SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2020, Vol. 63 122303:1–122303:14
https://doi.org/10.1007/s11432-019-2660-3

Quasi-concave optimization of secrecy redundancy rate in HARQ-CC system

Yue WU[1*], Shishu YIN[1], Jian ZHOU[1], Pei YANG[2] & Hongwen YANG[2]

[1]*School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu* 233030*, China;*
[2]*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing* 100876*, China*

Received 2 May 2019/Revised 4 July 2019/Accepted 3 September 2019/Published online 15 January 2019

Abstract In a hybrid automatic repeat request with chase combining (HARQ-CC) system, we analyze physical layer secure performance and determine the secrecy redundancy rate by proposed quasi-concave optimization methods with effective secrecy throughput (EST) criteria. First, key performance metrics, including connection outage probability (COP), secrecy outage probability (SOP), EST, and delay, are discussed. Then, under the constraint of COP, we optimize the secrecy redundancy rate to maximize the EST, which is a quasi-concave function, by both the bisection and fixed-point methods. Furthermore, under the simultaneous constraints of COP and SOP, the bisection and Lagrangian multiplier methods are applied to optimize the secrecy redundancy rate. From the comparison of the numerical and simulated results, it is concluded that EST demonstrates practical secure performance of HARQ-CC, and the proposed optimization methods adjust the secrecy redundancy rate for improved security.

Keywords physical layer security (PLS), hybrid automatic repeat request (HARQ), chase combining (CC), effective secrecy throughput (EST), quasi-concave optimization

Citation Wu Y, Yin S S, Zhou J, et al. Quasi-concave optimization of secrecy redundancy rate in HARQ-CC system. Sci China Inf Sci, 2020, 63(2): 122303, https://doi.org/10.1007/s11432-019-2660-3

1 Introduction

From the perspective of information theory, physical layer security (PLS) assures the confidentiality of data transmissions according to the characteristics of a wireless channel. With the increasing requirements of information security, PLS becomes a critical replacement for or supplement to traditional encryption technology. As a pioneer, Wyner [1] established the wiretap model and constructed the classical secure coding method. Based on his study, several performance-analysis and signal-processing methods were proposed to improve secrecy. Csiszar et al. [2] and Leung-Yan-Cheong et al. [3] extended the wiretap model to broadcast and Gaussian channels, respectively. The secrecy capacity, defined as the maximum secrecy transmission rate when an eavesdropper is unable to decode any information, was analyzed over a fading channel [4, 5]. Using the connection outage probability (COP) and secrecy outage probability (SOP), reliability and security were evaluated separately [6, 7], resulting in more comprehensive performance evaluation. As another important metric, the widely discussed secrecy throughput presented the average reliable and secure rate during each transmission [8–10]. Moreover, signal-processing methods, e.g., beamforming and artificial noise, efficiently enhanced the secrecy performance [11–18]. It was also proposed that diversity technologies had their special functions in PLS, including multi-input multi-output (MIMO) diversity and multi-user diversity [19].

* Corresponding author (email: wuyue@aufe.edu.cn)

As a typical time-diversity technology, hybrid automatic repeat request (HARQ) has also been discussed in regard to improving PLS. In HARQ with chase combining (HARQ-CC), the same codewords or redundancy versions of erroneous ones will be retransmitted upon the feedback of negative acknowledgement (NACK), and new transmissions will be triggered by acknowledgement (ACK) when decoding is successful. It was proved that the diversity gain of HARQ brought enhanced PLS performance, because retransmissions totally depended on the decoding of a legitimate user [20]. To efficiently use HARQ, Tomasin designed a multiple-encoding HARQ scheme with statistics channel state information (CSI). As channel capacity is not suitable for HARQ that combines retransmitted codewords, secrecy throughput was widely discussed with respect to PLS of HARQ [21–23]. Tang et al. [21] analyzed SOP, secrecy throughput, and their asymptotic properties; Mheich et al. [22] optimized secrecy throughput as extended; Treust et al. [23] designed an adaptive rate transmission scheme to improve secrecy throughput. The above studies did not consider the influence of secrecy outage on secrecy throughput. The definition of secrecy throughput only included connection outage, which led to overestimated secrecy throughput.

Inspired by this problem, this paper extends the proposed effective secrecy throughput (EST) of a single transmission [10] to a HARQ-CC system. Because the coding scheme is critical, we determine and analyze the secrecy redundancy rate to maximize EST by quasi-concave optimization. The major contributions of our study include the following: (1) The closed-form expressions of COP and SOP are deduced in the HARQ-CC system, and the EST of HARQ-CC is defined. Meantime, we discuss the delay performance as well. (2) Under the constraint of COP, the bisection method is applied to solve the quasi-concave optimization problem of the secrecy redundancy rate, so as to maximize EST. The optimal value is converted to the feasible solution of a reformulated concave set. By the fixed point method, we give the closed-form solution of the above optimization problem, and asymptotic results are considered. (3) Under the simultaneous constraints of COP and SOP, we use the bisection and Lagrangian multiplier methods to solve the above problem again, for special applications with a given secrecy requirement.

The rest of this paper is organized as follows. Section 2 describes the overall system model and assumptions. Section 3 gives closed-form expressions of COP and SOP with retransmissions and combinations, along with the definition of EST in a HARQ-CC system. Section 4 proposes the quasi-concave optimization of secrecy redundancy rate to maximize EST, and the numerical and simulated results are presented in Section 5. Section 6 provides our conclusion.

2 System model of secure HARQ-CC

We consider a secure transmission system of HARQ-CC, as shown in Figure 1. The transmitter (Alice) sends confidential message $\boldsymbol{w}$ with secrecy redundancy message $\boldsymbol{v}$ to the legitimate receiver (Bob) over the main channel, while a passive eavesdropper (Eve) intercepts the transmission through a wiretap channel. Assume that the main and wiretap channels are independent Rayleigh block-fading channels. On the one hand, if Bob decodes the received codeword successfully, a bit of an ACK message will be sent back to Alice over the error-free feedback channel to start new transmissions. On the other hand, if the decoding fails, a NACK message will trigger retransmissions until successful decoding occurs or the maximum transmission number (K) is reached. All of the feedback messages are completed depending on the decoding results of Bob. The feedback channel is assumed to be public, thus ACK/NACK messages transmitted over this channel can be also received by Eve. However, the erroneous codeword of Eve may not be retransmitted by Alice unless Bob has the same erroneous one. Therefore, there is much more diversity gain obtained by Bob than Eve.

Alice encodes confidential message $\boldsymbol{w}$ and secrecy redundancy message $\boldsymbol{v}$ into codeword $\boldsymbol{x}(k)$ by the Wyner secrecy code [1], where k is the transmission number ($1 \leqslant k \leqslant K$). The codeword rate and secrecy redundancy rate are denoted as R_B and R_E, respectively. Thus the secrecy rate is given by $R_S = R_B - R_E$. Assume that the transmission power is fixed at P, and $\mathrm{E}[|\boldsymbol{x}(k)|^2] = 1$, $\mathrm{E}[\cdot]$ is the expectation function. We denote the fading parameter of the main and wiretap channels by $\boldsymbol{h}_B(k)$ and $\boldsymbol{h}_E(k)$, respectively, which are independently and identically distributed (i.i.d.) complex Gaussian random variables with zero

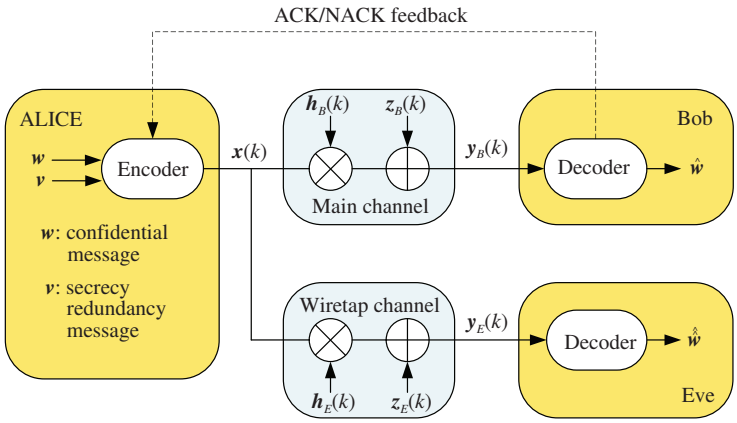

Figure 1 (Color online) Secure HARQ-CC system model.

mean and unit variance. We denote the additive Gaussian white noise by $\boldsymbol{z}_B(k)$ and $\boldsymbol{z}_E(k)$, respectively, their means are zero, and their variances are respectively $\boldsymbol{\sigma}_B^2$ and $\boldsymbol{\sigma}_E^2$. In each slot, the received signals of Bob and Eve after k transmissions are

$$\begin{cases} y_B(k) = \sqrt{P} h_B(k) x(k) + z_B(k), \\ y_E(k) = \sqrt{P} h_E(k) x(k) + z_E(k). \end{cases} \tag{1}$$

For simplicity, we denote the average received signal-to-noise ratio (SNR) of the main channel and wiretap channel by $\bar{\lambda}_B = \frac{P}{\sigma_B^2}$ and $\bar{\lambda}_E = \frac{P}{\sigma_E^2}$, respectively. After k transmissions of HARQ-CC, Bob and Eve use the maximal ratio combining (MRC) before decoding. Their combined SNR becomes:

$$\begin{cases} \gamma_B(k) = \sum\limits_{i=1}^{k} \bar{\lambda}_B \left| h_B(i) \right|^2, \\ \gamma_E(k) = \sum\limits_{i=1}^{k} \bar{\lambda}_E \left| h_E(i) \right|^2. \end{cases} \tag{2}$$

3 Secure performance metrics

Based on the above system model of secure HARQ-CC, we analyze some critical security performance metrics, including connection outage probability (COP), secrecy outage probability (SOP), and effective secrecy throughput (EST). Connection outage occurs when the legitimate receiver (Bob) cannot decode transmitted codewords, while secrecy outage occurs when the eavesdropper (Eve) cannot be confused by secrecy redundancy after the k-th transmission.

We first consider COP after k transmissions, denoted by $P_e(k)$. COP is defined as the probability that a connection outage occurs, i.e., the mutual information after the k-th transmission, $I_B(k)$, is less than the codeword rate R_B,

$$P_e(k) = \Pr\{I_B(k) < R_B\}. \tag{3}$$

As the combined SNR in (2), the mutual information of the main channel is

$$I_B(k) = \log_2 \left(1 + \sum_{i=1}^{k} \bar{\lambda}_B \left| h_B(i) \right|^2 \right). \tag{4}$$

Substituting (4) into (3), we have

$$P_e(k) = \Pr \left\{ \sum_{i=1}^{k} \left| h_B(i) \right|^2 < \frac{2^{R_B} - 1}{\bar{\lambda}_B} \right\}. \tag{5}$$

We know the fading parameters are independent zero-mean unit-variance complex Gaussian random variables. Hence, the sum of their modular square is distributed according to the chi-squared distribution:

$$P_e(k) = \mathcal{F}_{\chi^2}\left[\frac{2\left(2^{R_B}-1\right)}{\bar{\lambda}_B}, 2k\right] = \frac{\gamma(k, \frac{2^{R_B}-1}{\bar{\lambda}_B})}{\Gamma(k)}, \tag{6}$$

where $\mathcal{F}_{\chi^2}[\cdot]$ is the cumulative distribution function (CDF) for a chi-squared random variable.

The average transmission number $\bar{N}$ is determined by the main channel, and it equals the expectation of the actual transmission number N:

$$\bar{N} = \mathrm{E}[N] = 1 + \sum_{k=1}^{K-1} P_e(k). \tag{7}$$

Then we reformulate $\bar{N}$ as

$$\bar{N} = 1 + \sum_{k=1}^{K-1} k \cdot (P_e(k) - P_e(k+1)) + (K-1)P_e(K). \tag{8}$$

According to (6) and the properties of the Gamma function and incomplete Gamma function, i.e., when s is an integer, $\Gamma(s) = (s-1)!$ and $\gamma(s+1, x) = s\gamma(s, x) - x^s \mathrm{e}^{-x}$, we have

$$\begin{aligned} P_e(k+1) &= \frac{\gamma(k+1, \frac{2^{R_B}-1}{\bar{\lambda}_B})}{\Gamma(k+1)} \\ &= \frac{k\gamma(k, \frac{2^{R_B}-1}{\bar{\lambda}_B}) - (\frac{2^{R_B}-1}{\bar{\lambda}_B})^k \mathrm{e}^{-(\frac{2^{R_B}-1}{\bar{\lambda}_B})}}{k!} \\ &= P_e(k) - \frac{(\frac{2^{R_B}-1}{\bar{\lambda}_B})^k \mathrm{e}^{-(\frac{2^{R_B}-1}{\bar{\lambda}_B})}}{k!}. \end{aligned} \tag{9}$$

Therefore, the second part in the right-hand side (RHS) of (8) becomes

$$\begin{aligned} \sum_{k=1}^{K-1} k \cdot (P_e(k) - P_e(k+1)) &= \sum_{k=1}^{K-1} k \frac{(\frac{2^{R_B}-1}{\bar{\lambda}_B})^k \mathrm{e}^{-(\frac{2^{R_B}-1}{\bar{\lambda}_B})}}{k!} \\ &= \left(\frac{2^{R_B}-1}{\bar{\lambda}_B}\right) \mathrm{e}^{-(\frac{2^{R_B}-1}{\bar{\lambda}_B})} \sum_{k=1}^{K-1} \frac{(\frac{2^{R_B}-1}{\bar{\lambda}_B})^{k-1}}{(k-1)!}. \end{aligned} \tag{10}$$

The maximum transmission number K is generally large enough to ensure a low connection outage probability [24]. Then

$$\begin{aligned} \sum_{k=1}^{K-1} k \cdot (P_e(k) - P_e(k+1)) &\simeq \left(\frac{2^{R_B}-1}{\bar{\lambda}_B}\right) \mathrm{e}^{-(\frac{2^{R_B}-1}{\bar{\lambda}_B})} \mathrm{e}^{(\frac{2^{R_B}-1}{\bar{\lambda}_B})} \\ &= \frac{2^{R_B}-1}{\bar{\lambda}_B}. \end{aligned} \tag{11}$$

Under the same conditions, $P_e(K)$ is approximated as 0, and the third part in the RHS of (8) becomes

$$(K-1)P_e(K) \simeq 0. \tag{12}$$

Substituting (11) and (12) into (8), we can approximate $\bar{N}$ as

$$\bar{N} \simeq 1 + \frac{2^{R_B}-1}{\bar{\lambda}_B}. \tag{13}$$

The SOP of HARQ-CC, denoted by $P_s(k)$, is defined as the probability that a message transmitted by Alice can be decoded successfully by Eve after k transmissions. As a passive receiver, Eve only receives messages while retransmissions are requested by Bob. When the number of transmissions in the main channel is N,

$$P_s(k) = \sum_{i=1}^{k} \Pr\{N = i\} \cdot \Pr\{I_E(i) > R_E\}, \tag{14}$$

where I_E is the mutual information of the wiretap channel, $\Pr\{N = i\}$ is the probability that the i-th transmission occurs, and $\Pr\{N = i\} = P_e(i-1) - P_e(i)$. We define

$$\begin{aligned}
\phi(i) &= \Pr\{I_E(i) > R_E\} \\
&= \Pr\left\{\log_2\left(1 + \sum_{j=1}^{i} \bar{\lambda}_E \left|h_E(i)\right|^2\right) > R_E\right\} \\
&= 1 - \frac{\gamma(i, \frac{2^{R_E}-1}{\bar{\lambda}_E})}{\Gamma(i)} \\
&= Q\left(\frac{2^{R_E}-1}{\bar{\lambda}_E}, i\right),
\end{aligned} \tag{15}$$

where $Q(\cdot,\cdot)$ is a regularized Gamma function. Hence the SOP after K transmissions becomes

$$P_s(K) = \sum_{i=1}^{K} \Pr\{N = i\} \cdot \phi(i) = \mathrm{E}[\phi(N)]. \tag{16}$$

As N is an integer, $\phi(N)$ is also the CDF of a Poisson random variable. With a given R_E, this CDF is well known as a log-concave function of N. In other words, $\log\phi(N)$ is concave with respect to N. Under the above assumption that K is large enough to ensure a low $P_e(K)$, $\sum_{i=1}^{K} \Pr\{N = i\} = 1$. According to Jenson's inequality, we have

$$\begin{aligned}
\log\phi\left(\mathrm{E}[\mathrm{N}]\right) \leqslant \mathrm{E}\left[\log\phi(\mathrm{N})\right] &= \sum_{i=1}^{K} \Pr\{N = i\} \cdot \log\phi(i) \\
&= \sum_{i=1}^{K} \log\phi(i)^{\Pr\{N=i\}} = \log\prod_{i=1}^{K} \phi(i)^{\Pr\{N=i\}} \\
&\overset{(a)}{\leqslant} \log\sum_{i=1}^{K} \Pr\{N = i\} \cdot \phi(i) = \log P_s(K),
\end{aligned} \tag{17}$$

where (a) is true based on the general mean inequality. $P_s(K)$ and $\phi\left(\mathrm{E}[N]\right)$ are both positive. Thus

$$P_s(K) \geqslant \phi\left(\mathrm{E}[N]\right). \tag{18}$$

Substituting (15) into (18), we approximate the SOP of the K-th transmission by its lower bound, as follows:

$$P_s(K) \simeq 1 - \frac{\gamma(\bar{N}, \frac{2^{R_E}-1}{\bar{\lambda}_E})}{\Gamma(\bar{N})}. \tag{19}$$

For simplicity, we define $P_e = P_e(K)$ and $P_s = P_s(K)$, which means the maximum transmission number of COP and SOP has been reached.

Most analysis of secrecy throughput in the literatures does not consider the SOP [21], but this has been found to be inaccurate [25]. Therefore, we extend the EST with no feedback channel [10] to the HARQ-CC system.

Definition 1. Effective secrecy throughput (EST) of HARQ-CC is defined as

$$\eta_s = \frac{(R_B - R_E) \cdot (1 - P_e) \cdot (1 - P_s)}{\bar{N}}. \tag{20}$$

According to the renewal-reward theorem [21, 26, 27], EST can be obtained by $\eta_s = \mathrm{E}[R_s]/\mathrm{E}[N]$, where R_s represents the reliable and secure transmission rate. $R_B - R_E$ is the maximum rate of each transmission. When COP is P_e, SOP is P_s, we have $R_s = R_B - R_E$ if neither connection outage nor secrecy outage occurs, and $R_s = 0$ if either connection outage or secrecy outage occurs, or both of them take place. Hence, $\mathrm{E}[R_s] = (R_B - R_E) \cdot (1 - P_e) \cdot (1 - P_s)$. And the average transmission number is given by $\mathrm{E}[N] = \bar{N}$. Therefore, η_s in (20) indicates the average reliable and secure transmission rate of each transmission. This metric can be applied to evaluate secure performance more comprehensively and adapt the transmission rate or secrecy redundancy rate to enhance the performance.

As another critical metric, delay performance is also discussed in HARQ-CC system. In general, delay limit and average delay are presented by maximum transmission number and average transmission number, respectively, which denoted by K and $\bar{N}$ here. Most literatures focus on the relationship between delay limit and other performance metrics, such as outage probability and throughput, while $\bar{N}$ is determined by transmission scheme, transmission rate, and channel fading with given delay limit. Hence, this study mainly considers the COP, SOP and EST with different delay limit, K, in secure HARQ-CC system.

Owing to the diversity gain, COP decreases by retransmissions and combining when K increases. It has been well proved in conventional HARQ system. As mentioned above, retransmissions totally depends on the decoding result of Bob. In another word, Eve cannot obtain diversity gain when her erroneous codewords are successfully decoded by Bob. Hence, larger K may result in increased probability of secrecy outage, but this rise is limited. From (19), we know SOP will be stable when $\bar{N}$ reaches the maximum value given in (13). According to Definition 1, with given R_B and R_E, EST will also be stable when SOP and $\bar{N}$ converge, and COP is small enough to be trivial.

4 Quasi-concave optimization of secrecy redundancy rate

In this section, we optimize the secrecy redundancy rate R_E to maximize the EST of HARQ-CC, thus improving the performance of secrecy transmission. Two cases will be considered. Under the constraint of COP, we optimize R_E with the EST criteria. Then this problem is extended to the simultaneous constraints of COP and SOP.

4.1 Optimization with COP constraint

Reliability is the fundamental requirement in a wireless communication system. Thus the maximum transmission number is generally large enough to ensure a low COP, as mentioned above. Here, we consider the problem of how to determine the coding rate to maximize the EST:

$$\begin{aligned} \max_{R_B, R_E} \quad & \eta_{\mathrm{s}} \\ \text{s.t.} \quad & P_e \leqslant P_e^{\star},\ 0 \leqslant R_E \leqslant R_B, \end{aligned} \tag{21}$$

where P_e, P_s, and η_s are obtained by (6), (19), and (20), respectively. The target COP is $P_e^{\star}$, hence the COP constraint is $P_e \leqslant P_e^{\star}$. Because $P_e^{\star}$ is generally extremely small, such as 10^{-3} or 10^{-4}, we reflex COP constraint to $P_e = P_e^{\star}$. Correspondingly, from (6) we have the optimal R_B:

$$R_B^{\star} = \log_2 \left[1 + \frac{\bar{\lambda}_m}{2} \mathcal{F}_{\chi^2}^{-1}[P_e^{\star}, 2K] \right], \tag{22}$$

where $\mathcal{F}_{\chi^2}^{-1}[\cdot]$ is the inverse function of the CDF of the chi-squared distribution. Then the EST of HARQ-CC becomes

$$\eta_s = \frac{(1 - P_e^{\star})}{\bar{N}} \cdot (R_B^{\star} - R_E) \cdot (1 - P_s), \tag{23}$$

where $P_e^\star$, $R_B^\star$, and $\bar{N}$ are determined, while P_s is given in (14) and approximated in (19).

Proposition 1. η_s is a quasi-concave function on $0 \leqslant R_E \leqslant R_B^\star$, with existed maximum value.

Proof. Take the logarithm of both sides of (23),

$$\log \eta_s = \log\left(1 - P_e^\star\right) - \log \bar{N} + \log\left(R_B^\star - R_E\right) + \log\left(1 - P_s\right), \tag{24}$$

where the first two parts in the RHS of (24) are determined. In the third part, $\log\left(R_B^\star - R_E\right)$ is a composition function $f = \log\left(g\left(R_E\right)\right)$ on $0 \leqslant R_E \leqslant R_B^\star$, and $g\left(R_E\right) = R_B^\star - R_E$. $g\left(R_E\right)$ is obviously cancave. Based on the convexity-preserving properties, $\log\left(R_B^\star - R_E\right)$ is still concave on $0 \leqslant R_E \leqslant R_B^\star$. Finally, because $1 - P_s$ is the CDF of a chi-squared distribution, which is logarithmic concave, then $\log\left(1 - P_s\right)$ is concave. Therefore, η_s is logarithmic concave, and thus it is quasi-concave with maximum value [28].

Based on the properties of a quasi-concave function, all of the α-upper contour sets defined as

$$S_\alpha = \{R_E \in \mathrm{dom}\eta_s | \eta_s \geqslant \alpha\} \tag{25}$$

are concave when $R_E \in \mathbb{R}_{++}$, where $\mathrm{dom}\eta_s$ denotes the domain of η_s, and $\mathbb{R}_{++}$ denotes the set of positive real numbers.

Now, the upper contour sets of the quasi-concave function η_s are presented via a family of concave inequalities. We will choose ϕ_t, indexed by $t \in \mathbb{R}_{++}$, with

$$\eta_s \geqslant t \Leftrightarrow \phi_t \geqslant 0,$$

i.e., the t-upper contour set of the quasi-concave function η_s is the 0-upper contour set of the convex function ϕ_t. ϕ_t must satisfy $\phi_t \geqslant 0 \Rightarrow \phi_p \geqslant 0$ for $p \leqslant t$. This is satisfied if for each R_E, ϕ_t is a nonincreasing function of t, i.e., $\phi_p \geqslant \phi_t$ whenever $p \leqslant t$. Hence, its definition is given by

$$\phi_t = \begin{cases} 0, & \eta_s \geqslant t, \\ -\infty, & \eta_s < t. \end{cases} \tag{26}$$

To solve problem (21), we reformulate it as

$$\begin{aligned} \max_{R_E} \quad & t \\ \text{s.t.} \quad & \phi_t \geqslant 0,\ 0 \leqslant R_E \leqslant R_B^\star. \end{aligned} \tag{27}$$

By fixing t, the following problem of finding the feasible set is concave:

$$\begin{aligned} \text{find} \quad & R_E \\ \text{s.t.} \quad & \phi_t \geqslant 0,\ 0 \leqslant R_E \leqslant R_B^\star. \end{aligned} \tag{28}$$

The bisection method is a common technique to solve quasi-concave problems (27). In brief, the optimization problem (27) is tackled via the bisection method by iteratively increasing t until problem (28) is feasible for $t \in [t^\star, t^\star + \epsilon]$, where $t^\star$ denotes the optimal value of problem (27) and ϵ is a preassigned small positive real number, such as 10^{-3}. Specifically, it is first assumed that $t^\star$ lies within $[l, u]$, where both the lower bound l and the upper bound u of the interval are predetermined by the associated constraints. Here, we initialize them as $l = 0$ and $u = R_B^\star$. Next, we examine the feasibility of the midpoint $(l + u)/2$ according to problem (28). If problem (28) is feasible, then we set $l = t$, and otherwise we update $u = t$. The concave feasibility problem (28) will be tested again by using the new interval until $u - l \leqslant \epsilon$. Then the optimal R_E is output and denoted by R_E^{opt1}. The bisection method for an ϵ-suboptimal solution is summarized in Algorithm 1.

Proposition 2. Let $R_E^\dagger = \log_2\left(1 + \bar{N} \cdot \bar{\lambda}_m\right)$. When $R_E \geqslant R_E^\dagger$, we have $\eta_s \geqslant \eta_s(R_E^\dagger)$, which corresponds to the α-sublevel sets of EST, where $\alpha = \eta_s(R_E^\dagger)$ and η_s is concave.

Proof. Let $f(R_E) = R_B^\star - R_E$, $g(R_E) = 1 - P_s$. When $0 \leqslant R_E \leqslant R_B^\star$, we have that $f(R_E)$ is non-negative and monotonically decreases with R_E, $\frac{\mathrm{d}f}{\mathrm{d}R_E} = -1$, $\frac{\mathrm{d}^2 f}{\mathrm{d}R_E^2} = 0$. From (19), we know that $g(R_E)$ is

Algorithm 1 Bisection method for solving quasi-concave problem (21)

Input: $l = 0$, $u = R_B^\star$, $\epsilon = 10^{-3}$;
1: **while** $u - l \leqslant \epsilon$ **do**
2: $t \Leftarrow (u + l)/2$;
3: Solve the concave feasible problem (28);
4: **if** problem (28) is feasible **then**
5: $l \Leftarrow t$;
6: **else**
7: $u \Leftarrow t$;
8: **end if**
9: **end while**
Output: R_E^{opt1};

expressed by the CDF of the chi-squared distribution. When the degrees of freedom n is large enough, the chi-squared distribution can be approximated as a normalized distribution with mean and variance n and $2n$, respectively. Then we use the error function to state this CDF, i.e.,

$$g(R_E) = \frac{1}{2}\left(1 + \text{erf}\left(\frac{\frac{2^{R_E}-1}{\bar{\lambda}_E} - \bar{N}}{2\sqrt{\bar{N}}}\right)\right).$$

Let $g(R_E^\dagger) = \frac{1}{2}$, $R_E^\dagger = \log_2\left(1 + \bar{N}\cdot\bar{\lambda}_m\right)$. When $R_E > R_E^\dagger$, then $\frac{\mathrm{d}g}{\mathrm{d}R_E} > 0$, $\frac{\mathrm{d}^2 g}{\mathrm{d}R_E^2} < 0$. Hence

$$\frac{\mathrm{d}^2(f\cdot g)}{\mathrm{d}R_E^2} = \frac{\mathrm{d}^2 f}{\mathrm{d}R_E^2}\cdot g + 2\cdot\frac{\mathrm{d}f}{\mathrm{d}R_E}\cdot\frac{\mathrm{d}g}{\mathrm{d}R_E} + f\cdot\frac{\mathrm{d}^2 g}{\mathrm{d}R_E^2} < 0.$$

Thus $f\cdot g$ is concave with respect to R_E. From (23), we conclude that η_s is concave when $R_E > R_E^\dagger$. A maximum value of η_s must exist.

Based on the above analysis, we know that if the optimal R_E satisfies $R_E > R_E^\dagger$ and $\frac{\mathrm{d}\eta_s}{\mathrm{d}R_E} = 0$, then η_s has the maximum value on this R_E. From (23),

$$\frac{\mathrm{d}\eta_s}{\mathrm{d}R_E} = \frac{1-P_e^\star}{\bar{N}}\left[-(1-P_s) - (R_B^\star - R_E)\frac{\mathrm{d}P_s}{\mathrm{d}R_E}\right], \tag{29}$$

where P_s is approximated as (19), and its first derivative is

$$\frac{\mathrm{d}P_s}{\mathrm{d}R_E} \simeq -\frac{1}{\Gamma(\bar{N})}\cdot\left(\frac{2^{R_E}-1}{\bar{\lambda}_E}\right)^{\bar{N}-1}\cdot\exp\left(-\left(\frac{2^{R_E}-1}{\bar{\lambda}_E}\right)\right)\cdot\frac{2^{R_E}\ln 2}{\bar{\lambda}_E}. \tag{30}$$

Substitute (19) and (30) in (29) and let $\frac{\mathrm{d}\eta_s}{\mathrm{d}R_E} = 0$. Then we have the fixed-point equation of the approximated optimal R_E:

$$R_E^{\text{opt1}} \simeq R_B^\star - \frac{\gamma(\bar{N}, \frac{2^{R_E^{\text{opt1}}}-1}{\bar{\lambda}_E})\cdot\exp(\frac{2^{R_E^{\text{opt1}}}-1}{\bar{\lambda}_E})}{(\frac{2^{R_E^{\text{opt1}}}-1}{\bar{\lambda}_E})^{\bar{N}-1}\cdot\frac{2^{R_E^{\text{opt1}}}\ln 2}{\bar{\lambda}_E}}. \tag{31}$$

Some classical techniques, e.g., the fixed-point iterative method, are suitable to solve (31). When $R_E > R_E^\dagger$ is satisfied, the approximated optimal solution is obtained. It is obvious that $R_E^{\text{opt1}} > R_E^\dagger$.

Remark 1. As $\bar{\lambda}_E \to 0$, we obtain $R_E^{\text{opt1}} = 0$.

Proof. Because $\gamma(s,x) \to \Gamma(s)$ if $x \to \infty$, when $\bar{\lambda}_E \to 0$, we have $\gamma(\bar{N}, \frac{2^{R_E}-1}{\bar{\lambda}_E}) \to \Gamma(\bar{N})$. Hence, from (19), $P_s \to 0$, and Eq. (23) becomes

$$\eta_s = \frac{1-P_e^\star}{\bar{N}}\cdot(R_B^\star - R_E). \tag{32}$$

It is easy to find that the maximum value of η_s, $\frac{(1-P_e^\star)\cdot R_B^\star}{\bar{N}}$, is obtained when $R_E = 0$.

Remark 2. As $\bar{\lambda}_E \to \infty$, R_E^{opt1} can be obtained by solving the fixed-point equation:

$$R_E^{\text{opt1}} = R_B^\star - \frac{2^{R_E^{\text{opt1}}} - 1}{2^{R_E^{\text{opt1}}} \cdot \ln 2 \cdot \bar{N}}. \tag{33}$$

Proof. Applying $\frac{\gamma(s,x)}{x^s} \to \frac{1}{s}$ when $x \to 0$, we have

$$\lim_{\bar{\lambda}_E \to \infty} \frac{\gamma(\bar{N}, \frac{2^{R_E^{\text{opt1}}}-1}{\bar{\lambda}_E})}{(\frac{2^{R_E^{\text{opt1}}}-1}{\bar{\lambda}_E})^{\bar{N}}} = \frac{1}{\bar{N}}. \tag{34}$$

Substituting (34) in (31), Eq. (33) can be obtained.

4.2 Optimization with COP and SOP constraints

In most transmission scenarios, reliability and security are both required, and can be evaluated by COP and SOP. We now continue to discuss how to adapt the transmission rate with EST criteria under the simultaneous constraints of COP and SOP. The optimization problem becomes

$$\begin{aligned} \max_{R_B, R_E} \quad & \eta_{\text{s}} \\ \text{s.t.} \quad & P_e \leqslant P_e^\star,\ P_s \leqslant P_s^\star,\ 0 \leqslant R_E \leqslant R_B, \end{aligned} \tag{35}$$

where $P_e^\star$ and $P_s^\star$ are the target COP and SOP, respectively. Similar to the discussion above, we still consider a small COP and $R_B = R_B^\star$, as given in (22). Then η_s, as expressed in (23), is proved to be quasi-concave. Let ϕ_t be defined as in (26) again, and this optimization problem becomes

$$\begin{aligned} \max_{R_E} \quad & t \\ \text{s.t.} \quad & \phi_t \geqslant 0,\ P_s \leqslant P_s^\star,\ 0 \leqslant R_E \leqslant R_B^\star. \end{aligned} \tag{36}$$

By fixing t, the following problem of finding the feasible set is concave:

$$\begin{aligned} \text{find} \quad & R_E \\ \text{s.t.} \quad & \phi_t \geqslant 0,\ P_s \leqslant P_s^\star,\ 0 \leqslant R_E \leqslant R_B^\star. \end{aligned} \tag{37}$$

The bisection method is also applied to solve the quasi-concave optimization problem (36), named as Algorithm 2. For simplification, we do not repeat the discussion similarly to Algorithm 1. It is notable that in each iteration, we should examine the feasible solution depending on (37), to which the SOP constraint is added.

Below we will solve the quasi-concave optimization problem (35) using the Lagrangian multiplier method. The constraint of SOP, i.e., $P_s \leqslant P_s^\star$, requires that $R_E \geqslant R_E^\star$, where $R_E^\star$ can be obtained from (19) with $P_s = P_s^\star$. From Proposition 2, when $R_E^\star \geqslant R_E^\dagger$, the quasi-concave optimization is converted to a concave one:

$$\begin{aligned} \max_{R_E} \quad & \eta_s \\ \text{s.t.} \quad & P_s^\star - P_s \geqslant 0,\ R_E \geqslant 0,\ R_B^\star - R_E \geqslant 0, \end{aligned} \tag{38}$$

where η_s is expressed in (23). Define

$$L = \eta_s + \lambda_1(P_s^\star - P_s) + \lambda_2 R_E + \lambda_3(R_B^\star - R_E). \tag{39}$$

Then the KKT conditions are

$$\frac{\partial L}{\partial R_E} = 0, \tag{40a}$$

$$\lambda_1 \geqslant 0, \qquad P_s^\star - P_s \geqslant 0, \qquad \lambda_1(P_s^\star - P_s) = 0, \tag{40b}$$

$$\lambda_2 \geqslant 0, \qquad R_E \geqslant 0, \qquad \lambda_2 R_E = 0, \tag{40c}$$

$$\lambda_3 \geqslant 0, \qquad R_B^\star - R_E \geqslant 0, \qquad \lambda_3(R_B^\star - R_E) = 0. \tag{40d}$$

For non-negative η_s, $R_E \neq 0$. From (40c), we have $\lambda_2 = 0$. Similarly, from (40d), we have $\lambda_3 = 0$. Thus $L = \eta_s + \lambda_1(P_s^\star - P_s)$. As for λ_1, two cases are considered.

When $\lambda_1 = 0$, the optimal solution of problem (35), denoted by R_E^{opt2}, can be obtained only by (40a). From (29) to (31), $R_E^{\text{opt2}} = R_E^{\text{opt1}}$. Because $R_E \geqslant R_E^\star$ and $0 \leqslant R_E \leqslant R_B^\star$, $R_E^{\text{opt2}} = R_E^{\text{opt1}}$ is the feasible solution when $R_E^\star \leqslant R_E^{\text{opt1}} \leqslant R_B^\star$.

When $\lambda_1 > 0$, from (40b) we obtain $P_s = P_s^\star$. Thus $R_E^{\text{opt2}} = R_E^\star$. Then Eq. (40a) becomes $\frac{\mathrm{d}\eta_s}{\mathrm{d}R_E} - \lambda_1 \frac{\mathrm{d}P_s}{\mathrm{d}R_E} = 0$. Then $\frac{\mathrm{d}\eta_s}{\mathrm{d}R_E} = \lambda_1 \frac{\mathrm{d}P_s}{\mathrm{d}R_E} < 0$, and $R_E^{\text{opt1}} \leqslant R_E^\star$. Combined with $0 \leqslant R_E \leqslant R_B^\star$, $R_E^{\text{opt2}} = R_E^\star$ is the feasible solution when $R_E^{\text{opt1}} \leqslant R_E^\star \leqslant R_B^\star$.

There is no feasible solution when $R_E^\star > R_B^\star$.

Given the above, we summarize the solution of problem (38) when $R_E^\star \geqslant R_E^\dagger$:

$$R_E^{\text{opt2}} = \begin{cases} \max\{R_E^{\text{opt1}}, R_E^\star\}, & R_E^\star \leqslant R_B^\star, \\ \emptyset, & R_E^\star > R_B^\star. \end{cases} \tag{41}$$

When $R_E^\star < R_E^\dagger$, following the analysis above, we find $R_E^{\text{opt2}} = R_E^{\text{opt1}} = \max\{R_E^{\text{opt1}}, R_E^\star\}$. Therefore, Eq. (41) is the optimal solution of problem (35).

Remark 3. As $\bar{\lambda}_E \to 0$, we obtain $R_E^{\text{opt2}} = 0$.

Proof. From (19), if $\bar{\lambda}_E \to 0$, then we have $P_s \to 0$ and $R_E^\star \to 0$. According to (41), $R_E^{\text{opt2}} = R_E^{\text{opt1}}$. Based on Remark 1, $R_E^{\text{opt2}} = 0$ is proved.

Remark 4. As $\bar{\lambda}_E \to \infty$, the optimal solution of problem (35) is

$$R_E^{\text{opt2}} = \begin{cases} \max\left\{R_B^\star - \dfrac{2^{R_E^{\text{opt2}}} - 1}{2^{R_E^{\text{opt2}}} \cdot \ln 2 \cdot \bar{N}}, R_E^\star\right\}, & R_E^\star \leqslant R_B^\star, \\ \emptyset, & R_E^\star > R_B^\star. \end{cases} \tag{42}$$

Proof. When $\bar{\lambda}_E \to \infty$, from (41) and Remark 2, Eq. (42) is easily obtained.

5 Numerical results

In this section, we verify our analysis of secrecy performance in the HARQ-CC system by numerical (simulation) results. In Figure 2, we plot COP versus R_B of different $\bar{\lambda}_B$, which is completely determined by the main channel. The maximum transmission number is $K = 10$. Theoretical curves are obtained by (6). We first observe that Monte Carlo simulations almost precisely match theoretical curves given different channel conditions. Moreover, COP sharply increases with R_B until $P_e = 1$. Focusing on three groups of curves, we also observe that when $\bar{\lambda}_B$ increases, a larger R_B results in the same COP, which demonstrates that a higher reliable transmission rate can be obtained with better conditions of the main channel.

In Figure 3, we plot SOP versus R_E for different $\bar{\lambda}_E$, which are both determined by the main channel and eavesdropper channel. Theoretical and approximated P_s are obtained by (14) and (19), respectively. For all of the curves, $\bar{\lambda}_B = 10$ dB, $R_B = 5$, and $K = 10$. We first observe that simulation curves precisely match theoretical P_s, while their differences from the approximated P_s are small. Then, with more redundancy data of R_E, SOP monotonically decreases, which means more redundancy will enhance secrecy. Furthermore, it is critical to point out that to maintain the same value of SOP, a larger R_E is required when $\bar{\lambda}_E$ increases. In other words, when the eavesdropper channel is better, we need more secrecy redundancy to assure the same security level.

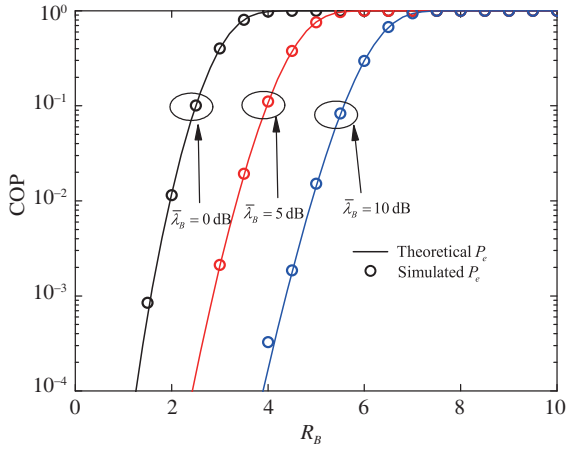

Figure 2 (Color online) COP versus R_B for different average received SNR of main channel. $\bar{\lambda}_B \in \{0, 5, 10\}$ dB and $K = 10$.

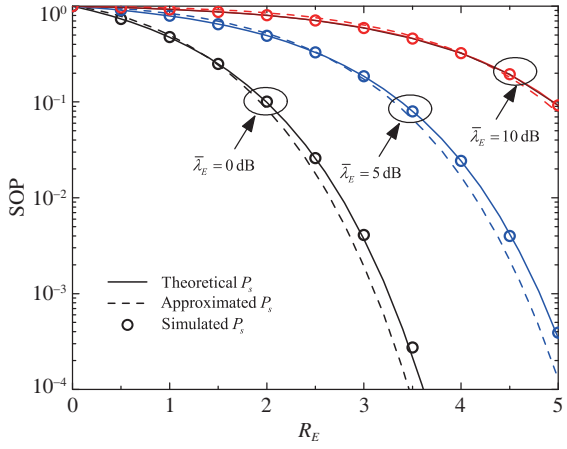

Figure 3 (Color online) SOP versus R_E for different average received SNR of wiretap channel. $\bar{\lambda}_E \in \{0, 5, 10\}$ dB, $\bar{\lambda}_B = 10$ dB, $R_B = 5$, $K = 10$.

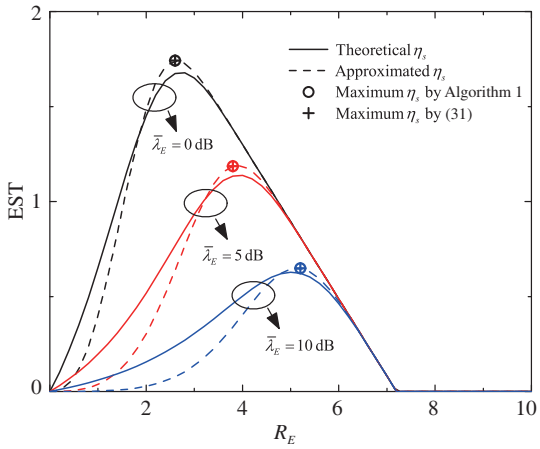

Figure 4 (Color online) EST versus R_E for COP constraint $P_e^\star = 10^{-4}$ and different average received SNR of wiretap channel $\bar{\lambda}_E \in \{0, 5, 10\}$ dB, $\bar{\lambda}_B = 10$ dB, $K = 10$.

Figure 4 shows EST curves versus R_E for the same COP constraint and different $\bar{\lambda}_E$, while the maximum ESTs corresponding to the calculated optimal R_E are marked. Parameters are set as $\bar{\lambda}_B = 10$ dB, $K = 10$, and $P_e^\star = 10^{-4}$. Theoretical and approximated η_s curves are generated according to P_s and the approximated P_s, respectively. We first observe that the difference between the theoretical and approximated η_s is limited, especially the maximum values. All of these η_s curves increase monotonically to the maximum value with R_E, and then decrease monotonically. When R_E is less than its optimal value R_E^{opt1}, its slope decreases from positive to negative. Although a similar rule is not obvious when $R_E > R_E^{\text{opt1}}$, we still conclude that η_s is concave with R_E. The maximum η_s, using the bisection method in Algorithm 1 and fixed-point method (31), are also plotted in Figure 4. We observe that these optimal points well match the maximum approximated η_s. Moreover, the difference between the maximum η_s and approximated η_s is small. Additionally, when $\bar{\lambda}_E$ increases, the optimal R_E increases and a higher secrecy redundancy rate results in a smaller EST.

Under both COP and SOP constraints, we plot EST curves versus R_E, and maximum EST corresponding to calculated optimal R_E again in Figure 5. The channel conditions are $\bar{\lambda}_B = 20$ dB and $\bar{\lambda}_E = 5$ dB. To demonstrate them explicitly, they are separated into three subfigures with the same COP constraint, i.e., $P_e^\star = 10^{-4}$, and different SOP constraints, i.e., $P_s^\star = 0.6, 10^{-1}, 10^{-3}$. Theoretical and approximated η_s curves are still generated according to P_s and the approximated P_s, respectively. Their difference is also limited. The maximum η_s obtained by the bisection method in Algorithm 2 and

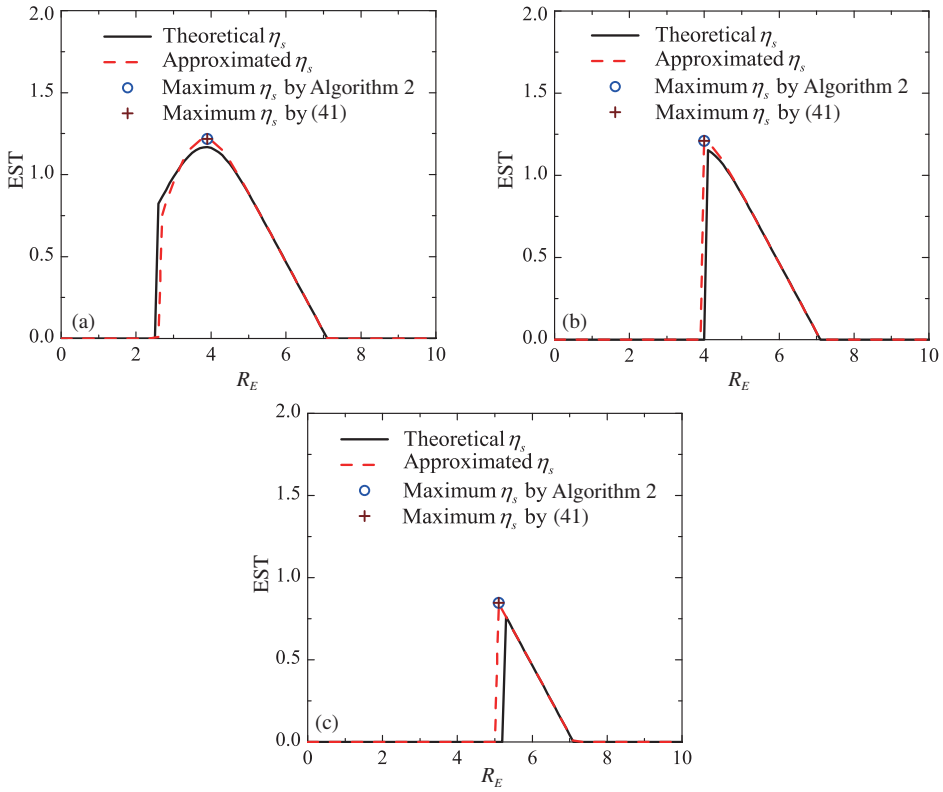

Figure 5 (Color online) EST versus R_E for same COP constraint $P_e^\star = 10^{-4}$ and different SOP constraints $P_s^\star \in \{0.6, 10^{-1}, 10^{-3}\}$, $\bar{\lambda}_B = 20$ dB, $\bar{\lambda}_E = 5$ dB, $K = 10$. (a) $P_s^\star = 0.6$; (b) $P_s^\star = 10^{-1}$; (c) $P_s^\star = 10^{-3}$.

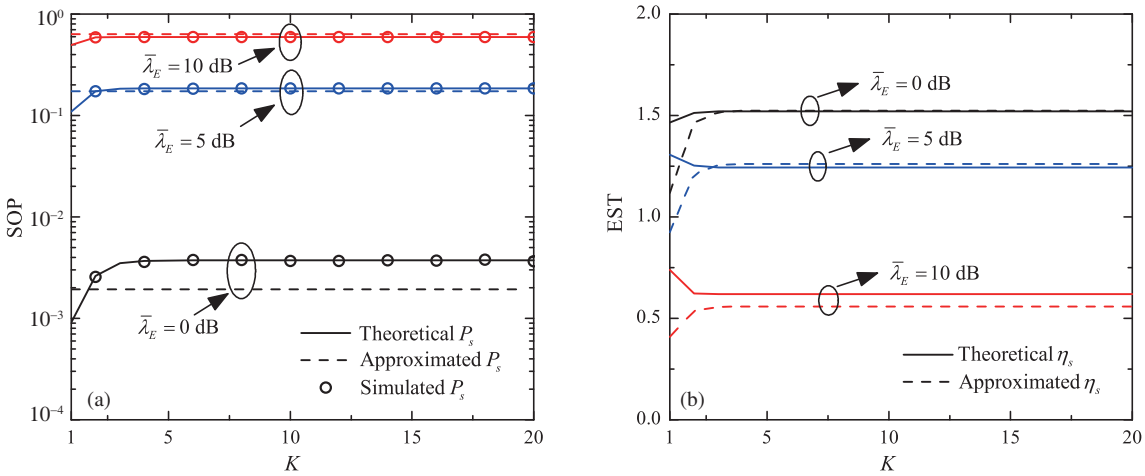

Figure 6 (Color online) The relationship between delay and secrecy performances for different average received SNR of wiretap channel. $\bar{\lambda}_B = 20$ dB, $\bar{\lambda}_E \in \{0, 5, 10\}$ dB, $R_B = 5$, $R_E = 3$. (a) SOP versus K; (b) EST versus K.

Lagrangian multiplier method in (41) both precisely match the maximum value of the approximated η_s curves. Then we compare these three groups of curves. From Figure 5(a), we validate the given solutions for the quasi-concave optimization when $R_E^{\text{opt1}} > R_E^\star$. Because $P_s^\star = 0.6$, we find that $R_E^\star$ is relatively small and its solution, i.e., R_E^{opt2}, equals R_E^{opt1}. From Figure 5(b) and (c), we validate these solutions again when $R_E^{\text{opt1}} \simeq R_E^\star$ and $R_E^{\text{opt1}} < R_E^\star$. For $P_s^\star = 10^{-1}$, $R_E^{\text{opt2}} \simeq R_E^{\text{opt1}}$ as $R_E^{\text{opt1}} \simeq R_E^\star$. For $P_s^\star = 10^{-3}$, $R_E^\star$ is relatively large and $R_E^{\text{opt2}} = R_E^\star$.

To verify the relationship between delay and secrecy performances, we demonstrate SOP and EST versus K for different $\bar{\lambda}_E$ in Figure 6, in which parameters are set as $\bar{\lambda}_B = 20$ dB, $\bar{\lambda}_E = 0$, 5 or 10 dB,

$R_B = 5$ and $R_E = 3$. In Figure 6(a), theoretical and approximated P_s are still obtained by (14) and (19), respectively. And their difference is also limited, considering the use of logarithmic coordinate. We observe that SOP rises slowly and converges to a stable value with increased K, that caused by limited diversity gain of wiretap channel and almost fixed $\bar{N}$ of main channel. When wiretap channel is better, i.e., $\bar{\lambda}_E$ is larger, a greater SOP occurs which means Eve can obtain more information. In Figure 6(b), the curves of theoretical and approximated η_s versus K are illustrated. It is confirmed that η_s tends to be stable with increased K because all its affecting factors, i.e., COP, SOP and $\bar{N}$, converge. Furthermore, larger $\bar{\lambda}_E$ inevitably results in lower η_s.

6 Conclusion

In this paper, we discussed the quasi-concave optimization of the secrecy redundancy rate, R_E, in the HARQ-CC system. We extended the metric of EST into multiple transmissions involving COP and SOP simultaneously. The quasi-concave optimization was solved by the bisection method and fixed-point method under COP constraints. This problem was also worked out using the bisection method and Lagrangian multiplier method with both COP and SOP constraints. Finally, numerical and simulation results verified our analysis and demonstrated that although the optimization of R_E is non-convex, our proposed solutions still perform efficiently to improve the secrecy coding.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61673049) and Natural Science Foundation of the Higher Education Institutions of Anhui Province (Grant No. KJ2018A0441).

References

1 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
2 Csiszar I, Korner J. Broadcast channels with confidential messages. IEEE Trans Inform Theor, 1978, 24: 339–348
3 Leung-Yan-Cheong S, Hellman M. The Gaussian wire-tap channel. IEEE Trans Inform Theor, 1978, 24: 451–456
4 Barros J, Rodrigues M R D. Secrecy capacity of wireless channels. In: Proceedings of IEEE International Symposium on Information Theory, Seattle, 2006. 451–456
5 Wang P Y, Yu G D, Zhang Z Y. On the secrecy capacity of fading wireless channel with multiple eavesdroppers. In: Proceedings of IEEE International Symposium on Information Theory, Nice, 2007. 1301–1305
6 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information-theoretic security. IEEE Trans Inform Theor, 2008, 54: 2515–2534
7 Xu X M, Yang W W, Cai Y M, et al. On the secure spectral-energy efficiency tradeoff in random cognitive radio networks. IEEE J Sel Areas Commun, 2016, 34: 2706–2722
8 Zheng T X, Wang H M, Liu F, et al. Outage constrained secrecy throughput maximization for DF relay networks. IEEE Trans Commun, 2015, 63: 1741–1755
9 Monteiro M E P, Rebelatto J L, Souza R D, et al. Maximum secrecy throughput of transmit antenna selection with eavesdropper outage constraints. IEEE Signal Process Lett, 2015, 22: 2069–2072
10 Yan S H, Yang N, Geraci G, et al. Optimization of code rates in SISOME wiretap channels. IEEE Trans Wirel Commun, 2015, 14: 6377–6388
11 Dong Y J, Hossain M J, Cheng J L, et al. Dynamic cross-layer beamforming in hybrid powered communication systems with harvest-use-trade strategy. IEEE Trans Wirel Commun, 2017, 16: 8011–8025
12 Goel S, Negi R. Guaranteeing secrecy using artificial noise. IEEE Trans Wirel Commun, 2008, 7: 2180–2189
13 Zhou F H, Li Z, Cheng J L, et al. Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT. IEEE Trans Wirel Commun, 2017, 16: 2450–2464
14 Liu S Y, Hong Y, Viterbo E. Guaranteeing positive secrecy capacity for MIMOME wiretap channels with finite-rate feedback using artificial noise. IEEE Trans Wirel Commun, 2015, 14: 4193–4203
15 Zhang S, Xu X M, Wang H M, et al. Enhancing the physical layer security of uplink non-orthogonal multiple access in cellular Internet of things. IEEE Access, 2018, 6: 58405–58417
16 Chen Y J, Ji X S, Huang K Z, et al. Opportunistic access control for enhancing security in D2D-enabled cellular networks. Sci China Inf Sci, 2018, 61: 042304
17 Wang S Y, Xu X M, Huang K Z, et al. Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems. IEEE Access, 2019, 7: 28597–28606
18 Chen Y J, Ji X S, Huang K Z, et al. Artificial noise-assisted physical layer security in D2D-enabled cellular networks. J Wirel Commun Netw, 2017, 2017: 178
19 Zou Y L, Zhu J, Wang X B, et al. Improving physical-layer security in wireless communications using diversity techniques. IEEE Netw, 2015, 29: 42–48

20 Wu Y, Olawoyin L A, Zhang N N, et al. The analysis of secure HARQ with chase combining over block fading channel. China Commun, 2016, 13: 82–88
21 Tang X J, Liu R H, Spasojevic P, et al. On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels. IEEE Trans Inform Theor, 2009, 55: 1575–1591
22 Mheich Z, Le Treust M, Alberge F, et al. Rate-adaptive secure HARQ protocol for block-fading channels. In: Proceedings of the 22nd European Signal Processing Conference, Lisbon, 2014. 830–834
23 Le Treust M, Szczecinski L, Labeau F. Rate adaptation for secure HARQ protocols. IEEE Trans Inform Forensic Secur, 2018, 13: 2981–2994
24 Lagrange X. Throughput of HARQ protocols on a block fading channel. IEEE Commun Lett, 2010, 14: 257–259
25 Guan X R, Cai Y M, Yang W W. On the reliability-security tradeoff and secrecy throughput in cooperative ARQ. IEEE Commun Lett, 2014, 18: 479–482
26 Zorzi M, Rao R R. On the use of renewal theory in the analysis of ARQ protocols. IEEE Trans Commun, 1996, 44: 1077–1081
27 Caire G, Tuninetti D. The throughput of hybrid-ARQ protocols for the Gaussian collision channel. IEEE Trans Inform Theor, 2001, 47: 1971–1988
28 Steven B, Lieven V. Convex Optimization. Cambridge: Cambridge University Press, 2004