Jammer Selection for Secure Two-way DF Relay Communications with Imperfect CSI

Jiajia Wang*, Jingchao Chen†, Hexiang Duan*, Hongbo Ba* and Jianjun Wu*
*Institution of Advanced Communications, EECS, Peking University, Beijing, China
†LinkedIn Corp, California, USA
Email:{wang_jiajia@pku.edu.cn, jcc8887@gmail.com, just@pku.edu.cn}

***Abstract*—This paper investigates jammer selection in a two-way decode-and-forward (DF) relay network with imperfect channel state information (CSI). The proposed scheme enables an selection of one conventional relay and two jamming nodes to enhance communication security against eavesdropper. The conventional relay assists two sources to exchange their data via a DF protocol. The two jamming nodes are used to create interference signals to confuse the eavesdropper. Furthermore, the asymptotic performance of proposed scheme is analyzed in detail. Under the assumption that the relay can decode received signals perfectly and when the jamming power is higher than that of source nodes, we find that the proposed scheme has a high secrecy performance which is almost independent of the position of the eavesdropper.**

Keywords*—Jammer selection, physical layer security, two-way, DF relay, imperfect CSI.

I. INTRODUCTION

Due to their inherent broadcasting nature, wireless communication systems are prone to security threats, which is typically addressed via cryptographic approaches in high layers. However, as the implementation of secrecy at higher layers becomes the subject of increasing potential attacks, much attention has been paid to the study on physical layer security, which proposed the basic idea of implementing perfectly secure communication without using cipher coeds [1]. In order to increase the secrecy rate of networks, cooperative relaying communication is introduced [2], the main objective is to boost the capacity of the primary links by decreasing simultaneously the capacity of the eavesdropper links. Meanwhile, there has been a growing of interest in two-way communications due to its bandwidth efficiency and potential applications to cellular and peer-to-peer networks. In [3], the sum-rate of two sources in two-way relay channel was increased using network coding and channel coding. [4] Introduced a two-way relay memoryless system to optimize the symbol error rate performance.

Based on above consideration, it is significant to investigate the secure two-way relaying communications. Many initiatives [5] [6] has been carried out based on perfect channel state information (CSI). However, the eavesdroppers perfect CSI is unlikely to be available in many scenarios, especially those involving purely passive eavesdroppers. Nevertheless, the statistic knowledge of the eavesdroppers link would be available from long term eavesdropper supervision in practice. Therefore, it is more significative to study the secure two-way DF relay communications based on imperfect CSI.

In this paper, we propose a jammer selection scheme for two-way DF relay communications with imperfect CSI, in which there are two sources, a cluster of intermediate nodes, and one eavesdropper. We assume that the communication process based on time division broadcasting protocol (TDBC), in which both sources transmit to the relay separately in the first two slot while another two jammers are selected from the intermediate nodes to degrade the eavesdropper links, the relay codes the received signals via XOR operation, and broadcasts it back to the source nodes in the third slot. In two-way relay networks, there are two XOR-based relay schemes, which are the 2-step-XOR and the 3-step-XOR. Although the 2-step-XOR scheme achieves larger sum-rate than 3-step-XOR from the information theoretical perspective, it requires synchronization, and is more difficult to be applied to existing networks [7]. Thus, we only consider the 3-step-XOR scheme here.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig.1, We consider a simple configuration consisting of two sources S_1 and S_2, one eavesdropper E and an intermediate node set $\mathbb{S}_{in}$ that includes K nodes. The intermediate nodes are confined within a small region. We assume that there is no direct link between the two sources, and all the intermediate nodes operate in a half-duplex way. Therefore, the complete communication process can be divided into three slots,

- 1): An intermediate node R is selected to operate as a conventional DF relay. Then, S_1 broadcasts its data s_1, which is decoded and stored by R. Meanwhile, another node J_1 is selected from $\mathbb{S}_{in}$ to operate as a jammer to interfere the eavesdropping link in this slot.
- 2): S_2 transmits its data s_2 to R and a second jammer J_2 is selected from $\mathbb{S}_{in}$ for the same reason.
- 3): R broadcasts a coded signal $s = s_1 \oplus s_2$, where $\oplus$ is bitwise XOR.

A slow, flat, block Rayleigh fading environment is assumed, where the channel remains static for one coherence interval (one slot) and changes independently in different coherence intervals with a variance $\sigma_{i,j}^2 = d_{i,j}^{-\beta}$, where $d_{i,j}$ is the Euclidean distance (in kilometers) between node i and j, β is the path-loss exponent. Furthermore, additive white Gaussian

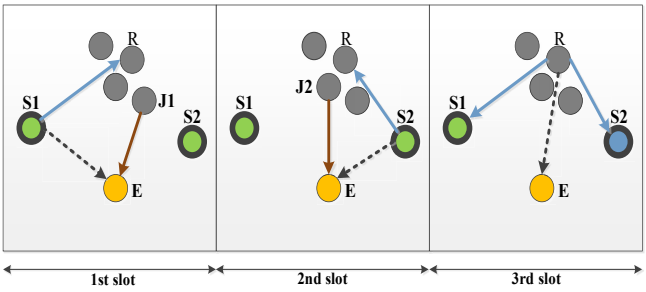

Fig. 1. The system model and the related communication scenario.

noise (AWGN) with zero mean and variance of σ. P_S, P_R, and P_J denote the transmitted power for the source $S_i(i=1,2)$, the relay R, and jammer $J_i(i=1,2)$. The secrecy rate for source $S_i(i=1,2)$ is,

$$R_{S_i} = \left[\frac{1}{3}\log_2\left(1+\gamma_i\right) - \frac{1}{3}\log_2\left(1+\overline{\gamma_{E_j}}\right)\right]^+ \tag{1}$$

Where $i,j=1,2, i\neq j$, and $[x]\triangleq max\{0,x\}$. The pre-log factor $\frac{1}{3}$ is because each traffic flow takes 3-step TDBC protocol.

We assume that R can perfectly decode the signals which received in the first two slots, and eavesdropper applies maximal ration combining (MRC) [8] to combines the received signals. Therefore, γ_i denoted the overall signal-to-noise ratio (SNR) of the channel $S_j \rightarrow S_i(i,j=1,2,i\neq j)$, which can be calculated as

$$\gamma_i = \frac{P_R|h_{R,S_i}|^2}{\sigma^2} \tag{2}$$

$\overline{\gamma_{E_j}}$ denoted the combined SNR for eavesdropper's link, which can be calculated as

$$\begin{aligned}\overline{\gamma_{E_j}} &= \frac{P_S\mathbb{E}\left[\left|h_{S_j,E}\right|^2\right]}{P_J\mathbb{E}\left[\left|h_{J_j,E}\right|^2\right]+\sigma^2} + \frac{P_R\mathbb{E}\left[\left|h_{R,E}\right|^2\right]}{\sigma^2} \\ &= \frac{P_S\sigma^2_{S_j,E}}{P_J\sigma^2_{J_j,E}+\sigma^2} + \frac{P_R\sigma^2_{R,E}}{\sigma^2}\end{aligned} \tag{3}$$

where $\mathbb{E}[\cdot]$ stands for the expectation operator.

The secrecy performance of the whole system is characterized by the secrecy outage probability of the lower secrecy rate of the two source links, which is defined as $\mathbb{P}\{\min(R_{S_1},R_{S_2})<T_S\}$, where T_S is the target secrecy outage threshold and $\mathbb{P}\{\cdot\}$ denotes probability. Therefore, the considered optimization problem is formulated as

$$(R^*,J_1^*,J_2^*) = \underset{\substack{R,J_1,J_2\in\mathbb{S}_{in}\\ R\neq J_1,J_2}}{\text{argmin}} \ \mathbb{P}\{min(R_{S_1},R_{S_2})<T_S\} \tag{4}$$

Where R^*,J_1^*,J_2^* denote the selected relay and jammer. Note that the jammer J_1^* and J_2^* may be the same in the first two slots.

III. SELECTION TECHNIQUE FOR JAMMING

A conventional selection (CS) is proposed in [9], which does not have a jamming process, and does not take the eavesdropper channels into account, so the relay node R is selected according to the instantaneous SNR of the links between node $S1$ and node $S2$. The conventional selection is written as

$$R^* = \arg\max_{R\in\mathbb{S}_{in}}\{min(\gamma_1,\gamma_2)\} \tag{5}$$

[10] investigates a selection technique without jamming (SS) based on imperfect CSI, which takes into account the relay-eavesdropper link.

$$R^* = \arg\max_{R\in\mathbb{S}_{in}}\left\{min\left(\frac{1+\gamma_1}{1+\overline{\gamma_{E_2}}},\frac{1+\gamma_2}{1+\overline{\gamma_{E_1}}}\right)\right\} \tag{6}$$

where

$$\begin{aligned}\overline{\gamma_{E_i}} &= \frac{P_S\mathbb{E}[|h_{S_i,E}|^2]}{\sigma^2} + \frac{P_R\mathbb{E}[|h_{R,E}|^2]}{\sigma^2} \\ &= \frac{P_S\sigma^2_{S_i,E}}{\sigma^2} + \frac{P_R\sigma^2_{R,E}}{\sigma^2}\end{aligned} \tag{7}$$

For high SNRs,

$$R^* = \arg\max_{R\in\mathbb{S}_{in}}\left\{min\left(\frac{\gamma_1}{\overline{\gamma_{E_2}}},\frac{\gamma_2}{\overline{\gamma_{E_1}}}\right)\right\} \tag{8}$$

If the Eavesdropper E has the same distance with source nodes S_1 and S_2, i.e, $\sigma^2_{S_1,E}=\sigma^2_{S_2,E}$, we have $\overline{\gamma_{E_1}}=\overline{\gamma_{E_2}}$. Thus, (8) can be modified as

$$R^* = \arg\max_{R\in\mathbb{S}_{in}}\{min(\gamma_1,\gamma_2)\} \tag{9}$$

which means the SS scheme selects the same relay node R as the conventional selection (CS) scheme does if E has the same distance with S_1 and S_2.

Compared with above selection schemes , we proposed a selection technique with jamming (SJ) based on the combined knowledge of instantaneous relay CSI and average CSI of eavesdropping links. Considering (1) and (4), the selection metrics is modified as

$$(R^*,J_1^*,J_2^*) = \underset{\substack{R,J_1,J_2\in\mathbb{S}_{in}\\ R\neq J_1,J_2}}{\text{argmax}} \left\{min\left(\frac{1+\gamma_1}{1+\overline{\gamma_{E_2}}},\frac{1+\gamma_2}{1+\overline{\gamma_{E_1}}}\right)\right\} \tag{10}$$

Where $\overline{\gamma_{E_j}}$ can be obtained from (3), for high SNRs, and the power ratio of the jammer to the source is much higher than 1, that is $L=P_J/P_S\gg 1$,

$$\begin{aligned}\mathbb{P}_{Asymp} &= \lim_{L\gg 1}\mathbb{P}\{min(R_{S_1},R_{S_2})<T_S\} \\ &= \mathbb{P}\left\{min\left(\frac{|h_{R,S_1}|^2}{\mathbb{E}|h_{R,E}|^2},\frac{|h_{R,S_2}|^2}{\mathbb{E}|h_{R,E}|^2}\right)<\rho\right\} \\ &= \mathbb{P}\{min(X,Y)<\rho Z\}\end{aligned} \tag{11}$$

Where $\rho = 2^{3T_S}$, $X = |h_{R,S_1}|^2$, $Y = |h_{R,S_2}|^2$, $Z = \mathbb{E}|h_{R,E}|^2 = \sigma^2_{R,E}$. Based the assumption that the channel coefficient $h_{R,M}(M = S_1, S_2, orE)$ is a zero-mean, independent, and complex Gaussian random variable with variance $\sigma^2_{R,M}$, for given selected R, $h_{R,M}$ following the exponential distribution with characteristic parameter $\lambda = \sigma^2_{R,M} = d^{-\beta}_{R,M}$. Let $A = min\{X, Y\}$, the cumulative distribution function can be calculated as

$$F_A(a) = 1 - e^{-(\frac{1}{\lambda_X}+\frac{1}{\lambda_Y})a} \tag{12}$$

Therefore,

$$\begin{aligned}
\mathbb{P}_{Asymp} &= \int_0^{+\infty} [F_A(\rho z)]^K \frac{1}{\lambda_Z} e^{-\frac{z}{\lambda_Z}} dz \\
&= \int_0^{+\infty} \sum_{n=0}^{K} C_K^n (-1)^n e^{-(\frac{1}{\lambda_X}+\frac{1}{\lambda_Y})n\rho z} \frac{1}{\lambda_Z} e^{-\frac{z}{\lambda_Z}} dz \\
&= \frac{1}{\lambda_Z} \sum_{n=0}^{K} C_K^n (-1)^n \int_0^{+\infty} e^{-(\frac{1}{\lambda_X}+\frac{1}{\lambda_Y})n\rho z} e^{-\frac{z}{\lambda_Z}} dz \\
&= \sum_{n=0}^{K} C_K^n (-1)^n \frac{1}{\left(\frac{\lambda_Z}{\lambda_X} + \frac{\lambda_Z}{\lambda_Y}\right)n\rho + 1} \\
&= \sum_{n=0}^{K} C_K^n (-1)^n \frac{1}{\left[\left(\frac{d_{R,S_1}}{d_{R,E}}\right)^{\beta} + \left(\frac{d_{R,S_2}}{d_{R,E}}\right)^{\beta}\right]n\rho + 1}
\end{aligned} \tag{13}$$

The minimum secrecy outage probability of SJ scheme can be gotten by setting $\rho = 1$, thus $T_S = 0$.

$$\mathbb{P}_{min} = \sum_{n=0}^{K} C_K^n (-1)^n \frac{1}{\left[\left(\frac{d_{R,S_1}}{d_{R,E}}\right)^{\beta} + \left(\frac{d_{R,S_2}}{d_{R,E}}\right)^{\beta}\right]n + 1} \tag{14}$$

When eavesdropper E is far away from relay R, that is $\delta = \frac{d_{R,S_i}}{d_{R,E}} \to 0 (i = 1, 2)$, (14) can be modified as,

$$\lim_{\delta \to 0} \mathbb{P}_{\min} = \sum_{n=0}^{K} C_K^n (-1)^n \tag{15}$$

IV. Numerical Results

In this section, we carried out computer simulation in order to validate the performance of the proposed selection scheme. Fig.2 shows the considered topology. The area of the network is a $1km \times 1km$ unit square. S_1 and S_2 are located at $(X_{S_1}, Y_{S_1}) = (0, 0)$ and $(X_{S_2}, Y_{S_2}) = (1, 0)$. The center of the intermediate nodes is at $(X_{in}, Y_{in}) = (0.5, 0)$. The number of the intermediate modes is equal to $K = 9$. The path-loss exponent is set $\beta = 3$. The target secrecy outage threshold is $T_S = 0.1$ bits per channel use (BPCU). The variance of the thermal noise is normalized to unit, $\sigma^2 = 30dBm$, and $P_S = P_R = 40dBm$.

The first simulation shows how the power ratio L affects the system secrecy performance. the eavesdropper E locates

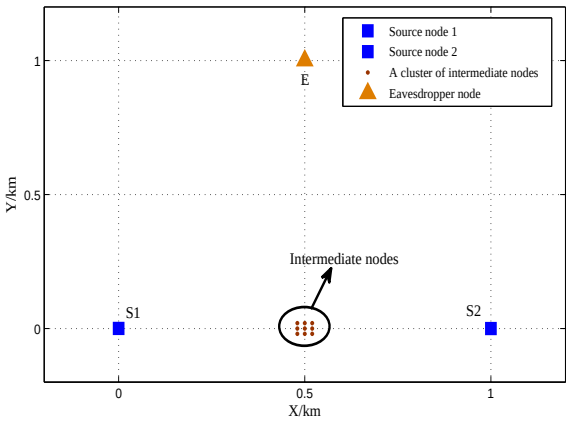

Fig. 2. The simulation environment.

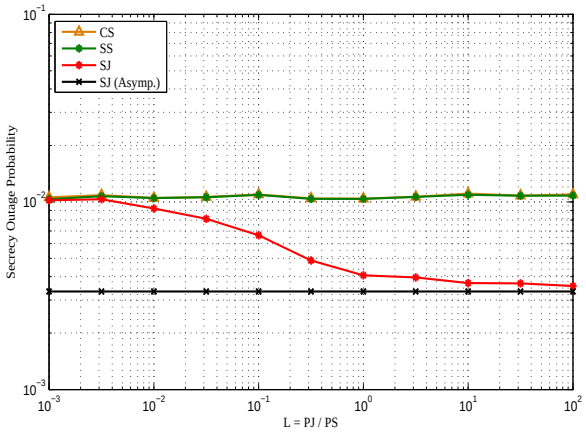

Fig. 3. Secrecy outage probability versus power ratio L for different selection schemes.

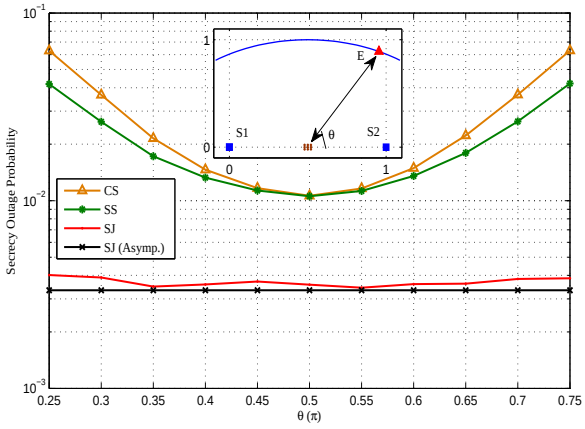

Fig. 4. Secrecy outage probability versus angle of the eavesdroppers position, L=10.

at $(X_E, Y_E) = (0.5, 1)$. we can see from Fig.3 that the conventional selection (CS) which doesn't take the eavesdropper into account has the worst secrecy performance. Although the SS scheme takes into account the relay-eavesdropper link, which based on the imperfect CSI, it performs as poor as the CS scheme in this configuration. When the jamming power is much lower than that of source power $(L < 10^{-3})$, the SJ is almost the same as the CS and SS schemes. As the ratio increases $(10^{-2} < L < 1)$, the secrecy outage probability experiences a substantial drop. When $L > 10$, the secrecy outage probability fits the asymptotic value very well and is much lower than CS and SS schemes. That is to say, the minimum power ratio is 10 in order to achieve better secrecy performance in this configuration.

In Fig.4, we let the eavesdropper E change along the boundary of a fan area. It is clear that the secrecy outage probability of proposed scheme remain at stable levels. In contrast, the CS and SS schemes have varying during this process. This is because the eavesdropping link is very strong when E is near to one of the sources in the first two slots in CS and SS schemes. However, the eavesdropping link is greatly interfered by the strong jamming signals in these two slots, no matter how near E is to the source nodes. Taking both the result in Fig.3 and Fig.4, the proposed scheme (SJ) can not only provide better secrecy performance, but also has more stable than the respecting non-jamming schemes.

V. Conclusion

In this paper, we have dealt with jammer selection for secure two-way DF relay communications based on imperfect CSI. The proposed scheme selects one conventional relay and two jamming nodes to confuse the eavesdropper. We can come to two conclusions by computer simulation, one is that cooperative jamming is an efficient solution to improve the system secrecy performance when the jamming power is much higher than the source power, and the other is that the proposed scheme ia able to provide more stable secrecy outage probability than that of non-jamming schemes.

Acknowledgment

This work is partly supported by the National Science Foundation of China (Grant No. NFSC #61071083, #61371073) and the National High-Tech Research and Development Program of China (863 Program), No.2012AA01A506. Corresponding author: Jianjun Wu, E-mail: just@pku.edu.cn.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Techical Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[2] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Secure wireless communications via cooperation," *in Proceedings of 46th Annual Allerton Conference on Communication, Control and Computing*, UIUC, Illinois, USA, Sep. 2008.

[3] C. Hausl, and J. Hagenauer, "Iterative network and channel decoding for the two-way relay channel," *in Proceedings of IEEE International Conference on Communications*, Istanbul, Turkey, Jun. 2006.

[4] T. Cui, T. Ho, and J. Kliewer, "Memoryless relay strategies for two-way relay channels," *IEEE Transactions on Communications*, vol. 57, no. 10, pp. 3132-3143, Oct. 2009.

[5] J. Chen, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure Decode-and-Forward tow-way relay communications," *IEEE Global Telecommunications Conference (Globecom 2011)*, Houston, TX, USA, Oct. 2009.

[6] R. Zhang, L. Song, Z. Han, B. Jiao and M. Debbah, "Physical layer security for two way relay communications with friendly jammers," *IEEE Global Telecommunications Conference (Globecom 2010)*, Miami, FL, Dec. 2010.

[7] L. Ding, M. Tao, F. Yang and W. Zhang, "Joint scheduling and relay selection in one- and two-way relay networks with buffering," *IEEE International Conference on Communicaitons (ICC 2009)*, Dresden, Jun. 2009.

[8] T. S. Rappaport, Wireless communicaitons principles and practice, 2nd ed. Prentice Hall, 2002.

[9] A. Bletsas, A. Khisti, D. P. Reed and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE Jounrnal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659-672, Mar. 2006.

[10] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, pp. 1787-1791, Oct. 2010.

Jiajia Wang received the B.S. degree in communication engineering from Xi'an Communications Institute, Xi'an, P. R. China, in 2005. He is currently pursuing his M.S. degree in Peking University under the supervision of Associate Prof. Jianjun Wu. His current research interests include satellite mobile communications and wireless communications. E-mail: wang_jiajia@pku.edu.cn.

Jianjun Wu received his B.S., M.S. and Ph.D. degree from Peking University, Beijing, P. R. China, in 1989, 1992 and 2006, respectively. Since 1992, he has joined the School of Electronics Engineering and Computer Science, Peking University, and has been appointed as an Associate Professor since 2002. His research interests are in the areas of satellite communications, wireless communications, and signal processing. The corresponding author. Email: just@pku.edu.cn.