Joint Source-Relay Selection for Improving Wireless Physical-Layer Security

Weifeng Cao*, Yulong Zou*, and Zhen Yang*
*School of Telecomm. & Inform. Eng., Nanjing Univ. of Posts & Telecomm., Nanjing, P. R. China
†School of Automation, Nanjing Institute of Tech., Nanjing, P. R. China

Abstract—We explore the physical-layer security for a multi-source multi-relay wireless network in the presence of an eavesdropper, in which one of multiple sources is scheduled to send its message to a destination with the assistance of multiple decode-and-forward (DF) relays. One eavesdropper is considered at the receiver side, and assumed to be capable of overhearing the transmission from relays to destination. In this paper, the round-robin scheduling and the joint source-relay selection schemes are presented to improve the physical-layer security of the multi-source multi-relay system, and their closed-form intercept probability expressions are derived over Rayleigh fading channels. Numerical results demonstrate that the proposed joint source-relay selection scheme achieves a better performance than the traditional round-robin scheduling in terms of the intercept probability.

Index Terms—Intercept probability, source-relay selection, round-robin scheduling, physical-layer security.

I. INTRODUCTION

The domain of wireless communications security has attracted considerable attention in the research community [1]. It remains a challenge to ensure the confidential transmission between legitimate users which is vulnerable to potential eavesdropping attacks due to the broadcast nature of the wireless medium. Physical-layer security has been actively examined as a promising approach to realize secure wireless communications against eavesdropping without relying on conventional cryptographic techniques. It was proved in [2] that perfect secrecy is achievable when a wiretap channel (from source to eavesdropper) is a degraded version of the main channel (from source to destination), where the difference of the channel capacities between the main link and wiretap link is defined as the secrecy capacity.

At present, various effective methods such as artificial noise [3], cooperative relaying [5]-[7], beamforming [8], and multiple-input multiple-output [9], are employed to enhance the wireless physical-layer security. Traditionally, artificial noise is a kind of specially-designed signal which is imposed on the null space of the legitimate channel to only interfere with the eavesdroppers. Later on, a generalized artificial noise scheme which allows the injection of artificial noise to the legitimate channel was proposed in multiple-input, single-output, single-antenna eavesdropper systems in [3] and the secrecy rate was shown to be improved significantly.

Cooperative relaying is an alternative means to be widely utilized in improving the security performance of wireless communications. The authors of [5] investigated the secrecy rate and power allocation for a wireless network comprised of one source-destination pair with the help of multiple cooperating relays in the presence of one or more eavesdroppers, where three cooperative schemes, namely the decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ) were examined and compared with each other. Zou et al. [6] studied the AF and DF based optimal relay selection for a cooperative wireless network with multiple relays and derived closed-form expressions of intercept probability over Rayleigh fading. Different from most of existing work on relay selection assuming the perfect channel state information (CSI), Tukmanov et al. [7] explored a Poisson relay selection with imperfect CSI knowledge and derived an exact outage probability expression.

Multiuser diversity is recognized as an effective technique to combat channel fading in wireless communications. Recently, a lot of work [10]-[15] is focused on improving the wireless transmission reliability by combining the multiuser diversity and cooperative diversity. Although multiuser diversity gain can be achieved to improve the reliability performance of wireless communications [10], [11], it comes at the cost of security degradation since more eavesdroppers would be encountered with increasing the users which may be potential eavesdroppers. To address this issue, the authors of [13] proposed an optimal user scheduling for the multiuser relay scheme with cooperative jamming aimed at maximizing the secrecy rate.

In this paper, we investigate the physical-layer security for a multi-source multi-relay wireless network in the presence of an eavesdropper. First, we propose a joint source-relay selection scheme, where a source-relay pair is opportunistically selected for the sake of maximizing the secrecy rate of wireless communications. The conventional round-robin scheduling is taken as a benchmark. Second, we derive exact closed-form expressions of the intercept probability for both the conventional round-robin scheduling and proposed joint source-relay selection over Rayleigh fading channels. Last, we evaluate the intercept performance of the two schemes, which shows that the proposed source-relay selection scheme generally outperforms the conventional round-robin scheduling in terms of the intercept probability.

The remainder of this paper is organized as follows. Section II presents the system model of a multi-source multi-relay
network in the presence of an eavesdropper. Then, the round-robin scheduling and the joint source-relay selection schemes are presented along with their closed-form intercept probability analysis in Section III. Section IV provides numerical intercept probability results of the conventional round-robin scheduling and proposed joint source-relay selection schemes. Finally, some conclusions are drawn in Section V.

II. SYSTEM MODEL

As illustrated in Fig. 1, we consider a multi-source multi-relay wireless network consisting of \(M\) sources \(S_m (m = 1, 2, \ldots, M)\), \(N\) relays \(R_n (n = 1, 2, \ldots, N)\) and a destination \(D\) in the presence of an eavesdropper \(E\), which attempts to intercept the transmission from relays to destination. All nodes are equipped with a single antenna and operate in a half-duplex mode. It is assumed that all the links follow independent Rayleigh flat fading distribution and there are no direct links from sources to destination and eavesdropper. The whole procedure of communication can be described as two phases. In phase I, in order to prevent the wiretap, the best source-relay pair \((S_m, R_n)\) is selected by maximizing the secrecy capacity. Then the source \(S_m\) broadcasts, while the relays listen. In phase II, the best relay \(R_n\) decodes and forwards its received signal to destination \(D\) as well as the eavesdropper \(E\) who may overhear the information. Suppose that the source \(S_m\) transmits \(x\) at a power \(P_S\), the signal received by relay \(R_n\) may be expressed as

\[
x_{R_n} = \sqrt{P_S} h_{S_m R_n} x + n_r,
\]

where \(h_{S_m R_n}\) represents the fading coefficient of the \(S_m-R_n\) channel and \(n_r\) is the zero-mean additive white Gaussian noise (AWGN) received at relay. Assuming that \(E\) knows all the parameters of \(R_n\), thus the received signals at \(D\) and \(E\) are given by

\[
y_d = \sqrt{P_R} h_{R_n D} x_{R_n} + n_d
\]

and

\[
y_e = \sqrt{P_R} h_{R_n E} x_{R_n} + n_e,
\]

where \(h_{R_n D}\) and \(h_{R_n E}\), respectively, represents the fading coefficient of the \(R_n-D\) and \(R_n-E\) channels. \(P_R\) is the transmit power at the relay \(R_n\), \(n_d\) and \(n_e\) are the AWGN received at \(D\) and \(E\). For simplicity, the power at source and relay is equally allocated by \(P/2\) in terms of the total transmit power \(P\).

According to Shannon’s capacity formula and (1), we obtain the capacity of the source to relay channel as

\[
C_{S_m R_n} = \log_2(1 + |h_{S_m R_n}|^2 \gamma)
\]

where \(\gamma = P / 2N_0\) is the signal-to-noise ratio (SNR). Similarly, from Eq. (2) and (3), the channel capacity from relay to destination and eavesdropper are given by

\[
C_{R_n D} = \log_2(1 + |h_{R_n D}|^2 \gamma)
\]

and

\[
C_{R_n E} = \log_2(1 + |h_{R_n E}|^2 \gamma),
\]

where \(|h_{S_m R_n}|^2\), \(|h_{R_n D}|^2\) and \(|h_{R_n E}|^2\) are independent and follow exponential distributions with different means \(\sigma_{S_m R_n}^2\), \(\sigma_{R_n D}^2\) and \(\sigma_{R_n E}^2\), respectively.

For DF protocol, to assure that both relay and destination are capable to succeed in decoding the messages, the capacity of DF transmission should be the minimum of the capacity from source to relay and that from relay to destination. Hence, the capacity of the transmission from source assisted by \(R_n\) to destination can be obtained as

\[
C_{R_n} = \min(C_{S_m R_n}, C_{R_n D}).
\]

It is known that the secrecy capacity is defined as the difference between the channel capacity of the main link and that of the wiretap channel. Thus, the secrecy capacity of DF relaying transmission with \(R_n\) is given by

\[
C_{sec \_DF}^{R_n} = C_{R_n} - C_{R_n E} = \log_2 \left( \frac{1 + \min(|h_{S_m R_n}|^2, |h_{R_n D}|^2) \gamma}{1 + |h_{R_n E}|^2 \gamma} \right).
\]

III. SOURCE-RELAY SELECTION SCHEME AND INTERCEPT PROBABILITY ANALYSIS

In this section, we present the round-robin scheduling and a joint source-relay selection schemes to enhance the physical-layer security, and their closed-form intercept probability expressions are derived for a multi-source multi-relay network.

A. Round-Robin Scheduling

We first present the conventional round-robin scheduling as a baseline for comparison purpose. As is discussed, the round-robin scheduling gives the equal chance to every source and relay to transmit messages. To be specific, \(M \times N\) different source-relay pairs comprised of \(M\) sources and \(N\) relays take turns in accessing the channel. As is known that when the capacity of main channel falls below that of wiretap channel, an intercept event occurs. Given that the source \(S_m\) and the relay \(R_n\) are selected in transmission, the intercept probability can be obtained as

\[
P_{int, SmR_n}^{RR} = \Pr(C_{R_n} < C_{R_n E}),
\]

where \(C_{R_n E}\) and \(C_{R_n}\) are given by (6) and (7), respectively.

Substituting (4) and (5) into (7) and combining with (9), we have

\[
P_{int, SmR_n}^{RR} = \Pr \left[ \min \left( |h_{S_m R_n}|^2, |h_{R_n D}|^2 \right) < |h_{R_n E}|^2 \right].
\]
which can be further expressed as (see Appendix A)

$$P_{int,SmRn}^{RR} = \frac{\sigma_{Rn,D}^2 + \sigma_{SmRn}^2}{\sigma_{Srn,Rn}^2 + \sigma_{SmRn}^2 \sigma_{Rn,E}^2 + \sigma_{Rn,D}^2}.$$  

(11)

Noting that the main-to-eavesdropper ratio (MER) is \(\lambda = \frac{\sigma_{Rn,D}^2}{\sigma_{Rn,E}^2}\), we have

$$P_{int,SmRn}^{RR} = \frac{\sigma_{Rn,D}^2 + \sigma_{SmRn}^2}{\sigma_{Srn,Rn}^2 + \sigma_{SmRn}^2 \lambda + \sigma_{Rn,D}^2}.$$  

(12)

As aforementioned, the conventional round-robin scheduling scheme gives the equal chance to each unique source-relay pair, therefore, the intercept probability of the round-robin scheduling is the mean of \(M \times N\) source-relay pairs intercept probabilities, yielding

$$P_{int}^{RR} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} P_{int,SmRn}^{RR},$$  

(13)

where \(M\) and \(N\) is the number of the sources and relays, respectively. And \(P_{int,SmRn}^{RR}\) is given by (12).

B. Proposed Joint Source-Relay Selection Scheme

In the traditional multi-source multi-relay scheduling, a source-relay pair with the highest instantaneous capacity was chosen as the "best" pair [10]. For protecting the secure transmissions against eavesdropping attacks, we select the optimal source-relay pair by maximizing the secrecy capacity. Accordingly, the best source-relay pair selection criterion is expressed from (8) as

$$(S_{m^*}, R_{n^*}) = \arg \max_{m \in M, n \in N} \frac{1 + \min_{n} |h_{SmRn}|^2, |h_{RnD}|^2}{1 + |h_{RnE}|^2} \gamma,$$  

(14)

which shows that the CSIs of both main links and wiretap links (i.e., \(|h_{SmRn}|^2\), \(|h_{RnD}|^2\) and \(|h_{RnE}|^2\)) are concerned and required. It is a common assumption in the physical-layer security literature [15] that the CSIs of all links are available. As mentioned before, an intercept event occurs when the capacity of main channel falls below that of wiretap channel. Thus, the intercept probability of joint source-relay selection scheme is defined as

$$P_{int}^{SR} = \Pr(\max_{m,n} C_{Rn} < C_{Rn,E}),$$  

(15)

Combining (4)-(7) with (15) gives

$$P_{int}^{SR} = \Pr\left\{\max_{m,n} \left[\min_{n} |h_{SmRn}|^2, |h_{RnD}|^2\right] < |h_{RnE}|^2\right\} = \Pr\left\{\max_{n} \left[\min_{n} |h_{SmRn}|^2, |h_{RnD}|^2\right] < |h_{RnE}|^2\right\} = \prod_{n=1}^{N} \Pr\left\{\min_{n} |h_{SmRn}|^2, |h_{RnD}|^2\right\} < |h_{RnE}|^2\right\},$$  

(16)

where \(|h_{SmRn}|^2 = \max_{m} |h_{SmRn}|^2\). Further proceeding as in Appendix B, we obtain a closed-form expression of intercept probability for the proposed joint source-relay selection scheme as

$$P_{int}^{SR} = \prod_{n=1}^{N} \left[1 + \sum_{j=1}^{M-1} \left(-1\right)^{j}\left(1 + \frac{\sigma_{Rn,D}^2}{\sigma_{Rn,E}^2 \lambda} \right)^{-1}\right],$$  

(17)

where \(\lambda = \frac{\sigma_{Rn,D}^2}{\sigma_{Rn,E}^2}\) represents the MER. \(\varepsilon_j\) is the j-th non-empty sub collection of \(\varepsilon = \{S_m \mid m = 1, 2, \cdots, M\}\) and \(|\varepsilon_j|\) represents the cardinality of set \(\varepsilon_j\).

IV. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we provide simulation results to verify the validity of the proposed schemes. Assume that not only \(M\) sources but also \(N\) relays are clustered together. Thus, the parameters \(\sigma_{SmRn}^2\) are assumed to be equal for different \(m\) and \(n\) as well as \(\sigma_{Rn,D}^2\). In computer simulations, firstly, generate the fading amplitudes (i.e., \(|h_{SmRn}|^2\), \(|h_{RnD}|^2\) and \(|h_{RnE}|^2\)) randomly based on the Rayleigh distribution with different variances for different channels. Then, substitute the generated fading amplitudes into the Eq. (10) and (16) to determine whether an intercept event occurs or not, and repeat this process. Finally, obtain the simulated intercept probability by calculating the relative frequency of occurrence for an intercept event.

Fig. 2 shows the system intercept probability versus MER \(\lambda\) of the joint source-relay selection scheme for different number of sources with the same relays number \(N = 6\). It can be seen that for the cases of \(M = 2, M = 6\) and \(M = 10\), the intercept probability performance is improved apparently. Meanwhile, Fig. 3 shows the system intercept probability versus MER \(\lambda\) of the joint source-relay selection scheme for different numbers of relays with the same sources number \(M = 3\). Similarly, for the case of \(N = 1, N = 6\) and \(N = 10\), the intercept probabilities decrease significantly in Fig. 3. This means that increasing the number of either sources or relays can enhance the secure transmission against eavesdropping attack.

Fig. 4 illustrates the intercept probability of the round robin scheduling and proposed joint source-relay selection schemes for different numbers of sources and relays. It is shown that for different values of \(M\) and \(N\), the theory results of intercept probability match well with the simulation ones, which validates the derived closed-form expressions of the intercept probability in (12) and (17). Moreover, as the numbers of sources and relays change, the intercept probability of the round-robin scheduling stays the same. On the contrary, when the sources and relays numbers increase from \(M = 3, N = 5\) to \(M = 10, N = 10\), the intercept probability performance of the joint source-relay selection scheme is improved significantly. Obviously, the proposed source-relay selection scheme outperforms the conventional round-robin scheduling in terms of intercept probability.

V. CONCLUSIONS

This paper investigated the physical-layer security for multi-source multi-relay cooperative networks in the presence of an eavesdropper. A joint source-relay selection scheme was proposed and the round-robin scheduling was presented as
intercept probability of the joint source-relay selection scheme increases.

Furthermore, upon increasing the number of either sources or relays (or both), the intercept probability of the joint source-relay selection scheme performs better than the round-robin scheme for different numbers of sources and relays.

Proposed scheme w. M=10,N=10 (s.)
Proposed scheme w. M=10,N=10 (t.)
Round-robin w. M=10, N=10 (s.)
Round-robin w. M=10, N=10 (t.)
Proposed scheme w. M=3,N=5 (s.)
Proposed scheme w. M=3,N=5 (t.)
Round-robin w. M=3, N=5 (s.)
Round-robin w. M=3, N=5 (t.)

**ACKNOWLEDGMENT**

This work was supported by the Key Project of Natural Science Research of Higher Education Institutions of Jiangsu Province (No. 14KJA510003 and 15KJA510003).

**APPENDIX A**

**DERIVATION OF (11)**

Denoting \( X = \min \left( |h_{Sm,Rn}|^2, |h_{Rn,D}|^2 \right) \), we can obtain the CDF of \( X \) as

\[
F_X(x) = F_{|h_{Sm,Rn}|^2}(x) + F_{|h_{Rn,D}|^2}(x) - F_{|h_{Sm,Rn}|^2}(x) F_{|h_{Rn,D}|^2}(x) = 1 - \exp \left( -\frac{x}{\sigma_{Rn,D}} - \frac{x}{\sigma_{Sm,Rn}} \right),
\]

wherein \( x \geq 0 \). Substituting (A.1) to (10), we have

\[
P_{int,SmRn}^{RR} = \Pr \left[ \min \left( |h_{Sm,Rn}|^2, |h_{Rn,D}|^2 \right) < |h_{Rn,E}|^2 \right] = \int_0^\infty \left[ 1 - \exp \left( -\frac{x}{\sigma_{Rn,D}} - \frac{x}{\sigma_{Sm,Rn}} \right) \right] \frac{1}{\sigma_{Rn,E}} \exp \left( -\frac{x}{\sigma_{Rn,E}} \right) dx.
\]

Performing integration on \( x \) yields

\[
P_{int,SmRn}^{RR} = \frac{\sigma_{Rn,E}^2 \sigma_{Rn,D}^2 + \sigma_{Sm,Rn}^2 \sigma_{Rn,E}^2}{\sigma_{Sm,Rn}^2 \sigma_{Rn,E}^2 + \sigma_{Sm,Rn}^2 \sigma_{Rn,D}^2 + \sigma_{Rn,E}^2 \sigma_{Rn,D}^2},
\]

which is (11).

**APPENDIX B**

**DERIVATION OF (17)**

Notice that random variables \( |h_{Sm,Rn}|^2, |h_{Rn,D}|^2 \) and \( |h_{Rn,E}|^2 \) follow exponential distributions with means \( \sigma_{Sm,Rn}^2 \),

\( \ldots \)

\( \ldots \)
\[
Pr \{ \min \left( |h_{S_m,R_n}|^2, |h_{R_n,D}|^2 \right) < |h_{R_n,E}|^2 \} \\
= \int_0^\infty \left[ \prod_{m=1}^M \left( 1 - \exp \left( -\frac{\sigma_{R_n,D}^2}{\sigma_{S_m,R_n}^2} \right) \right) \right] \left( \frac{1}{\sigma_{R_n,E}^2} \exp \left( -\frac{\sigma_{R_n,E}^2}{\sigma_{S,R_n}^2} \right) \right) dx
\]

(B.3)

\[
\sigma_{R_n,D}^2 \text{ and } \sigma_{R_n,E}^2, \text{ respectively. Thus, the cumulative density function (CDF) of } |h_{S_m,R_n}|^2 \text{ can be expressed as}
\]

\[
F_{|h_{S_m,R_n}|^2}(x) = \prod_{m=1}^M \left( 1 - \exp \left( -\frac{x}{\sigma_{S_m,R_n}^2} \right) \right), \quad \text{(B.1)}
\]

where \( |h_{S_m,R_n}|^2 = \max_m |h_{S_m,R_n}|^2 \).

Denoting \( X = \min \left( |h_{S_m,R_n}|^2, |h_{R_n,D}|^2 \right) \), the CDF of \( X \) can be given by

\[
F_X(x) = F_{|h_{S_m,R_n}|^2}(x) + F_{|h_{R_n,D}|^2}(x)
- F_{|h_{S_m,R_n}|^2}(x) F_{|h_{R_n,D}|^2}(x)
= 1 - \exp \left( -\frac{x}{\sigma_{S_m,R_n}^2} \right) + \exp \left( -\frac{x}{\sigma_{R_n,D}^2} \right)
\times \prod_{m=1}^M \left( 1 - \exp \left( -\frac{x}{\sigma_{S_m,R_n}^2} \right) \right),
\]

(B.2)

where \( x \geq 0 \). Using Eq. (B.2), we have (B.3) at the top of this page. Employing the binomial theorem, the term \( \prod_{m=1}^M \left[ 1 - \exp \left( -\frac{x}{\sigma_{S_m,R_n}^2} \right) \right] \) can be expanded as

\[
\prod_{m=1}^M \left[ 1 - \exp \left( -\frac{x}{\sigma_{S_m,R_n}^2} \right) \right] = 1 + \sum_{j=1}^{2^{M-1}} (-1)^{\left| \varepsilon_j \right|} \exp \left( -\sum_{S_m \in \varepsilon_j} \frac{x}{\sigma_{S_m,R_n}^2} \right),
\]

(B.4)

where \( \varepsilon_j \) is the \( j \)-th non-empty sub collection of \( \varepsilon = \{S_m | m = 1, 2, \cdots M \} \) and \( \left| \varepsilon_j \right| \) represents the cardinality of set \( \varepsilon \). Substituting (B.4) into (B.3) and performing integration on \( x \) yields

\[
\Omega = \left( 1 + \sigma_{R_n,E}^2 / \sigma_{R_n,D}^2 \right)^{-1}
+ \sum_{m=1}^{2^{M-1}} (-1)^{\left| \varepsilon_m \right|} \left( 1 + \sigma_{R_n,E}^2 / \sigma_{R_n,D}^2 + \sum_{j \in \varepsilon_m} \sigma_{R_n,E}^2 / \sigma_{S_j,R_n}^2 \right)^{-1}
\]

(B.5)

Subsequently combining (B.5), (B.3) and (16), we obtain

\[
P_{SBR}^{int} = \frac{N}{\lambda} \left[ 1 + \sum_{j=1}^{2^M} (-1)^{\left| \varepsilon_j \right|} \left( 1 + \frac{\lambda}{\sum_{S_m \in \varepsilon_j} \sigma_{S_m,R_n}^2} \right)^{-1} \right]
\]

(B.6)

as the desired result (17), where \( \lambda = \sigma_{R_n,D}^2 / \sigma_{R_n,E}^2 \) is the MER.

REFERENCES