EFFECTS OF IMPERFECT CSIs ON DECODE-AND- FORWARD RELAYING UNDER PHYSICAL LAYER SECURITY

ẢNH HƯỞNG CỦA CSI KHÔNG HOÀN HẢO TRÊN CHUYỂN TIẾP DECODE-AND- FORWARD VỚI BẢO MẬT LỚP VẬT LÝ

Pham Ngoc Son
Ho Chi Minh City university of Technology and Education

Received 01/3/2016, Peer reviewed 15/3/2016, Accepted for publication 15/5/2016

ABSTRACT

Previous works on cooperative communication protocols under physical layer security have only considered perfect channel state information (CSI). In practice, fading channel coefficients are estimated imperfectly at receivers. In this paper, I propose and analyze a cooperative communication scheme under physical layer security with imperfect CSI. In this scheme, a source node transmits secure data to a destination node D with a help of a relay node against an eavesdropper node without direct links of source-destination and source-eavesdropper. The secrecy performance of the proposed scheme is presented by the secrecy outage probability in the closed-form expression. Simulation and analysis results demonstrate that the proposed secrecy scheme is more effective when the channel estimation error at the destination node is smaller than that at the eavesdropper node, and when the distance of the wiretapping link increases. In addition, the analysis values of the secrecy outage probability matches well with the simulation results.

Keywords: *Physical layer security, imperfect channel state information, decode-and-forward relaying, secrecy outage probability, MMSE estimation method.*

TÓM TẮT

Các công việc trước đây trên các giao thức truyền thông hợp tác với bảo mật lớp vật lý chỉ quan tâm thông tin trạng thái kênh hoàn hảo. Trong thực tế, các hệ số kênh pha đinh được dự đoán ở các bộ nhận không hoàn hảo. Trong bài báo này, tôi đề xuất và phân tích một mô hình truyền thông hợp tác quan tâm bảo mật lớp vật lý với thông tin trạng thái kênh không hoàn hảo. Trong mô hình này, một nút nguồn phát dữ liệu bảo mật đến một nút đích với sự giúp đỡ của một nút chuyển tiếp chống lại một nút nghe lén không có kết nối trực tiếp nguồn-đích và nguồn-nghe lén. Hiệu suất bảo mật của mô hình đề xuất được trình bày bằng xác suất lỗi bảo mật trong một biểu thức dạng đóng. Các kết quả mô phỏng và phân tích chứng minh rằng mô hình bảo mật được đề xuất hiệu quả hơn khi lỗi dự đoán kênh ở nút đích nhỏ hơn lỗi dự đoán kênh ở nút nghe lén, và khi khoảng cách của tuyến nghe lén tăng. Hơn nữa, các giá trị phân tích của xác xuất lỗi bảo mật phù hợp tốt với các kết quả mô phỏng.

Từ khóa: *Bảo mật lớp vật lý, thông tin trạng thái kênh không hoàn hảo, chuyển tiếp decode-and-forward, xác suất lỗi bảo mật, phương pháp dự đoán MMSE.*

1. INTRODUCTION

Secrecy data transmission is investigated at the physical layer and is very important in wireless broadcasting systems [1-4]. Differently from higher layer security, secrecy communication does not exchange cipher keys between two source nodes. In [2], A.D. Wyner first proposed physical layer security has demonstrated that private information is secure at the intended destination if the capacity of a main link (source-to-destination) is larger than that of a wiretapping link (source-to-eavesdropper). In [3], the achievable secrecy rate (ASR) is indicated as an important metric for measuring the amount of secure information that is successfully get at the destination.

Cooperative communication is an efficient solution for overcoming the effect of the fading environment and obstruction [5-9]. In this solution, the diversity capacity as well as the channel quality is enhanced with the help of relaying nodes, called relays. The operation methods at the cooperative relays are the decode-and-forward (DF) and amplify-and-forward (AF) architectures. In the DF architecture, the relays must successfully decode the received signals from the source whereas in the AF architecture, the relays only amplify the received signals without complex decoding operations. Both the DF and AF architectures, the relays also forward the processed signals to the intended destination. Therefore, the AF architecture is simpler processing but creates more noise than the DF architecture. In addition, the AF architecture is efficient in the low signal-to-noise ratio (SNR) regions, where the DF architecture has difficulty in decoding operations. Imperfect channel state information (CSI) is investigated in cooperative communications to again evaluate system performances [7-10]. In the imperfect CSI, the receivers cannot perfectly detect the received fading channel coefficients. The minimum mean-square error (MMSE) estimation method with the non-zero error variance has been applied in [9-10] to model the fading channel coefficients.

In this paper, I propose and analyze a cooperative communication scheme under physical layer security with imperfect CSIs. In this scheme, a cooperative relay uses the DF architecture to help a source-destination communication under presence of an eavesdropper node. The analysis results are obtained by secrecy outage probabilities in exact closed-form expressions. My simulation results show that the secrecy performance of the proposed protocol is improved when the channel estimation error at the destination node is smaller than that at the eavesdropper node, and when the distance of the wiretapping link (relay-to-eavesdropper) is large.

The rest of the paper is organized as follows. Section 2 presents the system model. The secrecy performance analysis is obtained by the secrecy outage probability outlined in Section 3. Section 4 discusses the simulation results using the Monte Carlo method and theoretical expressions. Conclusions are summarized in Section 5.

2. SYSTEM MODEL

Figure 1 presents a cooperative communication scheme under physical layer security with imperfect CSIs. In this scheme, a source node S transmits secure data to a destination node D with a help of a relay node R against an eavesdropper node E without direct links of S-D and S-E. I assume that each node has a single antenna and the same transmit power P, and that all

channels are assumed to be complex Gaussian random variables [9].

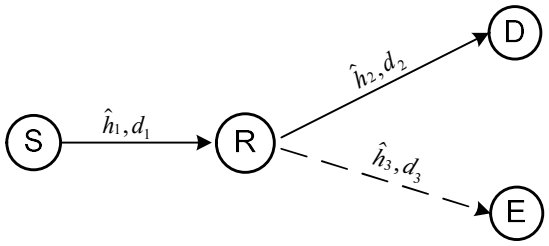

Figure 1. *System model.*

In addition, the nodes R, D, and E estimate channel coefficients S-R, R-D, and R-E, respectively, used the MMSE method with existing estimation errors [10]. The exact fading channel coefficients of links S-R, R-D, and R-E are expressed as

$$h_k = \hat{h}_k + e_k \quad (1)$$

where h_k are complex Gaussian random variables; and symbols $\hat{h}_k$ and e_k are estimated fading channel coefficients and estimation errors of channels h_k, respectively, $k \in \{1, 2, 3\}$.

For simplicity, all estimation errors e_k are also complex Gaussian random variables with variances σ_k^2, and these estimation errors e_k are independent with the estimated fading channel coefficients $\hat{h}_k$, respectively [10]. Hence, the channel coefficients $\hat{h}_k$ are complex Gaussian random variables with variances $\left(d_k^{-\beta} - \sigma_k^2\right)$, where symbols d_k are the link distances and β is the path-loss exponent.

The estimated channel gains $\left|\hat{h}_k\right|^2$ are the exponential distributions [9] with parameters as

$$\lambda_k = \frac{1}{d_k^{-\beta} - \sigma_k^2}, k \in \{1, 2, 3\} \quad (2)$$

The operation principle of the cooperative communication scheme under physical layer security with imperfect CSIs is split into two time slots as follows. In the first time slot, the source node S broadcasts its signals *x* to the relay R. Then, the relay R will try to decode the signals *x*, recode and forward the signals *x* to the nodes D and E in the second time slot.

The signal is received at the relay node R [10] as follows:

$$y_r = \sqrt{P}\left(\hat{h}_1 + e_1\right)x + n_r \quad (3)$$

where n_r is the zero-mean additive white Gaussian noise (AWGN) with variance σ_r^2.

If the relay R successfully decode the signals *x*, then the received signals at the destination node D and the eavesdropper node E are obtained, respectively, as

$$y_d = \sqrt{P}\left(\hat{h}_2 + e_2\right)x + n_d \quad (4)$$

$$y_e = \sqrt{P}\left(\hat{h}_3 + e_3\right)x + n_e \quad (5)$$

where n_d and n_e are the AWGNs with variances σ_d^2 and σ_e^2.

3. SECRECY OUTAGE PROBABILITY

I assume that the relay R successfully decodes the signals *x* from the source node S if the achievable data rate at the relay R is larger than a target data rate R_{de}. It is also assumed that the destination D receives secure signals if the ASR of the link R-D under eavesdropping of the eavesdropper E is larger than a target secrecy rate R_{se}, where $R_{se} \le R_{de}$ [4].

Based on the operation principle of the proposed scheme, the secrecy outage probability of the communication S-D is expressed by

$$P_{S-D}^{so} = \underbrace{\Pr\left[R_1 < R_{de}\right]}_{\Pr\_1} + \underbrace{\Pr\left[R_1 \geq R_{de}, ASR < R_{se}\right]}_{\Pr\_2} \quad (6)$$

where R_1 is the achievable data rate of the link S-R; ASR is the achievable secrecy rate of the link R-D under eavesdropping of the node E and is given as [3]

$$ASR = \left\{R_2 - R_3\right\}^+ \quad (7)$$

where $\{x\}^+$ is defined as $\max\{x,0\}$; R_2 and R_3 are the achievable data rates of the links R-D and R-E, respectively.

From formulas (3), (4) and (5), the instantaneous SNRs γ_1, γ_2 and γ_3 of the links S-R, R-D and R-E are obtained, respectively, as

$$\gamma_1 = P\left|\hat{h}_1\right|^2 \Big/ \left(P\sigma_1^2 + \sigma_r^2\right) \quad (8)$$

$$\gamma_2 = P\left|\hat{h}_2\right|^2 \Big/ \left(P\sigma_2^2 + \sigma_d^2\right) \quad (9)$$

$$\gamma_3 = P\left|\hat{h}_3\right|^2 \Big/ \left(P\sigma_3^2 + \sigma_e^2\right) \quad (10)$$

Then, the achievable data rates R_k, $k \in \{1, 2, 3\}$, are given as

$$R_k = \frac{1}{2}\log_2\left(1+\gamma_k\right), k \in \{1, 2, 3\} \quad (11)$$

where the ratio 1/2 denotes that the proposed scheme operates in two time slots.

Substituting (11) with *k=1* into the formula Pr_1 in (6), Pr_1 is obtained as

$$\begin{aligned}\Pr\_1 &= \Pr\left[\gamma_1 < \underbrace{4^{R_{de}} - 1}_{\theta_0}\right] \\ &= \Pr\left[\left|\hat{h}_1\right|^2 < \frac{\theta_0\left(P\sigma_{sr}^2 + \sigma_r^2\right)}{P}\right] \\ &= 1 - e^{\frac{-\lambda_{sr}\theta_0\left(P\sigma_{sr}^2+\sigma_r^2\right)}{P}}\end{aligned} \quad (12)$$

Substituting (11) with $k = 2, 3$ into (7), ASR is specifically expressed in hand, and then substituting (11) with *k=1* and (7) into the formula Pr_2 in (6), Pr_2 is expressed as

$$\Pr\_2 = \Pr\left[\gamma_1 \geq \theta_0, \gamma_2 < \theta_1 + \left(\theta_1 + 1\right)\gamma_3\right] \quad (13)$$

where $\theta_1 = 4^{R_{se}} - 1$.

Substituting (8-10) into (13), Pr_2 is obtained as

$$\begin{aligned}\Pr\_2 = \Pr\Bigg[&\left|\hat{h}_1\right|^2 \geq \frac{\theta_0\left(P\sigma_1^2 + \sigma_r^2\right)}{P}, \\ &\left|\hat{h}_2\right|^2 < \frac{\theta_1\left(P\sigma_2^2 + \sigma_d^2\right)}{P} + \frac{\left(\theta_1+1\right)\left(P\sigma_2^2 + \sigma_d^2\right)}{\left(P\sigma_3^2 + \sigma_e^2\right)}\left|\hat{h}_3\right|^2\Bigg]\end{aligned} \quad (14)$$

Because $\left|\hat{h}_1\right|^2$, $\left|\hat{h}_2\right|^2$ and $\left|\hat{h}_3\right|^2$ are independent random variables and have exponential distributions, (14) is solved as

$$\begin{aligned}\Pr\_2 &= \Pr\left[\left|\hat{h}_1\right|^2 \geq \frac{\theta_0\left(P\sigma_1^2 + \sigma_r^2\right)}{P}\right] \\ &\times \int_0^\infty \lambda_3 e^{-\lambda_3 x}\left\{1 - e^{-\lambda_2\left\{\theta_1\left(P\sigma_2^2+\sigma_d^2\right)/P + \frac{\left(\theta_1+1\right)\left(P\sigma_2^2+\sigma_d^2\right)}{\left(P\sigma_3^2+\sigma_e^2\right)}x\right\}}\right\}dx \\ &= e^{-\lambda_1\theta_0\left(P\sigma_1^2+\sigma_r^2\right)/P} \\ &\times\left\{1 - \frac{\lambda_3 e^{-\lambda_2\theta_1\left(P\sigma_2^2+\sigma_d^2\right)/P}}{\lambda_3 + \left(\theta_1+1\right)\left(P\sigma_2^2+\sigma_d^2\right)\lambda_2\Big/\left(P\sigma_3^2+\sigma_e^2\right)}\right\}\end{aligned} \quad (15)$$

Substituting (12) and (15) into (6), the secrecy outage probability of the communication S-D is exactly obtained by

$$P_{S-D}^{so} = 1 - \frac{\lambda_3 e^{-\lambda_2\theta_1\left(P\sigma_2^2+\sigma_d^2\right)/P - \lambda_1\theta_0\left(P\sigma_1^2+\sigma_r^2\right)/P}}{\lambda_3 + \frac{\left(\theta_1+1\right)\left(P\sigma_2^2+\sigma_d^2\right)\lambda_2}{P\sigma_3^2+\sigma_e^2}} \quad (16)$$

4. SIMULATION RESULTS AND DISCUSSIONS

In this section, results on the secrecy performance of the proposed cooperative communication scheme under physical layer security with different channel estimation errors are investigated and discussed. The simulation results are performed by the Monte Carlo method and the analysis results are obtained by the formula (16). In the simulation model, as shown in Figure 1, the distances d_1 and d_2, the path-loss exponent β, the target data rate R_{de} for decoding at the relay, the target secrecy rate R_{se} are set to constants ($d_1=d_2=0.5$, $\beta = 3$, $R_{de}=1$ (bit/s/Hz), $R_{se}=0.1$ (bit/s/Hz)). In addition, the AWGN noises at the nodes R, D and E have the identical unit variance ($\sigma_r^2 = \sigma_d^2 = \sigma_e^2 = 1$).

Figure 2 presents the secrecy outage probability of the communication S-D versus power P (dB) when considering the distance $d_3=2$, and the different estimation errors at the nodes R, D and E. In Figure 2, markers symbols are denoted to simulation results whereas solid lines are referred to analysis results. As shown in Figure 3, when the channel estimation error at the destination D is smaller than that at eavesdropper E ($\sigma_2^2 < \sigma_3^2$), the secrecy performance will be improved. In addition, as in the case ($\sigma_2^2 < \sigma_3^2$), the secrecy performance is better when the estimation error at the relay R decreases because the decoding capacity at the relay R is larger when the the estimation error is smaller. When the channel estimation error at the destination D is larger than that at eavesdropper E ($\sigma_2^2 > \sigma_3^2$), the secrecy outage probabilities decrease in the small P regions ($P \le 13\,dB$), and increase in the large P regions ($P > 13\,dB$) because of balancing of the decoding capacity and the secrecy condition.

As illustrated in the simulation results in Figure 2, the analysis expressions (16) match well with the simulation results.

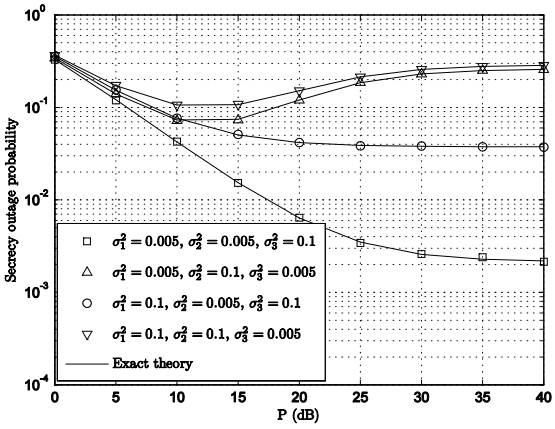

Figure 2. *Secrecy outage probability of the communication S-D versus power P (dB) when $d_3 = 2$.*

Figure 3 presents the secrecy outage probability of the communication S-D versus the link distance R-E (d_3) when $P = 20$ (dB). In Figure 3, the secrecy outage probabilities decrease when the node E moves farther from the relay R (d_3 increases) because the eavesdropping effect of the node E decreases.

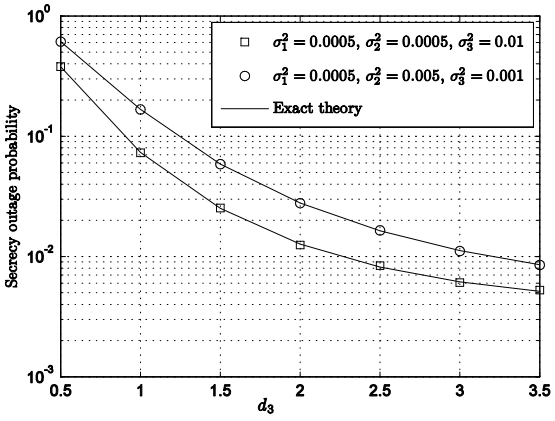

Figure 3. *Secrecy outage probability of the communication S-D versus the distance d_3 when P=20 (dB).*

5. CONCLUSIONS

In this paper, the physical layer security in the DF relaying scheme was proposed and

analyzed under the effect of imperfect CSIs. In the proposed protocol, the nodes relay, destination and eavesdropper imperfectly estimate the fading channel coefficients. The system performance of the proposed protocol was evaluated by the exact secrecy outage probability. Based on the simulation results, the secrecy performance of the proposed protocol is improved when the channel estimation error at the intended destination is smaller than that at the eavesdropper, and when the distance of the wiretapping link (from the relay to the eavesdropper) is large.

REFERENCES

[1] F. Delgosha and F. Fekri, Public-key cryptography using paraunitary matrices, *IEEE Transactions on Signal Processing*, vol. 54, no. 9, pp. 3489-3504, 2006.

[2] A.D. Wyner, The wire-tap channel, *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, 1975.

[3] Lun Dong, Zhu Han, A.P. Petropulu and H.V. Poor, Improving Wireless Physical Layer Security via Cooperating Relays, *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875-1888, 2010.

[4] H. Sakran, O. Nasr, M. Shokair, E.-S. El-Rabaie and A.A. El-Azm, Proposed relay selection scheme for physical layer security in cognitive radio networks, *IET Communications*, vol. 6, no. 16, pp. 2676-2687, 2012.

[5] A. Nosratinia, T.E. Hunter and A. Hedayat, Cooperative Communication in Wireless Networks, *IEEE Communications Magazine*, vol. 43, no. 10, pp. 74-80, 2004.

[6] J.N. Laneman, D.N.C. Tse and G.W. Wornell, Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior, *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 3062 – 3080, 2004.

[7] Y.M. Khattabi and M.M. Matalgah, Performance Analysis of Multiple-Relay AF Cooperative Systems Over Rayleigh Time-Selective Fading Channels With Imperfect Channel Estimation, *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 427 – 434, 2016.

[8] Z. He, X. Zhang, Y. Bi, W. Jiang and Y. Rong, Optimal Source and Relay Design for Multiuser MIMO AF Relay Communication Systems with Direct Links and Imperfect Channel Information, *IEEE Transactions on Wireless Communications*, DOI: 10.1109/TWC.2015.2497683, 2015.

[9] Liang Yang, K. Qaraqe, E. Serpedin and M.-S. Alouini, Performance Analysis of Amplify-and-Forward Two-Way Relaying with Co-Channel Interference and Channel Estimation Error, *IEEE Transactions on Communications*, vol. 61, no. 6, pp. 2221-2231, 2013.

[10] Devarajan, Rajiv, Punchihewa, Anjana, Bhargava and K. Vijay, Energy-Aware Power Allocation in Cooperative Communication Systems with Imperfect CSI, *IEEE Transactions on Communications*, vol. 61, no. 5, pp. 1633-1639, 2013.

Corresponding author:
Dr. Phạm Ngọc Sơn
Faculty of Electrical and Electronics Engineering
Email: sonpndtvt@hcmute.edu.vn