where $\overline{\gamma}'_{k_j} = \overline{\alpha}'_{l,n}\overline{\beta}'_{l,n}/(\overline{\alpha}'_{l,n} + \overline{\beta}'_{l,n})$, $\overline{\alpha}'_{l,n} = E(|h_{s,l,n}|^2)\rho/\sigma^2$, and $\overline{\beta}'_{l,n} = E(|h_{l,d,n}|^2)\rho/\sigma^2$. Since these two distinct links (direct and best indirect links) are mutually independent, then the overall pdf can be found by convoluting the above two individual pdfs. Specifically, the overall pdf for random variable $t = y + \gamma'_b$ can be expressed as

$$f(t) = \mu \sum_{n=1}^{L} (-1)^{n+1} \sum_{k_1=1}^{L-n+1} \sum_{k_2=k_1+1}^{L-n+2} \cdots \sum_{k_n=k_{n-1}+1}^{L} \times \exp(-\varphi t) \frac{erfc(\varphi') \exp(\varphi'^2)\varphi^{n+\frac{1}{2}}\sqrt{\pi}}{8} \quad (10)$$

where $\varphi = \sum_{j=1}^{n}(1/\overline{\gamma}'_{k_j})$, and $\varphi' = (\varphi + \mu)/(2\sqrt{\varphi})$. In particular, *erfc* is the complementary error function that can be written as $erfc(x) = (2/\sqrt{\pi}) \int_x^\infty \exp(-t^2)dt$. Finally, the average unconditional SNR outage probability can be obtained by integrating (2) from 0 to ∞, and then, we arrive at

$$\Pr(y+\gamma'_b \geq 0) = \int_0^\infty f(t)dt = \mu \sum_{n=1}^{L} (-1)^{n+1} \sum_{k_1=1}^{L-n+1} \sum_{k_2=k_1+1}^{L-n+2} \cdots \sum_{k_n=k_{n-1}+1}^{L} \frac{erfc(\varphi') \exp(\varphi'^2)\varphi^{n-\frac{1}{2}}\sqrt{\pi}}{8}. \quad (11)$$

REFERENCES

[1] Z. Mo, W. Su, S. Batalama, and J. Matyjas, "Cooperative communication protocol designs based on optimum power and time allocation," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4283–4296, Aug. 2014.

[2] I. Krikidis, J. S. Thompson, S. Mclaughlin, and N. Goertz, "Max-min relay selection for legacy amplify-and-forward systems with interference," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3016–3027, Jun. 2009.

[3] H. Hakim, H. Boujemaa, and W. Ajib, "Single relay selection schemes for broadcast networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2646–2657, Jun. 2013.

[4] Y. Li and Z. Zheng, "Energy-efficient power allocation for two-hop relay networks," *Electron. Lett.*, vol. 50, no. 2, pp. 123–125, Jan. 2014.

[5] M. Kaneko *et al.*, "Amplify-and-forward cooperative diversity schemes for multi-carrier systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1845–1850, May 2008.

[6] S. Ikki and M. H. Ahmed, "Performance analysis of cooperative diversity with incremental-best-relay technique over Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 59, no. 8, pp. 2152–2161, Aug. 2011.

Security–Reliability Tradeoff Analysis of Multirelay-Aided Decode-and-Forward Cooperation Systems

Jia Zhu, Yulong Zou, *Senior Member, IEEE*, Benoit Champagne, *Senior Member, IEEE*, Wei-Ping Zhu, *Senior Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—We consider a cooperative wireless network comprised of a source, a destination, and multiple relays operating in the presence of an eavesdropper, which attempts to tap the source–destination transmission. We propose a multirelay selection scheme for protecting the source against eavesdropping. More specifically, multirelay selection allows multiple relays to simultaneously forward the source's transmission to the destination, differing from the conventional single-relay selection, where only the best relay is chosen to assist in the transmission from the source to the destination. For the purpose of comparison, we consider the classic direct transmission and single-relay selection as benchmark schemes. We derive closed-form expressions of the intercept probability and the outage probability for the direct transmission, as well as for the single-relay and multirelay selection schemes over Rayleigh fading channels. It is demonstrated that as the outage requirement is relaxed, the intercept performance of the three schemes improves, and *vice versa*, implying that there is a *security-versus-reliability tradeoff* (SRT). We also show that both the single-relay and multirelay selection schemes outperform the direct transmission in terms of SRT, demonstrating the advantage of the relay selection schemes for protecting the source's transmission against the eavesdropping attacks. Finally, upon increasing the number of relays, the SRTs of both the single-relay and multirelay selection schemes significantly improve, and as expected, multirelay selection outperforms single-relay selection.**

***Index Terms*—Eavesdropping attack, intercept probability (IP), outage probability (OP), relay selection, security–reliability tradeoff (SRT).**

I. INTRODUCTION

Wireless security has attracted increasing research attention in recent years [1], [2]. Due to the broadcast nature of a wireless medium, legitimate transmissions may be readily tapped by unauthorized users,

Manuscript received January 22, 2015; revised May 3, 2015; accepted July 3, 2015. Date of publication July 8, 2015; date of current version July 14, 2016. This work was supported in part by the National Natural Science Foundation of China under Grant 61302104 and Grant 61401223, by the Scientific Research Foundation of Nanjing University of Posts and Telecommunications under Grant NY213014 and Grant NY214001, by the Natural Science Foundation of Jiangsu Province under Grant BK20140887, and by the Key Project of Natural Science Research of Higher Education Institutions of Jiangsu Province under Grant 15KJA510003. The review of this paper was coordinated by Dr. C. Xing. *(Corresponding author: Yulong Zou.)*

J. Zhu and Y. Zou are with the School of Telecommunication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210046, China (e-mail: yulong.zou@njupt.edu.cn; jiazhu@njupt.edu.cn).

B. Champagne is with the Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0E9, Canada (e-mail: benoit.champagne@mcgill.ca).

W.-P. Zhu is with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada, and also with the School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210046, China (e-mail: weiping@ece.concordia.ca).

L. Hanzo is with the Department of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

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/TVT.2015.2453364

leaving them vulnerable to eavesdropping attacks. Traditionally, cryptographic techniques have been adopted for protecting the confidentiality of legitimate transmissions against eavesdropping. Although classic cryptographic approaches relying on secret keys indeed do enhance transmission security, this imposes both an extra computational overhead and additional system complexity, for example, when distributing and managing the secret keys. Additionally, the classic cryptographic techniques are not perfectly secure, since they can still be decrypted by an eavesdropper with sufficiently high computing power through exhaustive key search.

Alternatively, physical-layer security [3], [4] is emerging as a promising paradigm against eavesdropping attacks, which relies on exploiting the physical characteristics of wireless channels. In [5], Leung-Yan-Cheong and Hellman proved that as long as the wiretap channel (spanning from the source to the eavesdropper) is a degraded version of the main channel (spanning from the source to the destination), the source–destination transmission can be perfectly reliable and secure. They also introduced the notion of secrecy capacity, which is the maximal rate achieved by the destination under the condition that the mutual information between the source and the eavesdropper remains zero. It was shown in [5] that the secrecy capacity is the difference between the capacity of the main channel and that of the wiretap channel. In [6] and [7], the secrecy capacity of wireless fading channels was further developed from an information-theoretic perspective. Moreover, the use of multiple-input multiple-output (MIMO) [8], cooperative relaying [9], [10], and beamforming techniques [11] was studied for the sake of combating the fading effects and for improving the wireless secrecy capacity.

Recently, transmit antenna selection has been studied in [12]–[15] for enhancing the physical-layer security of wireless communications. In [12], Alves *et al.* examined the secrecy outage performance of transmit antenna selection in a multiple-input single-output (MISO) system in the face of a multiantenna eavesdropper. It was shown in [12] that the secrecy outage probability (OP) of the MISO system relying on transmit antenna selection is significantly reduced. In [13], transmit antenna selection was further extended to a MIMO system, and a closed-form secrecy outage expression of the transmit-antenna-selection-aided MIMO system was derived in fading environments. After that, Ferdinand *et al.* in [14] studied the effect of outdated channel state information (CSI) on the secrecy performance of transmit antenna selection and showed that the secrecy OP expectedly degrades in the presence of the outdated CSI. Additionally, the secrecy diversity of the transmit-antenna-selection-assisted MIMO communications was examined in [15], where an asymptotic secrecy OP is characterized in high main-to-eavesdropper ratios.

In this paper, we explore the physical-layer security of a cooperative relay network in the presence of an eavesdropper, with an emphasis on the security–reliability tradeoff (SRT) of cooperative relay communications based on the decode-and-forward (DF) protocol without considering the amplify-and-forward (AF) protocol. As discussed in [16], in the AF protocol, the relay just simply retransmits a scaled version of its received signal from the source to the destination. This, however, has the relay noise propagation issue, since the noise received at the relay will be propagated to the destination. By contrast, the DF protocol allows the relay to decode its received signal. If the relay succeeds in decoding, e.g., through the use of a cyclic redundancy code, it then retransmits its decoded signal to the destination, which is called an adaptive DF [16]. It was shown in [16] that the adaptive DF achieves a better performance than the AF in terms of the frame error rate. Motivated by this fact, the DF protocol is adopted in this paper. Although only the DF is considered, similar SRT results can be obtained for the AF protocol.

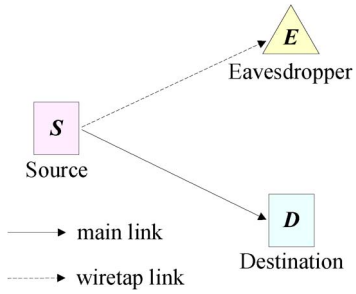

Fig. 1. Wireless network comprised of a source (S) and a destination (D) in the presence of an eavesdropper (E).

It is pointed out that the notion of SRT was first introduced in [17] and [18], where wireless security and reliability are characterized by the intercept probability (IP) and the OP, respectively. In this paper, we investigate the single-relay and multirelay selection for the sake of improving the physical-layer security of general wireless networks, instead of cognitive radio networks, as studied in [18]. We derive closed-form expressions of the IP and the OP for both the single-relay and multirelay selection schemes and show that the multirelay selection consistently outperforms the single-relay selection in terms of its SRT.

The remainder of this paper is organized as follows. In Section II, we present the single-relay and multirelay selection schemes for enhancing the attainable wireless physical-layer security and compare them against the classic direct transmission. Next, in Section III, we carry out the SRT analysis of these three schemes over Rayleigh fading channels, followed by Section IV, where numerical SRT results are presented. Finally, we provide our concluding remarks in Section V.

II. Single- and Multiple-Relay Selection Against Eavesdropping

A. Direct Transmission

Let us first consider the direct transmission as a benchmark invoked for comparison purposes. Fig. 1 shows a wireless system, where a source (S) transmits its scalar signal x_s ($E[|x_s|^2] = 1$) to a destination (D) at a particular time instant, while an eavesdropper (E) attempts to tap the source's transmission. In line with the physical-layer security literature [2]–[9], E is assumed to know the encoding and modulation schemes as well as the encryption algorithm and the secret key of the S–D transmission, except for the source signal x_s. When S transmits x_s at a power of P, we can express the received signal at D as

$$y_d = h_{sd}\sqrt{P}x_s + n_d \tag{1}$$

where h_{sd} is the fading coefficient of the S–D channel, and n_d is the additive white Gaussian noise (AWGN) at D. Meanwhile, due to the broadcast nature of wireless transmission, the transmission of S can be overheard by E, and the corresponding received signal is written as

$$y_e = h_{se}\sqrt{P}x_s + n_e \tag{2}$$

where h_{se} is the fading coefficient of the S–E channel, and n_e represents the AWGN at E. From (1), we obtain the channel capacity between S and D as

$$C_{sd} = \log_2\left(1 + |h_{sd}|^2\gamma\right) \tag{3}$$

where $\gamma = P/N_0$. Similarly, the channel capacity between S and E is obtained from (2) as

$$C_{se} = \log_2\left(1 + |h_{se}|^2\gamma\right). \tag{4}$$

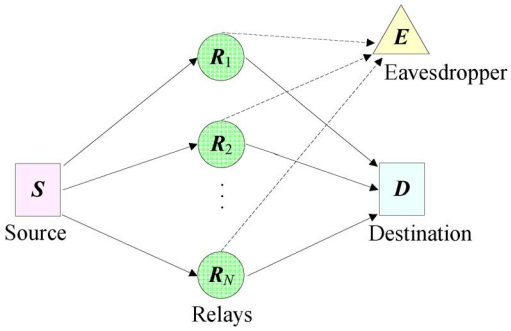

Fig. 2. Cooperative wireless network consisting of one source (S), one destination (D), and N relays (R_i) in the presence of an eavesdropper (E).

Throughout this paper, the Rayleigh fading model is considered for characterizing a transmission link between any two nodes of Fig. 1. Although only the Rayleigh fading is considered in this paper, similar SRT analysis and results can be obtained for other wireless fading models, e.g., Nakagami fading and Rice fading. Moreover, the complex AWGN encountered at the receiver has a zero mean and a variance of N_0.

B. Single-Relay Selection

Here, we consider the cooperative wireless network shown in Fig. 2, where both D and E are out of the coverage area of S, and N relays are used for assisting in the transmission of S. We invoke the DF protocol for the relays in forwarding the transmission of S to D. More specifically, S first broadcasts x_s to the N relays, which attempt to decode x_s. For notational convenience, let $\mathcal{D}$ denote the set of relays that successfully decode x_s, which is termed as the *decoding set*. Given N relays, there are 2^N possible subsets $\mathcal{D}$; thus, the sample space of $\mathcal{D}$ is given by

$$\Omega = \{\emptyset, \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n, \ldots, \mathcal{D}_{2^N-1}\} \tag{5}$$

where $\emptyset$ denotes an empty set, and $\mathcal{D}_n$ denotes the nth nonempty subset of the N relays. If the set $\mathcal{D}$ is empty (i.e., no relay succeeds in decoding x_s), all relays remain silent, and thus, both D and E are unable to decode x_s in this case. If the set $\mathcal{D}$ is nonempty, a specific relay is chosen from $\mathcal{D}$ for forwarding its decoded signal x_s to D. Therefore, considering that S broadcasts x_s to N relays at a power of P, the received signal at a specific relay R_i is expressed as

$$y_i = h_{si}\sqrt{P}x_s + n_i \tag{6}$$

where h_{si} is the fading coefficient of the channel spanning from S to R_i, and n_i is the AWGN at R_i. From (6), we obtain the channel capacity between S and R_i as

$$C_{si} = \frac{1}{2}\log_2\left(1 + |h_{si}|^2\gamma\right) \tag{7}$$

where the factor 1/2 in front of $\log(\cdot)$ arises from the fact that two time slots are required to complete the transmission from S to D via R_i. It is readily inferred from Shannon's coding theorem that if the channel capacity is lower than the data rate, the receiver is unable to recover the source signal. Otherwise, the receiver becomes capable of successfully decoding. Hence, by using (7), the event $\mathcal{D} = \emptyset$ is described as

$$C_{si} < R, \qquad i = 1, 2, \ldots, N \tag{8}$$

where R is the data rate. Meanwhile, the event $\mathcal{D} = \mathcal{D}_n$ can be described as

$$\begin{aligned} C_{si} &> R, \qquad i \in \mathcal{D}_n \\ C_{sj} &< R, \qquad j \in \bar{\mathcal{D}}_n \end{aligned} \tag{9}$$

where $\bar{\mathcal{D}}_n$ is the complementary set of $\mathcal{D}_n$. Without any loss of generality, we consider R_i as the "best" relay, which transmits its decoded signal x_s at a power of P. Hence, the received signal at D is written as

$$y_d = h_{id}\sqrt{P}x_s + n_d \tag{10}$$

where h_{id} is the fading coefficient of the channel spanning from R_i to D. From (10), the capacity of the channel between R_i and D is given by

$$C_{id} = \frac{1}{2}\log_2\left(1 + |h_{id}|^2\gamma\right) \tag{11}$$

where $i \in \mathcal{D}_n$. Typically, the relay having the highest capacity between R_i and D is viewed as the "best" relay. Thus, from (11), we obtain the selection criterion of finding the best relay as

$$\text{Best Relay} = \arg\max_{i\in\mathcal{D}_n} C_{id} = \arg\max_{i\in\mathcal{D}_n} |h_{id}|^2 \tag{12}$$

which shows that only the knowledge of the CSI $|h_{id}|^2$ is assumed in performing the relay selection, i.e., it is carried out without requiring the eavesdropper's CSI knowledge. Notice that in practical wireless systems, the CSI of the main channel (i.e., $|h_{id}|^2$) can be obtained by using some channel estimation methods [19]. Combining (11) and (12), we obtain the capacity of the channel between the "best" relay and D as

$$C_{bd} = \frac{1}{2}\max_{i\in\mathcal{D}_n}\log_2\left(1 + |h_{id}|^2\gamma\right) \tag{13}$$

where the subscript "b" represents the best relay. Meanwhile, given that the selected relay transmits x_s at a power of P, the signal received at E is written as

$$y_e = h_{be}\sqrt{P_s}x_s + n_e \tag{14}$$

where h_{be} is the fading coefficient of the channel spanning from the "best" relay to E. From (14), we express the capacity of the channel spanning from the "best" relay to E as

$$C_{be} = \frac{1}{2}\log_2\left(1 + |h_{be}|^2\gamma\right) \tag{15}$$

where $b \in \mathcal{D}_n$ is determined by the relay selection criterion of (12).

C. Multirelay Selection

This section proposes a multirelay selection scheme, where, given a nonempty set $\mathcal{D}_n$, all relays within $\mathcal{D}_n$ are employed for simultaneously transmitting x_s to D. Explicitly, this differs from the single-relay selection scheme, in which only a single relay is chosen from $\mathcal{D}_n$ for forwarding the source signal. A weight vector denoted by $\mathbf{w} = [w_1, w_2, \ldots, w_{|\mathcal{D}_n|}]^T$ is employed by all the relays of $\mathcal{D}_n$ in transmitting x_s, where $|\mathcal{D}_n|$ is the cardinality of $\mathcal{D}_n$. For the sake of a fair comparison with single-relay selection, the total transmit power of all relays is constrained to P, and thus, the weight vector $\mathbf{w}$ should have unit norm (i.e., $\|\mathbf{w}\| = 1$). Hence, given a nonempty decoding set $\mathcal{D}_n$ and considering that all relays within $\mathcal{D}_n$ simultaneously transmit x_s using a weight vector $\mathbf{w}$, the signal received at D is written as

$$y_d^{\text{multi}} = \sqrt{P}\mathbf{w}^T\mathbf{h}_d x_s + n_d \tag{16}$$

where $\mathbf{h}_d = [h_{1d}, h_{2d}, \ldots, h_{|\mathcal{D}_n|d}]^T$. Meanwhile, the signal received at E can be expressed as

$$y_e^{\text{multi}} = \sqrt{P}\mathbf{w}^T\mathbf{h}_e x_s + n_e \tag{17}$$

where $\mathbf{h}_e = [h_{1e}, h_{2e}, \ldots, h_{|\mathcal{D}_n|e}]^T$. From (16) and (17), the received signal-to-noise ratios (SNRs) at D and E are, respectively, given by

$$\text{SNR}_d^{\text{multi}} = \gamma|\mathbf{w}^T\mathbf{h}_d|^2 \tag{18}$$

$$\text{SNR}_e^{\text{multi}} = \gamma|\mathbf{w}^T\mathbf{h}_e|^2. \tag{19}$$

In this paper, the weight vector $\mathbf{w}$ is optimized by maximizing $\text{SNR}_d^{\text{multi}}$, yielding

$$\max_{\mathbf{w}} \ \text{SNR}_d^{\text{multi}}, \quad \text{s.t. } \|\mathbf{w}\| = 1 \tag{20}$$

where the constraint is used for normalization. Using the Cauchy–Schwarz inequality, we express the optimal weight vector $\mathbf{w}_{\text{opt}}$ from (20) as

$$\mathbf{w}_{\text{opt}} = \frac{\mathbf{h}_d^*}{|\mathbf{h}_d|} \tag{21}$$

where the optimal weight vector design only requires the CSI of the channel spanning from the relays to D (i.e., $\mathbf{h}_d$) without requiring the eavesdropper's CSI $\mathbf{h}_e$. Substituting $\mathbf{w}_{\text{opt}}$ from (21) into (18) and (19), we obtain the channel capacities achieved at D and E as

$$C_d^{\text{multi}} = \frac{1}{2}\log_2\left(1 + \gamma \sum_{i\in\mathcal{D}_n} |h_{id}|^2\right) \tag{22}$$

$$C_e^{\text{multi}} = \frac{1}{2}\log_2\left(1 + \gamma\frac{|\mathbf{h}_d^H\mathbf{h}_e|^2}{|\mathbf{h}_d|^2}\right) \tag{23}$$

for $\mathcal{D} = \mathcal{D}_n$, where H denotes the Hermitian transpose.

III. Security–Reliability Tradeoff Analysis Over Rayleigh Fading Channels

Here, we present the SRT analysis of the classic direct transmission as well as of both single-relay and multirelay selection schemes over Rayleigh fading channels. As discussed in [17], wireless security and reliability are characterized using the IP and the OP experienced by the eavesdropper and the destination, respectively. Let us first recall the definitions of OP and IP.

Definition 1: Denoting the channel capacities achieved at the destination and the eavesdropper by C_d and C_e, the OP and the IP are defined as [17], [20]

$$P_{\text{out}} = \Pr(C_d < R) \tag{24}$$

$$P_{\text{int}} = \Pr(C_e > R) \tag{25}$$

where R represents the data rate.

A. Direct Transmission

From (24), the OP of the direct transmission is obtained as

$$P_{\text{out}}^{\text{direct}} = \Pr(C_{sd} < R) \tag{26}$$

where C_{sd} is given by (3). Substituting C_{sd} from (3) into (26) yields

$$P_{\text{out}}^{\text{direct}} = \Pr\left(|h_{sd}|^2 < \Delta\right) \tag{27}$$

where $\Delta = (2^R - 1)/\gamma$. Noting that $|h_{sd}|^2$ is an exponentially distributed random variable with a mean of σ_{sd}^2, we arrive at

$$P_{\text{out}}^{\text{direct}} = 1 - \exp\left(-\frac{\Delta}{\sigma_{sd}^2}\right). \tag{28}$$

Additionally, we obtain the IP of the direct transmission from (4) and (25) as

$$P_{\text{int}}^{\text{direct}} = \Pr(C_{se} > R) = \exp\left(-\frac{\Delta}{\sigma_{se}^2}\right) \tag{29}$$

where σ_{se}^2 is the expected value of the random variable $|h_{se}|^2$.

B. Single-Relay Selection

This section presents the SRT analysis of the single-relay selection scheme. Using the law of total probability, the OP of the single-relay selection scheme is given by

$$P_{\text{out}}^{\text{single}} = \Pr(C_{bd} < R, \mathcal{D} = \emptyset) + \sum_{n=1}^{2^N-1} \Pr(C_{bd} < R, \mathcal{D} = \mathcal{D}_n) \tag{30}$$

where C_{bd} represents the capacity of the channel spanning from the "best" relay to D. In the case of $\mathcal{D} = \emptyset$, no relay is chosen to forward the source signal, leading to $C_{bd} = 0$. Substituting this result into (30) gives

$$P_{\text{out}}^{\text{single}} = \Pr(\mathcal{D} = \emptyset) + \sum_{n=1}^{2^N-1} \Pr(C_{bd} < R, \mathcal{D} = \mathcal{D}_n). \tag{31}$$

Using (8), (9), and (13), we can rewrite (31) as

$$P_{\text{out}}^{\text{single}} = \prod_{i=1}^{N} \Pr\left(|h_{si}|^2 < \Lambda\right) + \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda\right) \times \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda\right) \Pr\left(\max_{i\in\mathcal{D}_n} |h_{id}|^2 < \Lambda\right) \tag{32}$$

where $\Lambda = (2^{2R} - 1)/\gamma$. Noting that $|h_{si}|^2$ and $|h_{id}|^2$ are independent exponentially distributed random variables with respective means of σ_{si}^2 and σ_{id}^2, we obtain

$$\Pr\left(|h_{si}|^2 < \Lambda\right) = 1 - \exp\left(-\frac{\Lambda}{\sigma_{si}^2}\right) \tag{33}$$

$$\Pr\left(\max_{i\in\mathcal{D}_n} |h_{id}|^2 < \Lambda\right) = \prod_{i\in\mathcal{D}_n}\left[1 - \exp\left(-\frac{\Lambda}{\sigma_{id}^2}\right)\right]. \tag{34}$$

Moreover, the IP of the single-relay selection scheme is obtained from (25) as

$$P_{\text{int}}^{\text{single}} = \Pr(C_{be} > R, \mathcal{D} = \emptyset) + \sum_{n=1}^{2^N-1} \Pr(C_{be} > R, \mathcal{D} = \mathcal{D}_n) \tag{35}$$

where C_{be} denotes the capacity of the channel spanning from the "best" relay to E. Given $\mathcal{D} = \emptyset$, we have $C_{be} = 0$, since no relay

retransmits the source signal. Hence, substituting this result into (35) and using (8), (9), and (15), we obtain

$$P_{\text{int}}^{\text{single}} = \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda\right) \times \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda\right) \Pr\left(|h_{be}|^2 > \Lambda\right) \quad (36)$$

where the closed-form expressions of $\Pr(|h_{si}|^2 > \Lambda)$ and $\Pr(|h_{sj}|^2 < \Lambda)$ can be readily derived by using (33). Proceeding as in the Appendix, we obtain $\Pr(|h_{be}|^2 > \Lambda)$ as

$$\Pr\left(|h_{be}|^2 > \Lambda\right) = \sum_{i\in\mathcal{D}_n} \exp\left(-\frac{\Lambda}{\sigma_{ie}^2}\right) \times \left[1 + \sum_{m=1}^{2^{|\mathcal{D}_n|}-1} (-1)^{|\mathcal{C}_n(m)|} \left(1 + \sum_{j\in\mathcal{C}_n(m)} \frac{\sigma_{id}^2}{\sigma_{jd}^2}\right)^{-1}\right] \quad (37)$$

where $\mathcal{C}_n(m)$ represents the mth nonempty subset of "$\mathcal{D}_n - \{i\}$," and "$-$" represents the set difference.

C. Multirelay Selection

This section analyzes the SRT of multirelay selection. Similarly to (31), the OP of the multirelay selection scheme is given by

$$P_{\text{out}}^{\text{multi}} = \Pr(\mathcal{D} = \emptyset) + \sum_{n=1}^{2^N-1} \Pr\left(C_d^{\text{multi}} < R, \mathcal{D} = \mathcal{D}_n\right). \quad (38)$$

Using (8), (9), and (22), we can rewrite (38) as

$$P_{\text{out}}^{\text{multi}} = \prod_{i=1}^{N} \Pr\left(|h_{si}|^2 < \Lambda\right) + \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda\right) \times \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda\right) \Pr\left(\sum_{i\in\mathcal{D}_n} |h_{id}|^2 < \Lambda\right) \quad (39)$$

where the closed-form expressions of $\Pr(|h_{si}|^2 < \Lambda)$, $\Pr(|h_{si}|^2 > \Lambda)$, and $\Pr(|h_{sj}|^2 < \Lambda)$ can be easily determined as shown in (33). However, it is challenging to obtain the closed-form expression of $\Pr(\sum_{i\in\mathcal{D}_n} |h_{id}|^2 < \Lambda)$. For simplicity, we assume that the fading coefficients of all relay–destination channels $|h_{id}|^2$ are independent and identically distributed (i.i.d.) random variables with the same average channel gain denoted by $\sigma_d^2 = E(|h_{id}|^2)$. This assumption is widely used in the cooperative relaying literature [3]–[9], and it is valid in a statistical sense, when all relays are uniformly distributed geographically over a certain geographical area. Assuming that the random variables of $|h_{id}|^2$ for $i \in \mathcal{D}_n$ are i.i.d., we obtain

$$\Pr\left(\sum_{i\in\mathcal{D}_n} |h_{id}|^2 < \Lambda\right) = \Gamma\left(\frac{\Lambda}{\sigma_d^2}, |\mathcal{D}_n|\right) \quad (40)$$

where $\Gamma(x,k) = \int_0^x (t^{k-1}/\Gamma(k)) e^{-t} dt$ is known as the incomplete Gamma function. Let us now present the IP analysis of the multirelay selection scheme. Similarly to (36), the IP of multirelay selection can be obtained from (23) as

$$P_{\text{int}}^{\text{multi}} = \sum_{n=1}^{2^N-1} \prod_{i\in\mathcal{D}_n} \Pr\left(|h_{si}|^2 > \Lambda\right) \times \prod_{j\in\bar{\mathcal{D}}_n} \Pr\left(|h_{sj}|^2 < \Lambda\right) \Pr\left(\frac{|\mathbf{h}_d^H \mathbf{h}_e|^2}{|\mathbf{h}_d|^2} > \Lambda\right) \quad (41)$$

where the closed-form expressions of $\Pr(|h_{si}|^2 > \Lambda)$ and $\Pr(|h_{sj}|^2 < \Lambda)$ can be determined by using (33). However, it is challenging to obtain a closed-form solution for $\Pr((|\mathbf{h}_d^H \mathbf{h}_e|^2/|\mathbf{h}_d|^2) > \Lambda)$. Although finding a general closed-form IP expression is difficult for the multirelay selection scheme, we can evaluate the numerical IP through using computer simulations.

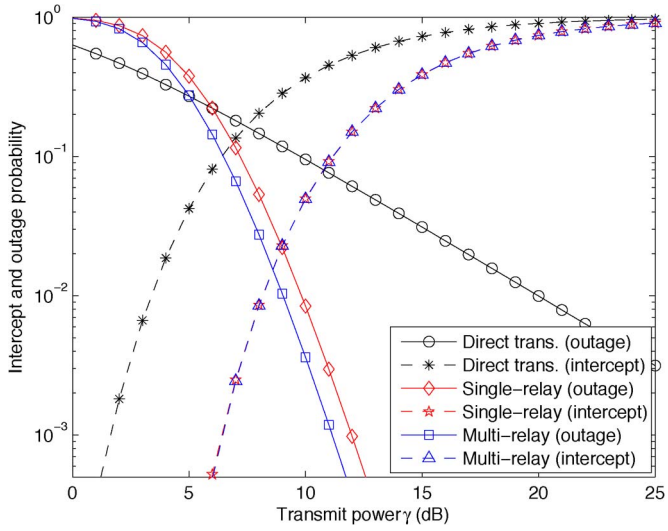

Fig. 3. IP and OP versus the transmit power γ of the direct transmission, the single-relay selection, and the multirelay selection schemes.

IV. Numerical Results and Discussions

Here, we present the numerical SRT results of the direct transmission as well as of the single-relay and multirelay selection schemes. Specifically, the IP and the OP of the three schemes are evaluated by using (28), (29), (32), (36), (39), and (41). In our numerical evaluation, the transmission link between any two nodes in Figs. 1 and 2 is modeled by the Rayleigh fading channel, and the average channel gains are specified as $\sigma_{sd}^2 = \sigma_{si}^2 = \sigma_{id}^2 = 1$ and $\sigma_{se}^2 = \sigma_{ie}^2 = 0.1$. Additionally, an SNR of $\gamma = 10$ dB, a data rate of $R = 1$ bit/s/Hz, and $N = 6$ relays are assumed, unless otherwise stated.

Fig. 3 shows IP and OP versus the transmit power γ of the direct transmission as well as of the single-relay and multirelay selection schemes. Notice that the numerical curves in Fig. 3 are obtained by plotting (28), (29), (32), (36), (39), and (41) as a function of the transmit power γ. It is shown in Fig. 3 that as the transmit power increases, the outage probabilities of the direct transmission, the single-relay selection, and the multirelay selection are reduced accordingly, whereas the corresponding intercept probabilities of the three schemes increase. This implies that an SRT between the IP and the OP exists for wireless transmissions in the presence of eavesdropping attacks. Fig. 3 also demonstrates that both the single-relay and multirelay selection schemes outperform the classic direct transmission in terms of their intercept and outage probabilities. Moreover, the multirelay

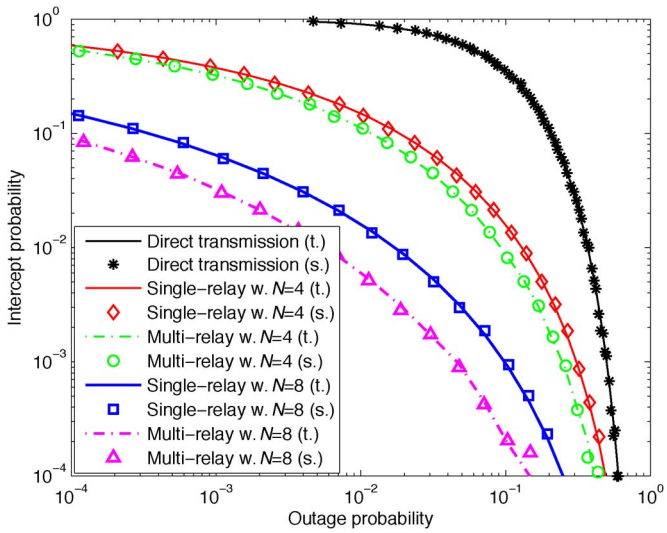

Fig. 4. IP versus OP of the direct transmission, the single-relay selection, and the multirelay selection schemes for different N values, where "t." and "s." stand for theoretical and simulation results, respectively.

selection strictly performs better than the single-relay selection in terms of the OP. Meanwhile, the intercept performance of the single-relay selection is almost identical to that of the multirelay selection. Therefore, given a required IP, the multirelay selection scheme can achieve a better outage performance than the single-relay selection. Conversely, with a target outage requirement, the IP of the multirelay selection would be lower than that of the single-relay selection scheme.

In Fig. 4, the intercept probabilities of the direct transmission as well as the single-relay and multirelay selection schemes are plotted as a function of the OP for $N = 4$ and $N = 8$ using (28), (29), (32), (36), (39), and (41). Meanwhile, simulation results of the IP versus OP of the three schemes are also given in Fig. 4. It is observed from Fig. 4 that the SRTs of the single-relay and multirelay selection schemes are consistently better than that of the direct transmission for both $N = 4$ and $N = 8$. Moreover, as the number of relays increases from $N = 4$ to $N = 8$, the SRTs of both single-relay and multirelay selection significantly improve, demonstrating the security and reliability benefits of using cooperative relays. In other words, the security and reliability of wireless transmissions can be concurrently improved by increasing the number of relays. Moreover, Fig. 4 shows that for both $N = 4$ and $N = 8$, the multirelay selection outperforms the single-relay selection in terms of their SRT performance. It is worth mentioning that in the proposed multirelay selection scheme, multiple selected relays should simultaneously forward the source signal to the destination, which, however, requires the complex symbol-level synchronization among different relays to avoid intersymbol interference. By contrast, the single-relay selection does not need such a complex synchronization process. Therefore, the SRT advantage of the multirelay selection over the single-relay selection is achieved at the cost of additional implementation complexity due to the symbol-level synchronization among the spatially distributed relays. Additionally, the theoretical and simulation results of Fig. 4 match well with each other, confirming the correctness of the SRT analysis.

V. Conclusion

In this paper, we have studied the relay selection of a cooperative wireless network in the presence of an eavesdropper and proposed the multirelay selection scheme for protecting wireless transmissions against eavesdropping. We used the classic direct transmission and single-relay selection as our benchmarks. We carried out the SRT analysis of the direct transmission as well as of both the single-relay and multirelay selection schemes over Rayleigh fading channels. We showed that the single-relay and multirelay selection schemes perform consistently better than the direct transmission in terms of their SRT performance. Moreover, the SRT of the multirelay selection is better than that of single-relay selection. Finally, upon increasing the number of relays, the SRTs of both the single-relay and multi-relay selection schemes significantly improve, showing the advantage of exploiting cooperative relays for enhancing wireless security and reliability.

Appendix
Derivation of (37)

Given $\mathcal{D} = \mathcal{D}_n$, any relay within $\mathcal{D}_n$ may be chosen as the "best" relay for forwarding the source signal to D. Thus, using the law of total probability, we have

$$\begin{aligned}&\Pr\left(|h_{be}|^2 > \Lambda\right)\\&= \sum_{i\in\mathcal{D}_n} \Pr\left(|h_{ie}|^2 > \Lambda, b = i\right)\\&= \sum_{i\in\mathcal{D}_n} \Pr\left(|h_{ie}|^2 > \Lambda, |h_{id}|^2 > \max_{j\in\mathcal{D}_n-\{i\}} |h_{jd}|^2\right)\\&= \sum_{i\in\mathcal{D}_n} \Pr\left(|h_{ie}|^2 > \Lambda\right) \Pr\left(\max_{j\in\mathcal{D}_n-\{i\}} |h_{jd}|^2 < |h_{id}|^2\right) \quad \text{(B.1)}\end{aligned}$$

where the second equality is obtained by using (12), and "$-$" denotes the set difference. Noting that $|h_{ie}|^2$ is an exponentially distributed random variable with a mean of σ_{ie}^2, we arrive at

$$\Pr\left(|h_{ie}|^2 > \Lambda\right) = \exp\left(-\frac{\Lambda}{\sigma_{ie}^2}\right). \quad \text{(B.2)}$$

Letting $|h_{jd}|^2 = x_j$ and $|h_{id}|^2 = y$, we have

$$\begin{aligned}&\Pr\left(\max_{j\in\mathcal{D}_n-\{i\}} |h_{jd}|^2 < |h_{id}|^2\right)\\&= \int_0^\infty \frac{1}{\sigma_{id}^2} \exp\left(-\frac{y}{\sigma_{id}^2}\right) \prod_{j\in\mathcal{D}_n-\{i\}} \left[1 - \exp\left(-\frac{y}{\sigma_{jd}^2}\right)\right] dy \quad \text{(B.3)}\end{aligned}$$

wherein $\prod_{j\in\mathcal{D}_n-\{i\}} \left[1 - \exp(-(y/\sigma_{jd}^2))\right]$ is expanded by

$$\begin{aligned}&\prod_{j\in\mathcal{D}_n-\{i\}} \left[1 - \exp\left(-\frac{y}{\sigma_{jd}^2}\right)\right]\\&\quad= 1 + \sum_{m=1}^{2^{|\mathcal{D}_n|-1}-1} (-1)^{|\mathcal{C}_n(m)|} \exp\left(-\sum_{j\in\mathcal{C}_n(m)} \frac{y}{\sigma_{jd}^2}\right) \quad \text{(B.4)}\end{aligned}$$

where $\mathcal{C}_n(m)$ represents the mth nonempty subset of "$\mathcal{D}_n - \{i\}$," and $|\mathcal{C}_n(m)|$ is the cardinality of the set $\mathcal{C}_n(m)$. Combining (B.3) and (B.4), we obtain

$$\begin{aligned}&\Pr\left(\max_{j\in\mathcal{D}_n-\{i\}} |h_{jd}|^2 < |h_{id}|^2\right)\\&\quad= 1 + \sum_{m=1}^{2^{|\mathcal{D}_n|-1}-1} (-1)^{|\mathcal{C}_n(m)|} \left(1 + \sum_{j\in\mathcal{C}_n(m)} \frac{\sigma_{id}^2}{\sigma_{jd}^2}\right)^{-1}. \quad \text{(B.5)}\end{aligned}$$

Substituting (B.2) and (B.5) into (B.1) gives (37).

REFERENCES

[1] M. Elkashlan, L. Wang, T. Q. Duong, G. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Trans. Veh. Technol.*, accepted for publication.

[2] G. Ding *et al.*, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014.

[3] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications through diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[4] J. Ni *et al.*, "Secrecy-rate balancing for two-user MISO interference channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 6–9, Feb. 2014.

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

[6] M. Bloch, J. O. 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.

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

[8] C. Xing, S. Ma, and Y.-C. Wu, "Robust joint design of linear relay precoder and destination equalizer for dual-hop amplify-and-forward MIMO relay systems," *IEEE Trans. Signal Process.*, vol. 58, no. 4, pp. 2273–2283, Apr. 2010.

[9] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[10] W. Chen, "CAO-SIR: Channel aware ordered successive relaying," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6513–6527, Dec. 2014.

[11] C. Xing, S. Ma, and Y.-C. Wu, "On low complexity robust beamforming with positive semidefinite constraints," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4942–4945, Dec. 2009.

[12] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[13] 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.

[14] 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.

[15] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna selection aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016.

[16] M. Souryal and B. Vojcic, "Performance of amplify-and-forward and decode-and-forward relaying in Rayleigh fading with turbo codes," in *Proc. IEEE ICASSP*, Toulouse, France, May 2006, pp. IV-681–IV-684.

[17] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[18] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security–reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

[19] G. Wang, F. Gao, Y.-C. Wu, and C. Tellambura, "Joint carrier frequency offset and channel estimation for two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 456–465, Feb. 2011.

[20] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.