On the Secure Outage Performance for Dual-Hop Network Coding Systems with Cooperative Jamming

Hequn Liu, Mingtai He, Yameng Zhou, Tianli Wu, Gaofeng Pan, and Tingting Li

***Abstract*—In this paper, a design of cooperative network coding (NC) and jammer relay (JR) is proposed for this two-way network in order to improve the security of the date exchange. Considering the system over Rayleigh fading channels in the presence of one eavesdropper and two relays, we study secrecy outage (including the probability of non-zero secrecy capacity and secure outage probability), respectively. In this paper, one relay is regarded as NC relay which is used to make codes by xor in order to prevent eavesdropper's interception while the other one is regarded as a jammer relay which can send interference to eavesdropper. We derive exact expressions for the secure outage probability. The accuracy of our performance analysis is verified by simulation results.**

***Index Terms*—Network coding, jammer relay, secure outage probability, secure communications.**

I. Introduction

The broadcast nature of the wireless medium makes the communication process vulnerable to eavesdroppers which are in the coverage area of the transmission. Thus, security in physical layer of wireless communication networks has taken on an increasingly important role. Traditionally, security was viewed as an independent issue addressed above the physical layer until eavesdropping attack was first studied in the 1970s by Wyner [1] and later by Csisz ́ar and Korner [2].

Recently, there has been a considerable recent attention on studying physical layer secure in cooperative communication scenarios. The main idea is to exploit user cooperation in facilitating the transmission of confidential messages from the source to the destination. In [3], conventional method is using a jammer relay to send jamming to eavesdroppers in order to interfere its capture ability. [4] adopts two types of relays, one is used to transmit confidential messages and the other one is used to send interference to the eavesdropper. To be different from [4], [5] and [6] use the destination node as the jammer witch sends interference to the untrusted relay (potential eavesdropper). In [7], destination sends intended jamming noise to relay and then relay transmit messages with noise to destination and eavesdropper, in another word, this relay is both a transfer station and a jammer. In [8], the authors do not consider the direct link between eavesdropper and source while the destination sends an intended jamming noise to the relay, referred to as cooperative jamming.

In this work, we consider network coding (NC) as the cooperation scheme as it is much more superior to other relaying schemes in secure communication. NC disguises messages by the way that NC relay takes several packets and combines them together for transmission. Thus, it can improve a network's throughput, efficiency and scalability, as well as resilience to attacks and eavesdropping [9]. In this paper, we study the secure outage performance for a dual-hop NC cooperative system in presence of an eavesdropper and two relays. The closed-form expressions of the probability of nonzero secrecy capacity and secure outage probability have been derived.

II. System Model

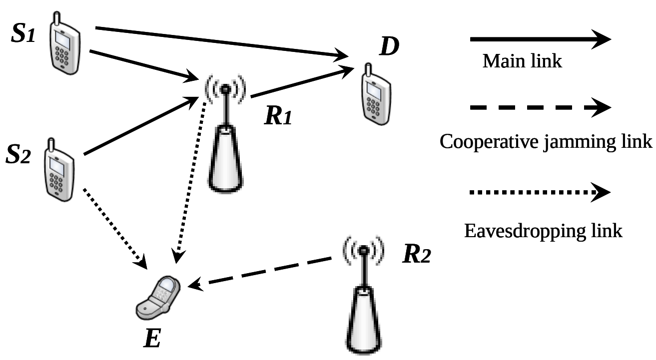


Fig. 1. System model.

Consider a two-way network consisting of two relays, two sources, one destination and one eavesdropper, as shown in Fig. 1. All nodes in the network are equipped with a single half-duplex antenna. In phase 1, both S_1 and S_2 send their message m_{S_1} and m_{S_2} to the relay node R_1 and S_1 also sends its message to the destination D. The received signals at R_1 can be given by

$$y_{S_1R_1} = \sqrt{P_{S_1}} h_{S_1R1} \cdot m_{S_1} + n_{R_1}, \tag{1}$$

and

$$y_{S_2R_1} = \sqrt{P_{S_2}} h_{S_2R_1} \cdot m_{S_2} + n_{R_1}, \tag{2}$$

and the received signal at D can be given by

$$y_{S_1D} = \sqrt{P_{S_1}} h_{S_1D} \cdot m_{S_1} + n_D, \tag{3}$$

Manuscript received April 12, 2014; revised June 13, 2014. This research was supported in part by National Undergraduate Training Programs for Innovation and Entrepreneurship under Grant 201310635044, in part by the doctor foundation of Southwest University under Grant SWU112028, the Fundamental Research Funds for the Central Universities under Grant XDJK2013C093, Natural Science Foundation Project of CQ CSTC under Grant cstc2013jcyjA40040, Science and Technology Personnel Training Program Fund of Chongqing (NO.cstc2013kjrcqnrc40011), Research Fund for the Doctoral Program of Higher Education of China under Grant 20130182120017.

Hequn Liu, Mingtai He, Yameng Zhou, Tianli Wu, and Gaofeng Pan are with the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China (e-mail: pan.156@osu.edu).

Tingting Li is with School of Mathematics and Statistics, Southwest University, Chongqing, 400715, China.

DOI: 10.7763/IJIEE.2014.V4.488

$$\Pr\{C \le R\} = 1 - \left\{\exp\left[-\left(\alpha_{S_1R_1} + \alpha_{S_1D} + \alpha_{R_1D}\right)\left(2^{2R}-1\right)\right]\right\}$$

$$\cdot\left[\frac{\alpha_{S_2E}}{\alpha_{R_2E}} + \alpha_{S_2R_1}2^{2R}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\right]\cdot\frac{\alpha_{R_2E}\exp\left(-\alpha_{S_2R_1}2^{2R}+\alpha_{S_2R}\right)}{\alpha_{S_2E}} \quad (11)$$

where P_i is the transmit power at node i ($i \in \{S_1, S_2, R_1\}$); n_j ($j \in \{R_1, D\}$) is the complex additive white Gaussian noise (AWGN) with zero mean and variance σ^2 and h_{ij} is the channel coefficient from the node i to node j.

In phase 2, R_1 decodes out the message m_{S_1} and m_{S_2} from the received signal y_{S_1} and y_{S_2} and then sends the signal m_{R_1} which is given by $m_{R_1} = m_{S_1} \oplus m_{S_2}$ to node D. The received signal y_{R_1D} at D is given by

$$y_{R_1D} = \sqrt{P_{R_1}}h_{R_1D} \cdot m_{R_1} + n_D. \quad (4)$$

At the node D, D can decode out the message m_{S_2} by the expression $m_{S_2} = m_{S_1} \oplus m_{R_1}$, so D can get both m_{S_1} and m_{S_2}.

In both phase 1 and 2, the eavesdropper node E can capture partial messages of the link from S_2 to R_1 and the link from R_1 to D, at the meantime, the node R_2 sends interference to E.

III. Secure Outage Probability

In this section, we derive the closed-form expressions for PNSC and SOP.

Let γ_{ij} represents the Signal-to-Noise-Ratio (SNR) of the link i-to-j ($i, j \in \{S_1, S_2, D, R_1, E\}$), we have

$$\gamma_{ij} = P_i\left|h_{ij}\right|^2 / N_0, \quad (5)$$

where N_0 is the power of the AGWN.

For h_{ij} follows Rayleigh distribution, γ_{ij} follows exponential distribution, $\gamma_{ij} \sim \exp\left(\frac{N_0}{2\sigma_{ij}^2P_i}\right)$.

The secrecy capacity of the link from S_1 to R_1 can be given by

$$C_1 = C_{S_1R_1} = \frac{1}{2}\log_2\left(1+\gamma_{S_1R_1}\right), \quad (6)$$

so we can get the following secrecy capacities which can be given by

$$C_2 = C_{S_2R_1} = \frac{1}{2}\log_2\left(1+\gamma_{S_2R_1}\right) - \frac{1}{2}\log_2\left(1+\frac{\gamma_{S_2E}}{1+\gamma_{R2E}}\right), \quad (7)$$

$$C_3 = C_{S_1D} = \frac{1}{2}\log_2\left(1+\gamma_{S_1D}\right), \quad (8)$$

$$C_4 = C_{R_1D} = \frac{1}{2}\log_2\left(1+\gamma_{R_1D}\right). \quad (9)$$

Then the PNSC can be expressed as

$$\begin{aligned}\Pr\{C>0\} &= \Pr\{\min\{C_1, C_2, C_3, C_4\} > 0\} \\ &= 1 + \frac{\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\right),\end{aligned} \quad (10)$$

where $\alpha_{ij} = \frac{N_0}{2\sigma_{ij}^2P_i}$ and $Ei(x)$ is exponential integral function. The detailed derivation of Eq.(10) can be found in Appendix.

And the secure outage probability (SOP) can be given by the Eq. (11), where $\alpha_{ij} = \frac{N_0}{2\sigma_{ij}^2P_i}$ and and $Ei(x)$ is exponential integral function. The detailed derivation of Eq.(11) can be found in Appendix.

IV. Numerical Results and Discussion

In this section, we present Monte Carlo simulation, theoretical and analytical results corresponding to the secrecy outage (including the PNSC and SOP) over independent Rayleigh fading channels. The main parameters used in simulation and analysis are set as $\sigma_{s_1d} = 1.5$, $\sigma_{r_1d} = 2.5$, $\sigma_{r_1e} = \sqrt{3/2}$, $\sigma_{s_2e} = \sqrt{3/2}$, $P_{S_1} = P_{S_2} = P_D = P_{R_1} = P_{R_2} = 1$, $\lambda = \sigma_{S_2R_1}/\sigma_{R_2E}$.

In Fig. 2-Fig. 3, we compare simulation, theoretical and analytical results of PNSC. It is seen that the simulation results match very well with the theoretical and analytical results. Further, it could be observed that PNSC for a higher σ_3 outperforms that of a lower σ_3. Fig. 2 describes that the PNSC versus ω. We also find that PNSC has been improved while ω increases because a larger ω means a better S-R1 link. Fig. 3 describes that PNSC versus SNR. We can see that the increasing of SNR can improve PNSC.

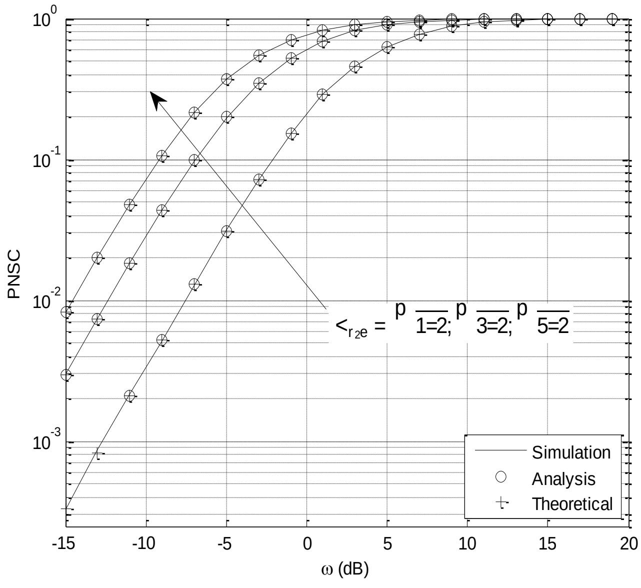


Fig. 2. PNSC versus ω.

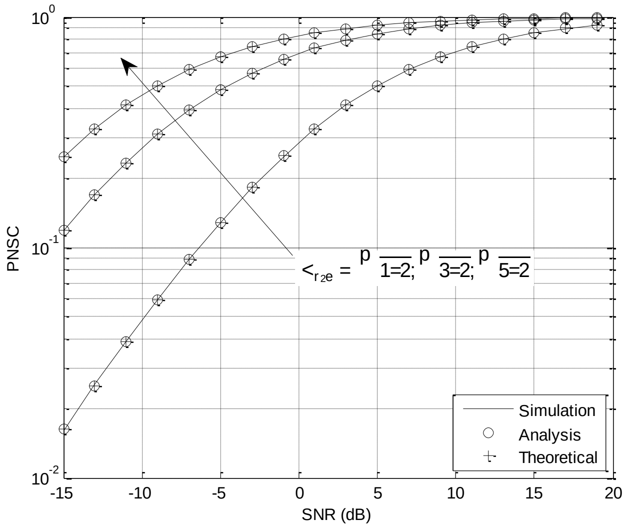


Fig. 3. PNSC versus SNR.

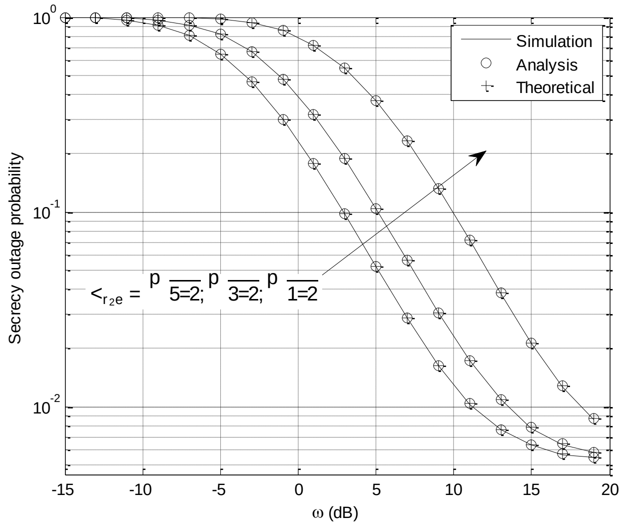


Fig. 4. SOP versus ω (R = 0.01).

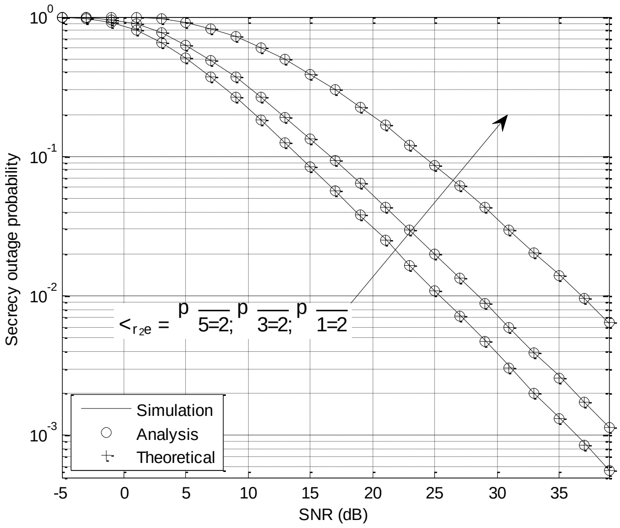


Fig. 5. SOP versus SNR (R = 1).

In Fig. 4 - Fig. 5, we present the comparisons among simulation, theoretical and analytical results of SOP. It is obvious that simulation, theoretical and analytical results match with each other very well. Further, we also see that SOP for a higher σ_{r2e} outperforms that of a lower σ_{r2e}. Some similar observations can be found in Figs. 4 and 5 with the ones found in Fig. 2 and Fig. 3, i.e., the effect of ω and SNR on PNSC and SOP.

V. Conclusion

In this paper, we have investigated the secure outage performance for cooperative NC communication systems over independent Rayleigh fading channels. The closed-form expressions for the probability of nonzero secrecy capacity and secure outage probability have been derived. The simulation results are in excellent agreement with the theoretical and analytical results obtained in this work.

Appendix

In order to get the PNSC and SOP, we can first calculate the probabilities of that each instantaneous secrecy capacity C_i ($i \in \{1,2,3,4\}$) is below a target secrecy rate R.

We have already known that $\gamma_{i,j}$ follows an exponential distribution, so the SOP of the C_i ($i \in \{1,3,4\}$) can be given by

$$\Pr\{C_1 \le R\} = 1 - \exp\left[-\alpha_{S_1R_1}\left(2^{2R}-1\right)\right], \tag{12}$$

$$\Pr\{C_3 \le R\} = 1 - \exp\left[-\alpha_{S_1D}\left(2^{2R}-1\right)\right], \tag{13}$$

$$\Pr\{C_4 \le R\} = 1 - \exp\left[-\alpha_{R_1D}\left(2^{2R}-1\right)\right]. \tag{14}$$

If $R=0$, we can get

$$\Pr\{C_1 \le 0\} = \Pr\left\{\gamma_{S_1R_1} \le 0\right\} = 0 , \tag{15}$$

$$\Pr\{C_3 \le 0\} = \Pr\left\{\gamma_{S_1D} \le 0\right\} = 0 , \tag{16}$$

$$\Pr\{C_4 \le 0\} = \Pr\left\{\gamma_{R_1D} \le 0\right\} = 0 . \tag{17}$$

The item $\Pr\{C_2 \le R\}$ can be given by

$$\begin{aligned}
\Pr\{C_2 \le R\} &= \Pr\left\{\frac{1+\gamma_{S_2R_1}}{1+\dfrac{\gamma_{S_2E}}{\gamma_{R_2E}}} \le 2^{2R}\right\} \\
&= \Pr\left\{\gamma_{S2R_1} \le 2^{2R}\left(1+\gamma_e\right)-1\right\} \\
&= \int_0^\infty \Pr\left\{\gamma_{S_2R_1} \le 2^{2R}\left(1+s\right)-1\right\} dF_{\gamma_e}(s) \\
&= \int_0^\infty \Pr\left\{\gamma_{S_2R_1} \le 2^{2R}\left(1+s\right)-1\right\} f_{\gamma_e}(s) ds
\end{aligned} \tag{18}$$

where $F_{\gamma_e}(s)$ denotes the probability distribution function of γ_e which denotes $\frac{\gamma_{S_2E}}{\gamma_{R_2E}}$ and $f_{\gamma_e}(s)$ denotes the probability density function of γ_e .We use $f_2(x)$ and $f_3(x)$ respectively denote the PDF of γ_{S_2E} and γ_{R_2E} , so the calculation of γ_e can be given by

$$\begin{aligned}
f_{\gamma_e}(s) &= \int_0^\infty x f_2(sx) f_3(x) dx \\
&= \int_0^\infty x \cdot \alpha_{S_2E} \exp\left(-\alpha_{S_2E} s x\right) \cdot \alpha_{R_2E} \exp\left(-\alpha_{R_2E} x\right) dx \\
&= \alpha_{S_2E}\alpha_{R_2E} \int_0^\infty x \exp\left(-\left(\alpha_{S_2E} s + \alpha_{R_2E}\right) x\right) dx
\end{aligned}$$

$$=\frac{\alpha_{S_2E}\alpha_{R_2E}}{\left(\alpha_{S_2E}s+\alpha_{R_2E}\right)^2}. \tag{19}$$

Then the SOP of C_2 can be given by

$$\begin{aligned}
\Pr\{C_2\le R\} &= \Pr\left\{\frac{1+\gamma_{S_2R_1}}{1+\dfrac{\gamma_{S_2E}}{\gamma_{R2E}}}\le 2^{2R}\right\} \\
&= \Pr\left\{\gamma_{S2R_1}\le 2^{2R}(1+\gamma_e)-1\right\} \\
&= \int_0^\infty \Pr\left\{\gamma_{S_2R_1}\le 2^{2R}(1+s)-1\right\} f_{\gamma_e}(s)ds \\
&= \int_0^\infty \left\{1-\exp\left[-\alpha_{S_2R_1}\left(2^{2R}(1+s)-1\right)\right]\right\}\frac{\alpha_{S_2E}\alpha_{R_2E}}{\left(\alpha_{S_2E}s+\alpha_{R_2E}\right)^2}ds \\
&= 1-\frac{\alpha_{R_2E}\exp\left(-\alpha_{S_2R_1}2^{2R}+\alpha_{S_2R_1}\right)}{\alpha_{S_2E}}. \\
&\cdot\left[\frac{\alpha_{S_2E}}{\alpha_{R_2E}}+\alpha_{S_2R_1}2^{2R}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\right]
\end{aligned} \tag{20}$$

When $R=0$, we can get

$$\begin{aligned}
\Pr\{C_2\le 0\} &= \Pr\left\{\frac{1+\gamma_{S_2R_1}}{1+\dfrac{\gamma_{S_2E}}{\gamma_{R2E}}}\le 1\right\}=\Pr\left\{\gamma_{S2R_1}\le\gamma_1\right\} \\
&= -\frac{\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\right).
\end{aligned} \tag{21}$$

Finally, the PNSC can be given by

$$\begin{aligned}
\Pr\{C>0\} &= \Pr\left\{\min\{C_1,C_2,C_3,C_4\}>0\right\} \\
&= \Pr\{C_1>0\}\Pr\{C_2>0\}\Pr\{C_3>0\}\Pr\{C_4>0\} \\
&= \prod_{i=1}^{4}\left(1-\Pr\{C_i\le 0\}\right) \\
&= 1+\frac{\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}}{\alpha_{S_2E}}\right),
\end{aligned} \tag{22}$$

and the SOP can be given by

$$\begin{aligned}
\Pr\{C\le R\} &= \Pr\left\{\min\{C_1,C_2,C_3,C_4\}\le R\right\} \\
&= 1-\Pr\left\{\min\{C_1,C_2,C_3,C_4\}>R\right\} \\
&= 1-\Pr\{C_1>R\}\Pr\{C_2>R\}\Pr\{C_3>R\}\Pr\{C_4>R\} \\
&= 1-\prod_{i=1}^{4}\left(1-\Pr\{C_i\le R\}\right) \\
&= 1-\left\{\exp\left[-\alpha_{S_1R_1}\left(2^{2R}-1\right)\right]\right\}\left\{\exp\left[-\alpha_{S_1D}\left(2^{2R}-1\right)\right]\right\} \\
&\cdot\left\{\exp\left[-\alpha_{R_1D}\left(2^{2R}-1\right)\right]\right\}\cdot\frac{\alpha_{R_2E}\exp\left(-\alpha_{S_2R_1}2^{2R}+\alpha_{S_2R_1}\right)}{\alpha_{S_2E}} \\
&\cdot\left[\frac{\alpha_{S_2E}}{\alpha_{R_2E}}+\alpha_{S_2R_1}2^{2R}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\right] \\
&= 1-\left\{\exp\left[-\left(\alpha_{S_1R_1}+\alpha_{S_1D}+\alpha_{R_1D}\right)\left(2^{2R}-1\right)\right]\right\} \\
&\cdot\left[\frac{\alpha_{S_2E}}{\alpha_{R_2E}}+\alpha_{S_2R_1}2^{2R}\exp\left(\frac{\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\cdot Ei\left(\frac{-\alpha_{S_2R_1}\alpha_{R_2E}2^{2R}}{\alpha_{S_2E}}\right)\right] \\
&\cdot\frac{\alpha_{R_2E}\exp\left(-\alpha_{S_2R_1}2^{2R}+\alpha_{S_2R}\right)}{\alpha_{S_2E}}
\end{aligned} \tag{23}$$

REFERENCES

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

[2] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] E. Tekin and A. Yener, “Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy,” in *Proc. 44th Annu. Allerton Conf. Commun. Contr., Comput.*, 2006.

[4] I. Krikidis, J. S. Thompson, and S. Mclaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

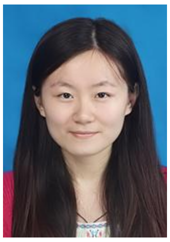
[5] X. He and A. Yener, “Two-hop secure communication using an untrusted relay,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1-13, Oct. 2009.

[6] J. Huang, A. Mukherjee, and A. L. Swindlehurst, “Secure communication via an untrusted non-regenerative relay in fading channels,” *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp.2536-2550, May 2013.

[7] Li Sun *et al*, “Performance study of two-hop amplify -and-forward systems with untrustworthy relay nodes,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801-3807, Oct. 2012.

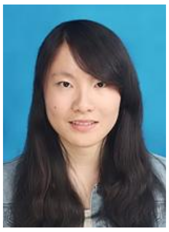
[8] K. H. Park, T. Wang, and M. S. Alouini, “On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741-1750, Sept. 2013.

[9] R. Bassoli, H. Marques, J. Rodriguez *et al*., “Network coding theory: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 1950-1978, Dec. 2013.



Hequn Liu is currently working toward the B.Eng. degree in communication engineering at the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China. Her research interests include performance modeling and evaluation of wireless communication systems.

Mingtai He is currently working toward the B.Eng. degree in communication engineering at the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China. Her research interests include performance modeling and evaluation of wireless communication systems.



Yameng Zhou is currently working toward the B.Eng. degree in communication engineering at the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China. Her research interests include performance evaluation of wireless communication systems.

Tianli Wu is currently working toward the B.Eng. degree in communication engineering at the School of Electronic and Information Engineering, Southwest University, Chongqing, 400715, China. Her research interests include performance modeling and evaluation of wireless communication systems.

Gaofeng Pan received his B.Sc in communication engineering from Zhengzhou University, Zhengzhou, China, in 2005, and the Ph.D. degree in communication and information systems from Southwest Jiaotong University, Chengdu, China, in 2011.

In May 2012, he joined the School of Electronic and Information Engineering, Southwest University, Chongqing, China, where he is currently a Specially Appointed Associate Professor. His research interest spans special topics in communications theory and signal processing, including cooperative communications, and CR communications. He has served as the reviewer for IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Transactions on Vehicular Technology, IEEE Communications Letters, Wireless Communications and Mobile Computing (Wiley), International Journal of Communication Systems.

Tingting Li received her B.Sc in mathematics and applied mathematics from Chongqing University, Chongqing, China, in 2006 and the Ph. D degree in Computational Mathematics from Chongqing University, Chongqing, China, in 2012.

In July 2012, she joined the School of Mathematics and Statistics, Southwest University, Chongqing, China, where she is currently a lecturer in Department of Statistics. Her research interests are theory and applications on probability and statistics.