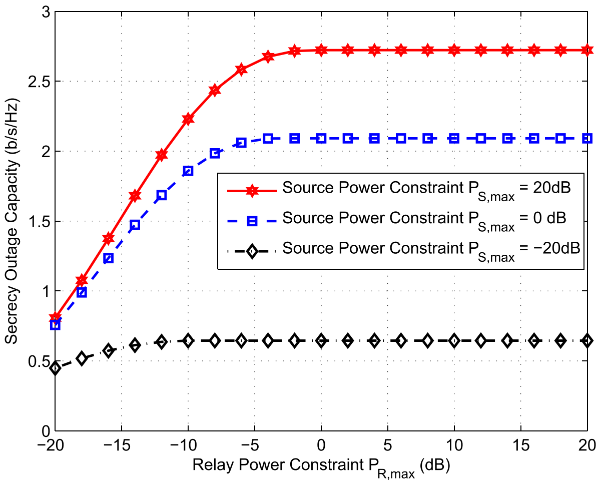


Fig. 4. The impact of source and power transmit power constraints on secrecy outage capacity for JPTA.

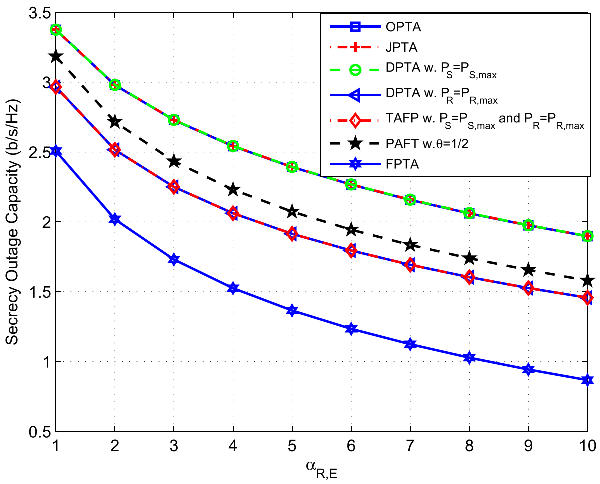


Fig. 5. Performance comparison of different resource allocation schemes.

point of $r_l = 1$ simultaneously, since the condition for positive secrecy outage capacity is independent of θ. However, once r_l satisfies the condition for positive secrecy outage capacity, namely $0 < r_l < 1$, the positive secrecy outage capacity is a function of θ.

Third, we show the impact of source and relay transmit power constraints on the proposed JPTA with $\alpha_{R,E} = 1.5$. As seen in Fig. 4, as $P_{R,\max}$ increases, the secrecy outage capacity first improves rapidly, and then saturates. This is because secrecy outage capacity is an increasing function of $P_{R,\max}$ in the region of small $P_{R,\max}$ or equivalently when $P_{R,\max} < \frac{(1+P_S A)^{\frac{\theta}{1-\theta}}-1}{B}$ according to Theorem 2. It is found that the saturated secrecy outage capacity is independent of $P_{R,\max}$ and increases with $P_{S,\max}$, which matches with the result in Proposition 4. Moreover, the performance gain achieved by increasing $P_{S,\max}$ from 0 dB to 20 dB is obviously smaller than that by increasing $P_{S,\max}$ from -20 dB to 0 dB, since the secrecy outage capacity is saturated as $P_{S,\max}$ increases, as predicted in Proposition 3.

Next, we compare the performances of the proposed scheme JPTA and some baseline schemes, including OPTA, DPTA with $P_S = P_{S,\max}$, DPTA with $P_R = P_{R,\max}$, PAFT with $\theta = 0.5$, TAFP with $P_S = P_{S,\max}$ and $P_R = P_{R,\max}$, and FPTA with $P_S = P_{S,\max}$, $P_R = P_{R,\max}$ and $\theta = 0.5$. In this study, we set $\alpha_{R,D} = 3$. As depicted in Fig. 5, JPTA always achieves the same performance as OPTA, but JPTA has a significantly lower computational complexity. Interestingly, it is found that DPTA with $P_S = P_{S,\max}$ also has the same performance as JPTA. This is because $P_{S,\max}$ is always the optimal transmit power at the source according to the proof of Theorem 3. Thus, it is likely to achieve the optimal performance with a low complexity by using DPTA with $P_S = P_{S,\max}$. However, JPTA has a higher energy efficiency, since it may consume a lower power. Due to the same reason, DPTA with $P_R = P_{R,\max}$ is equivalent to TAFP with $P_S = P_{S,\max}$ and $P_R = P_{R,\max}$. It is also observed that FPTA has the worst performance, since it distributes power and time resources regardless of channel conditions and system parameters. In particular, compared with FPTA, JPTA achieves more performance gain as $\alpha_{R,E}$ increases, which proves that JPTA has the capability of anti-eavesdropping of short distance.

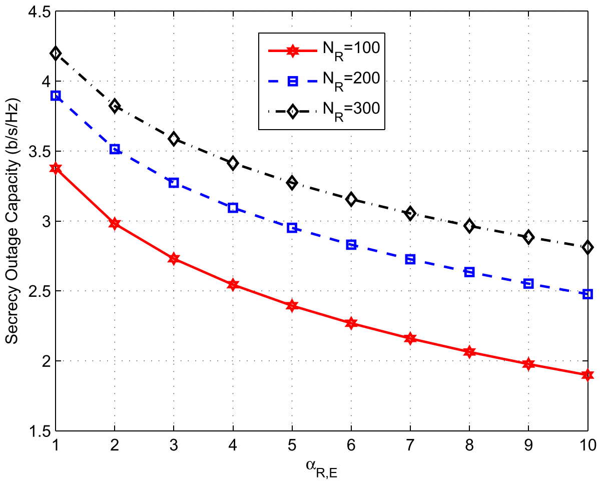


Fig. 6. Performance comparison of different numbers of relay antennas.

Finally, we examine the impact of the number of antennas at the relay on the secrecy outage capacity of the proposed scheme JPTA with $\alpha_{R,D} = 3$. As shown in Fig. 6, with the increase of $\alpha_{R,E}$, all the secrecy outage capacities with different numbers of relay antennas decrease. However, for a given $\alpha_{R,E}$, as N_R increases, the secrecy outage capacity improves significantly. Hence, even in the case of short-distance interception, we can improve the performance to satisfy various quality of service (QoS) requirements by simply adding relay antennas, which is a main advantage of M-MIMO relaying systems.

V. Conclusion

This paper provided a comprehensive performance analysis and optimization for DF M-MIMO secure relaying systems taking into account no instantaneous eavesdropper CSI and imperfect instantaneous legitimate CSI. Firstly, we derived a closed-form expression of secrecy outage capacity, revealed the condition for positive secrecy outage capacity, and presented the requirement of the minimum number of relay antennas. Then, we proposed a joint power and time allocation scheme for maximizing the secrecy outage capacity. Afterwards, some degraded resource allocation schemes were given, which may achieve the optimal performance with a low computational complexity but a higher power consumption. Moreover, we found that the secrecy outage capacity would be saturated if maximum available source or relay power is sufficiently large.

Appendix A
Proof of Theorem 1

According to equation (12), the legitimate channel capacity can be computed as

$$\begin{aligned}
C_D &= \min(C_{S,R}, C_{R,D})\\
&= \min\Bigg(\theta\log_2(1+P_S\alpha_{S,R}\|\mathbf{h}_{S,R}\|^2, (1-\theta)\\
&\qquad \times\log_2\Bigg(1+P_R\alpha_{R,D}\Bigg|\mathbf{h}_{R,D}^H\frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}\Bigg|^2\Bigg)\Bigg) &(30)\\
&= \min\Bigg(\theta\log_2(1+P_S\alpha_{S,R}\|\mathbf{h}_{S,R}\|^2, (1-\theta)\\
&\qquad \times\log_2\Bigg(1+P_R\alpha_{R,D}\\
&\qquad \times\Bigg|(\sqrt{\rho}\hat{\mathbf{h}}_{R,D}^H+\sqrt{1-\rho}\mathbf{e}^H)\frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}\Bigg|^2\Bigg)\Bigg) &(31)\\
&= \min\Bigg(\theta\log_2(1+P_S\alpha_{S,R}\|\mathbf{h}_{S,R}\|^2, (1-\theta)\\
&\qquad \times\log_2\Bigg(1+P_R\alpha_{R,D}(\rho\|\hat{\mathbf{h}}_{R,D}\|^2\\
&\qquad +2\sqrt{(1-\rho)\rho}\mathcal{R}(\mathbf{e}^H\hat{\mathbf{h}}_{R,D})+(1-\rho)\frac{\|\mathbf{e}\hat{\mathbf{h}}_{R,D}^H\|^2}{\|\hat{\mathbf{h}}_{R,D}\|^2})\Bigg)\Bigg)\\
&\approx \min\Bigg(\theta\log_2(1+P_S\alpha_{S,R}\|\mathbf{h}_{S,R}\|^2), (1-\theta)\\
&\qquad \times\log_2(1+P_R\alpha_{R,D}\rho\|\hat{\mathbf{h}}_{R,D}\|^2)\Bigg) &(32)\\
&\approx \min\big(\theta\log_2(1+P_S\alpha_{S,R}N_R), (1-\theta)\\
&\qquad \times\log_2(1+P_R\alpha_{R,D}\rho N_R)\big), &(33)
\end{aligned}$$

where $\mathcal{R}(x)$ denotes the real part of x. $\mathbf{h}_{R,D}$ is replaced with $\sqrt{\rho}\hat{\mathbf{h}}_{R,D}+\sqrt{1-\rho}\mathbf{e}$ in (31). Equation (32) follows from the fact that $\rho\|\hat{\mathbf{h}}_{R,D}\|^2$ scales with the order $\mathcal{O}(\rho N_R)$ as $N_R\to\infty$ while $2\sqrt{\rho(1-\rho)}\mathcal{R}(\mathbf{e}^H\hat{\mathbf{h}}_{R,D})+(1-\rho)\frac{\|\mathbf{e}\hat{\mathbf{h}}_{R,D}^H\|^2}{\|\hat{\mathbf{h}}_{R,D}\|^2}$ scales with the order $\mathcal{O}(\sqrt{N_R})$, which is negligible. Equation (33) holds true because of $\lim\limits_{N_R\to\infty}\frac{\|\hat{\mathbf{h}}_{R,D}\|^2}{N_R}=1$ and $\lim\limits_{N_R\to\infty}\frac{\|\mathbf{h}_{S,R}\|^2}{N_R}=1$ according to Property A of very long random vectors in (7).

Similarly, for the eavesdropper, its channel capacity is given by

$$\begin{aligned}
C_E &= \min(C_{S,R}, C_{R,E})\\
&= \min\Bigg(\theta\log_2(1+P_S\alpha_{S,R}N_R),\\
&\qquad (1-\theta)\log_2\Bigg(1+P_R\alpha_{R,E}\Bigg|\mathbf{h}_{R,E}^H\frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}\Bigg|^2\Bigg)\Bigg).
\end{aligned} \qquad (34)$$

Thus, according to the definition in (6), the secrecy outage probability ε with respect to a secrecy outage capacity C_{SOC} can be computed as follows:

$$\begin{aligned}
\varepsilon &= P_r(C_{soc} > C_D - C_E)\\
&= P_r\big(\min(C_{S,R}, C_{R,E}) > C_D - R_{soc}\big)\\
&= P_r(C_{S,R} < C_{R,E})P_r(C_{S,R} > C_D - R_{soc})\\
&\quad + P_r(C_{S,R} \geq C_{R,E})P_r(C_{R,E} > C_D - R_{soc})\\
&= P_r\Bigg((1+P_S\alpha_{S,R}N_R)^{\frac{\theta}{1-\theta}}-1 < P_R\alpha_{R,E}\Bigg|\mathbf{h}_{R,E}^H\frac{\hat{\mathbf{h}}_{R,D}}{\|\mathbf{h}_{R,D}\|}\Bigg|^2\Bigg)\\
&\quad + P_r\Bigg((1+P_S\alpha_{S,R}N_R)^{\frac{\theta}{1-\theta}}-1 \geq P_R\alpha_{R,E}\Bigg|\mathbf{h}_{R,E}^H\frac{\hat{\mathbf{h}}_{R,D}}{\|\mathbf{h}_{R,D}\|}\Bigg|^2\Bigg)\\
&\quad \times P_r\Bigg(P_R\alpha_{R,E}\Bigg|\mathbf{h}_{R,E}^H\frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}\Bigg|^2 > 2^{(C_D-R_{soc})/(1-\theta)}-1\Bigg)\\
&= \exp\Bigg(-\frac{(1+P_S\alpha_{S,R}N_R)^{\frac{\theta}{1-\theta}}-1}{P_R\alpha_{R,E}}\Bigg)\\
&\quad + \Bigg(1-\exp\Bigg(-\frac{(1+P_S\alpha_{S,R}N_R)^{\frac{\theta}{1-\theta}}-1}{P_R\alpha_{R,E}}\Bigg)\Bigg)\\
&\quad \times\exp\Bigg(-\frac{2^{(C_D-R_{soc})/(1-\theta)}-1}{P_R\alpha_{R,E}}\Bigg) &(35)\\
&\approx \exp\Bigg(-\frac{2^{(C_D-R_{soc})/(1-\theta)}-1}{P_R\alpha_{R,E}}\Bigg), &(36)
\end{aligned}$$

where equation (35) follows the fact that $\Big|\mathbf{h}_{R,E}^H\frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}\Big|^2$ is χ^2 distributed with 2 degrees of freedom according to Property B of very long random vectors in (8), and equation (36) holds true since the term $\exp\Bigg(-\frac{(1+P_S\alpha_{S,R}N_R)^{\frac{\theta}{1-\theta}}-1}{P_R\alpha_{R,E}}\Bigg)$ approaches zero if N_R is sufficiently large. Theorem 1 follows immediately after equation (36).

Appendix B
Proof of Proposition 1 and Theorem 2

To find the condition for achieving a positive secrecy outage capacity, we check the secrecy outage capacity in two cases respectively.

First, when $P_R \geq \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}$, the secrecy outage capacity is reduced as

$$\begin{aligned}
R_{soc}(P_R, P_S, \theta) &= \theta\log_2(1+P_SA)\\
&\quad -(1-\theta)\log_2(1+P_RBr_l), &(37)
\end{aligned}$$

Apparently, (37) is a monotonously decreasing function of P_R, and thus the maximum secrecy outage capacity is achieved when $P_R = \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}$.

Then, in the case of $P_R \leq \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}$, the secrecy outage capacity is equivalent to

$$\begin{aligned}
R_{soc}(P_R, P_S, \theta) &= (1-\theta)\log_2(1+P_RA)\\
&\quad -(1-\theta)\log_2(1+P_RBr_l)\\
&= (1-\theta)\log_2\Bigg(1+\frac{1-r_l}{\frac{1}{P_RB}+r_l}\Bigg). &(38)
\end{aligned}$$

If $r_l \geq 1$, $C_{soc}(P_R, P_S, \theta)$ in (38) is a monotonously decreasing function of P_R when $P_R \leq \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}$. Considering the monotonicity and continuity in the whole P_R region, the maximum secrecy outage capacity is 0, which is achieved at the point $P_R = 0$. Thus, in order to guarantee R_{soc} positive, r_l must not be equal to or greater than 1. Otherwise, if $0 < r_l < 1$, $R_{soc}(P_R, P_S, \theta)$ in (38) is a monotonously increasing function of P_R when $P_R \leq \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}$. Therefore, the corresponding maximum secrecy outage capacity is obtained at the point $P_R = \frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}$ and is positive provenly. Hence, we get the Proposition 1.

In summary, the secrecy outage capacity is an increasing function of P_R if the positive condition is satisfied, namely $0 < r_l < 1$. Considering the constraint on P_R, the actual optimal power at the relay is $P_R^\star = \min\left(\frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}\right)$, where $P_{R,\max}$ is the maximum available transmit power at the relay. Substituting $P_R^\star$ into $R_{soc}(P_R, P_S, \theta)$, we get the Theorem 2.

Appendix C
Proof of Theorem 3

We first examine the monotonicity of the objective function in H_2. It is found that when $P_S \geq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$, namely $\frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B} \geq P_{R,\max}$, the objective function is equivalent to

$$\begin{aligned} R_1(P_S, \theta) = (1-\theta)\log_2\left(1 + P_{R,\max}B\right) \\ - (1-\theta)\log_2\left(1 + P_{R,\max}Br_l\right), \quad (39) \end{aligned}$$

where (39) holds true since the term $\min\left(\frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B}, P_{R,\max}B\right)$ in $R_1(P_S, \theta)$ is equal to $P_{R,\max}$ in the case of $\frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B} \geq P_{R,\max}$. It is worth pointing out that $R_1(P_S, \theta)$ in (39) is a constant independent of P_S.

Otherwise, if $P_S \leq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$ or $\frac{(1+P_SA)^{\frac{\theta}{1-\theta}}-1}{B} \leq P_{R,\max}$, the objective function is reduced as

$$\begin{aligned} R_1(P_S, \theta) &= (1-\theta)\log_2\left((1+P_SA)^{\frac{\theta}{1-\theta}}\right) \\ &\quad - (1-\theta)\log_2\left(1 + \left((1+P_SA)^{\frac{\theta}{1-\theta}} - 1\right)r_l\right) \\ &= (1-\theta)\log_2\left(1 - \frac{1-r_l}{(1+P_SA)^{\frac{\theta}{1-\theta}}r_l^2 + (1-r_l)r_l}\right). \end{aligned} \quad (40)$$

Note that $R_1(P_S, \theta)$ in (40) monotonously increases as P_S enlarges. In this context, $R_1(P_S, \theta)$ in (40) attains its maximum value at the point of $P_S = \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$.

In conclusion, $R_1(P_S, \theta)$ is a monotonously increasing function of P_S when $P_S \leq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$, and is a constant independent of P_S when $P_S \geq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$. Considering the constraint on the transmit power at the source, if $P_{S,\max} \leq \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}$, the optimal source transmit power is $P_{S,\max}$ or $\min\left(P_{S,\max}, \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}\right)$. Otherwise, the optimal source transmit power is an arbitrary value in $\left[\frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}, P_{S,\max}\right]$. In the sense of minimizing the energy consumption, it is better to take the value of $\min\left(\frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}, P_{S,\max}\right)$. Thus, the optimal source transmit power from the perspectives of both maximizing the secrecy outage capacity and minimizing the energy consumption is given by $P_S^\star = \min\left(P_{S,\max}, \frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}\right)$.

Since $R_1(P_S, \theta)$ is an increasing function of P_S, the maximum secrecy outage capacity in the case of $P_S = P_S^\star$ is given by $R_2(\theta) = \min\left(R_1\left(P_{S,\max}, \theta\right), R_1\left(\frac{(P_{R,\max}B+1)^{\frac{1-\theta}{\theta}}-1}{A}, \theta\right)\right)$. Thus, we get the Theorem 3.

Appendix D
Proof of Lemma 1

Taking the second derivative of the objective function of G_2, namely $R_3(\theta)$, we have

$$R_3''(\theta) = \frac{r_l(1-r_l)(1+P_{S,\max}A)^{\frac{\theta}{1-\theta}}(\ln(1+P_{S,\max}A))^2}{(\theta-1)^3\left((P_{S,\max}A)^{\frac{\theta}{1-\theta}}r_l + (1-r_l)\right)^2}. \quad (41)$$

Due to the fact of $0 < \theta < 1$ and $0 < r_l < 1$, it is easy to verify $R_3''(\theta) < 0$. Thus, we get the Lemma 1.

References

[1] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[4] Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the secrecy capacity of block fading channels with a hybrid adversary," *IEEE Trans. Inf. Theory*, vol. 61, no. 3, pp. 1325–1343, Mar. 2015.

[5] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Jul. 2006, pp. 356–360.

[6] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr. 2011.

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

[8] X. Chen and R. Yin, "Performance analysis for physical layer security in multi-antenna downlink networks with limited CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 2, no. 5, pp. 503–506, Oct. 2013.

[9] D. W. K. Ng and R. Schober, "Secure and green SWIPT in distributed antenna networks with limited backhaul capacity," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5082–5097, Sep. 2015.

[10] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.

[11] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[12] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part I: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[15] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 4985–4997, Oct. 2011.

[16] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[17] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016, doi: 10.1109/TIFS.2016.2516917.

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

[19] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

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

[21] C. Jeong, I.-M. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[22] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 39, no. 10, pp. 4871–4884, Oct. 2011.

[23] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[24] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[25] X. Zhang, X. Zhou, and R. M. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1802–1814, Nov. 2013.

[26] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "On the security of large scale spectrum sharing networks," in *Proc. IEEE ICC*, Jun. 2015, pp. 4877–4882.

[27] X. Chen and H.-H. Chen, "Physical layer security in multi-cell MISO downlinks with incomplete CSI—A unified secrecy performance analysis," *IEEE Trans. Signal Process.*, vol. 62, no. 23, pp. 6286–6297, Dec. 2014.

[28] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[29] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, 2016. [Online]. Available: http://arxiv.org/abs/1507.00789

[30] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[31] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[32] X. Chen, J. Chen, and T. Liu, "Secure transmission in wireless powered massive MIMO relaying systems: Performance analysis and optimization," *IEEE Trans. Veh. Technol.*, 2015. doi: 10.1109/TVT.2015.2511808.

[33] A. Jindal and R. Bose, "Resource allocation for secure multicarrier AF relay system under total power constraint," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 231–234, Feb. 2015.

[34] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[35] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative networking towards secure communications for CRNs," in *Proc. IEEE WCNC*, Apr. 2013, pp. 1691–1696.

[36] J. Chen, X. Chen, and W. Gerstacker, "Optimal power allocation for a massive MIMO relay aided secure communication," in *Proc. IEEE GLOBECOM*, Dec. 2015, pp. 1–6.

[37] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[38] K. H. Park, T. Wang, and M. S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[39] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

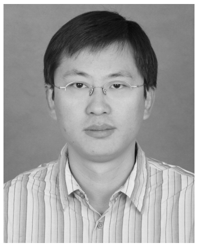
[40] D. S. W. Hui and V. K. N. Lau, "Design and analysis of delay-sensitive cross-layer OFDMA systems with outdated CSIT," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3484–3491, Jul. 2009.

[41] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep. 2013.

[42] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.

[43] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

Jian Chen received the B.S. degree in information engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2013, where he is currently pursuing the M.Sc. degree with the College of Electronic and Information Engineering. His research interests include massive MIMO and wireless physical layer security.



Xiaoming Chen (M'10–SM'14) received the B.Sc. degree from Hohai University, in 2005, the M.Sc. degree from the Nanjing University of Science and Technology, in 2007, and the Ph.D. degree from Zhejiang University, in 2011, all in electronics engineering. He is currently with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China. Since 2015, he has been a Humboldt Resarch Fellow with the Institute for Digital Communications, University of Erlangen-Nürnberg, Erlangen, Germany. His research interests mainly focus on multiple-antenna techniques, wireless security, interference network, and wireless power transfer.

Dr. Chen serves as an Associate Editor for the IEEE ACCESS and an Editor of the IEEE COMMUNICATIONS LETTERS. He was honored as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS in 2015 and the IEEE TRANSACTIONS ON COMMUNICATIONS in 2016.

Wolfgang H. Gerstacker (S'93–M'98–SM'11) received the Dipl.-Ing. degree in electrical engineering, the Dr.-Ing. degree, and the Habilitation degree from the University of Erlangen-Nürnberg, Erlangen, Germany, in 1991, 1998, and 2004, respectively. Since 2002, he has been with the Institute for Digital Communications, University of Erlangen-Nürnberg, where he is currently a Professor.

His research interests are in the broad area of digital communications and statistical signal processing. He has conducted various projects with partners from industry. He was a recipient of several awards, including the Research Award of the German Society for Information Technology in 2001, the EEEfCOM Innovation Award in 2003, the Vodafone Innovation Award in 2004, a best paper award of EURASIP Signal Processing in 2006, and the Mobile Satellite & Positioning Track Paper Award of VTC2011-Spring.

Prof. Gerstacker is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. Furthermore, he is an Area Editor of *Physical Communication* (Elsevier). He was a member of the Editorial Board of the *EURASIP Journal on Wireless Communications and Networking* from 2004 to 2012 and served as a Guest Editor for several special issues of journals. He has served as a member of the Technical Program Committee of various conferences. He was a Technical Program Co-Chair of the IEEE International Black Sea Conference on Communications and Networking in 2014, and a Co-Chair of the Cooperative Communications, Distributed MIMO, and Relaying Track of VTC2013-Fall, and serves as a General Chair of ACM NanoCom in 2016.

Derrick Wing Kwan Ng (S'06–M'12) received the bachelor's (Hons.) and the M.Phil. degree in electronics engineering from The Hong Kong University of Science and Technology (HKUST), in 2006 and 2008, respectively, and the Ph.D. degree from the University of British Columbia (UBC), in 2012. In the summer of 2011 and spring of 2012, he was a Visiting Scholar with the Centre Tecnològic de Telecomunicacions de Catalunya, Hong Kong. He was a Senior Post-Doctoral Fellow with the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg, Germany. He is currently a Lecturer with the University of New South Wales, Sydney, Australia. His research interests include convex and nonconvex optimization, physical layer security, wireless information and power transfer, and green (energy-efficient) wireless communications.

Dr. Ng received the best paper awards at the IEEE International Conference on Computing, Networking and Communications in 2016, the IEEE Wireless Communications and Networking Conference (WCNC) in 2012, the IEEE Global Telecommunication Conference (Globecom) in 2011, and the IEEE Third International Conference on Communications and Networking in China in 2008. He also received the IEEE Student Travel Grants for attending the IEEE WCNC 2010, the IEEE International Conference on Communications (ICC) 2011, and the IEEE Globecom 2011. He was a recipient of the 2009 Four Year Doctoral Fellowship from the UBC, Sumida, and Ichiro Yawata Foundation Scholarship in 2008, and the R&D Excellence Scholarship from the Center for Wireless Information Technology in HKUST in 2006. He has served as an Editorial Assistant to the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS since 2012. He is currently an Editor of the IEEE COMMUNICATIONS LETTERS. He was a Co-Chair of the Wireless Access Track of 2014 IEEE 80th Vehicular Technology Conference. He has been a TPC Member of various conferences, including the Globecom, WCNC, ICC, VTC, and PIMRC. He was honored as an Exemplary Reviewer of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015, the top reviewer of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2014, and an Exemplary Reviewer of the IEEE WIRELESS COMMUNICATIONS LETTERS for 2012, 2014, and 2015.