SCIENCE CHINA
Information Sciences

• LETTER •

June 2017, Vol. 60 069303:1–069303:3
doi: 10.1007/s11432-015-0942-8

Impacts of outdated CSI for secure cooperative systems with opportunistic relay selection

Rui ZHAO[1,2*], Hongxin LIN[3], Yu-Cheng HE[1,2], Dong-Hua CHEN[1] & Yongming HUANG[3]

[1]*Xiamen Key Laboratory of Mobile Multimedia Communications, Huaqiao University, Xiamen* 361021*, China;*
[2]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China;*
[3]*School of Information Science and Engineering, Southeast University, Nanjing* 210018*, China*

Received August 29, 2016; accepted November 11, 2016; published online May 8, 2017

Citation Zhao R, Lin H X, He Y C, et al. Impacts of outdated CSI for secure cooperative systems with opportunistic relay selection. Sci China Inf Sci, 2017, 60(6): 069303, doi: 10.1007/s11432-015-0942-8

Dear editor,

Cooperative relaying has been proven to be capable of improving the reliability and throughput of wireless transmissions [1, 2], and thus its application in physical layer security communication systems has recently been intensively investigated to enhance the secrecy performance against eavesdropping attacks [3, 4]. In particular, in the multiple-relay systems where one or more eavesdroppers try to overhear the re-transmissions from the relays, several relay selection schemes were studied in [4], due to their advantages in lower cost and complexity over other techniques, such as cooperative jamming [5] and cooperative beamforming [3].

Much efforts have been devoted to investigating the impacts of outdated CSI (channel state information) on the performance of relay selection in cooperative relay systems without eavesdroppers [6]. Meanwhile, for secure cooperative systems with outdated CSI, the performance of joint relay and jammer selection was studied in [7]. However, the existing works provide neither exact closed-form expressions nor asymptotic analysis for the secrecy performance of DF (decode-and-forward) relay selection using outdated CSI. This letter is mainly concerned about the analysis of the secrecy performances for secure DF relay systems with outdated CSI on Nakagami-m fading channels.

System models. We consider a dual-hop half-duplex relaying secure communication system, which consists of one source S with single antenna, a set of K adaptive decode-and-forward (DF) relays R_k ($k = 1, \ldots, K$) with single antenna, one destination D with N_D antenna and one eavesdropper E with N_E antenna. The S-D and S-E links are unavailable due to long distances. For three types of links S-R_k, R_k-D, and R_k-E, $k = 1, \ldots, K$, the channel coefficients are represented by h_{SR_k}, $\boldsymbol{h}_{R_kD}$ and $\boldsymbol{h}_{R_kE}$, respectively. The channel coefficients follow independent identically distributed (i.i.d.) Nakagami-m distributions with parameters m_{SR}, m_{RD} and m_{RE}, respectively. The received noise at R_k, D, and E are assumed as additive white Gaussian noise with zero-mean and variances $\sigma^2_{R_k}$, σ^2_D, and σ^2_E.

The transmission duration is divided into two

* Corresponding author (email: rzhao@hqu.edu.cn)
The authors declare that they have no conflict of interest.

time slots, and each time slot is allocated with a constant transmit power P. In the first time slot, S broadcasts the source signal, and the SNR at R_k is $\gamma_{R_k} = P\left|h_{SR_k}\right|^2/\sigma_{R_k}^2$. If the mutual information between S and R_k is greater than a certain target transmission rate R_{th}, the relay R_k can correctly decode and forward the source signal to D. In this case, R_k is belong to a decoding set $\mathcal{D}$. In the second time slot, the best relay R_{k^*} in $\mathcal{D}$ is selected by D. In the absence of the eavesdropper's CSI, the relay that maximizes the instantaneous SNR at D is selected in order to achieve the best transmission performance. To maximize the instantaneous received SNRs at D and E, the maximal ratio combining (MRC) receiver is assumed at both nodes. The mutual information over the two links R_{k^*}-D and R_k-E are computed as $C_D = \frac{1}{2}\log_2(1+\gamma_D)$ and $C_E = \frac{1}{2}\log_2(1+\gamma_E)$, where $\gamma_D = P\left\|\boldsymbol{h}_{R_{k^*}D}\right\|^2/\sigma_D^2$ and $\gamma_E = P\left\|\boldsymbol{h}_{R_kE}\right\|^2/\sigma_E^2$ are the instantaneous SNRs. The instantaneous secrecy rate can be calculated by

$$C_S^{(|\mathcal{D}|)} = \begin{cases} 0, & |\mathcal{D}| = 0, \\ \left[C_D - C_E\right]^+, & |\mathcal{D}| > 0, \end{cases} \tag{1}$$

where $[x]^+ \triangleq \max\{0, x\}$, and $|\mathcal{D}|$ denotes the number of relays contained in the decoding set $\mathcal{D}$.

In practice, the CSI of any R_k-D link used for relay selection is usually inaccurate and outdated with respect to the actual channel. We consider the channel feedback error model for the links $R_k - D$ below [6]:

$$\boldsymbol{h}_{R_kD}(t) = \rho\boldsymbol{h}_{R_kD}(t-\tau) + \sqrt{1-\rho^2}\boldsymbol{e}(t), \tag{2}$$

where ρ is the normalized correlation coefficient between $\boldsymbol{h}_{R_kD}(t)$ and $\boldsymbol{h}_{R_kD}(t-\tau)$ for delay τ, and $\boldsymbol{e}(t)$ is the error vector incurred from the feedback delay.

Secrecy performance metrics. The secrecy outage probability (SOP) is defined as the probability that the achievable secrecy rate $C_S^{(|\mathcal{D}|)}$ is less than a given secrecy rate R_S, and can be formulated as

$$\begin{aligned} &P_{\text{out}}(R_S)\Pr\left(C_S^{(|\mathcal{D}|)} < R_S\right) \\ &= \sum_{L=0}^{K}\Pr(|\mathcal{D}| = L)\Pr\left(C_S^{(L)} < R_S \Big| |\mathcal{D}| = L\right) \\ &= \sum_{L=0}^{K}\binom{K}{L}\left[1 - F_{\gamma_{R_k}}(\gamma_{th})\right]^L\left[F_{\gamma_{R_k}}(\gamma_{th})\right]^{K-L} \\ &\quad\times\int_0^\infty F_{\widetilde{\gamma}_D}(\theta - 1 + \theta x)f_{\gamma_E}(x)\,\mathrm{d}x, \end{aligned} \tag{3}$$

where $\gamma_{th} = 2^{2R_{th}}$, $F_{\gamma_{R_k}}(x)$ and $F_{\widetilde{\gamma}_D}(x)$ denote the the cumulative distribution function (CDF) of γ_{R_k} and $\widetilde{\gamma}_D$, respectively, and $f_{\gamma_E}(x)$ denotes probability density function (PDF) of γ_E, those function can be obtained in similar ways as [6].

Thus, we can derive the closed-form expression for (3) following [8, Eq. (9.211.4)] upon substitution of $F_{\gamma_{R_k}}(x)$, $F_{\widetilde{\gamma}_D}(x)$ and $f_{\gamma_E}(x)$ yields

$$\begin{aligned} P_{\text{out}}(R_S) = &\sum_{L=0}^{K}\sum_{l=0}^{L}\sum_{p=0}^{K-L+l}\sum_{q=0}^{(m_{SR}-1)p}\binom{K}{L}\binom{K-L+l}{p} \\ &\times\binom{L}{l}\left(\frac{m_{SR}}{\overline{\gamma}_R}\right)^q(-1)^{l+p}a_q^{p,m_{SR}}\gamma_{th}^q e^{-\frac{pm_{SR}}{\overline{\gamma}_R}\gamma_{th}} \\ &\times\Bigg[1 - \sum_{u=0}^{L-1}\sum_{v=0}^{(N_Dm_{RD}-1)u}\sum_{t_1=0}^{v}\sum_{t_2=0}^{N_Dm_{RD}+t_1-1}\binom{L-1}{u} \\ &\times\binom{v}{t_1}\left(\frac{m_{RD}}{\overline{\gamma}_D}\right)^{t_2}\left(\frac{m_{RE}}{\overline{\gamma}_E}\right)^{N_Em_{RE}}L(-1)^u a_v^{u,N_Dm_{RD}} \\ &\times\frac{\rho^{t_1}(1-\rho)^{v-t_1}\Gamma(N_Dm_{RD}+v)e^{-\frac{m_{RD}(1+u)}{\xi\overline{\gamma}_D}(\theta-1)}}{t_2!\xi^{v+t_2}\Gamma(N_Dm_{RD})(1+u)^{N_Dm_{RD}+t_1-t_2}} \\ &\times\frac{(\theta-1)^{\beta_2}}{\theta^{N_Em_{RE}}}\Psi\left(N_Em_{RE}, \beta_2+1; \eta_2\frac{\theta-1}{\theta}\right)\Bigg], \end{aligned} \tag{4}$$

where $\overline{\gamma}_R$, $\overline{\gamma}_D$, and $\overline{\gamma}_E$ denote the average SNRs at R_k, D, and E, respectively, $\theta = 2^{2R_S}$, $\xi = 1 + u(1-\rho)$, $\eta_2 = m_{RD}(1+u)\theta/(\xi\overline{\gamma}_D) + m_{RE}/\overline{\gamma}_E$, $\beta_2 = N_Em_{RE} + t_2$, $\Gamma(\cdot)$ and $\Psi(\cdot,\cdot;\cdot)$ are the gamma function [8, Eq. (8.339.1)] and confluent hypergeometric function [8, Eq. (9.211.4)], respectively, and $a_n^{c,d}$ $(0 \leqslant n \leqslant c(d-1))$ for positive integers c and d is a constant defined in [2].

Asymptotic SOP. (1) $\overline{\gamma}_D \to \infty$ with fixed $\overline{\gamma}_R$: This is applicable in a scenario where D is located quite close to R_k. In this case, it is readily shown from (1) that for $|\mathcal{D}| > 0$, $C_S^{(|\mathcal{D}|)} \to \infty$. By (3), the secrecy outage event can happen only when $|\mathcal{D}| = 0$, i.e., none of the K relays can correctly decode the received source message. So, we have

$$P_{\text{out}}^{\overline{\gamma}_D\to\infty}(R_S) = \left[1 - \frac{\Gamma\left(m_{SR}, \frac{m_{SR}}{\overline{\gamma}_R}\gamma_{th}\right)}{\Gamma(m_{SR})}\right]^K, \tag{5}$$

where $\Gamma(\cdot,\cdot)$ denotes the incomplete gamma function [8, Eq. (8.352.2)].

(2) $\overline{\gamma}_D \to \infty$ and $\overline{\gamma}_R \to \infty$: In this case, D is located close to R_k and R_k is located close to S. We assume that $\overline{\gamma}_R$ is proportional to $\overline{\gamma}_D$. In high SNR regime where $\overline{\gamma}_R \to \infty$, all the relays can correctly decode the received message at high probability, i.e., $\Pr(|\mathcal{D}| = K) \to 1$ and $\Pr(|\mathcal{D}| = L) \to 0$ for $0 \leqslant L \leqslant K-1$. Therefore, subtituting the asymptotic expression for $F_{\widetilde{\gamma}_D}(x)$ [6] into (3) and solve the integral, we have

$$\begin{aligned} P_{\text{out}}^{\overline{\gamma}_R,\overline{\gamma}_D\to\infty}(R_S) &= \Pr\left(C_S^{(K)} < R_S \Big| |\mathcal{D}| = K\right) \\ &= \begin{cases} \left(\widetilde{\Phi}\overline{\gamma}_D\right)^{-\widetilde{G}} + o\left(\overline{\gamma}_D^{-\widetilde{G}}\right), & \rho < 1, \\ \left(\Phi\overline{\gamma}_D\right)^{-G} + o\left(\overline{\gamma}_D^{-G}\right), & \rho = 1, \end{cases} \end{aligned} \tag{6}$$

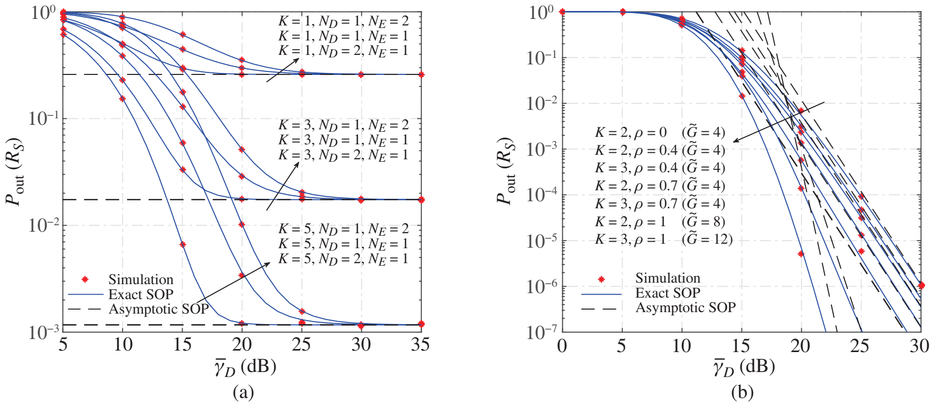

Figure 1 (Color online) Exact and asymptotic SOP versus $\overline{\gamma}_D$ for (a) $R_{th}=R_S=1$ bits/s/Hz, $\overline{\gamma}_R=10$ dB, $\overline{\gamma}_E=5$ dB, $m_{SR}=m_{RE}=1$, $m_{RD}=2$, and $\rho=1$; (b) $R_{th}=R_S=1$ bits/s/Hz, $\overline{\gamma}_R=\overline{\gamma}_D$, $\overline{\gamma}_E=5$ dB, $N_D=N_E=2$, and $m_{SR}=m_{RD}=m_{RE}=2$.

where $o(\cdot)$ denotes the higher order terms, $\widetilde{G}=N_D m_{RD}$ and $G{=}N_D m_{RD} K$ denote the secrecy diversity order, and the corresponding secrecy array gains can be given by

$$\widetilde{\Phi}=\left[\frac{K m_{RD}^{N_D m_{RD}}}{\Gamma(N_D m_{RD})}\sum_{u=0}^{K-1}\sum_{v=0}^{(N_D m_{RD}-1)u}\binom{K-1}{u}(-1)^u \times\frac{a_v^{u,N_D m_{RD}} m_{RE}^{N_E m_{RE}}(1-\rho)^v\Gamma(N_D m_{RD}+v)(\theta-1)^{\beta_3}}{\xi^{N_D m_{RD}+v}\overline{\gamma}_E^{N_E m_{RE}}\Gamma(N_D m_{RD}+1)\,\theta^{N_E m_{RE}}} \times\Psi\left(N_E m_{RE},\beta_3+1;\frac{m_{RE}(\theta-1)}{\theta\overline{\gamma}_E}\right)\right]^{-\frac{1}{\widetilde{G}}}, \quad (7)$$

$$\Phi=\left[\frac{m_{RD}^{N_D m_{RD} K} m_{RE}^{N_E m_{RE}}(\theta-1)^{N_D m_{RD} K+N_E m_{RE}}}{\theta^{N_E m_{RE}}\overline{\gamma}_E^{N_E m_{RE}}\left[\Gamma(N_D m_{RD}+1)\right]^K} \times\Psi\left(N_E m_{RE},\beta_4;\frac{(\theta-1)m_{RE}}{\theta\overline{\gamma}_E}\right)\right]^{-\frac{1}{G}} \quad (8)$$

with shorthand notations $\beta_3=N_D m_{RD}+N_E m_{RE}$ and $\beta_4=N_D m_{RD}K+N_E m_{RE}+1$.

Numerical results. Figure 1 evaluates the exact and asymptotic SOP performances versus $\overline{\gamma}_D$ by (4)–(6), respectively. In Figure 1(a), there is an evident decrease in exact SOP whether by increasing $\overline{\gamma}_D$, K, and N_D or by decreasing N_E. As $\overline{\gamma}_D$ grows large, all the exact SOP curves with K fixed approach a constant asymptotic SOP value dominated by the K value, regardless of the values of N_D and N_E. In Figure 1(b) we see that for given ρ, the SOP performances can be improved by increasing K. Meanwhile, for fixed K, an SOP gain can also be achieved by increasing ρ. However, for $\rho<1$, the secrecy diversity order remains constant $\widetilde{G}=N_D m_{RD}$. Only when $\rho=1$, the full secrecy diversity order $G=N_D m_{RD}K$ can be obtained.

Conclusion. In this letter, we have investigated the secrecy performances of adaptive DF relay selection under Nakagami-m fading channels. We find that the SOP for the system can be significantly reduced by increasing the number of relays. In particular, our asymptotic results can provide two valuable insights: (1) when D is located close to R_k, the SOP approaches a constant value with the zero secrecy diversity order; (2) when D is close to R_k while R_k is close to S, a positive secrecy diversity order can always be achieved by using outdated CSI, and the full secrecy diversity order can be obtained only by using perfect CSI.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61401165, 61302095, 61422105, 61531011), in part by Natural Science Foundation of Fujian Province of China (Grant Nos. 2015J01262, 2014J01243), and in part by Promotion Program for Young and Middle-aged Teacher in Science and Technology Research of Huaqiao University (Grant No. ZQN-PY407).

References

1 Laneman J N, Tse D N, Wornell G W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. IEEE Trans Inf Theory, 2004, 50: 3062–3080
2 Zhao R, Yuan Y, Fan L S, et al. Secrecy Performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels. IEEE Trans Commun, 2016, doi: 10.1109/TCOMM.2016.2618793
3 Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process, 2010, 58: 1875–1888
4 Ding Z G, Leung K K, Goeckel D L, et al. Opportunistic relaying for secrecy communications: cooperative jamming vs. relay chatting. IEEE Trans Wirel Commun, 2011, 10: 1725–1729
5 Zhao R, Huang Y M, Wang W, et al. Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming. IEEE Trans Wirel Commun, 2016, 15: 2537–2551
6 Yang N, Elkashlan M, Yeoh P L, et al. Multiuser MIMO relay networks in Nakagami-m fading channels. IEEE Trans Commun, 2012, 60: 3298–3310
7 Wu N E, Li H J. Effect of feedback delay on secure cooperative networks with joint relay and jammer selection. IEEE Wirel Commun Lett, 2013, 2: 415–418
8 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series and Products. 7th ed. New York: Academic, 2007