Secure Multiple Amplify-and-Forward Relaying over Correlated Fading Channels

Lisheng Fan, Rui Zhao, Fengkui Gong, Nan Yang, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—This paper quantifies the impact of correlated fading on secure communication of multiple amplify-and-forward (AF) relaying networks. In such a network, the base station (BS) is equipped with multiple antennas and communicates with the destination through multiple AF relays, while the message from the relays can be overheard by an eavesdropper. We focus on the practical communication scenario, where the main and eavesdropper's channels are correlated. In order to enhance the transmission security, transmit antenna selection (TAS) is performed at the BS, and the best relay is chosen according to the full or partial relay selection criterion, which relies on the dual-hop relay channels or the second-hop relay channels, respectively. For these criteria, we study the impact of correlated fading on the network secrecy performance, by deriving an analytical approximation for the secrecy outage probability (SOP) and an asymptotic expression for the high main-to-eavesdropper ratio (MER). From these results, it is concluded that the channel correlation is always beneficial to the secrecy performance of full relay selection. However, it deteriorates the secrecy performance if partial relay selection is used, when the number of antennas at the BS is less than the number of relays.**

***Index Terms*—Secure communication, correlated fading, relay selection, secrecy diversity order.**

I. Introduction

Driven by the rapidly increasing demand on data transmission over the open wireless medium, in the last few years the privacy and security in wireless networks have attracted widespread attention from both academia and industry [1]. Besides the traditional encryption schemes, physical-layer security (PLS) has been proposed to achieve the information-theoretical security. PLS can be traced back to the pioneering Shannon's work [2], who proposed that a perfect secrecy can be achieved in wireless communication systems. Several years later, Wyner proposed a classical wiretap model to analyze the secure communication [3], which was extended to study the PLS over fading channels. Furthermore, in [4], [5], secure communication over Rayleigh fading channels was investigated, and analytical expressions for the secrecy outage probability (SOP) and secrecy capacity were provided. In [6]–[8], the impact of more complicated fading channels on the secrecy performance, was investigated. Finally, some fundamental works on the physical lay security in interference alignment networks were initially done by Zhao Nan [9], which focused on the anti-jamming, anti-eavesdropping, and collusive eavesdropping issues for interference alignment.

Antenna selection [10]–[12] has been proposed as an easy-to-implement strategy to enhance security of multi-antenna wireless communication systems, by exploiting the channel fluctuation among multiple antennas. In [13], transmit antenna selection (TAS) was used at the base station (BS) to improve the secrecy performance by increasing the number of antennas. In [14], TAS was implemented for MIMO wiretap channel, and the secrecy performance was studied by deriving analytical expressions for the secrecy capacity and SOP. Apart from antenna selection, secure relaying is another effective strategy to enhance wireless security, since it exploits the channel fluctuation among multiple relays. There are two fundamental relaying protocols, namely, amplify-and-forward (AF) and decode-and-forward (DF) [15]–[17]. In [18], [19], relay selection was performed to secure multiple AF relay networks, where several relay selection criteria were proposed and examined. In [20]–[23], relay selection was used to secure multiple DF relay networks, and an analytical expression for the SOP and asymptotic results in the high main-to-eavesdropper ratio (MER)[1], were derived. We note that although the security analysis has been well studied for the DF relay network [20]–[22], [24], [25], it is rarely studied for the AF relay network. This is because the received signal-to-noise ratio (SNR) expressions at the destination and the eavesdropper in the AF relay network are much more complicated than those in the DF relay network, which increases the complexity of the analysis. Hence, a thorough and accurate analysis for the secrecy performance is of significant importance for the AF

This work was supported by the NSF of China (No. 61372129/61401165/61372067), by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2014A030306027, by the Innovation Team Project of Guangdong Province University (No. 2016KCXTD017), and by the open research fund of State Key Laboratory of Integrated Services Networks under Grant ISN17-05. The work of N. Yang was supported by the Australian Research Council Discovery Project under Grant DP150103905. The review of this paper was coordinated by Prof. Z. Ding. (Corresponding author: Rui Zhao).

L. Fan is with Department of Electronic Engineering, Shantou University, Shantou China, and is with the School of Computer Science and Educational Software, Guangzhou University, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710126, China (e-mail: lsfan@gzhu.edu.cn).

R. Zhao is with the College of Information Science and Engineering, Huaqiao University, China (e-mail: rzhao@hqu.edu.cn).

F. Gong is with the State Key Laboratory of ISN, Xidian University, Xi'an 710071, China (e-mail: fkgong@xidian.edu.cn).

N. Yang is with Australian National University, Canberra ACT 0200, Australia (e-mail: nan.yang@anu.edu.au).

G. K. Karagiannidis is with Aristotle University of Thessaloniki, Thessaloniki 54 124, Greece (e-mail: geokarag@auth.gr).

Digital Object Identifier 10.1109/TCOMM.2017.2691712

[1]In practice, the high MER is encountered when the eavesdropper is located far from the relay or the received antenna gain at the eavesdropper is small.

relay network.

A major limitation of the aforementioned studies lies in the assumption that the eavesdropper's channel is independent from the main channel. However, this assumption may not hold in practical communication scenarios, due to the existence of several factors, such as radio scattering environments and antenna deployments [26]–[28]. In such scenarios, the main and eavesdropper's channels are correlated, which affects the system secrecy performance. Motivated by this, the authors in [29] studied the impact of correlated fading on the secrecy performance in the high SNR regime. Furthermore, in [30], the performance of secure communication over correlated fading channels was studied, and expressions for both the secrecy capacity and SOP were provided in the form of infinite series. Hence, to the best of our knowledge, the effect of correlated fading has been concentrated on the secure non-cooperative communications, and its impact on the secure cooperative relay networks has not yet been investigated.

In this paper, we analytically investigate the impact of correlated fading on secure multiple AF relaying networks, which are composed of one BS equipped with M antennas, N AF relays, one receiver, and one eavesdropper. The BS transmits its signal to the receiver through N relays, which can be overheard by an eavesdropper. We consider the practical communication scenario, where the main and eavesdropper's channels are correlated. In order to enhance the network security, TAS is adopted at the BS and full or partial relay selection is used to choose the best relay. The novelty of our work can be summarized as follows:

- We analytically evaluate the impact of correlated fading channels on a multiple AF relaying network, where two relay selection criteria are considered, namely, full relay selection and partial relay selection. For both criteria, we derive a novel analytical approximation for the SOP, in order to evaluate the impact of correlated fading on the secrecy performance in the whole SNR and MER regimes.
- We derive an asymptotic expression for the SOP in the high MER regime, to determine the factors, that govern the network secrecy performance. Based on the asymptotic SOP expressions, we find that the secrecy diversity order of the full and partial relay selection criteria is equal to N and $\min(M, N)$, respectively. Moreover, we show that the channel correlation is beneficial for the full relay selection criterion, but detrimental to the partial relay selection criterion when $M < N$.

The rest of this paper is organized as follows. Section II introduces the system model with correlated fading and then the two relay selection criteria. Section III derives the analytical approximation for the SOP, along with the asymptotic expressions in the high MER region. Numerical and simulation results are provided and discussed in Section IV. Finally, Section V concludes this work.

Notations: We use $\mathcal{CN}(0, \sigma^2)$ to represent a circularly symmetric complex Gaussian random variable (RV) with zero mean and variance σ^2. We use $f_X(\cdot)$ and $F_X(\cdot)$ to represent the probability density function (PDF) and cumulative density function (CDF) of the RV X, respectively. The function, $I_0(x)$, is the modified Bessel function of the first kind of order zero [31], while $\Pr[\cdot]$ denotes probability, and $E[\cdot]$ denotes statistical average.

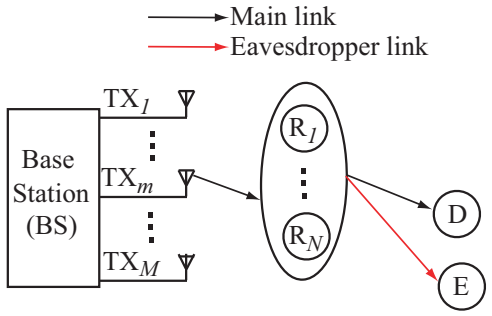

Fig. 1. Secure multiple AF relays with multi-antenna at the BS.

II. System Model

Fig. 1 depicts a secure multiple AF relay network over correlated fading channels. In this network, the BS is equipped with M antennas $\{\text{TX}_m | 1 \leq m \leq M\}$, and there are N intermediate AF relays $\{R_n | 1 \leq n \leq N\}$, to assist the secure transmission from the BS to the destination D. One eavesdropper[2], E, exists in the network, and overhears the messages from the relays. In this work, we consider the communication scenario where the direct channel between the BS and eavesdropper suffers severer shadowing, due to an obstacle or the eavesdropper is located far from the BS. If the eavesdropper can overhear the message from the BS, the network secrecy performance becomes worse, since the direct links can be used by the eavesdropper for secrecy data detection. We consider the practical communication scenario, where the channels from the relays to D and E are correlated, due to e.g. radio scattering and antenna deployments. In order to enhance the security, the best relay, R_{n^*}, is selected among N relays, and the BS employs TAS[3] to choose the best antenna, TX_{m^*}, in order to transmit the information.

We assume that the m-th antenna, TX_m, and the n-th relay, R_n, are used for secure data transmission. In the following, we present the two-phase transmission process and the relay selection criterion. In the first phase, TX_m sends the normalized signal, x_s, with power P to R_n. The received signal at R_n is given by

$$y_{R_n} = \sqrt{P} h_{m,R_n} x_s + n_R, \tag{1}$$

[2]In this paper, the eavesdropper is equipped with a single antenna due to size limitation. However, if there are multiple antennas at the eavesdropper, the network secrecy performance becomes worse, since the eavesdropper can exploit the multi-antenna diversity at itself. But in this case, the network secrecy diversity order will remain unchanged with the increased number of antennas at the eavesdropper [18].

[3]Although TAS technique presents slightly worse performance than beamforming, it needs much less implementation complexity and RF chain cost. Therefore, TAS is adopted in this paper, and it can be applied for the scenarios where the system has a complexity constraint, e.g., the hardware cost. Moreover, the channels from the BS to relays are not correlated with the channels from relays to receivers, since the channel correlation is only considered at the receivers. Hence, using all antennas at the BS will not change the analytical framework of performance evaluation in this paper.

where $h_{m,R_n} \sim \mathcal{CN}(0,\alpha)$ denotes the channel coefficient of the TX$_m$–R_n link and $n_R \sim \mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise (AWGN) at the relay. Then R_n amplifies the received signal, y_{R_n}, by the factor, κ, given by

$$\kappa = \sqrt{\frac{P}{P|h_{m,R_n}|^2+\sigma^2}}, \tag{2}$$

and then forwards the resultant signal to D. The received signals at D and E are given by

$$y_D = h_{R_n,D}\kappa y_{R_n} + n_D, \tag{3}$$

and

$$y_E = h_{R_n,E}\kappa y_{R_n} + n_E, \tag{4}$$

respectively, where $h_{R_n,D} \sim \mathcal{CN}(0,\beta)$ and $h_{R_n,E} \sim \mathcal{CN}(0,\varepsilon)$ represent the channel coefficients of the R_n–D and R_n–E links, respectively, and $n_D \sim \mathcal{CN}(0,\sigma^2)$ and $n_E \sim \mathcal{CN}(0,\sigma^2)$ are the AWGN at the D and E, respectively. We assume that due to factors such as radio scattering and antenna deployments, the channels $h_{R_n,D}$ and $h_{R_n,E}$ are correlated, characterized by the joint PDF [30]

$$f_{|h_{R_n,D}|^2,|h_{R_n,E}|^2}(x,y) = \frac{I_0\Big(\frac{2}{1-\rho}\sqrt{\frac{\rho xy}{\beta\varepsilon}}\Big)}{(1-\rho)\beta\varepsilon} e^{-\frac{\frac{x}{\beta}+\frac{y}{\varepsilon}}{1-\rho}}, \tag{5}$$

where, $\rho = \frac{\text{cov}(|h_{R_n,D}|^2,|h_{R_n,E}|^2)}{\sqrt{\text{var}(|h_{R_n,D}|^2)\text{var}(|h_{R_n,E}|^2)}} \in [0,1]$, is the power correlation coefficient. In particular, $\rho = 0$, denotes the independent channel scenario, while $\rho = 1$ indicates that $h_{R_n,D}$ and $h_{R_n,E}$ are completely correlated. Since the channel correlation coefficient ρ is a long-term statistical variable, we can estimate it by some samples of $h_{R_n,D}$ and $h_{R_n,E}$ during non-secure data transmission, where both D and E are served by the BS. Then the estimated ρ can be used for the secure data transmission, where E acts as the eavesdropper.

From (1)–(4), we obtain the received end-to-end SNRs at D and E as

$$\text{SNR}_{mn}^{D} = \frac{\tilde{P}^2 u_{mn} v_n}{\tilde{P}u_{mn} + \tilde{P}v_n + 1}, \tag{6}$$

and

$$\text{SNR}_{mn}^{E} = \frac{\tilde{P}^2 u_{mn} w_n}{\tilde{P}u_{mn} + \tilde{P}w_n + 1}, \tag{7}$$

respectively, where $\tilde{P} = P/\sigma^2$ is the transmit SNR, and $u_{mn} = |h_{m,R_n}|^2$, $v_n = |h_{R_n,D}|^2$ and $w_n = |h_{R_n,E}|^2$ are the associated instantaneous channel gains.

The secrecy outage probability (SOP) is defined as the probability that the data rate difference between the main and eavesdropper's channels falls below a certain threshold, R_s,

$$\begin{aligned}\mathcal{P}_{mn,out} &= \Pr\Big[\frac{1}{2}\log_2(1+\text{SNR}_{mn}^{D}) \\ &\quad - \frac{1}{2}\log_2(1+\text{SNR}_{mn}^{E}) < R_s\Big] \qquad (8)\\ &= \Pr\Big[\frac{1+\text{SNR}_{mn}^{D}}{1+\text{SNR}_{mn}^{E}} < \gamma_s\Big], \qquad (9)\end{aligned}$$

where $\gamma_s = 2^{2R_s}$ is the secrecy SNR threshold. Since it is difficult to obtain an accurate analytical expression for the SOP of the network, we use [19, eq. (16)] to give a lower bound on the SOP as

$$\begin{aligned}\mathcal{P}_{mn,out} &> \Pr\Big[\min\big(\frac{u_{mn}}{\gamma_s-1}, \frac{v_n+1/\tilde{P}}{\gamma_s}\big) < \frac{1}{\tilde{P}} + w_n\Big], \qquad (10)\\ &> \Pr\Big[\min\big(\frac{\gamma_s}{\gamma_s-1}u_{mn}, v_n\big) < \eta + \gamma_s w_n\Big], \qquad (11)\end{aligned}$$

where $\eta = \frac{\gamma_s-1}{\tilde{P}}$, and we apply $\min\big(\frac{u_{mn}}{\gamma_s-1}, \frac{v_n+1/\tilde{P}}{\gamma_s}\big) < \min\big(\frac{u_{mn}}{\gamma_s-1}, \frac{v_n}{\gamma_s}\big) + \frac{1}{\tilde{P}\gamma_s}$ from (10) to (11). Note that the lower bound in (11) is effective to evaluate the SOP, especially when the transmit power is large.

In this work, we consider the practical secure communication scenario, where the eavesdropper is not willing to feedback its channel parameters, and hence, only the main channel parameters can be used for the relay selection. From (11), a full relay selection criterion based on the main links is given by

$$(n^*, m^*) = \arg \max_{1\le n\le N} \max_{1\le m\le M} \min\big(\frac{\gamma_s}{\gamma_s-1}u_{mn}, v_n\big), \tag{12}$$

where the TAS is jointly performed at the BS. Note that the selection in (12) requires the availability of the channel parameters of the dual-hop relaying, which adds a load in the practical implementation, especially for a large number of antennas at the BS. In order to reduce the implementation complexity, a simpler partial relay selection is considered as

$$n^* = \arg \max_{1\le n\le N} v_n, \tag{13}$$

and the antenna is selected at the BS as

$$m^* = \arg \max_{1\le m\le M} u_{mn^*}. \tag{14}$$

Note that this criterion is a separate relay and antenna selection, and it only needs the availability of the parameters of the second-hop relaying channels.

From the above description, we provide the following remark: Different from the secure non-cooperative communications, the secure cooperative communications may require the first-hop relaying links to be used for the relay selection criterion. Moreover, the first-hop relaying links interact with the second-hop main and eavesdropper's links in the performance analysis, making the derivation much more complicated. Furthermore, the impact of the system parameters such as the channel correlation coefficient on the network secrecy performance is also affected by the first-hop relaying links.

III. Secrecy outage probability

In this section, we derive an analytical approximation for the SOP for the full and partial relay selection criteria, and provide the asymptotic expressions with high MER. Note that in the security analysis with independent fading, the eavesdropper's channel parameters can be easily separated from the main channel parameters. This simplifies the derivation of the security analysis. Differently, in the security analysis with correlated fading, it is very difficult to separate the eavesdropper's channel parameters from the main channel parameters, and

these parameters need to be jointly computed to derive the security. This makes the derivation much more complicated and challenging. Moreover, the impact of channel correlation coefficient on the network secrecy performance may depend on many factors, such as the specific relay selection criterion and the network parameters including the number of the relays and antennas. Hence, it is another challenge to explicitly examine the impact of channel correlation coefficient on the secrecy performance. To fulfill this task, we derive the asymptotic SOP expression in the high MER regime, to determine the factors that govern the network secrecy performance.

A. Analytical approximation for the SOP in full relay selection

According to the full relay selection criterion in (12), the lower bound on the SOP achieved, when the full relay selection criterion is used, can be written as

$$\mathcal{P}_{out,\mathsf{Full}}^{\mathsf{LB}} = \Pr\Big[\min\big(\frac{\gamma_s}{\gamma_s-1}u_{m^*n^*}, v_{n^*}\big) < \eta + \gamma_s w_{n^*}\Big] \tag{15}$$

$$= \sum_{n=1}^{N} \Pr\big[\min(\tilde{u}_n, v_n) < \eta + \gamma_s w_n, \min(\tilde{u}_n, v_n) > \max_{k=1,\cdots,N,k\neq n} \min(\tilde{u}_k, v_k)\big], \tag{16}$$

where $\tilde{u}_n$ is defined as

$$\tilde{u}_n = \max_{1\leq m\leq M} \frac{\gamma_s}{\gamma_s-1}u_{mn}. \tag{17}$$

Due to the symmetry among the N relays,

$$\mathcal{P}_{out,\mathsf{Full}}^{\mathsf{LB}} = N\Pr\big[\min(\tilde{u}_1, v_1) < \eta + \gamma_s w_1, \min(\tilde{u}_1, v_1) > Z_1\big] \tag{18}$$

$$= N\Pr\big[\min(\tilde{u}_1, v_1) > Z_1\big] - N \times \Pr\big[\min(\tilde{u}_1, v_1) \geq \eta + \gamma_s w_1, \min(\tilde{u}_1, v_1) > Z_1\big], \tag{19}$$

where Z_1 is given by

$$Z_1 = \max_{k=2,\cdots,N} \min(\tilde{u}_k, v_k). \tag{20}$$

Note that the first term in (19) is equivalent to the probability of random choose the maximal among N independent and identically distributed RVs. As such, we have $\Pr\big[\min(\tilde{u}_1, v_1) > Z_1\big] = \frac{1}{N}$. Then $\mathcal{P}_{out,\mathsf{Full}}^{\mathsf{LB}}$ can be rewritten as

$$\mathcal{P}_{out,\mathsf{Full}}^{\mathsf{LB}} = 1 - N\Pr\big[\min(\tilde{u}_1, v_1) \geq \eta + \gamma_s w_1, \min(\tilde{u}_1, v_1) > Z_1\big]$$

$$= 1 - N\Pr\big[\min(\tilde{u}_1, v_1) > Z_1, Z_1 > \eta + \gamma_s w_1\big] - N\Pr\big[\min(\tilde{u}_1, v_1) \geq \eta + \gamma_s w_1, Z_1 < \eta + \gamma_s w_1\big]$$

$$= 1 - N\int_0^\infty \int_{\eta+\gamma_s w}^\infty \int_z^\infty \int_z^\infty f_{\tilde{u}_1}(\tilde{u}) f_{v_1,w_1}(v,w) \times f_{Z_1}(z) dz d\tilde{u} dv dw - N\int_0^\infty \int_0^{\eta+\gamma_s w} \int_{\eta+\gamma_s w}^\infty \int_{\eta+\gamma_s w}^\infty f_{\tilde{u}_1}(\tilde{u}) f_{v_1,w_1}(v,w) f_{Z_1}(z) dz d\tilde{u} dv dw. \tag{21}$$

In order to solve the integral in (21), we need to provide the PDFs of $f_{v_1,w_1}(v,w)$, $f_{\tilde{u}_1}(\tilde{u})$ and $f_{Z_1}(z)$. The PDF of $f_{v_1,w_1}(v_1,w_1)$ can be represented in the form of infinite series as [30]

$$f_{v_1,w_1}(v,w) = \sum_{q=0}^{\infty} b_{0q} v^q w^q e^{-b_1 v} e^{-b_2 w}, \tag{22}$$

with

$$b_{0q} = \frac{\rho^q}{(1-\rho)^{2q+1}(\beta\varepsilon)^{q+1}(q!)^2}, \tag{23}$$

$$b_1 = \frac{1}{(1-\rho)\beta}, \quad b_2 = \frac{1}{(1-\rho)\varepsilon}. \tag{24}$$

In [30], it was proved that this series converges, since the error after the truncation is exponentially bounded. Next, we use the first T terms in (22), where T is selected in order to ensure that the truncation error is lower than a very small certain value $e(T)$.

From (17), we now provide the CDF and PDF of $\tilde{u}_1$ as [32]

$$F_{\tilde{u}_1}(\tilde{u}) = (1 - e^{-\frac{\tilde{u}}{\tilde{\alpha}}})^M, \tag{25}$$

and

$$f_{\tilde{u}_1}(\tilde{u}) = \frac{d}{d\tilde{u}} F_{\tilde{u}_1}(\tilde{u}) = \sum_{m=1}^{M} \binom{M}{m} (-1)^{m-1} \frac{m}{\tilde{\alpha}} e^{-\frac{m\tilde{u}}{\tilde{\alpha}}}, \tag{26}$$

respectively, where $\tilde{\alpha} = \frac{\gamma_s}{\gamma_s-1}\alpha$. From (20), the CDF of Z_1 is written as

$$F_{Z_1}(z) = \big[\Pr[\min(\tilde{u}_1, v_1) < z]\big]^{N-1} = \big[1 - F_{\tilde{u}_1}(z)F_{v_1}(z)\big]^{N-1} = \big[1 - e^{-\frac{z}{\beta}}(1-(1-e^{-\frac{z}{\tilde{\alpha}}})^M)\big]^{N-1}. \tag{27}$$

By using the binomial expansion, we write the PDF of Z_1 as

$$f_{Z_1}(z) = \frac{d}{dz} F_{Z_1}(z) = \widetilde{\sum_{\{i\}}} c_{1i} c_{2i} e^{-c_{2i} z}, \tag{28}$$

with

$$\widetilde{\sum_{\{i\}}} = \sum_{i_1=0}^{N-1} \sum_{i_2=0}^{i_1} \cdots \sum_{i_M=0}^{i_{M-1}}, \tag{29}$$

$$c_{1i} = (-1)^{i_1+\cdots+i_M} \binom{N-1}{i_1} \binom{i_1}{i_2} \cdots \binom{i_{M-1}}{i_M} \left(\binom{M}{1}\right)^{i_1-i_2} \times \left(\binom{M}{2}\right)^{i_2-i_3} \cdots \left(\binom{M}{M-1}\right)^{i_{M-1}-i_M}, \tag{30}$$

and

$$c_{2i} = \frac{i_1+\cdots+i_M}{\tilde{\alpha}} + \frac{i_1}{\beta}. \tag{31}$$

Since the Fubini-Tonelli theorem holds, we can exchange the summation and integration, by applying the PDFs of $f_{v_1,w_1}(v,w)$, $f_{\tilde{u}_1}(\tilde{u})$ and $f_{Z_1}(z)$ into (21), and thus, to solve

the resultant integral. Finally, we obtain the analytical approximation for the secrecy outage probability for the full relay selection criterion as

$$\mathcal{P}_{out,\mathsf{Full}} \approx 1 - \sum_{m=1}^{M}\sum_{q=0}^{T}\sum_{k=0}^{q}\sum_{j_1=0}^{k}\sum_{j_2=0}^{j_1}\widetilde{\sum_{\{i\}}}\theta_{1,mqkj_1j_2i}L_{q+j_2}(b_2 + b_3\gamma_s)e^{-b_3\eta} - \sum_{m=1}^{M}\sum_{q=0}^{T}\sum_{k=0}^{q}\sum_{j=0}^{k}\widetilde{\sum_{\{i\}}}\theta_{2,mqkji} \times L_{q+j}(b_2 + b_3\gamma_s)e^{-b_3\eta}, \tag{32}$$

with $L_n(x) = n!x^{-(n+1)}$,

$$\theta_{1,mqkj_1j_2i} = N\binom{M}{m}\binom{j_1}{j_2}\frac{q!}{j_1!}(-1)^{m-1}\frac{b_{0q}c_{1i}c_{2i}\eta^{j_1-j_2}\gamma_s^{j_2}}{b_1^{q-k+1}b_3^{k-j_1+1}}, \tag{33}$$

$$b_3 = b_1 + c_{2i} + \frac{m}{\tilde{\alpha}}, \tag{34}$$

and

$$\theta_{2,mqkji} = N\binom{M}{m}\binom{k}{j}\frac{q!}{k!}(-1)^{m-1}\frac{b_{0q}c_{1i}\eta^{k-j}\gamma_s^{j}}{b_1^{q-k+1}}. \tag{35}$$

Note that the derived analytical approximation in (32) consists of elementary functions only. Hence it is easily to be evaluated.

B. Analytical approximation for the SOP in partial relay selection

According to the partial relay selection criterion in (13), we write the lower bound on the secrecy outage probability as

$$\begin{aligned}\mathcal{P}_{out,\mathsf{Partial}}^{\mathsf{LB}} &= \Pr\Big[\min\big(\frac{\gamma_s}{\gamma_s-1}u_{m^*n^*}, v_{n^*}\big) < \eta + \gamma_s w_{n^*}\Big] \\ &= \sum_{n=1}^{N}\Pr\Big[\min\big(\tilde{u}_n, v_n\big) < \eta + \gamma_s w_n, \\ &\qquad v_n > \max_{k=1,\cdots,N,k\neq n} v_k\Big].\end{aligned} \tag{36}$$

Due to symmetry among N relays, we further write $\mathcal{P}_{out,\mathsf{Partial}}^{\mathsf{LB}}$ as

$$\begin{aligned}\mathcal{P}_{out,\mathsf{Partial}}^{\mathsf{LB}} &= N\Pr\Big[\min\big(\tilde{u}_1, v_1\big) < \eta + \gamma_s w_1, v_1 > Z_2\Big] \\ &= N\Pr[v_1 > Z_2] - N\Pr\Big[\min\big(\tilde{u}_1, v_1\big) \geq \\ &\qquad \eta + \gamma_s w_1, v_1 > Z_2\Big],\end{aligned} \tag{37}$$

where

$$Z_2 = \sum_{k=2,\cdots,N} v_k, \tag{38}$$

and its PDF is given by [32]

$$f_{Z_2}(z) = \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^{n-1}\frac{n}{\beta}e^{-\frac{nz}{\beta}}. \tag{39}$$

Since $\Pr[v_1 > Z_2] = \frac{1}{N}$, we can compute $\mathcal{P}_{out,\mathsf{Partial}}^{\mathsf{LB}}$ as

$$\begin{aligned}\mathcal{P}_{out,\mathsf{Partial}}^{\mathsf{LB}} &= 1 - N\Pr\Big[\min\big(\tilde{u}_1, v_1\big) \geq \eta + \gamma_s w_1, v_1 > Z_2\Big] \\ &= 1 - N\int_0^\infty\int_{\eta+\gamma_s w}^\infty\int_{\eta+\gamma_s w}^\infty\int_0^z f_{\tilde{u}_1}(\tilde{u}) \\ &\quad \times f_{v_1,w_1}(v,w)f_{Z_2}(z)dzdvdwd\tilde{u}.\end{aligned} \tag{40}$$

By following the same way as above and by applying the PDFs of $f_{\tilde{u}_1}(\tilde{u})$ in (26), $f_{v_1,w_1}(v,w)$ in (22) and $f_{Z_2}(z)$ in (39) into (40), and solving the resultant integral, we obtain the analytical approximation for the secrecy outage probability for the partial relay selection criterion as

$$\mathcal{P}_{out,\mathsf{Partial}} \approx 1 - \sum_{m=1}^{M}\sum_{n=0}^{N-1}\sum_{q=0}^{T}\sum_{k=0}^{q}\sum_{j=0}^{k}\theta_{3,mnqkj}L_{q+j}(b_2 + b_4\gamma_s)e^{-b_4\eta}, \tag{41}$$

with

$$\theta_{3,mnqkj} = N\binom{M}{m}\binom{N-1}{n}\binom{k}{j}(-1)^{m-1}\frac{q!}{k!}\frac{b_{0q}\eta^{k-j}\gamma_s^{j}}{(b_1+\frac{n}{\beta})^{q-k+1}}, \tag{42}$$

and

$$b_4 = b_1 + \frac{m}{\tilde{\alpha}} + \frac{n}{\beta}. \tag{43}$$

Note that the analytical approximation for the secrecy outage probability in (41) is tight and composed of elementary functions only. As such, it is easy to use to evaluate the secrecy outage probability for the partial relay selection criterion.

C. Asymptotic SOP for full relay selection

To obtain useful insights into the network performance achieved by the full relay selection criterion, we now present the asymptotic SOP from the lower bound. When the transmit power P is large, we approximate the SOP of the full relay selection from (15) as

$$\mathcal{P}_{out,\mathsf{Full}} \simeq \Pr[\min(\tilde{u}_{n^*}, v_{n^*}) < \gamma_s w_{n^*}]. \tag{44}$$

For the full relay selection criterion in (12), the asymptotic CDFs of $\tilde{u}_{n^*}$ and v_{n^*} are given by [18]

$$F_{\tilde{u}_{n^*}}(x) \simeq \begin{cases}\big(1+\frac{\tilde{\alpha}}{\beta}\big)^{N-1}\big(\frac{x}{\tilde{\alpha}}\big)^N, & \text{If } M=1 \\ \frac{MN}{M+N-1}\frac{x^{M+N-1}}{\tilde{\alpha}^M\beta^{N-1}}, & \text{If } M\geq 2\end{cases}, \tag{45}$$

$$F_{v_{n^*}}(x) \simeq \begin{cases}\big(1+\frac{\tilde{\alpha}}{\beta}\big)^{N-1}\frac{\tilde{\alpha}}{\beta}\big(\frac{x}{\tilde{\alpha}}\big)^N, & \text{If } M=1 \\ \big(\frac{x}{\beta}\big)^N, & \text{If } M\geq 2\end{cases}. \tag{46}$$

From these two equations, we can rewrite the asymptotic $\mathcal{P}_{out,\mathsf{Full}}$ as

$$\begin{aligned}\mathcal{P}_{out,\mathsf{Full}} &\simeq 1-\Pr[\min(\tilde{u}_{n^*},v_{n^*})\geq\gamma_s w_{n^*}]\\ &=1-\int_0^\infty\int_0^\infty[1-F_{\tilde{u}_{n^*}}(\gamma_s w_{n^*})][1-F_{v_{n^*}}(\gamma_s w_{n^*})]dw_{n^*}v_{n^*}\\ &\simeq\int_0^\infty\int_0^\infty F_{v_{n^*}}(\gamma_s w_{n^*})+F_{\tilde{u}_{n^*}}(\gamma_s w_{n^*})dw_{n^*}v_{n^*}\\ &=\Pr(v_{n^*}<\gamma_s w_{n^*})+\Pr(\tilde{u}_{n^*}<\gamma_s w_{n^*}).\end{aligned}\tag{47}$$

We first calculate $\Pr(v_{n^*}<\gamma_s w_{n^*})$ with $M\geq 2$. Similar to [28], we use θ to denote v_{n^*}/w_{n^*} and derive its PDF as

$$f_\theta(\theta)=\int_0^\infty w f_{v_{n^*},w_{n^*}}(w\theta,w)dw\tag{48}$$

$$=\sum_{n=1}^{N}\binom{N}{n}\frac{n(-1)^{n-1}}{\beta\varepsilon(1-\rho)}\frac{\frac{n\theta}{\beta}+(\frac{\rho\theta}{\beta}+\frac{1}{\varepsilon})\frac{1}{1-\rho}}{\left[\left(\frac{n\theta}{\beta}+(\frac{\rho\theta}{\beta}+\frac{1}{\varepsilon})\frac{1}{1-\rho}\right)^2-\frac{4\rho\theta}{(1-\rho)^2\beta\varepsilon}\right]^{3/2}},\tag{49}$$

where [31, eq.(6.623.2)] is used in the last equality. Let $\lambda=\frac{\beta}{\varepsilon}$, and for the high MER, we approximate $f_\theta(\theta)$ as

$$f_\theta(\theta)=\sum_{n=1}^{N}\binom{N}{n}\frac{(-1)^{n-1}(1-\rho)\lambda}{[\lambda+n(1-\rho)\theta+\rho\theta]^2}.\tag{50}$$

From (50), we compute $\Pr(v_{n^*}<\gamma_s w_{n^*})$ as

$$\Pr(v_{n^*}<\gamma_s w_{n^*})=\int_0^{\gamma_s}f_\theta(\theta)d\theta\tag{51}$$

$$\simeq N!\Big(\frac{(1-\rho)\gamma_s}{\lambda}\Big)^N,\tag{52}$$

where we apply the approximation of $(1+x)^{-1}\simeq\sum_{k=0}^{N}(-1)^k x^k$ [31]. Since the asymptotic CDFs of $\tilde{u}_{n^*}$ and v_{n^*} have the same form of power function, we can compute $\Pr(v_{n^*}<\gamma_s w_{n^*})$ with $M=1$ and $\Pr(\tilde{u}_{n^*}<\gamma_s w_{n^*})$, in a similar way. By summarizing these results, we obtain the asymptotic SOP achieved by the full relay selection with high MER as

$$\mathcal{P}_{out,\mathsf{Full}}\simeq\begin{cases}\frac{\gamma_s^N N!}{\lambda^N}\big(1+\frac{\beta}{\tilde{\alpha}}\big)^{N-1}\Big(\frac{\beta}{\tilde{\alpha}}+(1-\rho)^N\Big), & \text{If } M=1\\ \frac{\gamma_s^N N!}{\lambda^N}(1-\rho)^N, & \text{If } M\geq 2\end{cases}.\tag{53}$$

From the asymptotic result in (53), we can obtain useful insights into the network secrecy performance, as follows:

Remark 1: The secrecy diversity order is N, indicating that the secrecy performance achieved by the full relay selection criterion can be rapidly improved by increasing the number of relays.

Remark 2: The asymptotic SOP decreases when ρ increases, indicating that the channel correlation between the main and eavesdropper's links enhances the secure transmission facilitated by the full relay selection criterion. This is because that when the channel correlation coefficient increases, the channel fluctuation of the second-hop main link becomes more similar to that of the eavesdropper's link, which helps prevent the wiretap in the high MER regime. Hence, the network secrecy performance can be improved with larger ρ for the full relay selection.

Remark 3: For multiple antennas at the BS with $M\geq 2$, the first hop does not affect the secure transmission, and only the second hop affects the secrecy performance. Hence, increasing the number of antennas at the BS does not profoundly improve the secrecy performance, achieved by the full relay selection criterion.

D. Asymptotic SOP for partial relay selection

In this subsection, we derive an asymptotic expression for the SOP, when the partial relay selection criterion is used, in order to provide some useful insights in the network performance. Assuming large transmit power P, the SOP achieved by the partial relay selection criterion can be approximated as

$$\mathcal{P}_{out,\mathsf{Partial}}\simeq\Pr[\min(\tilde{u}_{n^*},v_{n^*})<\gamma_s w_{n^*}]\tag{54}$$

$$\simeq\Pr(\tilde{u}_{n^*}<\gamma_s w_{n^*})+\Pr(v_{n^*}<\gamma_s w_{n^*}).\tag{55}$$

Note that from the partial relay selection criterion in (13), we can obtain the asymptotic CDF of v_{n^*} as

$$F_{v_{n^*}}(x)\simeq\big(\frac{x}{\beta}\big)^N.\tag{56}$$

Hence, according to (52), we compute $\Pr(v_{n^*}<\gamma_s w_{n^*})$ as

$$\Pr(v_{n^*}<\gamma_s w_{n^*})\simeq N!\Big(\frac{(1-\rho)\gamma_s}{\lambda}\Big)^N.\tag{57}$$

Now we turn to calculate $\Pr(\tilde{u}_{n^*}<\gamma_s w_{n^*})$ as

$$\begin{aligned}\Pr(\tilde{u}_{n^*}<\gamma_s w_{n^*})&=N\Pr(\tilde{u}_1<w_1,v_1>Z_2)\\ &=N\int_0^\infty\int_0^\infty F_{Z_2}(v_1)F_{\tilde{u}_1}(w_1)\\ &\quad\times f_{v_1,w_1}(v_1,w_1)dv_1dw_1\\ &\simeq NM!\zeta_{MN}\frac{\big((\gamma_s-1)\frac{\beta}{\alpha}\big)^M}{\lambda^M},\end{aligned}\tag{58}$$

where [31, eq. (6.614.3)] and the series approximation of $(1+x)^{-1}\simeq\sum_{k=0}^{M}(-1)^k x^k$ are applied in the last equality, and ζ_{MN} is given by

$$\zeta_{MN}=\sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n\frac{(1+n(1-\rho))^M}{(1+n)^{M+1}}.\tag{59}$$

Summarizing the results in (57) and (59), we obtain the asymptotic SOP achieved by the partial relay selection criterion as

$$\mathcal{P}_{out,\mathsf{Partial}}\simeq NM!\zeta_{MN}\frac{\big((\gamma_s-1)\frac{\beta}{\alpha}\big)^M}{\lambda^M}+N!\frac{(\gamma_s(1-\rho))^N}{\lambda^N},\tag{60}$$

From (60), we conclude the following insights into the network performance:

Remark 1: The secrecy diversity order is $\min(M,N)$. In particular, when $M<N$, the first hop becomes the bottleneck of the secrecy performance of the network. On the contrary, when $M>N$, the second hop limits the secrecy performance of the network.

Remark 2: The impact of the channel correlation between main and eavesdropper's links on the secrecy performance

depends on the relationship between M and N. Specifically, when $M > N$, the second term of the asymptotic $\mathcal{P}_{out,\text{Partial}}$ dominates, and hence the channel correlation is beneficial to the secrecy performance of the network. On the contrary, when $M < N$, the first term of the asymptotic $\mathcal{P}_{out,\text{Partial}}$ dominates. Since ζ_{MN} increases slightly with larger ρ, the channel correlation is detrimental to the secrecy performance of the network achieved by the partial relay selection criterion when $M < N$. This is because that when the channel correlation coefficient increases, the channel fluctuation of the second-hop main link becomes more similar to that of the eavesdropper's link, which helps prevent the wiretap in the high MER regime. Hence the network secrecy performance can be improved with larger ρ for the partial relay selection with $M > N$. However, for the partial relay selection with $M < N$, we can find from *Remark 1* that the first relay hop becomes the bottleneck of the network security, and increasing ρ helps strengthen the eavesdropper's link, which conversely deteriorates the network security. Accordingly, it would be recommended to increase ρ for the partial relay selection criterion when $M > N$, but decrease ρ when $M < N$.

From the above analysis, we can find that the full relay selection criterion is better than the partial relay selection criterion in the secrecy performance, but it needs more implementation complexity. Hence, the work in this paper provides a flexible choice for the practical system design: the full relay selection is preferred to obtain a better secrecy performance; while the partial relay selection is adopted to reduce the complexity.

IV. Simulations and Numerical Results

In this section, we provide simulations and numerical examples to validate the derived analytical results. All links in the network undergo Rayleigh fading, and the path-loss channel model is adopted, with the loss factor equal to 4. Without loss of generality, the distance between the BS and receiver D is normalized to unity. Let d denote the distance between the BS and relays, so that $\alpha = d^{-4}$ and $\beta = (1-d)^{-4}$. The secrecy date rate R_s is set to 0.5 bps/Hz, so that $\gamma_s = 2$. To accurately compute the analytical approximations in (32) and (41), we set the exponentially bounded truncation error to a small value of 10^{-10}, leading to that $T = \text{round}\big(\frac{-10}{\log_{10}\rho}\big)$. Accordingly, only the first T terms are kept in the analytical approximations.

Figs. 2 and 3 demonstrate the secrecy outage probability achieved by the full and partial relay selection criteria versus the transmit SNR $\tilde{P}$, where $d = 0.5$, $\lambda = 20$ dB, $M = 3$ and N varies from 1 to 3. Specifically, Figs. 2 and 3 correspond to the full and partial relay selection, respectively. To show how close the analytical approximation approaches to the exact value, we also present the simulated results of (15) and (36) for the full and partial relay selection, respectively. Several cases of channel correlation are investigated, with $\rho = 0.3, 0.5$, and 0.7. As observed from these figures, the analytical approximation is close to the simulations, while the asymptotic curve converges to the exact one, when the transmit SNR is high. In particular, the proposed analytical approximation matches well with the simulated results of (15) and (36) for the full and partial relay selection, respectively. This validates the derived analytical approximation for the secrecy outage probability and the asymptotic expression for both criteria. Moreover, the SOP improves when ρ increases for different values of N, indicating that the channel correlation is beneficial to the secure transmission. Furthermore, the SOP becomes smaller when N increases, as more relays strengthen the secure transmission.

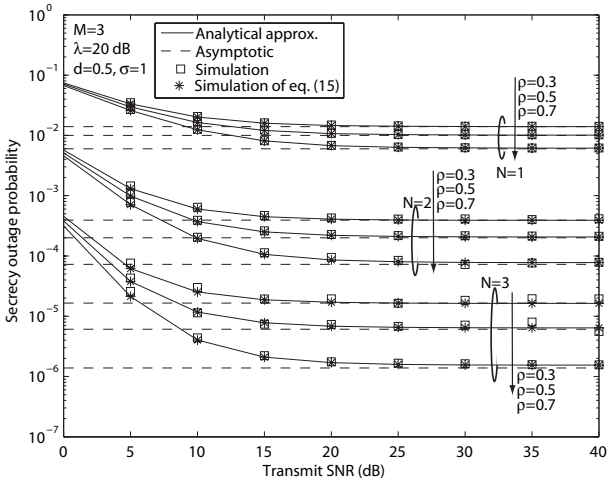

Fig. 2. Secrecy outage probability versus the transmit SNR $\tilde{P}$: Full relay selection

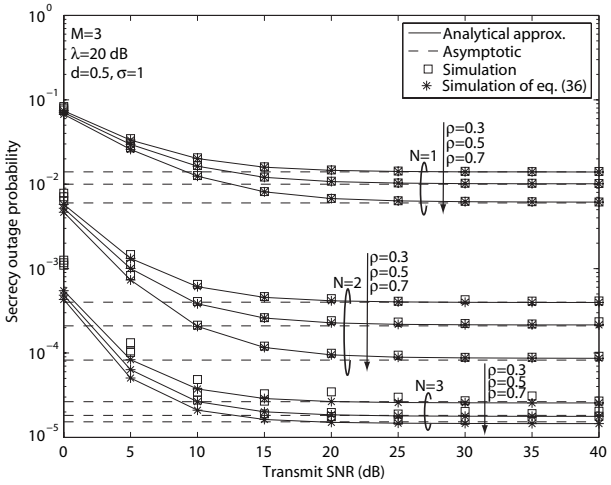

Fig. 3. Secrecy outage probability versus the transmit SNR $\tilde{P}$: Partial relay selection

Figs. 4 and 5 illustrates the effect of the number of relays on the secrecy outage probability achieved by both selection criteria versus MER, where $d = 0.5$, $P = 40$ dB, $M = 3$ and N varies from 1 to 3. We also consider $\rho = 0.3$, 0.5, and 0.7. Figs. 4 and 5 depict the full and partial relay selection, respectively. It is evident from these figures that for different values of N and ρ, the analytical approximation is an effective approximated result, especially with high MER, and the asymptotic result converges to the simulation one in the high MER regime. This shows the accuracy of the derived analytical approximation and the asymptotic results. Moreover, we find that the secrecy outage probability curves are in

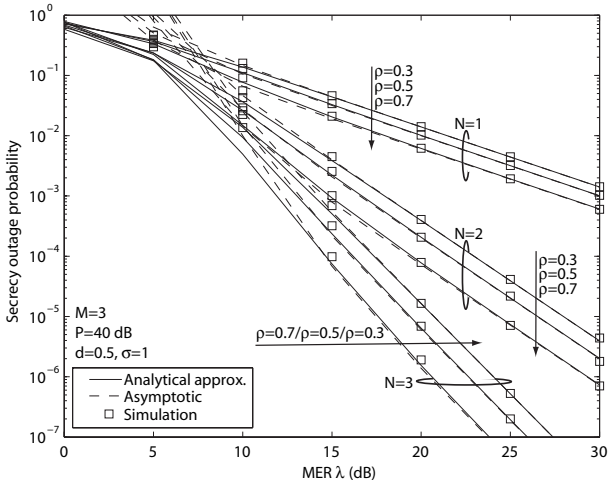

Fig. 4. Effect of relay number on the secrecy outage probability versus MER: Full relay selection

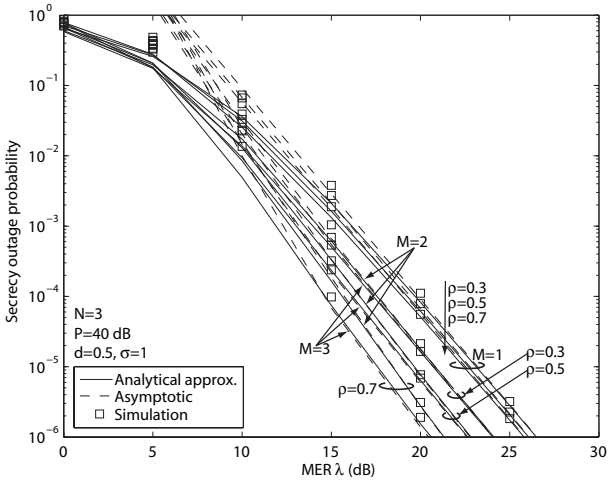

Fig. 6. Effect of antenna number on the secrecy outage probability versus MER: Full relay selection

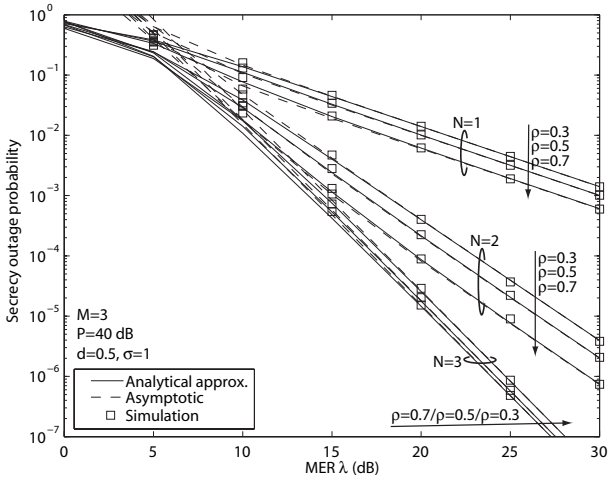

Fig. 5. Effect of relay number on the secrecy outage probability versus MER: Partial relay selection

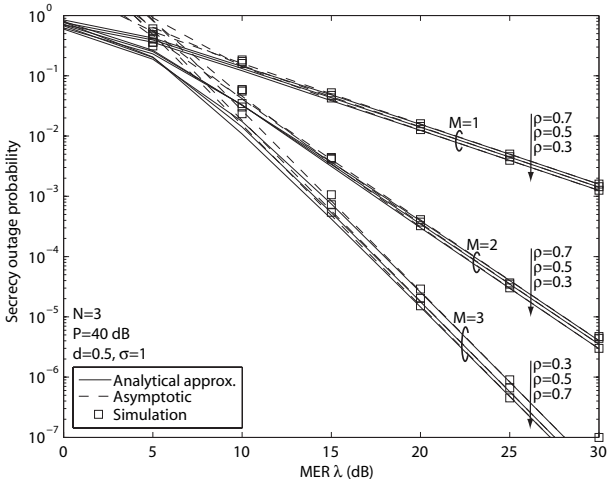

Fig. 7. Effect of antenna number on the secrecy outage probability versus MER: Partial relay selection

parallel with the number of relays, indicating that the secrecy diversity order of both selection criteria is equal to N when $M \geq N$. Furthermore, the secrecy outage probability achieved by both criteria improves with larger channel correlation or more relays, since the secure transmission can be enhanced by a larger ρ and a larger N.

Figs. 6 and 7 show the effect of number of BS antennas on the secrecy outage probability achieved by both relay selection criteria versus MER, where $d = 0.5$, $P = 40$ dB, $N = 3$ and M varies from 1 to 3. Again, we consider $\rho = 0.3$, 0.5, and 0.7. Figs. 6 and 7 address the full and partial relay selection, respectively. As observed from Fig. 6, the secrecy outage probability curves are in parallel with each other for different values of M, indicating that the secrecy diversity order of the full relay selection criterion depends on the number of relays only. In contrast, the secrecy outage probability curves in Fig. 7 are in parallel with M, and hence the secrecy outage probability achieved by the partial relay selection criterion is determined by the number of BS antennas. Moreover, the secrecy outage probability achieved by the full relay selection criterion improves with larger ρ, as the channel correlation is beneficial to the secrecy performance. On the contrary, the secrecy outage probability achieved by the partial relay selection criterion becomes worse with larger ρ when $M < N$, indicating that the channel correlation becomes detrimental to the secrecy performance when the partial relay selection criterion is adopted.

Figs. 8 and 9 depict the impact of channel correlation coefficient ρ on the secrecy outage probability achieved by both relay selection criteria, where $d = 0.5$, $P = 40$ dB, $\lambda = 20$dB, $M = 2$ and N varies 1 to 4. The channel correlation coefficient varies from 0 to 0.9. Figs. 8 and 9 concentrate on the full and partial relay selection, respectively. As observed from these two figures, we find that for the full relay selection criterion, the secrecy performance improves with larger channel correlation. In contrast, for the partial relay selection criterion, the secrecy outage probability improves with larger ρ if $M \geq N$; otherwise deteriorates. This phenomenon validates the insights gained from the asymptotic expression for the partial relay selection criterion in (60). Moreover, the

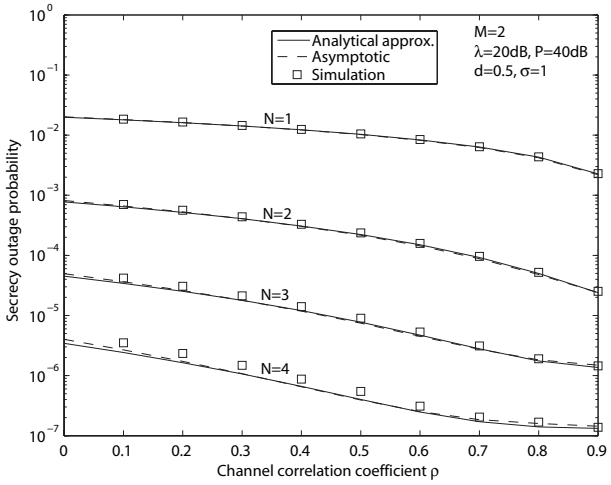

Fig. 8. Impact of channel correlation efficient on the secrecy outage probability: Full relay selection

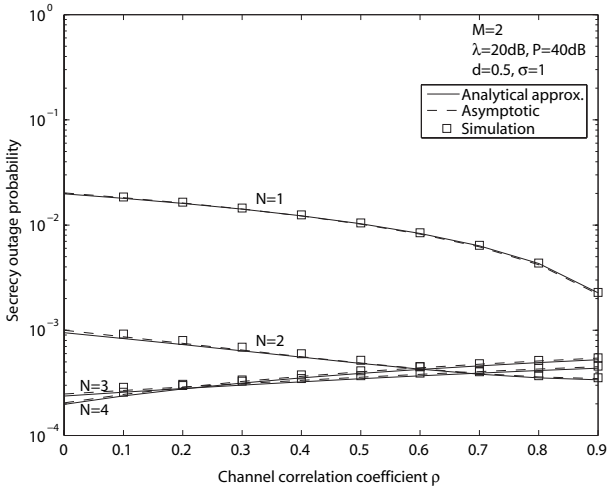

Fig. 9. Impact of channel correlation efficient on the secrecy outage probability: Partial relay selection

analytical approximation for the SOP and the asymptotic result match well with the simulation result for different values of N and ρ, which further verifies the effectiveness of the derived results for both relay selection criteria.

V. Conclusions

In this paper, we investigated the impact of correlated fading channels on the performance of secure AF relaying, where the M-antenna BS adopts TAS to transmit its signal to the destination with the best relay out of N relays. The eavesdropper overhears the message from the relays, and the main and eavesdropper's channels were assumed correlated. Apart from TAS at the BS, we addressed both the full and partial relay selection criteria for secrecy enhancement. For both criteria, we analyzed the network secrecy performance by deriving the analytical approximation for the SOP and its asymptotic expression with high MER. From the asymptotic expression, we conclude that the channel correlation is beneficial to the secrecy performance achieved by the full relay selection criterion, but it degrades the secrecy performance achieved by the partial relay selection criterion when $M < N$. Furthermore, the secrecy diversity order of the full and partial relay selection criteria is equal to N and $\min(M, N)$, respectively. In the future work, we will investigate the communication scenario where the eavesdropper can also overhear the message from the BS. Since the direct eavesdropping links may be correlated with the main links, the performance evaluation will become much more complicated, and a new analytical framework needs to be developed.

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1948.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

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

[6] M. Z. I. Sarkar and T. Ratnarajah, "Secure communication through Nakagami-m fading MISO channel," in *IEEE Inter. Conf. on Commun. (ICC)*, Kyoto, Japan, 2011.

[7] X. Liu, "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel," *IEEE Wireless Commun. Lett.*, vol. 2, no. 1, pp. 50–53, Feb. 2013.

[8] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 861–867, Sept. 2011.

[9] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. Leung, "Physical layer security issues in interference-alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, 2016.

[10] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. PP, pp. 1–12, to appear in 2017.

[11] H. Xie, F. Gao, and S. Jin, "An overview of low-rank channel estimation for massive MIMO systems," *IEEE Trans. Veh. Technol.*, vol. 4, pp. 7313–7321, Nov. 2016.

[12] H. Xie, B. Wang, F. Gao, and S. Jin, "A full-space spectrum-sharing strategy for massive MIMO cognitive radio," *IEEE J. Select. Areas Commun.*, vol. 34, no. 10, pp. 2537–2549, Oct. 2016.

[13] H. Alves, R. DemoSouza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Sig. Proc. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[14] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[15] S. Jin, M. R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward MIMO dual-hop systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2204–2224, May 2010.

[16] S. Jin, X. Liang, K.-K. Wong, X. Gao, and Q. Zhu, "Ergodic rate analysis for multipair massive MIMO two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 3, no. 14, pp. 1480–1491, Mar. 2015.

[17] L. Fan, X. Lei, R. Q. Hu, and W. Seah, "Outdated relay selection in two-way relay network," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4051–4057, Oct. 2013.

[18] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299–3310, Sept. 2014.

[19] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with co-channel interference," *IEEE Journal of Sel. Topics in Sig. Proc.*, vol. 10, no. 8, pp. 1494–1505, Dec. 2016.

[20] V. N. Q. Bao, N. L. Trung, and M. Debbah, "Relay selection scheme for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[21] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
[22] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787–1791, Oct. 2010.
[23] L. Fan, S. Zhang, T. Q. Duong, and G. K. Karagiannidis, "Secure switch-and-stay combining (SSSC) for cognitive relay networks," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 70–82, Jan. 2016.
[24] 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.
[25] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.
[26] W. C.-Y. Lee, "Effects on correlation between two mobile radio base-station antennas," *IEEE Trans. Commun.*, vol. COM-21, pp. 1214–1224, Nov. 1973.
[27] S. B. Rhee and G. I. Zysman, "Results of suburban base-station spatial diversity measurements on the UHF bands," *IEEE Trans. Commun.*, vol. COM-22, pp. 1630–1634, Oct. 1974.
[28] D.-S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Trans. Commun.*, vol. 48, pp. 502–513, Mar. 2000.
[29] 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. 4005–4019, Apr. 2011.
[30] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Sig. Proc. Lett.*, vol. 19, no. 8, pp. 479–482, Aug. 2012.
[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.
[32] M. K. Simon and M. S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. John Wiley, 2005.