

Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF?

Xiaoming Chen, *Senior Member, IEEE*, Lei Lei, *Member, IEEE*, Huazi Zhang, *Member, IEEE*, and Chau Yuen, *Senior Member, IEEE*

Abstract—In this paper, we consider a large scale multiple input multiple output (LS-MIMO) relaying system, where an information source sends the message to its intended destination aided by an LS-MIMO relay, while a passive eavesdropper tries to intercept the information forwarded by the relay. The advantage of a large scale antenna array is exploited to improve spectral efficiency and enhance wireless security. In particular, the challenging issue incurred by short-distance interception is well addressed. Under very practical assumptions, i.e., no eavesdropper channel state information (CSI) and imperfect legitimate CSI at the relay, this paper gives a thorough secrecy performance analysis and comparison of two classic relaying techniques, i.e., amplify-and-forward (AF) and decode-and-forward (DF). Furthermore, asymptotical analysis is carried out to provide clear insights on the secrecy performance for such an LS-MIMO relaying system. We show that under large transmit powers, AF is a better choice than DF from the perspectives of both secrecy performance and implementation complexity, and prove that there exists an optimal transmit power at medium regime that maximizes the secrecy outage capacity.

Index Terms—Physical layer security, LS-MIMO, AF, DF, performance analysis.

I. INTRODUCTION

THE broadcast nature of the wireless channel gives rise to many wireless security problems. Traditionally, wireless security is guaranteed through high layer encryption. With the development of interception techniques, encryption becomes more complex, leading to high computation burden. Thanks to physical layer security measures enlightened by information theory, we may exploit wireless channel characteristics, i.e., fading and noise, to guarantee secure communications [1]–[4] even without encryption. Thus, the heavy dependence on complex higher-layer encryption may be dispensed, leaving more computation resources for communications.

Manuscript received August 7, 2014; revised March 2, 2015; accepted May 10, 2015. Date of publication May 14, 2015; date of current version September 7, 2015. This work was supported by the Natural Science Foundation of China (No. 61301102, 61401388), the Natural Science Foundation of Jiangsu Province (No. BK20130820, BK2014041565), the Fundamental Research Funds for the Central Universities (No. NJ20150014) and the iTrust. The associate editor coordinating the review of this paper and approving it for publication was N. C. Sagias.

X. Chen and L. Lei are with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: chenxiaoming@nuaa.edu.cn; leilei@nuaa.edu.cn).

H. Zhang is with the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: tom.zju@gmail.com).

C. Yuen is with the Singapore University of Technology and Design, Singapore 487372 (e-mail: yuenchau@sutd.edu.sg).

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/TWC.2015.2433291

A. Related Works

The performance of physical layer security is usually measured by secrecy rate, namely the capacity difference between the legitimate channel (from the information source to the destination) and the eavesdropper channel (from the information source to the eavesdropper) [5]–[7]. The introduction of relay into physical layer security can improve the legitimate channel capacity through cooperative diversity, and thus enhances transmission security [8]–[12]. Some feasible relaying schemes and their performances were discussed in [13]. Similar to the traditional relaying systems, amplify-and-forward (AF) [14] and decode-and-forward (DF) [15] are two commonly used relaying schemes in secure relaying systems.

Intuitively, the position of relay has a great impact on the secrecy performance. Some optimization schemes for relay position were presented from the perspective of minimizing the interception probability in [16]. If there are multiple relays, higher performance gains can be obtained by relay selection or cooperation. In [17], an optimal relay selection scheme was proposed to suppress the interception probability by exploiting selective gain in multiple relay systems. Additionally, multiple relay cooperative beamforming combined with jamming was also adopted to maximize the secrecy rate in [18] and [19]. Considering the CSI sharing overhead, an iterative distributed precoding was proposed in [20] to enhance the received signal power at the destination node and to mitigate the signal leakage to the eavesdropper simultaneously.

In fact, if the relay is equipped with multiple antennas, it is likely to enhance the desired signal power and impair the eavesdropper signal quality simultaneously, and thus increase the secrecy rate. In this context, multi-antenna relays received considerable attention, and more effective relaying schemes were proposed to optimize the secrecy rate [21], [22]. Linear precoding schemes were investigated in a MIMO relay network assuming global CSI [23]. Moreover, two precoding schemes based on the idea of information leakage neutralization were proposed to enhance wireless security over the multi-antenna non-regenerative relay assisted multi-carrier interference channel [24]. However, the quality and availability of the legitimate and eavesdropper CSI are two research challenges. Due to the fact that there is a feedback delay or error for legitimate channel and the eavesdroppers are usually well hidden, the relay may only have imperfect legitimate CSI and no eavesdropper CSI. Therefore, it is impossible to realize absolutely secure communications over the fading channel. To this end, the conception of secrecy outage capacity was adopted to guarantee secure communications with a high probability [25], [26].

However, without the eavesdropper CSI, a challenging problem rises when the eavesdropper is close to the transmitter. The so-called *short-distance interception* scenario is not yet fully addressed in literature. Even with a multi-antenna relay, the secrecy outage capacity is too small to fulfill the requirement on quality of service (QoS), due to the relatively high quality of interception signal. Recently, it is found that large-scale MIMO (LS-MIMO) systems can significantly improve the transmission performance by utilizing its enormous array gain [27], [28]. Through deploying hundreds of or even more antennas, the spatial resolution of the transmit beam can be very high even with just simple linear precoding methods, e.g., maximum ratio transmission (MRT). Then, the information leakage to the eavesdropper can be quite small, and is negligible if the number of antennas approaches infinity [29]–[31]. In [32], the achievable secrecy sum-rate based on regularized channel inversion precoding was derived for large-scale MISO broadcast channels with confidential message. Furthermore, large-scale MIMO technology together with artificial noise (AN) was applied in multicell systems to enhanced wireless security [33]. It was shown that even with a low complexity random AN shaping scheme, it was possible to provide a favorite performance.

Again, the CSI at the LS-MIMO transmitter has a great impact on the secrecy performance. In general, the CSI in LS-MIMO is obtained by making use of channel reciprocity of time division duplex (TDD) systems. Due to duplex delay or pilot contamination, the estimated CSI may be imperfect, resulting in inevitable performance loss [34]. To the best of our knowledge, the research on physical layer security based on LS-MIMO relaying techniques is just beginning, especially in the case of imperfect CSI. In [35], we analyzed the secrecy performance of large-scale MIMO relay in two-hop secure communications with imperfect CSI, and derived closed-form expressions of secrecy outage capacity for amplify-and-forward (AF) and decode-and-forward (DF) relaying protocols, respectively.

B. Main Contributions

In this paper, we focus on performance analysis and comparison of two classic relaying schemes, including amplify-and-forward (AF) and the decode-and-forward (DF), for physical layer security in an LS-MIMO relaying system with imperfect CSI. The contributions of this paper are summarized as follows:

- 1) We are the first to introduce LS-MIMO techniques into a relaying system, and solve the challenging problem of short-distance (relay and eavesdropper) interception.
- 2) We derive explicit expressions of the secrecy outage capacity for both AF and DF relaying schemes, and compare their performance under different conditions, e.g., the CSI accuracy, transmit powers at the source and the relay, and interception distance.
- 3) We analyze the asymptotic behavior of secrecy outage capacity under large transmit power, and obtain some insights on the secrecy performance as follows:
 - a) As the transmit power at the source approaches infinity, the secrecy outage capacity for both AF and DF relaying schemes is upper bounded by the same

performance ceiling. The bound is invariant with respect to transmit powers, but declines as the interception distance and the outage probability decrease, and increases as the number of antennas at the relay adds.

- b) As the transmit power at the relay approaches infinity, the secrecy outage capacity of both AF and DF relaying schemes tends to zero, but the interception event occurs with probability 0 and 1, respectively.
- c) Under large transmit powers, AF is a better choice than DF from the perspectives of both secrecy performance and implementation complexity.
- d) Both too low and too high relay transmit powers at the relay result in poor secrecy performance. There exists an optimal transmit power at medium regime that maximizes the secrecy outage capacity.

C. Paper Organization

The rest of this paper is organized as follows. We first give an overview and system model of the LS-MIMO relaying system employing physical layer security in Section II, and then derive the secrecy outage capacities for AF and DF relaying schemes with imperfect CSI, and compare their performance in Section III. In Section IV, we perform asymptotic analysis to obtain several insights on the secrecy performance. We then present some simulation results to validate the effectiveness of the proposed scheme in V. Finally, we conclude the whole paper in Section VI.

Notations: We use bold upper (lower) letters to denote matrices (column vectors), $(\cdot)^H$ to denote conjugate transpose, $E[\cdot]$ to denote expectation, $\|\cdot\|$ to denote the L_2 norm of a vector, $|\cdot|$ to denote the absolute value, and $(a)^+$ to denote $\max(a, 0)$. The acronym i.i.d. means “independent and identically distributed”, pdf means “probability density function” and cdf means “cumulative distribution function.”

II. SYSTEM MODEL

We consider a time division duplex (TDD) LS-MIMO relaying system, including one source, one destination equipped with a single antenna each and one relay deploying N_R antennas in presence of a passive eavesdropper, as shown in Fig. 1. It is worth pointing out that N_R is usually quite large in such an LS-MIMO relaying system, i.e., $N_R = 100$ or greater. In addition, the eavesdropper is usually a legitimate destination or pretends to be a legitimate destination [36], so we consider the eavesdropper is equipped with one antenna, like the destination. The system works in a half-duplex mode, so the information transmission from the source to the destination with the aid of the LS-MIMO relay requires two time slots. Specifically, during the first time slot, the source transmits the signal to the relay, and then the relay forwards the post-processing signal to the destination within the second time slot. Note that the direct link from the source to the destination is unavailable due to a long distance. Meanwhile, the eavesdropper monitors the transmission from the relay to the destination, and tries to intercept the signal. In practice, the relay is far away from the source, so it is difficult for the eavesdropper to overhear both the source

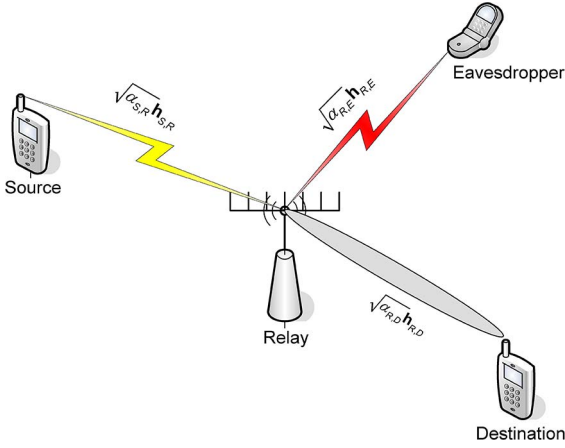


Fig. 1. An overview of the large-scale MIMO relaying system employing physical layer security.

and the relay. Following previous related literatures [14] and [17], we also assume that the eavesdropper only monitors the relay, since it thought that the signal is from the relay directly.

We use $\sqrt{\alpha_{i,j}}\mathbf{h}_{i,j}$ to denote the channel from i to j , where $i \in \{S, R\}$, $j \in \{R, D, E\}$ with S, R, D and E representing the source, the relay, the destination and the eavesdropper, respectively. $\alpha_{i,j}$ is the distance-dependent path loss and $\mathbf{h}_{i,j}$ is the channel small scale fading. In this paper, we model $\mathbf{h}_{i,j}$ as Gaussian distribution with zero mean and covariance matrix \mathbf{I}_{N_R} . $\alpha_{i,j}$ remains constant during a relatively long period and $\mathbf{h}_{i,j}$ fades independently slot by slot. Thus, the received signal at the relay in the first time slot can be expressed as

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

where s is the normalized Gaussian distributed transmit signal, P_S is the transmit power at the source, \mathbf{n}_R is the additive Gaussian white noise with zero mean and covariance matrix \mathbf{I}_{N_R} at the relay. Through post-processing to \mathbf{y}_R according to the CSI $\mathbf{h}_{S,R}$ and $\mathbf{h}_{R,D}$, the relay forwards a normalized signal \mathbf{r} to the destination with power P_R , then the received signals at the destination and the eavesdropper are given by

$$y_D = \sqrt{P_R \alpha_{R,D}} \mathbf{h}_{R,D}^H \mathbf{r} + n_D, \quad (2)$$

and

$$y_E = \sqrt{P_R \alpha_{R,E}} \mathbf{h}_{R,E}^H \mathbf{r} + n_E, \quad (3)$$

respectively, where n_D and n_E are the additive Gaussian white noises with zero mean and unit variance at the destination and the eavesdropper.

Assuming the achievable legitimate channel rate and the achievable eavesdropper channel rate are C_D and C_E , from the perspective of information theory, the achievable secrecy rate is given by $C_{SEC} = [C_D - C_E]^+$, where $[x]^+ = \max(x, 0)$ [5]. Since there is no knowledge of the eavesdropper channel at the source and relay, it is impossible to maintain a steady secrecy rate over all realizations of the fading channels. In this paper, we take the secrecy outage capacity C_{SOC} as the performance metric, which is defined as the maximum achievable rate under

the condition that the outage probability of the transmission rate surpasses the secrecy rate is equal to a given value ε , namely

$$P_r(C_{SOC} > C_D - C_E) = \varepsilon. \quad (4)$$

III. SECRECY PERFORMANCE ANALYSIS AND COMPARISON

In this section, we concentrate on secrecy performance analysis and comparison of two commonly used relaying techniques, namely AF and DF, for physical layer security in an LS-MIMO relaying system with imperfect CSI. In what follows, we first derive explicit expressions of the secrecy outage capacity related to a given outage probability for the two relaying techniques, and then compare their performance under different channel conditions.

A. Amplify-and-Forward (AF) Case

In this case, the relay forwards the signal \mathbf{r}^{AF} via multiplying the received signal \mathbf{y}_R by a $N_R \times N_R$ processing matrix \mathbf{F} , namely

$$\mathbf{r}^{AF} = \mathbf{F} \mathbf{y}_R. \quad (5)$$

We assume the relay has full CSI $\mathbf{h}_{S,R}$ through channel estimation, and gets partial CSI $\mathbf{h}_{R,D}$ by making use of channel reciprocity in TDD systems. Due to duplex delay between uplink and downlink, there is a certain degree of mismatch between the estimated CSI $\hat{\mathbf{h}}_{R,D}$ and the real CSI $\mathbf{h}_{R,D}$, whose relation can be expressed as [37]

$$\mathbf{h}_{R,D} = \sqrt{\rho} \hat{\mathbf{h}}_{R,D} + \sqrt{1 - \rho} \mathbf{e}, \quad (6)$$

where \mathbf{e} is the error noise vector with independent and identically distributed (i.i.d.) zero mean and unit variance complex Gaussian entries. ρ , scaling from 0 to 1, is the correlation coefficient between $\hat{\mathbf{h}}_{R,D}$ and $\mathbf{h}_{R,D}$. A large ρ means better CSI accuracy. If $\rho = 1$, the relay has full CSI $\mathbf{h}_{R,D}$. Additionally, due to the hidden property of the eavesdropper, the CSI $\mathbf{h}_{R,E}$ is unavailable. Therefore, \mathbf{F} is designed only based on $\mathbf{h}_{S,R}$ and $\hat{\mathbf{h}}_{R,D}$, but is independent of $\mathbf{h}_{R,E}$. Since maximum ratio combination (MRC) and maximum ratio transmission (MRT) can achieve asymptotically optimal performance in LS-MIMO systems with low complexity [27], [28], we design \mathbf{F} by combining MRC and MRT. Specifically, the received signal \mathbf{y}_R is first combined with an MRC vector $\frac{\mathbf{h}_{S,R}^H}{\|\mathbf{h}_{S,R}\|}$, then normalized by a scaling factor $\frac{1}{\sqrt{P_S \alpha_{S,R} \|\mathbf{h}_{S,R}\|^2 + 1}}$, and finally multiplied by an MRT vector $\frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|}$. In other words, the processing matrix is given by

$$\mathbf{F} = \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \frac{1}{\sqrt{P_S \alpha_{S,R} \|\mathbf{h}_{S,R}\|^2 + 1}} \frac{\mathbf{h}_{S,R}^H}{\|\mathbf{h}_{S,R}\|}. \quad (7)$$

It is assumed that the destination has perfect CSI by channel estimation, thus the received signal and the corresponding

signal-to-noise ratio (SNR) can be expressed as

$$\gamma_D^{AF} = \frac{\sqrt{P_S P_{R\alpha S, R} \alpha_{R, D}} \hat{\mathbf{h}}_{R, D}^H \hat{\mathbf{h}}_{S, R} \mathbf{h}_{S, R}}{\|\hat{\mathbf{h}}_{R, D}\| \sqrt{P_S \alpha_{S, R} \|\mathbf{h}_{S, R}\|^2 + 1} \|\mathbf{h}_{S, R}\|} + \frac{\sqrt{P_R \alpha_{R, D}} \hat{\mathbf{h}}_{R, D}^H \hat{\mathbf{h}}_{S, R} \mathbf{h}_{S, R}}{\|\hat{\mathbf{h}}_{R, D}\| \sqrt{P_S \alpha_{S, R} \|\mathbf{h}_{S, R}\|^2 + 1} \|\mathbf{h}_{S, R}\|} \mathbf{n}_R + n_D, \quad (8)$$

and

$$\gamma_D^{AF} = \frac{\frac{P_S P_{R\alpha S, R} \alpha_{R, D} \|\hat{\mathbf{h}}_{R, D}\|^2 \|\mathbf{h}_{S, R}\|^2}{\|\hat{\mathbf{h}}_{R, D}\|^2 (P_S \alpha_{S, R} \|\mathbf{h}_{S, R}\|^2 + 1)}}{\frac{P_R \alpha_{R, D} \|\hat{\mathbf{h}}_{R, D}\|^2}{\|\hat{\mathbf{h}}_{R, D}\|^2 (P_S \alpha_{S, R} \|\mathbf{h}_{S, R}\|^2 + 1)} + 1} = \frac{a \|\hat{\mathbf{h}}_{R, D}\|^2 \|\mathbf{h}_{S, R}\|^2}{b \|\hat{\mathbf{h}}_{R, D}\|^2 + \|\hat{\mathbf{h}}_{R, D}\|^2 (c \|\mathbf{h}_{S, R}\|^2 + 1)}, \quad (9)$$

where $a = P_S P_{R\alpha S, R} \alpha_{R, D}$, $b = P_R \alpha_{R, D}$, and $c = P_S \alpha_{S, R}$. Based on the received SNR in (9), we have the following theorem:

Theorem 1: The legitimate channel capacity in an LS-MIMO relaying system in presence of imperfect CSI can be approximated as $C_D^{AF} = W \log_2(1 + \frac{P_S P_{R\alpha S, R} \alpha_{R, D} \rho N_R^2}{P_R \alpha_{R, D} \rho N_R + P_S \alpha_{S, R} N_R + 1})$ when the number of relay antennas is very large, where W is a half of the spectral bandwidth.

Proof: Please refer to Appendix I. \square

It is found that the legitimate channel capacity is a constant due to channel hardening in such an LS-MIMO relaying system. Similar to (9), we assume the eavesdropper has perfect CSI by channel estimation, and thus the SNR is given by

$$\gamma_E^{AF} = \frac{d \|\hat{\mathbf{h}}_{R, E}\|^2 \|\mathbf{h}_{S, R}\|^2}{e \|\hat{\mathbf{h}}_{R, E}\|^2 + \|\hat{\mathbf{h}}_{R, D}\|^2 (c \|\mathbf{h}_{S, R}\|^2 + 1)}, \quad (10)$$

where $d = P_S P_{R\alpha S, R} \alpha_{R, E}$ and $e = P_R \alpha_{R, E}$. Hence, according to the definition of secrecy outage capacity in (4), we have the following theorem:

Theorem 2: Given an outage probability bound by ε , the secrecy outage capacity based on the AF relaying strategy can be approximated as $C_{SOC}^{AF} = W \log_2(1 + \frac{P_S P_{R\alpha S, R} \alpha_{R, D} \rho N_R^2}{P_R \alpha_{R, D} \rho N_R + P_S \alpha_{S, R} N_R + 1}) - W \log_2(1 + \frac{P_S P_{R\alpha S, R} \alpha_{R, E} N_R \ln \varepsilon}{P_R \alpha_{R, E} \ln \varepsilon - P_S \alpha_{S, R} N_R - 1})$ when the number of relay antennas is very large.

Proof: Please refer to Appendix II. \square

Based on Theorem 2, we may obtain the interception probability P_0^{AF} , namely the probability that the legitimate channel capacity is less than the eavesdropper channel capacity. By letting $C_{SOC}^{AF} = 0$ in (28), the interception probability can be computed as

$$P_0^{AF} = 1 - F\left(2^{C_D^{AF}/W} - 1\right) = \exp\left(-\frac{(P_S \alpha_{S, R} N_R + 1) \left(\frac{P_S P_{R\alpha S, R} \alpha_{R, D} \rho N_R^2}{P_R \alpha_{R, D} \rho N_R + P_S \alpha_{S, R} N_R + 1}\right)}{P_S P_{R\alpha S, R} \alpha_{R, E} N_R - P_R \alpha_{R, E} \left(\frac{P_S P_{R\alpha S, R} \alpha_{R, D} \rho N_R^2}{P_R \alpha_{R, D} \rho N_R + P_S \alpha_{S, R} N_R + 1}\right)}\right). \quad (11)$$

It is found that the interception probability of AF relaying scheme is independent of the spectral bandwidth W .

B. Decode-and-Forward (DF) Case

Different from the AF relaying scheme, DF decodes the received signal at the relay, and then forwards the original signal to the destination, so as to avoid noise amplification. Also by using the MRC technique at the relay, the channel capacity from the source to the relay can be expressed as

$$C_{S, R}^{DF} = W \log_2(1 + P_S \alpha_{S, R} \|\mathbf{h}_{S, R}\|^2) \approx W \log_2(1 + P_S \alpha_{S, R} N_R), \quad (12)$$

where (12) holds true because of channel hardening when $N_R \rightarrow \infty$. Then, the relay performs MRT based on the estimated CSI $\hat{\mathbf{h}}_{R, D}$. The channel capacity from the relay to the destination is given by

$$C_{R, D}^{DF} = W \log_2\left(1 + P_R \alpha_{R, D} \left|\hat{\mathbf{h}}_{R, D}^H \frac{\hat{\mathbf{h}}_{R, D}}{\|\hat{\mathbf{h}}_{R, D}\|}\right|^2\right) \approx W \log_2(1 + P_R \alpha_{R, D} \rho N_R), \quad (13)$$

where (13) is obtained similarly to Theorem 1. Thus, the legitimate channel capacity for the DF relaying scheme can be expressed as

$$C_D^{DF} = \min(C_{S, R}^{DF}, C_{R, D}^{DF}) = W \log_2(1 + \min(P_S \alpha_{S, R} N_R, P_R \alpha_{R, D} \rho N_R)). \quad (14)$$

It is found that C_D^{DF} is also a constant due to channel hardening in an LS-MIMO system. Meanwhile, the eavesdropper intercepts the signal from the relay, the corresponding channel capacity from the relay to the destination can be computed as

$$C_{R, E}^{DF} = W \log_2\left(1 + P_R \alpha_{R, E} \left|\hat{\mathbf{h}}_{R, E}^H \frac{\hat{\mathbf{h}}_{R, D}}{\|\hat{\mathbf{h}}_{R, D}\|}\right|^2\right). \quad (15)$$

For the secrecy outage capacity in an LS-MIMO DF relaying system, we have the following theorem:

Theorem 3: Given an outage probability bound by ε , the secrecy outage capacity for the DF relaying scheme can be approximated as $C_{SOC}^{DF} = W \log_2(1 + \min(P_S \alpha_{S, R} N_R, P_R \alpha_{R, D} \rho N_R)) - W \log_2(1 - P_R \alpha_{R, E} \ln \varepsilon)$ when the number of relay antennas is very large.

Proof: Please refer to Appendix III. \square

Similarly, we can also obtain the interception probability in this case. Letting $C_{SOC}^{DF} = 0$ in (35), we have

$$P_0^{DF} = \exp\left(-\frac{2^{C_D^{DF}/W} - 1}{P_R \alpha_{R, E}}\right) = \exp\left(-\frac{\min(P_S \alpha_{S, R} N_R, P_R \alpha_{R, D} \rho N_R)}{P_R \alpha_{R, E}}\right). \quad (16)$$

It is also found that the interception probability of the DF relaying scheme is independent of the spectral bandwidth W .

C. Performance Comparison Between AF and DF

AF and DF are two commonly used relaying techniques. Their respective merits have been well studied in literature. However, less is known about their secrecy performance. In this subsection, we provide an analytical comparison in terms of secrecy outage capacity and interception probability, and provide explicit criteria for choosing between AF and DF.

1) *Secrecy Outage Probability Criteria*: For a given requirement on the outage probability ε , the difference between the secrecy outage capacity of AF and that of DF can be computed as (17), shown at the bottom of the page. Then, given a set of channel conditions and transmit powers, it is easy to choose the better relaying technique according to (17). This result can be explained as follows. AF forwards the noise from the first hop, which not only degrades the performance at the destination, but also impair the quality of the eavesdropper signal. In particular, at low source SNR region, the noise has a greater impact on the eavesdropper signal than the legitimate signal. In this case, the noise is helpful to improve the secrecy performance. However, for DF, the benefit brought by the first hop noise is eliminated through decoding. In other words, decoding for the legitimate receiver is also in the interest of the eavesdropper. Thus, AF may outperform DF in this case. AF and DF have different secrecy performance under various conditions. Thus, we propose to switch the two relaying protocols according to system parameters.

2) *Interception Probability Criteria*: Interception probability is the outage probability corresponding to zero secrecy outage capacity. In other words, interception probability is the lower bound on the outage probability. Then, in terms of interception probability, the secrecy performance gap is given by (18), shown at the bottom of the page. Similarly, we can choose the better relaying technique from the perspective of interception probability according to (18).

IV. ASYMPTOTIC ANALYSIS

In the last section, we successfully obtained closed-form analytical results of the secrecy outage capacity for AF and

DF relaying techniques in an LS-MIMO relaying system with imperfect CSI, and compared their performance. However, the complex structure of the expressions prevents us from extracting direct guidelines for system design. In order to obtain clear insights on the secrecy performance and hence provide some simple but effective relaying schemes, we carry out asymptotic performance analysis in two extreme cases, i.e., large transmit powers P_S and P_R . In what follows, we give a detailed investigation of their asymptotic secrecy performance.

A. AF Case

1) *Large P_S* : In the case of high transmit power P_S at the source, we have the following theorem:

Theorem 4: There exists a ceiling effect on the secrecy outage capacity at high P_S . This bound is invariant with respect to P_S and P_R , but declines as the interception distance and the outage probability decrease, and decreases as the number of antennas at the relay adds.

Proof: Please refer to Appendix IV. \square

In this case, for the interception probability, we have the following lemma:

Lemma 1: Under high P_S , the interception probability is invariant with respect to P_S and P_R , but increases as the interception distance and the outage probability decrease, and decreases as the number of antennas adds.

Proof: From (38), the interception probability for the AF relaying scheme at high P_S can be obtained by letting $C_{SOC}^{AF} = 0$ as follows

$$P_0^{AF} = \exp\left(-\frac{\alpha_{R,D}\rho N_R}{\alpha_{R,E}}\right). \quad (19)$$

It is easy to validate the claims of Lemma 1 from (19). Note that if N_R is large, the interception probability asymptotically approaches zero. \square

Remarks: Combining Theorem 4 and Lemma 1, the secrecy performance, including interception probability and secrecy outage capacity, can be improved *significantly* by increasing the

$$\begin{aligned} \Delta C_{SOC} &= C_{SOC}^{AF} - C_{SOC}^{DF} \\ &= W \log_2 \left(\frac{(P_R \alpha_{R,D} \rho N_R + P_S \alpha_{S,R} N_R + P_S P_R \alpha_{S,R} \alpha_{R,D} \rho N_R^2 + 1)(P_R \alpha_{R,E} \ln \varepsilon - P_S \alpha_{S,R} N_R - 1)}{(P_R \alpha_{R,D} \rho N_R + P_S \alpha_{S,R} N_R + 1)(P_R \alpha_{R,E} \ln \varepsilon - P_S \alpha_{S,R} N_R + P_S P_R \alpha_{S,R} \alpha_{R,E} N_R \ln \varepsilon - 1)} \right) \\ &\quad - W \log_2 \left(\frac{1 + \min(P_S \alpha_{S,R} N_R, P_R \alpha_{R,D})}{1 - P_R \alpha_{R,E} \ln \varepsilon} \right). \end{aligned} \quad (17)$$

$$\Delta P_0 = P_0^{AF} - P_0^{DF} = \exp\left(-\frac{(P_S \alpha_{S,R} N_R + 1) \left(\frac{P_S P_R \alpha_{S,R} \alpha_{R,D} \rho N_R^2}{P_R \alpha_{R,D} \rho N_R + P_S \alpha_{S,R} N_R + 1} \right)}{P_S P_R \alpha_{S,R} \alpha_{R,E} N_R - P_R \alpha_{R,E} \left(\frac{P_S P_R \alpha_{S,R} \alpha_{R,D} \rho N_R^2}{P_R \alpha_{R,D} \rho N_R + P_S \alpha_{S,R} N_R + 1} \right)}\right) - \exp\left(-\frac{\min(P_S \alpha_{S,R} N_R, P_R \alpha_{R,D} \rho N_R)}{P_R \alpha_{R,E}}\right). \quad (18)$$

number of antennas at the relay N_R . Thus, even in the *short-distance interception* scenario, a high secrecy performance can be realized by adding antennas, which is a main advantage of LS-MIMO relaying systems with respect to traditional relaying systems. Again, this result may be well explained by the extra-high angular resolution of LS-MIMO which is capable of creating a strong null-space at an even close-by eavesdropper.

2) *Large P_R* : If the transmit power at the relay P_R is sufficiently large, we have the following theorem:

Theorem 5: At high P_R , the secrecy outage capacity is always equal to zero under arbitrary channel conditions and transmit powers.

Proof: Please refer to Appendix V. \square

For the interception of the AF relaying scheme, we also have the following lemma:

Lemma 2: Under high P_R , the interception probability of the AF relaying scheme is always equal to zero.

Proof: Examining (11), as P_R tends to infinity, we have

$$P_0^{AF} \approx \exp\left(-\frac{(P_S\alpha_{S,R}N_R + 1)P_S\alpha_{S,R}N_R}{P_S P_R \alpha_{S,R} \alpha_{R,E} N_R - P_R \alpha_{R,E} P_S \alpha_{S,R} N_R}\right) \quad (20)$$

$$= 0, \quad (21)$$

where (20) holds true since the denominator of (20) is equal to zero. \square

Remarks: A high P_R will result in zero secrecy outage capacity, so one should avoid using very high transmit power at the relay. In fact, we have the following lemma regarding the transmit power P_R :

Lemma 3: The secrecy outage capacity first monotonically increases and finally degrades as P_R increases from 0 to infinity. There exists an optimal transmit power P_R at medium regime.

Proof: As proved in Lemma 2, the secrecy outage capacity tends to zero at high P_R regime. Meanwhile, the secrecy outage capacity is zero at $P_R = 0$. Thus, there must an optimal transmit power P_R at medium regime. Similarly, the interception probability has the same property. \square

B. DF Case

1) *Large P_S* : In the case of high transmit power P_S at the source, we have the following theorem:

Theorem 6: There exists a bound on the secrecy outage capacity at high P_S . This bound is invariant with respect to P_S , but declines as the interception distance and the outage probability decrease, and increases as the number of antennas at the relay adds. If P_R is relatively large, the bound is independent of P_R .

Proof: Please refer to Appendix VI. \square

According to Theorem 6, it is easy to derive the interception probability as follows:

$$P_0^{DF} = \exp\left(-\frac{\alpha_{R,D}\rho N_R}{\alpha_{R,E}}\right), \quad (22)$$

Remarks: The interception probability decreases as N_R increases. In such an LS-MIMO relaying system, the interception probability asymptotically approaches zero.

2) *Large P_R* : If the transmit power P_R at the relay is sufficiently large, we have the following theorem:

TABLE I
SECRECY OUTAGE CAPACITY AND INTERCEPTION PROBABILITY FOR AF AND DF RELAYING SCHEMES AT HIGH TRANSMIT POWER REGIME

		large P_S	large P_R
Secrecy Outage	AF	$W \log_2 \left(-\frac{\alpha_{R,D}\rho N_R}{\alpha_{R,E} \ln \varepsilon} \right)$	0
Capacity	DF	$W \log_2 \left(\frac{1+P_R\alpha_{R,D}\rho N_R}{1-P_R\alpha_{R,E}} \right)$	0
Interception Probability	AF	0	0
	DF	0	1

Theorem 7: At high P_R , the secrecy outage capacity is always equal to zero under arbitrary channel conditions and transmit powers.

Proof: Please refer to Appendix VII. \square

Moreover, for the interception probability of the DF relaying scheme, we have the following lemma:

Lemma 4: The interception probability of the DF relaying scheme at high P_R is always equal to 1.

Proof: Examining (16), as P_R tends to infinity, we have

$$P_0^{DF} = \exp\left(-\frac{\min(P_S\alpha_{S,R}N_R, P_R\alpha_{R,D}\rho N_R)}{P_R\alpha_{R,E}}\right) \quad (23)$$

$$= \exp\left(-\frac{P_S\alpha_{S,R}N_R}{P_R\alpha_{R,E}}\right) \quad (24)$$

where (24) holds true since the denominator of (23) tends to infinity. \square

Note that there also exists an optimal P_R at medium regime in the sense of maximizing the secrecy performance, and due to page limitation, we will study this problem in our future works.

In Table I, we list the secrecy performance of AF and DF relaying schemes in an LS-MIMO relaying system, so as to compare their performance conveniently.

C. Performance Comparison Between AF and DF

Similarly, we compare the secrecy performance of AF and DF relaying schemes based on their asymptotic behaviors, so as to provide some simple and effective guideline for relaying scheme selection in different scenarios.

1) *Secrecy Outage Capacity Criteria:* From the perspective of secrecy outage capacity, we have the following two lemmas regarding the relaying scheme selection.

Lemma 5: At high P_S regime and P_R is relatively large, DF has the same secrecy outage capacity as AF. Since AF has lower complexity than DF, it is a better choice in this case.

Proof: It is proved by combining Theorem 4 and 6 directly. \square

Remark: Due to high P_S , the noise at the relay during the first hop is negligible for AF. Meanwhile if P_R is large enough, AF can asymptotically achieve the same performance as DF.

Lemma 6: Under large P_R , the secrecy outage capacity for both AF and DF tends to zero. So AF is also more appealing.

Proof: It is easy to prove Lemma 6 by combining Theorem 5 and 7. \square

Remark: Intuitively, if P_R is sufficiently large, the capacities of the channels from the relay to the destination and from the relay to the eavesdropper asymptotically approach the same values, thus secrecy outage capacity tends to zero.

2) *Interception Probability Criteria:* Again, we can obtain the following two lemmas regarding the relaying scheme selection by comparing their interception probability.

Lemma 7: At high P_S regime, the interception probability for both AF and DF approaches zero, so AF is a better choice.

Proof: It can be proved by comparing (19) and (22) directly. \square

Remark: Due to high P_S , the noise at the relay during the first hop is negligible. Meanwhile, by making use of the large array gain of LS-MIMO relay, the capacity of legitimate channel is always greater than that of the eavesdropper channel. Thus, the interception probability tends to zero.

Lemma 8: Under large P_R , the interception probability for AF and DF tends to 0 and 1, so AF is more appealing.

Proof: It is obtained from (21) and (24). \square

Remark: If P_R is sufficiently large, for DF, the capacity of the channel from the relay to the eavesdropper asymptotically approaches that of the channel from the relay to the destination. Thus, the interception probability tends to 1. However, for AF, the noise at the relay is amplified. By exploiting the array gain of the LS-MIMO relay, the capacity of the legitimate channel is always greater than the capacity of the eavesdropper, so the interception probability tends to zero.

Above all, AF is a better choice at high transmit power regime based on the criteria of secrecy outage capacity and interception probability. However, as shown later in simulation results, DF may be better in the low transmit power region. Hence, there is a switching point between AF and DF from the perspective of maximizing the secrecy performance.

V. SIMULATION RESULTS

To examine the accuracy and effectiveness of the theoretical results for the LS-MIMO AF and DF relaying systems, we present several simulation results in the following scenarios: we set $N_R = 100$, $W = 10$ KHz and $\rho = 0.9$. The relay is in the middle of a line between the source and the destination. We normalize the path loss as $\alpha_{S,R} = \alpha_{R,D} = 1$ and use $\alpha_{R,E}$ to denote the relative path loss. For example, if $\alpha_{R,E} > 1$, then the eavesdropper is closer to the relay than the destination. In addition, we use $\text{SNR}_S = 10 \log_{10} P_S$ and $\text{SNR}_R = 10 \log_{10} P_R$ to represent the transmit signal-to-noise ratio (SNR) in dB at the source and the relay, respectively. Note that the theoretical results are drawn according to the derived theoretical expressions, and the simulation results are obtained by averaging over 10 000 times Monte Carlo simulations under the same condition.

Firstly, we testify the accuracy of the theoretical expression for the AF relaying scheme with $\text{SNR}_S = \text{SNR}_R = 20$ dB. As seen in Fig. 2, the theoretical results are well consistent with the simulations in the whole $\alpha_{R,E}$ region with different outage probability requirements, which proves the high accuracy of the derived performance expressions. Given an outage probability bound by ε , as $\alpha_{R,E}$ increases, the secrecy outage capacity decreases gradually. This is because the interception capability of the eavesdropper enhances due to the shorter interception distance. In addition, given an $\alpha_{R,E}$, the secrecy outage capacity improves with the increase of ε , since the outage probability is an increasing function of the secrecy outage capacity.

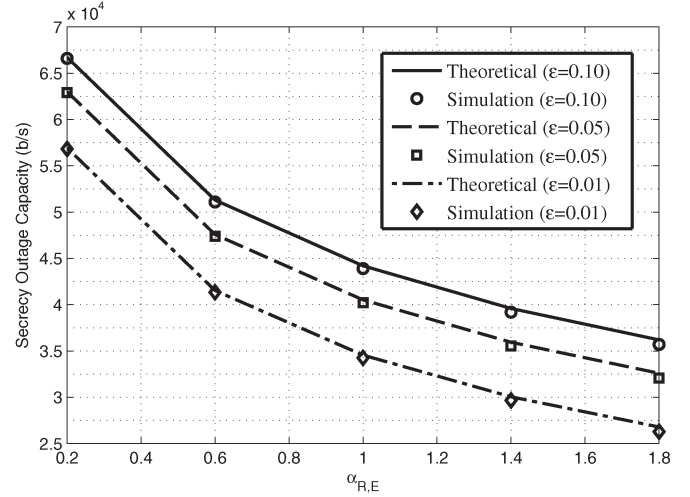


Fig. 2. Comparison of theoretical and simulation results for the AF relaying scheme.

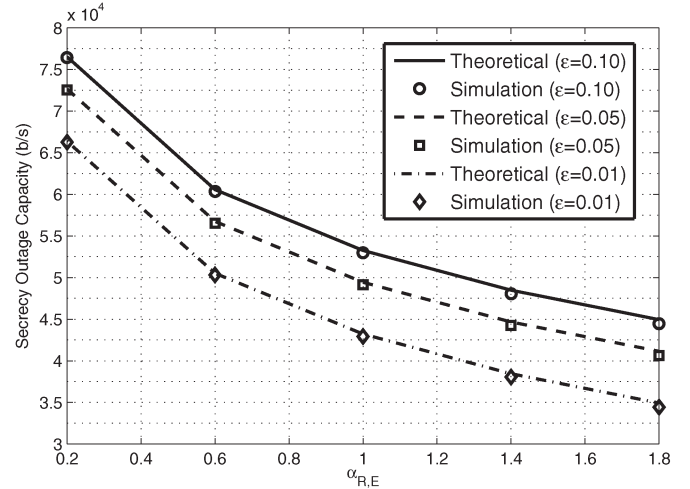


Fig. 3. Comparison of theoretical and simulation results for the DF relaying scheme.

Secondly, we testify the accuracy of the derived theoretical expressions for the DF relaying scheme with $\text{SNR}_S = \text{SNR}_R = 20$ dB. As seen in Fig. 3, the theoretical results coincide with the simulations nicely. Similar to the AF relaying scheme, the secrecy outage capacity decreases as $\alpha_{R,E}$ increases and ε reduces. Note that, compared to the secrecy outage capacity of the AF relaying scheme in Fig. 2, the secrecy outage capacity of the DF relaying scheme is better under the same conditions, since the DF relaying scheme avoids amplifying the noise at the relay at low and medium SNR regimes.

Thirdly, we validate the function of N_R on the secrecy outage capacity of AF and DF relaying schemes with $\varepsilon = 0.01$, and $\text{SNR}_S = \text{SNR}_R = 10$ dB. As shown in Fig. 4, the secrecy outage capacity can be improved significantly by adding antennas, even at a large $\alpha_{R,E}$. Thus, LS-MIMO relaying schemes can effectively solve the problem of short-distance interception. In addition, it is found that the number of antennas at the relay has different effects on the secrecy outage capacity for AF and DF relaying schemes. The secrecy outage capacity of DF with $N_R = 100$ is close to that of AF with $N_R = 200$ under such

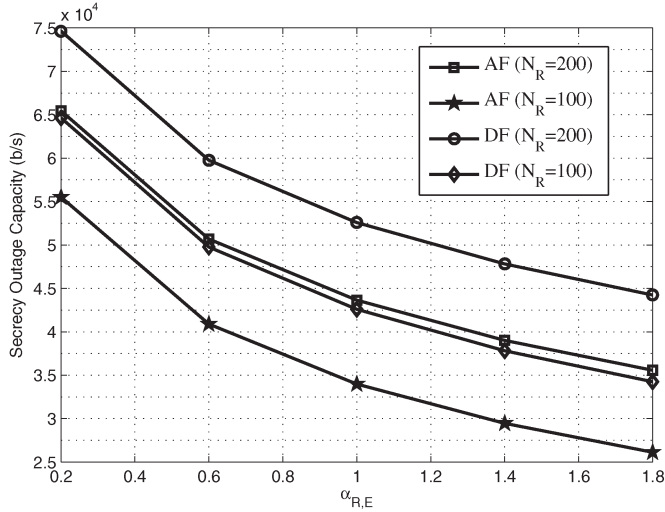


Fig. 4. Secrecy outage capacity comparison of AF and DF relaying schemes with different N_R .

condition. Hence, it makes sense to select the optimal relaying scheme according to system parameters.

Fourthly, we show the impact of SNR_S on the secrecy outage capacity of AF and DF relaying schemes with $\varepsilon = 0.05$, $\alpha_{R,E} = 1$, and $\text{SNR}_R = 10$ dB. As seen in Fig. 5, the secrecy outage capacity of both AF and DF relaying schemes increases as SNR_S adds. However, there exists the same performance bound at high SNR_S regime for both AF and DF, which confirms the claims in Theorem 4, Theorem 6, and Lemma 5. It is also found that AF performs better than DF at low SNR_S regime, performs poorer at medium SNR_S regime, and has the same performance at high SNR_S regime. This is because at low SNR_S , the forwarding noise of AF may significantly depress the channel capacity from the relay to the destination, and improve the secrecy performance. But at medium SNR_S , the noise is negligible, so DF performs better than AF. Therefore, it is better to switch the two relaying schemes according to system parameters, so as to maximize the secrecy outage capacity. These cross points are the switching points indeed.

Then, we investigate the impact of SNR_R on the secrecy outage capacity of AF and DF relaying schemes with $\varepsilon = 0.05$, $\alpha_{R,E} = 1$ and $\text{SNR}_S = 10$ dB. As seen in Fig. 6, the secrecy outage capacity is a convex function of SNR_R for both AF and DF. At low and high SNR_R regimes, the secrecy outage capacity asymptotically approaches zero, and the maximum secrecy outage capacity appears at medium SNR_R regime, which proves Theorem 5, Theorem 7, and Lemma 6 again. Different from the function of SNR_S , AF first performs poorer, since AF would amplify the noise at the relay. But, AF performs better than DF as SNR_R increases, since the channel capacity from the relay to the eavesdropper increases and thus the secrecy outage capacity of DF decreases sharply. Hence, it also makes sense to switch the relaying schemes according to system parameters.

Next, we show the impact of SNR_S on the interception probability of AF and DF relaying schemes with $\alpha_{R,E} = 1$, and $\text{SNR}_R = 10$ dB. It is found from Fig. 7 that AF has a zero interception probability in the whole SNR_S region, because it can always support a nonzero rate, as shown in Fig. 3. At high

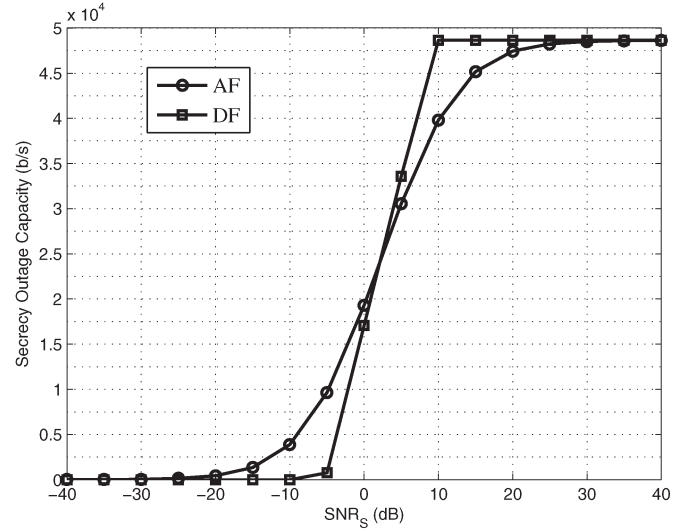


Fig. 5. Secrecy outage capacity comparison of AF and DF relaying schemes with different SNR_S .

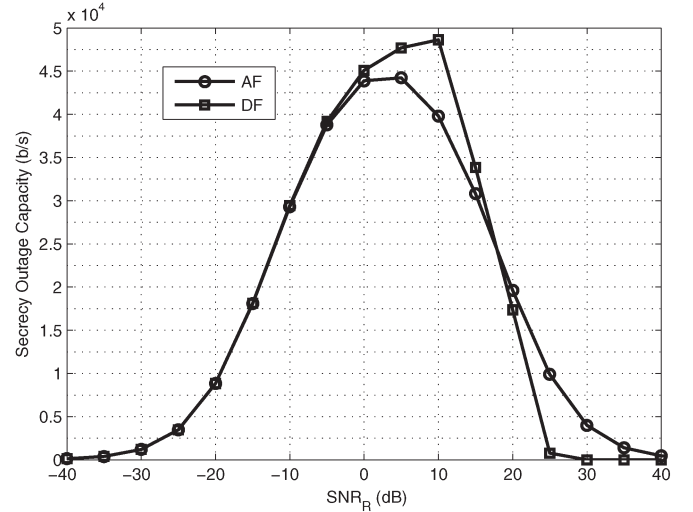


Fig. 6. Secrecy outage capacity comparison of AF and DF relaying schemes with different SNR_R .

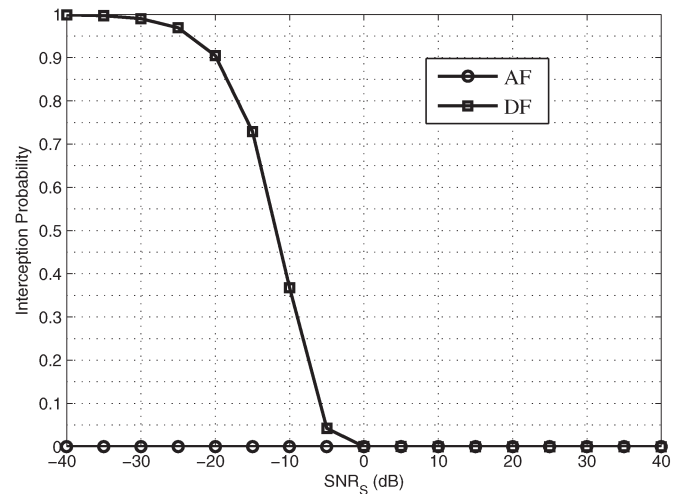


Fig. 7. Interception probability comparison of AF and DF relaying schemes with different SNR_S .

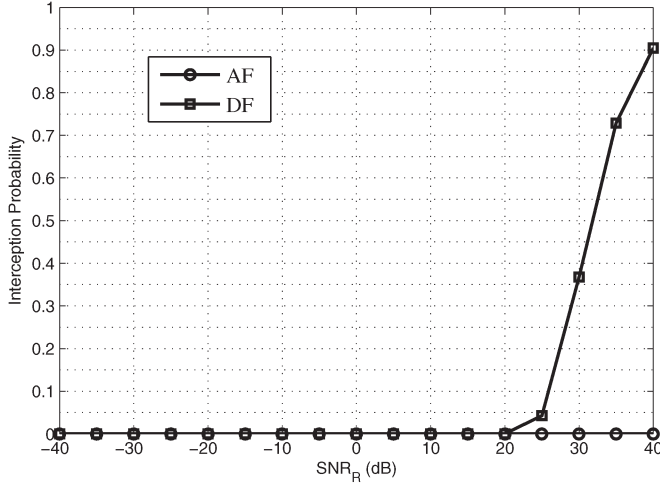


Fig. 8. Interception probability comparison of AF and DF relaying schemes with different SNR_R .

SNR_R regime, the interception probability of both AF and DF approaches a bound independent of P_S and P_R , which reconfirms the claims in Lemma 1 and 7. In this case, due to a large N_t , the bound on the interception probability in (19) is nearly equal to zero.

Finally, we investigate the impact of SNR_R on the interception probability of AF and DF relaying schemes with $\text{SNR}_S = 10$ dB and $\alpha_{R,E} = 1$. As seen in Fig. 8, similar to the last case, AF has a zero interception probability in the whole SNR_R region. As SNR_R increases, the bounds on the interception probability for AF and DF are 0 and 1 respectively, which proves Lemma 2, Lemma 4, and Lemma 8 again.

VI. CONCLUSION

A major contribution of this paper is the introduction of LS-MIMO relaying techniques into physical layer security that leads to significant enhancement of secrecy outage capacity, even when the interception distance is short. This paper focuses

on the analysis and comparison of secrecy outage capacity under AF and DF relaying schemes, and derives explicit expressions in terms of transmit SNRs, CSI accuracy, antenna number and interception distance. Furthermore, we carry out asymptotic analysis on the secrecy outage capacity and interception probability and get clear insights from them. Altogether, these results provide some important guidelines for the design of LS-MIMO relaying schemes for secure communications. For example, AF and DF has the same performance at high source transmit power. It is better to choose AF due to the lower complexity. Moreover, there is an optimal relay transmit power at medium regime.

APPENDIX A PROOF OF THEOREM 1

Based on the $\text{SNR } \gamma_D^{AF}$ at the destination, the achievable legitimated channel rate is given by (27), shown at the bottom of the page, where W is a half of the spectral bandwidth, since a complete transmission requires two time slots. $\mathcal{R}(x)$ denotes the real part of x . $\mathbf{h}_{R,D}$ is replaced by $\sqrt{\rho}\mathbf{h}_{R,D} + \sqrt{1-\rho}\mathbf{e}$ in (25), shown at the bottom of the page. Equation (26), shown at the bottom of the page, follows from the fact that $\rho\|\hat{\mathbf{h}}_{R,D}\|^2$ scales with the order $\mathcal{O}(\rho N_R)$ as $N_R \rightarrow \infty$ while $2\sqrt{\rho(1-\rho)}\mathcal{R}(\mathbf{e}^H \hat{\mathbf{h}}_{R,D}) + (1-\rho)\|\mathbf{e}\mathbf{h}_{R,D}^H\|^2/\|\hat{\mathbf{h}}_{R,D}\|^2$ scales as the order $\mathcal{O}(\sqrt{N_R})$, which can be negligible. Eq. (27) holds true because of $\lim_{N_R \rightarrow \infty} \frac{\|\hat{\mathbf{h}}_{R,D}\|^2}{N_R} = 1$ and $\lim_{N_R \rightarrow \infty} \frac{\|\mathbf{h}_{S,R}\|^2}{N_R} = 1$, namely channel hardening [38]. Therefore, we get the Theorem 1.

APPENDIX B PROOF OF THEOREM 2

According to (4), for a given ε , we have

$$\begin{aligned} \varepsilon &= P_r \left(C_{SOC}^{AF} > C_D^{AF} - W \log_2(1 + \gamma_E^{AF}) \right) \\ &= P_r \left(\gamma_E^{AF} > 2^{(C_D^{AF} - C_{SOC}^{AF})/W} - 1 \right) \\ &= 1 - F \left(2^{(C_D^{AF} - C_{SOC}^{AF})/W} - 1 \right), \end{aligned} \quad (28)$$

$$\begin{aligned} C_D^{AF} &= W \log_2 \left(1 + \frac{a|\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}|^2 \|\mathbf{h}_{S,R}\|^2}{b|\mathbf{h}_{R,D}^H \hat{\mathbf{h}}_{R,D}|^2 + \|\hat{\mathbf{h}}_{R,D}\|^2 (c\|\mathbf{h}_{S,R}\|^2 + 1)} \right) \\ &= W \log_2 \left(1 + \frac{a \left| (\sqrt{\rho}\hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho}\mathbf{e})^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 \|\mathbf{h}_{S,R}\|^2}{b \left| (\sqrt{\rho}\hat{\mathbf{h}}_{R,D} + \sqrt{1-\rho}\mathbf{e})^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 + (c\|\mathbf{h}_{S,R}\|^2 + 1)} \right) \end{aligned} \quad (25)$$

$$\begin{aligned} &= W \log_2 \left(1 + \frac{a \left(\rho\|\hat{\mathbf{h}}_{R,D}\|^2 + 2\sqrt{\rho(1-\rho)}\mathcal{R}(\mathbf{e}^H \hat{\mathbf{h}}_{R,D}) + (1-\rho)\frac{\|\mathbf{e}\mathbf{h}_{R,D}^H\|^2}{\|\hat{\mathbf{h}}_{R,D}\|^2} \right) \|\mathbf{h}_{S,R}\|^2}{b \left(\rho\|\hat{\mathbf{h}}_{R,D}\|^2 + 2\sqrt{\rho(1-\rho)}\mathcal{R}(\mathbf{e}^H \hat{\mathbf{h}}_{R,D}) + (1-\rho)\frac{\|\mathbf{e}\mathbf{h}_{R,D}^H\|^2}{\|\hat{\mathbf{h}}_{R,D}\|^2} \right) + c\|\mathbf{h}_{S,R}\|^2 + 1} \right) \\ &\approx W \log_2 \left(1 + \frac{a\rho\|\hat{\mathbf{h}}_{R,D}\|^2 \|\mathbf{h}_{S,R}\|^2}{b\rho\|\hat{\mathbf{h}}_{R,D}\|^2 + c\|\mathbf{h}_{S,R}\|^2 + 1} \right) \end{aligned} \quad (26)$$

$$\approx W \log_2 \left(1 + \frac{a\rho N_R^2}{b\rho N_R + cN_R + 1} \right), \quad (27)$$

where $F(x)$ is the cumulative distribution function (cdf) of γ_E^{AF} . In order to derive the secrecy outage capacity, the key is to get the cdf of γ_E^{AF} . Examining (10), due to channel hardening, we have

$$\gamma_E^{AF} = \frac{dN_R \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2}{e \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 + cN_R + 1}. \quad (29)$$

Since $\hat{\mathbf{h}}_{R,D}/\|\hat{\mathbf{h}}_{R,D}\|$ is an isotropic unit vector and independent of $\mathbf{h}_{R,E}$, $\left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2$ is χ^2 distributed with 2 degrees of freedom. Let $y \sim \chi_2^2$, we can derive the cdf of γ_E^{AF} as

$$F(x) = P_r \left(\frac{dN_R y}{ey + cN_R + 1} \leq x \right). \quad (30)$$

If $x < dN_R/e$, then we have

$$F(x) = P_r \left(y \leq \frac{(cN_R + 1)x}{dN_R - ex} \right) = 1 - \exp \left(-\frac{(cN_R + 1)x}{dN_R - ex} \right). \quad (31)$$

Since $x \geq N_R/e$ is impossible when $x = 2^{(C_D^{AF} - C_{SOC}^{AF})/W} - 1$, we have

$$\varepsilon = \exp \left(-\frac{(cN_R + 1) \left(2^{(C_D^{AF} - C_{SOC}^{AF})/W} - 1 \right)}{dN_R - e \left(2^{(C_D^{AF} - C_{SOC}^{AF})/W} - 1 \right)} \right). \quad (32)$$

Hence, we get the Theorem 2.

APPENDIX C PROOF OF THEOREM 3

In an LS-MIMO DF relaying system, the eavesdropper channel capacity can be expressed as

$$C_E^{DF} = W \log_2 \left(1 + \min \left(P_S \alpha_{S,R} N_R, P_R \alpha_{R,E} \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 \right) \right). \quad (33)$$

Then, the secrecy outage probability ε with respect to a secrecy outage capacity C_{SOC}^{DF} can be computed as (35), shown at the bottom of the page, where (34), shown at the bottom of the page, follows from the fact that $\left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2$ is χ^2 distributed with 2 degrees of freedom, and (35) holds true since $\exp(-\frac{P_S \alpha_{S,R} N_R}{P_R \alpha_{R,E}})$ approaches zero when N_R is sufficient large. Based on (35), it is easy to get the Theorem 3.

APPENDIX D PROOF OF THEOREM 4

If P_S is sufficiently large, the secrecy outage capacity with respect to a given outage probability ε in an LS-MIMO AF relaying system can be approximated as

$$\begin{aligned} C_{SOC}^{AF} &= W \log_2 \left(1 + \frac{P_S P_R \alpha_{S,R} \alpha_{R,D} \rho N_R^2}{P_R \alpha_{R,D} \rho N_R + P_S \alpha_{S,R} N_R + 1} \right) \\ &\quad - W \log_2 \left(1 + \frac{P_S P_R \alpha_{S,R} \alpha_{R,E} N_R \ln \varepsilon}{P_R \alpha_{R,E} \ln \varepsilon - 1 - P_S \alpha_{S,R} N_R} \right) \\ &\approx W \log_2 \left(1 + \frac{P_S P_R \alpha_{S,R} \alpha_{R,D} \rho N_R^2}{P_S \alpha_{S,R} N_R} \right) \\ &\quad - W \log_2 \left(1 + \frac{P_S P_R \alpha_{S,R} \alpha_{R,E} N_R \ln \varepsilon}{-P_S \alpha_{S,R} N_R} \right) \end{aligned} \quad (36)$$

$$\approx W \log_2(P_R \alpha_{R,D} \rho N_R) - W \log_2(-P_R \alpha_{R,E} \ln \varepsilon) \quad (37)$$

$$= W \log_2 \left(-\frac{\alpha_{R,D} \rho N_R}{\alpha_{R,E} \ln \varepsilon} \right), \quad (38)$$

where (36) follows the fact that the terms “ $P_R \alpha_{R,D} \rho N_R + 1$ ” and “ $P_R \alpha_{R,E} \ln \varepsilon - 1$ ” in the denominators is negligible when P_S is large enough, and (37) holds true since the constant “1” is dropper in the case of large P_S . From (38), it is known that the secrecy outage capacity is independent of transmit power P_S and P_R , and reduces as the interception distance and the outage probability decreases, which proves Theorem 4.

$$\begin{aligned} \varepsilon &= P_r(C_{SOC}^{DF} > C_D^{DF} - C_E^{DF}) \\ &= P_r \left(\min \left(P_S \alpha_{S,R} N_R, P_R \alpha_{R,E} \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 \right) > 2^{(C_D^{DF} - C_{SOC}^{DF})/W} - 1 \right) \\ &= P_r \left(P_S \alpha_{S,R} N_R \leq P_R \alpha_{R,E} \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 \right) P_r \left(P_S \alpha_{S,R} N_R > 2^{(C_D^{DF} - C_{SOC}^{DF})/W} - 1 \right) \\ &\quad + P_r \left(P_S \alpha_{S,R} N_R > P_R \alpha_{R,E} \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 \right) P_r \left(P_R \alpha_{R,E} \left| \mathbf{h}_{R,E}^H \frac{\hat{\mathbf{h}}_{R,D}}{\|\hat{\mathbf{h}}_{R,D}\|} \right|^2 > 2^{(C_D^{DF} - C_{SOC}^{DF})/W} - 1 \right) \\ &= \exp \left(-\frac{P_S \alpha_{S,R} N_R}{P_R \alpha_{R,E}} \right) + \left(1 - \exp \left(-\frac{P_S \alpha_{S,R} N_R}{P_R \alpha_{R,E}} \right) \right) \exp \left(-\frac{2^{(C_D^{DF} - C_{SOC}^{DF})/W} - 1}{P_R \alpha_{R,E}} \right) \\ &\approx \exp \left(-\frac{2^{(C_D^{DF} - C_{SOC}^{DF})/W} - 1}{P_R \alpha_{R,E}} \right), \end{aligned} \quad (34)$$

$$\approx \exp \left(-\frac{2^{(C_D^{DF} - C_{SOC}^{DF})/W} - 1}{P_R \alpha_{R,E}} \right), \quad (35)$$

APPENDIX E PROOF OF THEOREM 5

In the case of large P_R , the secrecy outage capacity with respect to a given outage probability ε in an LS-MIMO AF relaying system can be approximated as

$$\begin{aligned} C_{SOC}^{AF} &= W \log_2 \left(1 + \frac{P_S P_{R\alpha_{S,R}\alpha_{R,D}\rho N_R^2}}{P_{R\alpha_{R,D}\rho N_R} + P_S \alpha_{S,R} N_R + 1} \right) \\ &\quad - W \log_2 \left(1 + \frac{P_S P_{R\alpha_{S,R}\alpha_{R,E} N_R \ln \varepsilon}}{P_{R\alpha_{R,E} \ln \varepsilon} - 1 - P_S \alpha_{S,R} N_R} \right) \\ &\approx W \log_2 \left(1 + \frac{P_S P_{R\alpha_{S,R}\alpha_{R,D}\rho N_R^2}}{P_{R\alpha_{R,D}\rho N_R}} \right) \\ &\quad - W \log_2 \left(1 + \frac{P_S P_{R\alpha_{S,R}\alpha_{R,E} N_R \ln \varepsilon}}{P_{R\alpha_{R,E} \ln \varepsilon}} \right) \end{aligned} \quad (39)$$

$$\approx W \log_2(P_S \alpha_{S,R} N_R) - W \log_2(P_S \alpha_{S,R} N_R) \quad (40)$$

$$= 0, \quad (41)$$

where (39) follows the fact that the terms “ $P_S \alpha_{S,R} N_R + 1$ ” and “ $P_{R\alpha_{R,E} \ln \varepsilon} - 1$ ” in the denominators is negligible when P_R is large enough, and (40) holds true since the constant “1” is dropper in the case of large P_R . From (41), it is found that the secrecy outage capacity is always equal to zero with arbitrary transmit powers P_S and P_R , interception distance and outage probability, which proves Theorem 5.

APPENDIX F PROOF OF THEOREM 6

If P_S is sufficiently large, the secrecy outage capacity with respect to a given outage probability ε in an LS-MIMO DF relaying system can be computed as

$$\begin{aligned} C_{SOC}^{DF} &= W \log_2 (1 + \min(P_S \alpha_{S,R} N_R, P_{R\alpha_{R,D}\rho N_R})) \\ &\quad - W \log_2 (1 - P_{R\alpha_{R,E} \ln \varepsilon}) \\ &= W \log_2 (1 + P_{R\alpha_{R,D}\rho N_R}) \\ &\quad - W \log_2 (1 - P_{R\alpha_{R,E} \ln \varepsilon}) \end{aligned} \quad (42)$$

$$= W \log_2 \left(\frac{1 + P_{R\alpha_{R,D}\rho N_R}}{1 - P_{R\alpha_{R,E} \ln \varepsilon}} \right), \quad (43)$$

where (42) follows the fact of $\min(P_S \alpha_{S,R} N_R, P_{R\alpha_{R,D}\rho N_R}) = P_{R\alpha_{R,D}\rho N_R}$ at a large P_S . From (43), it is found that the secrecy outage capacity is independent of P_S , and declines as the interception distance the outage probability decrease. Furthermore, if P_R is relatively large, the secrecy outage capacity can be approximated as

$$C_{SOC}^{DF} = W \log_2 \left(-\frac{\alpha_{R,D}\rho N_R}{\alpha_{R,E} \ln \varepsilon} \right), \quad (44)$$

where (44) holds true since the constant “1” in both the denominator and the numerator is negligible when P_R is high. Interestingly, it is found that DF has the same secrecy outage capacity as AF, which proves the claims in Theorem 6.

APPENDIX G PROOF OF THEOREM 7

In the case of large P_R , the secrecy outage capacity with respect to a given outage probability ε in an LS-MIMO DF relaying system can be approximated as

$$\begin{aligned} C_{SOC}^{DF} &= W \log_2 (1 + \min(P_S \alpha_{S,R} N_R, P_{R\alpha_{R,D}\rho N_R})) \\ &\quad - W \log_2 (1 + P_{R\alpha_{R,E} \ln \varepsilon}) \\ &= W \log_2 (1 + P_S \alpha_{S,R} N_R) \\ &\quad - W \log_2 (1 - P_{R\alpha_{R,E} \ln \varepsilon}) \end{aligned} \quad (45)$$

$$= 0, \quad (46)$$

where (45) follows the fact of $\min(P_S \alpha_{S,R} N_R, P_{R\alpha_{R,D}\rho N_R}) = P_S \alpha_{S,R} N_R$ at a large P_R , and (46) holds true because of $C_{SOC}^{DF} \geq 0$. From (46), it is found that the secrecy outage capacity is always equal to zero with arbitrary transmit powers P_S and P_R , interception distance and outage probability. In addition, DF has the same secrecy outage capacity as AF, which proves Theorem 7.

REFERENCES

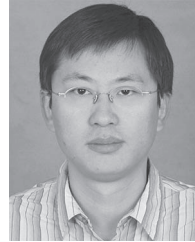
- [1] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] Y. Shui, S. Chang, H. Wu, S. Huang, and H. Chen, “Physical layer security in wireless networks: A tutorial,” *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.
- [3] D. W. K. Ng, E. S. Lo, and R. Schober, “Energy-efficient resource allocation for secure OFDMA systems,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.
- [4] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Feb. 2011.
- [5] P. K. Gopala, L. Lai, and H. El. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [6] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
- [7] 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.
- [8] L. Dong, Z. Han, A. Petropulu, and H. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
- [9] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, “Multi-antenna relay aided wireless physical layer security,” *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 1–17, Jun. 2015.
- [10] 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.
- [11] X. Wang, K. Wang, and X. Zhang, “Secure relay beamforming with imperfect channel side information,” *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.
- [12] S. Vishwakarma and A. Chockalingam, “Decode-and-forward relay beamforming for secrecy with finite-alphabet input,” *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 912–915, May 2013.
- [13] J. Li, A. P. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
- [14] K. Park, T. Wang, and M. 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.
- [15] D. Ng, E. 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.
- [16] J. Mo, M. Tao, and Y. Liu, “Relay placement for physical layer security: A secure connection perspective,” *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Jun. 2012.

- [17] 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.
- [18] G. Zhang, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
- [19] H. Wang, M. Luo, X. 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.
- [20] H. Long, W. Xiang, Y. Zhang, Y. Liu, and W. Wang, "Secrecy capacity enhancement with distributed precoding in multirelay wiretap systems," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 229–238, Jan. 2013.
- [21] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.
- [22] C. Jeong, I. 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.
- [23] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.
- [24] Z. Ho, E. Jorswieck, and S. Engelmann, "Information leakage neutralization for the multi-antenna non-regenerative relay-assisted multi-carrier interference channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1672–1686, Sep. 2013.
- [25] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 637–640, Apr. 2013.
- [26] N. Yang, H. Suraweera, I. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.
- [27] T. L. Marzetta, "Noncooperative cellular wireless with unlimited number of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.
- [28] F. Ruseket *et al.*, "Scaling to MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 20, no. 1, pp. 40–60, Jan. 2013.
- [29] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, and X. Gao, "Ergodic secrecy sum-rate for multiuser downlink transmission via regularized channel inversion: Large system analysis," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1627–1630, Jul. 2014.
- [30] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," submitted to *IEEE Trans. Wireless Commun.*, 2015. [Online]. Available: <http://arxiv.org/pdf/1505.00330.pdf>
- [31] X. Chen, C. Yuen, and Z. Zhang, "Exploiting large-scale MIMO techniques for physical layer security with imperfect CSI," in *Proc. IEEE GLOBECOM*, Dec. 2014, pp. 1648–1635.
- [32] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential message," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.
- [33] 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.
- [34] J. Jose, A. Ashikhmin, T. L. Marzetta, and S. Vishwanath, "Pilot contamination and precoding in multi-cell TDD systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2640–2651, Aug. 2011.
- [35] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the secrecy outage capacity of physical layer security in large-scale MIMO relaying systems with imperfect CSI," in *Proc. IEEE ICC*, Jun. 2014, pp. 2052–2057.
- [36] 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.

- [37] 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.

- [38] B. M. Hochwald, T. L. Marzetta, and V. Tarokh, "Multiple-antenna channel hardening and its implications for rate-feedback and scheduling," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893–1909, Sep. 2004.



Xiaoming Chen (M'10–SM'14) received the B.Sc. degree from Hohai University in 2005, the M.Sc. degree from Nanjing University of Science and Technology in 2007 and the Ph. D. degree from Zhejiang University in 2011, all in electronic engineering. He is now with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests mainly focus on cognitive radio, multi-antenna techniques, wireless security, interference network and wireless power transfer, etc.



Lei Lei (M'14) received the B.S. degree in electronic and information engineering from Northwestern Polytechnical University, Xi'an China, in 2002, and the Ph.D. degree in communication and information systems from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2008. He is currently an Associate Professor with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics. His research interests include wireless ad hoc networks and cooperative communications.



Huazi Zhang (S'11–M'13) received the B.S. and Ph.D. degrees in electrical engineering from Zhejiang University, Hangzhou, China, in 2008 and 2013, respectively. From 2011 to 2013, he worked as a visiting scholar in the Department of Electrical and Computer Engineering, NC State University, Raleigh, NC. His research interests include OFDM and MIMO systems, clustering and compressive sensing, coding techniques and cognitive radio networks.



Chau Yuen (SM'12) received the B.Eng. and Ph.D. degrees from Nanyang Technological University, Singapore, in 2000 and 2004, respectively. In 2005, he was a Postdoctoral Fellow with Lucent Technologies Bell Labs, Murray Hill, NJ, USA. In 2008, he was a Visiting Assistant Professor with Hong Kong Polytechnic University, Kowloon, Hong Kong. From 2006 to 2010, he was with the Institute for Infocomm Research, Singapore, as a Senior Research Engineer. Since 2010, he has been an Assistant Professor with the Singapore University of Technology and Design, Singapore. Dr. Yuen serves as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He received the IEEE Asia-Pacific Outstanding Young Researcher Award in 2012.