Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels

Lisheng Fan, Xianfu Lei, Nan Yang, *Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—In this paper, we study the impact of correlated fading on the secrecy performance of multiple decode-and-forward (DF) relaying with outdated relay selection. It is assumed that the information transmission, assisted by N DF relays from the source to the destination, can be overheard by an eavesdropper. Particularly, we consider the realistic scenario where the eavesdropper's and the main channels are correlated. In order to enhance the network security, the best relay is selected among N available DF relays to assist the secure transmission. Due to the time-varying channel environments, we note that the selected relay may be outdated. In order to study the impact of both channel correlation and outdated relay selection on the secrecy performance, we first derive an analytical expression for the secrecy outage probability (SOP). Also, we derive the asymptotic expression for the SOP in the high main-to-eavesdropper ratio (MER) regime. Numerical results are provided to demonstrate the correctness of our analytical expressions.**

***Index Terms*—Secure communications, correlated fading channels, outdated relay selection, secrecy diversity order.**

I. Introduction

Due to the broadcast nature, wireless transmission may be overheard by eavesdroppers in the network, and the severe issue of information leakage arises [1]. To prevent the wiretap, encryption algorithms and the concept of physical-layer security (PLS) have been presented in the literature. Specifically, in the pioneering work of Wyner [2], the wiretap channel model was firstly proposed. Several researchers extended this approach to fading channels and studied important metrics, such as the secrecy capacity and the secrecy outage probability (SOP) [3]–[7]. Furthermore, as relaying is a promising technique for the next-generation communication networks, it is of vital importance to investigate the PLS of relaying systems. For amplify-and-forward (AF) and decode-and-forward (DF) relaying, the secrecy performance has been studied by deriving analytical expression of SOP in [8]–[10]. Moreover, the asymptotic SOP with high main-to-eavesdropper ratio (MER) was provided, in order to obtain insights on the system design.

In most of the works in the open literature, the eavesdropping and the main channels are assumed to be statistically independent. However, this ideal assumption may not hold in practice due to reasons such as antenna deployment, proximity of the legitimate receiver and eavesdropper, and scattering environments. The impact of channel correlation between the main and eavesdropping links on the secrecy performance was studied in [11], [12], where it was found that the channel correlation is harmful to the transmission security, especially in the low MER region. In order to enhance the security, opportunistic selection is an effective technique, which exploits the channel fluctuation between antennas, users and relays [9], [13]. The selection can be implemented in a centralized or distributed manner through dedicated feedback links, which may take some time to complete. However, in time-varying environments, channels may vary from the instant of selection to that of actual data transmission. This results in the selection based on outdated channel state information (CSI) [14] and the best relay is not always selected [15], [16].

In this paper, we investigate the PLS of multi-relay networks, assuming channel correlation between the main and eavesdropping links. The information transmission, assisted by N DF relays from the source to the destination, may be overheard by the eavesdropper in the network. To strengthen the secure transmission, the best relay is selected among N relays, which is however based on the outdated CSI in time-varying channel environments. We study the impact of both channel correlation and outdated relay selection by deriving the analytical and asymptotic expressions for the SOP. From the asymptotic result, we find that the secrecy diversity order is equal to the number of relays N, only if perfect CSI is assumed; otherwise it becomes unity. Moreover, the channel correlation does not affect the secrecy diversity order, but it can

L. Fan is with the School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710126, China (e-mail: sfan@gzhu.edu.cn).

X. Lei is with the Provincial Key Lab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, and also with National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: xflei@home.swjtu.edu.cn).

N. Yang is with Australian National University, Canberra ACT 0200, Australia (e-mail: yangnan1616@gmail.com).

T. Q. Duong is with Queen's University Belfast, Belfast BT7 1NN, United Kingdom (e-mail: trung.q.duong@qub.ac.uk).

G. K. Karagiannidis is with the Provincial Key Lab of Information Coding and Transmission, Southwest Jiaotong University, and is also with Aristotle University of Thessaloniki, Thessaloniki 54 124, Greece (e-mail: geokarag@auth.gr).

This work was supported by the NSF of China (No. 61372129/61501382), by the Guangdong Natural Science Funds for Distinguished Young Scholar under Grant 2014A030306027, by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, by the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2017D15), by the open research fund of State Key Laboratory of Integrated Services Networks under Grant ISN17-05, by the Fundamental Research Funds for the Central Universities (No. 2682015RC20 & 2682016CY22), and by Sichuan Provincial International Science & Technology Cooperation and Exchanges Research Program (No. 2017HH0035). The work of N. Yang was supported by the Australian Research Council Discovery Project under Grant DP150103905.

Manuscript received July, 15, 2016; revised December, 16, 2016.

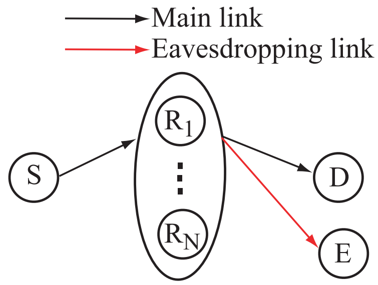

Fig. 1. A two-phase secure multiple DF relaying network.

strengthen the secure transmission in the high MER region.

Notations: $\mathcal{CN}(0,\sigma^2)$ denotes a circularly symmetric complex Gaussian random variable (RV) with zero mean and variance σ^2. We use $f_X(\cdot)$ to represent the probability density function (PDF) of the RV X. In addition, $I_0(x)$ is the modified Bessel function of the first kind of order zero [17], $\Pr[\cdot]$ returns the probability. We use $h_{A,B}$ to denote the channel parameter of the A–B link.

II. System Model

Fig. 1 shows the system model of a two-phase secure multiple DF relays network, where the information transmission from the source, S, to the destination, D, can be overheard by the eavesdropper, E. When S is far from D and E, the direct links are hard to be established, due to severe shadowing. Thus, the data communication can only be performed through the relaying links. There are no direct links from S to D and E, and the information transmission are only performed through the N relays $\{R_n|1\le n\le N\}$. The best relay is chosen among N available relays to assist the secure transmission. However, the selection may be outdated in time-varying channel environments, and the best relay is not always chosen. In addition, due to reasons such as antenna deployment and radio scattering, the channels at the receivers D and E are correlated, i.e., $h_{R_n,D}$ is correlated with $h_{R_n,E}$. Due to the size limitation, the nodes in the network are equipped with only one antenna, and all links experience time-varying Rayleigh fading. In what follows, we discuss the two-phase secure data transmission process and the relay selection criterion for the considered system.

Suppose that the relay, R_n, is used for the two-phase secure data transmission. In the first phase, S transmits the signal, x_S, to R_n with transmit power P. The R_n receives,

$$y_{R_n}=\sqrt{P}h_{S,R_n}x_S+n_{R_n}, \tag{1}$$

where $h_{S,R_n}\sim\mathcal{CN}(0,\alpha)$ denotes the channel coefficient of the S–R_n link, and $n_{R_n}\sim\mathcal{CN}(0,\sigma^2)$ is the additive white Gaussian noise (AWGN) at the relay R_n. If the relay, R_n, can correctly decode the message from the source, i.e., it can support a target data rate,

$$R_t\le\frac{1}{2}\log_2\left(1+\frac{P|h_{S,R_n}|^2}{\sigma^2}\right). \tag{2}$$

Then, the relay in the second phase forwards the message to D with transmit power P. Accordingly, D and E receive,

$$y_D=\sqrt{P}h_{R_n,D}x_S+n_D, \tag{3}$$

$$y_E=\sqrt{P}h_{R_n,E}x_S+n_E, \tag{4}$$

where $h_{R_n,D}\sim\mathcal{CN}(0,\beta_1)$ and $h_{R_n,E}\sim\mathcal{CN}(0,\beta_2)$ are the channel coefficients of the R_n–D and R_n–E links, respectively. Accordingly, the average channel gains of $h_{R_n,D}$ and $h_{R_n,E}$ are represented by β_1 and β_2, respectively. The noise terms $n_D\sim\mathcal{CN}(0,\sigma^2)$ and $n_E\sim\mathcal{CN}(0,\sigma^2)$ are the AWGN at D and E, respectively.

We use $u_n=|h_{S,R_n}|^2$, $v_n=|h_{R_n,D}|^2$ and $w_n=|h_{R_n,E}|^2$ to represent the channel gains of the S–R_n, R_n–D and R_n–E links, respectively. The secrecy outage occurs when the data rate difference between the main and eavesdropping links falls below a target secrecy data rate R_s, i.e.,

$$\frac{1}{2}\log_2\left(1+\frac{P}{\sigma^2}v_n\right)-\frac{1}{2}\log_2\left(1+\frac{P}{\sigma^2}w_n\right)<R_s, \tag{5}$$

which is equivalent to

$$\frac{1+\tilde{P}v_n}{1+\tilde{P}w_n}<\gamma_s, \tag{6}$$

where $\tilde{P}=P/\sigma^2$ denotes the transmit SNR, and $\gamma_s=2^{2R_s}$ is the secrecy SNR threshold.

To enhance the transmission security, we select the best relay to strengthen the secure data transmission. Let Ω denote the candidate set of relays that can successfully decode the message from the source. Then based on the main channels only[1], the relay selection is performed to choose the best relay R_{n^*} among Ω,

$$n^*=\arg\max_{n\in\Omega}v_n, \tag{7}$$

which maximizes the received SNR at the destination D.

III. Channel Correlation and Outdated Relay Selection

In this work, we consider correlated channels between the receiver D and E, which is characterized by the conditional PDF [12]

$$f_{w_n|v_n}(w|v)=\frac{I_0\left(\frac{2}{1-\rho}\sqrt{\frac{\rho vw}{\beta_1\beta_2}}\right)}{(1-\rho)\beta_1\beta_2}e^{-\frac{\frac{\rho v}{\beta_1}+\frac{w}{\beta_2}}{1-\rho}}, \tag{8}$$

where $\rho\in[0,1]$ is the power correlation coefficient. Specifically, for $\rho=0$, v_n is independent of w_n, while for $\rho=1$, completely linear correlation is assumed.

Besides the channel correlation, the outdated relay selection has a significant impact on the network security. In practice, the selection of (7) can be implemented in a distributed or centralized manner, through some dedicated feedback channels [9]. However, due to the limited feedback resources, the channels may vary from the instant of relay selection to that of actual data transmission in time-varying channel environments.

[1]The instantaneous channel parameters of eavesdropping links are not involved in the relay selection criterion, since they are generally hard to obtain in practice.

Let $\tilde{v}_{n^*}$ and v_{n^*} denote the channels of R_{n^*}–D at the instants of relay selection and actual data transmission, respectively. The outdated selection can be characterized by the conditional PDF $f_{v_{n^*}|\tilde{v}_{n^*}}(v|\tilde{v})$ [14],

$$f_{v_{n^*}|\tilde{v}_{n^*}}(v|\tilde{v}) = \frac{1}{(1-\eta)\beta_1} e^{-\frac{\eta\tilde{v}+v}{(1-\eta)\beta_1}} I_0\Big(\frac{2\sqrt{\eta v\tilde{v}}}{(1-\eta)\beta_1}\Big), \quad (9)$$

where $\eta \in [0,1]$ represents the outdated degree of relay selection. In particular, $\eta = 1$ corresponds to the case where the selection is based on the perfect CSI, while $\eta = 0$ represents the completely outdated relay selection.

In the following, we will study the impact of channel correlation and outdated relay selection on the network secrecy performance, by providing the analytical and asymptotic expressions of secrecy outage probability.

IV. Secrecy Outage Probability

A. Analytical Expression

The set Ω may have $K(K = 1, 2, \cdots, N)$ candidates that can correctly decode the message from the source. Hence, we can express the SOP of the considered system as

$$\mathcal{P}_{out} = \sum_{K=1}^{N} \binom{N}{K} \Pr\Big[\tilde{P}u_1 \geq \gamma_t, \cdots, \tilde{P}u_K \geq \gamma_t, \tilde{P}u_{K+1} < \gamma_t, \cdots, \tilde{P}u_N < \gamma_t, \frac{1+\tilde{P}v_{n^*}}{1+\tilde{P}w_{n^*}} < \gamma_s\Big], \quad (10)$$

where $\gamma_t = 2^{2R_t} - 1$ denotes the SNR threshold of successful decoding at the relay. The analytical SOP for the multiple secure relaying with channel correlation and outdated relay selection as

$$\mathcal{P}_{out} = \sum_{K=1}^{N} \binom{N}{K} e^{-\frac{K\gamma_t}{\tilde{P}\alpha}} \big(1 - e^{-\frac{\gamma_t}{\tilde{P}\alpha}}\big)^{N-K} \Bigg(1 - \sum_{k=1}^{K}\sum_{m=0}^{T}\sum_{i=0}^{m} \sum_{j=0}^{i} C_{km} d_{m,ij} (m+j)! (b_1\gamma_s + b_2)^{-(m+j+1)}\Bigg), \quad (11)$$

where T is a given number of terms related to ρ, '!' denotes the factorial operation, and

$$b_1 = \Big(\frac{k}{k(1-\eta)+\eta} + \frac{\rho}{1-\rho}\Big)\frac{1}{\beta_1}, \quad b_2 = \frac{1}{(1-\rho)\beta_2}, \quad (12)$$

$$C_{km} = \binom{K}{k} \frac{k(-1)^{k-1}}{k(1-\eta)+\eta} \frac{\rho^m}{(1-\rho)^{2m+1}(\beta_1\beta_2)^{m+1}(m!)^2}, \quad (13)$$

and

$$d_{m,ij} = \frac{m!}{i!}\binom{i}{j} \frac{e^{-b_1(\gamma_s-1)/\tilde{P}}}{b_1^{m-i+1}} \gamma_s^j \big(\frac{\gamma_s-1}{\tilde{P}}\big)^{i-j}. \quad (14)$$

Proof: Since the random variable u_n is independent of v_{n^*} and w_{n^*}, we can rewrite $\mathcal{P}_{out}$ in (10) as

$$\mathcal{P}_{out} = \sum_{K=1}^{N} \binom{N}{K} \Pr\Big[\tilde{P}u_1 \geq \gamma_t, \cdots, \tilde{P}u_K \geq \gamma_t, \tilde{P}u_{K+1} < \gamma_t, \cdots, \tilde{P}u_N < \gamma_t\Big] \Pr\Big[\frac{1+\tilde{P}v_{n^*}}{1+\tilde{P}w_{n^*}} < \gamma_s\Big] \quad (15)$$

$$= \sum_{K=1}^{N} \binom{N}{K} e^{-\frac{K\gamma_t}{\tilde{P}\alpha}} \big(1 - e^{-\frac{\gamma_t}{\tilde{P}\alpha}}\big)^{N-K} \underbrace{\Pr\Big[\frac{1+\tilde{P}v_{n^*}}{1+\tilde{P}w_{n^*}} < \gamma_s\Big]}_{J_K}, \quad (16)$$

where $f_{u_n}(u) = \frac{1}{\alpha}e^{-\frac{u}{\alpha}}$ is used and the probability J_K denotes the conditional SOP with given K active relays. From the selection criterion in (7) and the conditional PDF of $f_{v_{n^*}|\tilde{v}_{n^*}}(v|\tilde{v})$ in (9), the PDF of v_{n^*} is [14]

$$f_{v_{n^*}}(v) = \sum_{k=1}^{K} \binom{K}{k} \frac{k(-1)^{k-1}}{\beta_1[k(1-\eta)+\eta]} e^{-\frac{kv}{[k(1-\eta)+\eta]\beta_1}}. \quad (17)$$

From (8) and (17), we obtain the joint PDF of v_{n^*} and w_{n^*} as,

$$f_{v_{n^*},w_{n^*}}(v,w) = f_{w_{n^*}|v_{n^*}}(w|v) f_{v_{n^*}}(v) = \sum_{k=1}^{K} \binom{K}{k} \frac{k(-1)^{k-1}}{\beta_1\beta_2(1-\rho)[k(1-\eta)+\eta]} I_0\Big(\frac{2}{1-\rho}\sqrt{\frac{\rho v w}{\beta_1\beta_2}}\Big) \times e^{-\frac{kv}{[k(1-\eta)+\eta]\beta_1} - (\frac{\rho v}{\beta_1} + \frac{w}{\beta_2})\frac{1}{1-\rho}}. \quad (18)$$

Note that the Bessel function $I_0(x)$ can be expressed by infinite series as [17]

$$I_0(x) = \sum_{m=0}^{\infty} \frac{x^{2m}}{4^m(m!)^2} \approx \sum_{m=0}^{T} \frac{x^{2m}}{4^m(m!)^2}, \quad (19)$$

where the truncation error decays exponentially with T, i.e., ρ^T [12]. Hence with an efficient number of terms, we can obtain an accurate approximation for $I_0(x)$. In this paper, we set the truncation error to a very small value of 10^{-10}, leading to $T = \text{round}\big(\frac{-10}{\log_{10}\rho}\big)$. In the following, we ignore the approximation error, and re-express $f_{v_{n^*},w_{n^*}}(v,w)$ as

$$f_{v_{n^*},w_{n^*}}(v,w) = \sum_{k=1}^{K}\sum_{m=0}^{T} C_{km} v^m w^m e^{-b_1 v} e^{-b_2 w}, \quad (20)$$

where b_1, b_2 and C_{km} are defined in (12)-(13). From (20), we can compute J_K as

$$J_K = \Pr\big(v_{n^*} < \frac{\gamma_s - 1}{\tilde{P}} + \gamma_s w_{n^*}\big) \quad (21)$$

$$= \int_0^{\infty}\int_0^{\frac{\gamma_s-1}{\tilde{P}}+\gamma_s w} f_{v_{n^*},w_{n^*}}(v,w)\,dv\,dw \quad (22)$$

$$= 1 - \sum_{k=1}^{K}\sum_{m=0}^{T}\sum_{i=0}^{m}\sum_{j=0}^{i} C_{km} d_{m,ij} (m+j)! \times (b_1\gamma_s + b_2)^{-(m+j+1)}. \quad (23)$$

By applying the result of J_K into (16), we can obtain the analytical SOP given in (11). ■

Note that the obtained analytical SOP in (11) consists of elementary functions only, and hence is easily to be evaluated.

B. Asymptotic Expression

To obtain insights on the system design, we now investigate the asymptotic SOP in the high MER. The asymptotic $\mathcal{P}_{out}$ for the multiple secure relaying with channel correlation and outdated relay selection is given by

$$\mathcal{P}_{out} \simeq \begin{cases} N!\Big(\frac{(1-\rho)\gamma_s}{\lambda}\Big)^N, & \text{If } \eta = 1 \\ \frac{(1-\rho)\gamma_s}{\lambda}\left(\sum_{k=1}^{N}\binom{N}{k}\frac{k(-1)^{k-1}}{k(1-\eta)+\eta}\right), & \text{If } \eta < 1 \end{cases}, \tag{24}$$

where $\lambda = \beta_1/\beta_2$ is the MER.

Proof: With a large transmit power P, we can approximate $\mathcal{P}_{out}$ as

$$\mathcal{P}_{out} \simeq J_N \simeq \Pr\big(\frac{v_{n^*}}{w_{n^*}} < \gamma_s\big). \tag{25}$$

Let $z = \frac{v_{n^*}}{w_{n^*}}$, and then the PDF of z is derived as

$$f_z(z) = \int_0^\infty w f_{v_{n^*},w_{n^*}}(wz, w)dw \tag{26}$$

$$= \sum_{k=1}^{N}\binom{N}{k}\frac{k(-1)^{k-1}}{\beta_1\beta_2(1-\rho)[k(1-\eta)+\eta]} \times \frac{\frac{kz}{[k(1-\eta)+\eta]\beta_1} + \big(\frac{\rho z}{\beta_1}+\frac{1}{\beta_2}\big)\frac{1}{1-\rho}}{\Big[\Big(\frac{kz}{[k(1-\eta)+\eta]\beta_1} + \big(\frac{\rho z}{\beta_1}+\frac{1}{\beta_2}\big)\frac{1}{1-\rho}\Big)^2 - \frac{4\rho z}{(1-\rho)^2\beta_1\beta_2}\Big]^{3/2}}, \tag{27}$$

where [17, eq. (6.623.2)] is applied in the last equality. For high MER with $\beta_1 \gg \beta_2$, we can approximate $f_z(z)$ as

$$f_z(z) \simeq \sum_{k=1}^{N}\binom{N}{k}\frac{(-1)^{k-1}(1-\rho)\lambda[k(1-\eta)+\eta]}{\{\lambda + k(1-\rho)z + \rho z[k(1-\eta)+\eta]\}^2}. \tag{28}$$

Using (28), we can approximate $\mathcal{P}_{out}$ as

$$\mathcal{P}_{out} \simeq \int_0^{\gamma_s} f_z(z)dz, \tag{29}$$

and obtain the asymptotic SOP expression in (24), where we apply the approximation of $(1+x)^{-1} = \sum_{k=0}^{N}(-1)^k x^k$ [17]. ■

From the asymptotic result in (24), we conclude the following remarks on the network security:

Remark 1: For a given number of relays, the network secrecy diversity order depends on the outdated degree of relay selection, but not on the channel correlation.

Remark 2: The network secrecy diversity order is equal to N when $\eta = 1$, indicating that the network security can be rapidly enhanced by increasing the number of relays in the perfect CSI environments.

Remark 3: As long as the relay selection is outdated, the network secrecy diversity order degenerates to unity. This is because that a wrong relay selection due to outdated CSI limits the whole network secrecy performance.

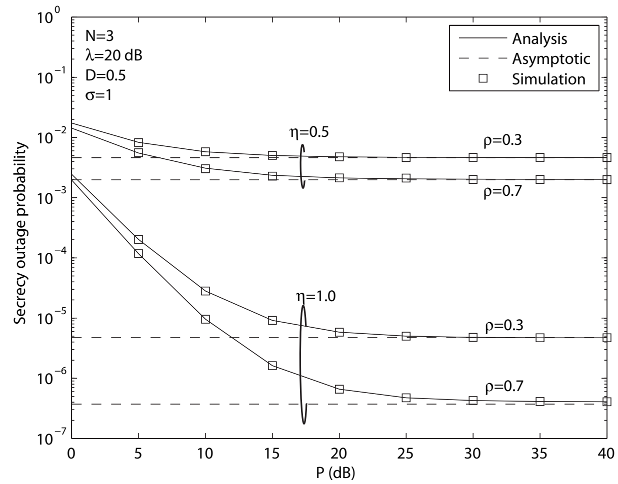

Fig. 2. Secrecy outage probability versus the transmit power P.

Remark 4: The channel correlation between the main and eavesdropping channels is beneficial to the transmission security in high MER region[2]. With higher channel correlation, the destination has more information about the channel fluctuation of eavesdropping links. In particular, for the completely linear correlation with $\rho = 1$, the fluctuation of eavesdropping channels is completely accordance with that of main channels and hence the destination has the perfect information about the channel fluctuation of eavesdropping links, making v_{n^*}/w_{n^*} equal to β_1/β_2. This helps the network suppress the wiretap perfectly, leading to a zero SOP.

V. Numerical and Simulation Results

In this section, we provide some numerical and simulation results to verify the presented studies. All links in the network experience Rayleigh fading, and we adopt the path-loss model with exponent of four to measure the average channel gains of main links, where the path loss exponent of four is valid for suburban areas [18]. Without loss of generality, we normalize the distance between the source and destination to unity, where the relays are in between of them. Let D denote the distance between the source and relays, and accordingly, $\alpha = D^{-4}$ and $\beta_1 = (1-D)^{-4}$ are set. The target data rate R_t of the first hop is 1 bps/Hz, and hence the associated γ_t is 3. The secrecy data rate R_s is 0.2 bps/Hz, so that the secrecy SNR threshold γ_s is 1.32.

Fig. 2 demonstrates the numerical and simulated secrecy outage probabilities versus the transmit power P, where $N = 3$, $\lambda = $ 20dB and $D = 0.5$. Several cases of channel correlation are considered with $\rho = 0.3$, 0.5 and 0.7. Both perfect and outdated CSI environments are studied with $\eta = 1.0$ and 0.5, respectively. As observed from the figure, for different values of ρ and η, the analytical result matches well with the simulation one, and the asymptotic result converges to the exact one when P is large. This validates the derived analytical and asymptotic expressions of the SOP. Moreover, in both perfect and outdated CSI environments, the secrecy

[2]Note that in the low MER region, the channel correlation is however harmful to the secure transmission [11], [12].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2669240, IEEE Transactions on Vehicular Technology

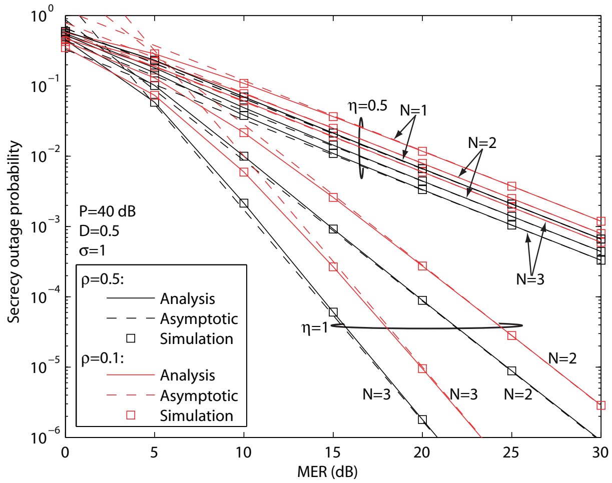

Fig. 3. Secrecy outage probability versus MER.

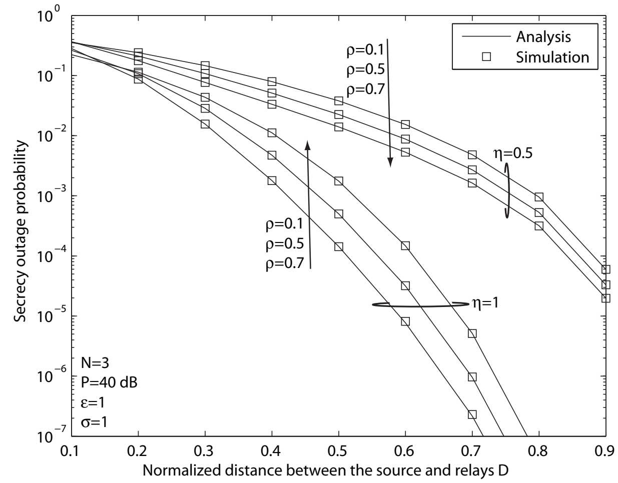

Fig. 4. Impact of D on the secrecy outage probability.

performance becomes better with larger ρ, as higher channel correlation helps the destination have more information about the channel fluctuation of eavesdropping links. The secrecy performance also improves with larger η, as better CSI helps select the best relay to assist the secure transmission. Furthermore, the secrecy performance improves with larger P. But the improvement is saturated in high P region, as the fixed MER becomes the bottleneck of the secrecy performance.

Fig. 3 illustrates the secrecy outage probability versus MER with different values of ρ and η, where $P = 40$dB and N varies from 1 to 3. We can see from this figure that for different values of N, ρ and η, the analytical result fits well with the simulation one, and the asymptotic result converges to the simulation one in the high MER region. Moreover, only the value of η affects the curve slopes, but ρ does not. This indicates that the secrecy diversity order depends on the outdated degree of relay selection, but not on the channel correlation. In particular, the curves are in parallel with each other for different relay numbers when $\eta = 0.5$, indicating that the system secrecy diversity order is unity for different values of ρ as long as the selection is outdated. On the contrast, the curve slope is proportional to N in the perfect CSI with $\eta = 1$, indicating that the system full secrecy diversity order can be achieved for different values of ρ. Such observations validate the insights from the asymptotic expression of the SOP.

Fig. 4 depicts the impact of D on the secrecy outage probability with $N = 3$ and $P = 40$dB, where $\varepsilon = 1$ and D varies from 0.1 to 0.9. Several cases of channel correlation and outdated relay selection are considered with $\rho = 0.1, 0.5$ and 0.7, and η=0.5 and 1. We can find that for different values of ρ and η, the analytical result matches well with the simulation one for the wide range of D. Moreover, the secrecy performance improves when D increases, due to the improved quality of the main channel and the increasing MER. In further, the secrecy performance improves with larger ρ and η. This is because that higher channel correlation helps the destination have more information about the channel fluctuation of eavesdropping links, and better CSI helps select the best relay to assist the secure transmission.

VI. Conclusion

In this paper, we investigated the secure relaying with N DF relays, where the main and eavesdropping channels are correlated. The relay selection was performed to choose one best relay to assist the secure transmission, which is however maybe outdated. We studied the impact of channel correlation and outdated relay selection on the secrecy performance by deriving the analytical SOP as well as the asymptotic expression with high MER. From the asymptotic SOP, we found that the channel correlation does not affect the secrecy diversity order, but can be beneficial to the transmission security. Importantly, we confirmed that the full secrecy diversity order of N is achieved only when the selection is based on the perfect CSI.

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

[3] 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.

[4] 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.

[5] 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.

[6] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[7] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

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

[9] 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.

[10] 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2017.2669240, IEEE Transactions on Vehicular Technology

[11] 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.

[12] 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.

[13] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.

[14] M. Torabi and D. Haccoun, "Capacity analysis of opportunistic relaying in cooperative systems with outdated channel information," *IEEE Commun. Lett.*, vol. 14, no. 12, pp. 1137–1139, Dec. 2010.

[15] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 864–867, May 2013.

[16] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[17] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA: Academic, 2007.

[18] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. NJ, USA: Prentice Hall PTR, 2001.