entropy

MDPI

Article

Rate Adaption for Secure HARQ-CC System with Multiple Eavesdroppers

Yue Wu [1,*], Shishu Yin [1], Jian Zhou [1], Pei Yang [2] and Hongwen Yang [2]

[1] Department of Electronic and Information Engineering, Anhui University of Finance and Economics, Bengbu 233030, China; yin_shishu@163.com (S.Y.); ac_zj_course@163.com (J.Z.)

[2] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; yp@bupt.edu.cn (P.Y.); yanghong@bupt.edu.cn (H.Y.)

* Correspondence: wuyue@aufe.edu.cn

Received: 3 March 2020; Accepted: 30 March 2020; Published: 31 March 2020

Abstract: In this paper, we studied the secure transmission of a hybrid automatic repeat request with chase combining (HARQ-CC) system, under the existence of multiple eavesdroppers and limited latency. First, we analyzed some critical performance metrics, including connection outage probability (COP), secrecy outage probability (SOP) and effective secrecy throughput (EST). Then, to maximize the EST, three optimization problems of rate adaption were discussed: (i) optimizing the code rate with a given secrecy redundancy rate by a parameterized closed-form solution; (ii) optimizing the secrecy redundancy rate with a given code rate by a fixed-point method; (iii) optimizing both code rate and secrecy redundancy rate by an iterative optimization algorithm. We also considered COP and SOP constraints among the problems while corresponding solutions were deduced. Finally, numerical and simulated results verified our conclusions that the approximated SOP matches well with Monte–Carlo simulation for a strict reliable constraint, and that the optimized transmitting rate enhances EST efficiently with multiple eavesdroppers and retransmissions. Moreover, the influence of the number of eavesdroppers on secrecy performance was analyzed. Briefly, secrecy performance inevitably deteriorates with increasing number of eavesdroppers due to raised information leakage.

Keywords: physical layer security (PLS); hybrid automatic repeat request (HARQ); chase combining (CC); secrecy outage probability (SOP); effective secrecy throughput (EST)

1. Introduction

In modern wireless communication systems, physical layer security (PLS) is regarded as a critical aspect in providing confidential message transmission according to the characteristics of wireless channels. Differing from traditional encryption techniques, PLS can be proved and quantified without the risk of brute-force cracking. Shannon first proposed the notion of information-theoretic secrecy in his groundbreaking work [1]. The more practical framework, named 'the wiretap channel', was established by Wyner in terms of a binary symmetric channel (BSC) [2]. Another important contribution of Wyner was the designing of a secrecy coding scheme, in which the secrecy redundancy rate worked to confuse an eavesdropper. As extended versions, the wiretap channel has been considered in broadcast channels by Csiszar [3] and in Gaussian channels by Leung-Yan-Cheong [4].

On the basis of the above work, PLS has contributed to considerable progress, especially in performance optimization and signal processing. Secrecy capacity, which evaluates the effectiveness of secure transmission, has been defined as the maximum rate in each reliable and secure transmission [5]. This metric has been adopted in the security analysis and optimization of 5G mmWave small cell networks [6], co-operative non-orthogonal multiple access with proactive jamming [7], artificial noise (AN)-aided multi-input multi-output (MIMO) Rician channels [8] and so on. As the secrecy capacity may be less than target secrecy redundancy rate, the secrecy outage probability (SOP) has

been applied to present a more comprehensive performance evaluation. For instance, [9] discussed a security region with AN based on SOP, and [10] minimized SOP in a D2D-enabled cellular network by access control. When a certain SOP constraint is required, secrecy throughput has widely been considered, especially in optimization problems where the transmission rate or power is adjusted for improved security [11,12]. On the other hand, signal processing-related methods have also been proposed, mainly including beamforming and precoding, AN, co-operative and relay and diversity technologies [13–16].

Recently, many excellent contributions have focused on the PLS of hybrid automatic repeat request (HARQ) methods capable of typical time diversity features. In HARQ with chase combining (HARQ-CC), the transmitter retransmits erroneous codewords (or their redundant versions) if the legitimate receiver fails to decode them. On the contrary, new transmissions are triggered when either the decoding is successful or the maximum transmission number is reached [17]. Due to the increased comprehensive requirements, Makki et al. [18] proposed a low-latency reliable HARQ protocol using finite blocklength codes. When a passive eavesdropper exists, it has been proven that retransmissions and combinations are capable of enhancing security, due to the diversity gain of the legitimate receiver [19]. In order to efficiently design secure HARQ, Tang et al. [20] discussed SOP, secrecy throughput and their asymptotic properties; Tomasin [21] proposed a multiple-encoding HARQ scheme with statistics channel state information (CSI); Mheich et al. and Treust et al. [22,23] optimized secrecy throughput using multi-level feedback and rate adaption. However, most of them did not consider the influence of secrecy outage on secrecy throughput, which generally led to overestimated performance [24]. Hence, in our previous work, we extended the effective secrecy throughput (EST) of a single transmission [25] into a HARQ-CC system with a passive eavesdropper, and optimized secrecy redundancy rate for improved security [26]. Nevertheless, another common scenario, which includes multiple eavesdroppers, rate adaption and limited latency, has not yet been analyzed.

Inspired by this problem, in this paper, we completed the optimization of both the code rate and secrecy redundancy rate to maximize EST in a general scenario with multiple eavesdroppers. At the same time, different latency requirements were also considered. The major contributions of our work include:

- The closed-form expressions of COP, average transmission number and SOP in the HARQ-CC system with multiple eavesdroppers and different latencies are given. The corresponding approximations were also deduced, while EST was defined considering both reliable outage and secrecy outage.
- With a given secrecy redundancy rate, the optimization problem of code rate to maximize the EST was discussed. This problem was solved with a parameterized closed-form solution, with and without the COP constraint.
- When the code rate is given, the optimization problem of secrecy redundancy rate with EST criteria was also analyzed. We solved this problem by applying a fixed-point method, with and without the SOP constraint.
- The joint optimization problem of the rate pair (i.e., code rate and secrecy redundancy rate), in order to maximize the EST, was discussed. To solve this problem, an iterative optimization algorithm was designed which involves the two methods mentioned above. COP and SOP constraints were also considered.
- Numerical and simulated results confirm our expressions of critical secure performance metrics, as well as the proposed optimization methods, under different cases. We also found that secrecy performance inevitably deteriorates with an increasing number of eavesdroppers, due to more information leakage.

The rest of this paper is organized as follows: The overall system model and assumptions are described in Section 2. Section 3 expresses COP, average transmission number, SOP and its approximation, along with the definition of EST in a HARQ-CC system with multiple eavesdroppers. Section 4 proposes the optimization of code rate, secrecy redundancy rate and both of them, in order

to maximize EST under different constraints and the numerical and simulated results are presented in Section 5. Section 6 concludes our work.

Notation: $\mathbb{E}[\cdot]$ denotes the expectation operator. The function $\Gamma(a,x)$ is the upper incomplete gamma function, $\Gamma(a)$ is the gamma function, $\Gamma_{\mathrm{r}}(a,x)=\Gamma(a,x)/\Gamma(a)$ and $\gamma_{\mathrm{r}}(a,x)=1-\Gamma_{\mathrm{r}}(a,x)$ are the regularized upper and lower incomplete gamma functions, respectively. $N(a,b)$ denotes a Gaussian distribution with mean a and variance b, respectively. $f_X(x)$ and $F_X(x)$ denote the probability density function (PDF) and the cumulative distribution function (CDF) of a random variate X, respectively. The function $W_0(x)$ is the principal branch ($W_0(x)>-1$) of Lambert's W-function, defined through the implicit equation $x=W(x)e^{W(x)}$ [27].

2. System Model of Secure HARQ-CC With Multi-Eavesdroppers

We considered a secure HARQ-CC transmission system with multiple eavesdroppers, as shown in Figure 1. The transmitter (Alice) sends a confidential message $\boldsymbol{w}$ with a secrecy redundancy message $\boldsymbol{v}$ to the legitimate receiver (Bob) over the main channel, while several passive eavesdroppers (Eve1, ..., EveM) intercept the transmission through M wiretap channels. We assumed that the main and wiretap channels are independent Rayleigh block-fading channels. Retransmissions are triggered only by Bob, depending on his decoding failure. To avoid unexpected retransmissions, the maximum transmission number (K) guarantees limited latency. A major security advantage of this protocol is that the erroneous codewords received by eavesdroppers may not be retransmitted by Alice, unless Bob had the same erroneous ones. Hence, there was much more diversity gain obtained by Bob than Eve1, ..., EveM.

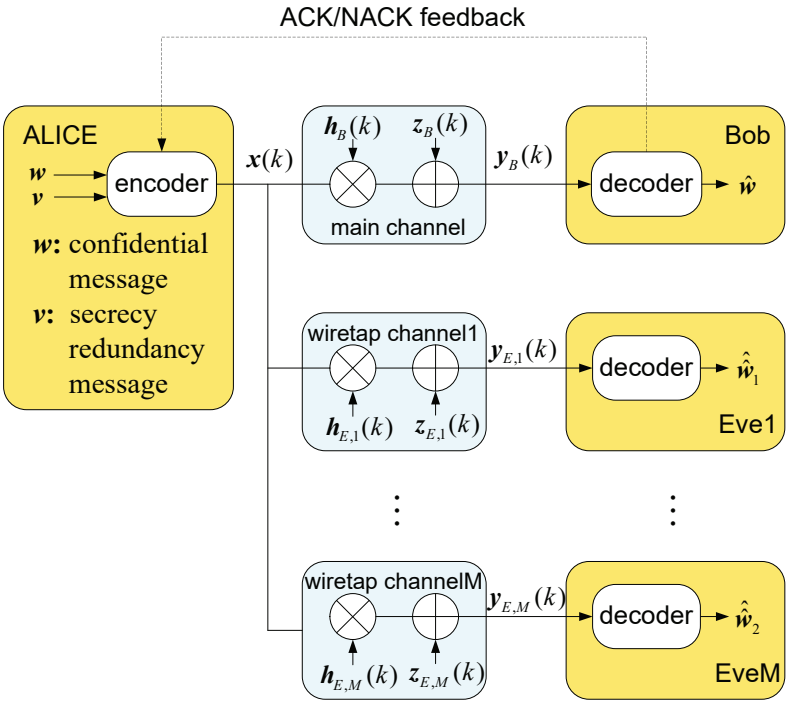

Figure 1. Secure hybrid automatic repeat request (HARQ) with chase combining (HARQ-CC) system model with multiple eavesdroppers.

Alice encodes the confidential message $\boldsymbol{w}$ and the secrecy redundancy message $\boldsymbol{v}$ into the codeword $\boldsymbol{x}(k)$ using the Wyner secrecy code [2], where k is the transmission number ($1\le k\le K$). The code rate and secrecy redundancy rate are denoted by 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 $\mathbb{E}\left[|x(k)|^2\right]=1$. We denote the fading parameters of the main and wiretap channels by $\boldsymbol{h}_B(k)$ and $\boldsymbol{h}_{E,1}(k),\ldots,\boldsymbol{h}_{E,M}(k)$, respectively, which are independently and identically distributed (i.i.d.) complex Gaussian random

variables with zero mean and unit variance. We denote the additive Gaussian white noise by $z_B(k)$ and $z_{E,1}(k), \ldots, z_{E,M}(k)$, respectively. Their means are zero and their variances are, respectively, σ_B^2 and $\sigma_{E,1}^2, \ldots, \sigma_{E,M}^2$. In each slot, the received signals of Bob and Eve1, ..., EveM after k transmissions are

$$\begin{cases} y_B(k) = \sqrt{P} h_B(k) x(k) + z_B(k) \\ y_{E,m}(k) = \sqrt{P} h_{E,m}(k) x(k) + z_{E,m}(k), m = 1, \ldots, M \end{cases}. \tag{1}$$

For simplicity, we define $S_B = P/\sigma_B^2$ and $S_{E,m} = P/\sigma_{E,m}^2, (m = 1, \ldots, M)$ as the average received signal-to-noise ratio (SNR) through the main channel and the wiretap channels, respectively. After k transmissions, Bob and Eve1, ..., EveM uses the maximal ratio combining (MRC) before decoding. Their combined SNR becomes:

$$\begin{cases} \gamma_B(k) = \sum_{i=1}^{k} S_B \left| h_B(i) \right|^2 \\ \gamma_{E,m}(k) = \sum_{i=1}^{k} S_{E,m} \left| h_{E,m}(i) \right|^2, m = 1, \ldots, M \end{cases}. \tag{2}$$

3. Security Performance Metrics

Based on the above secure HARQ-CC system model with multiple eavesdroppers, we analyzed some critical security performance metrics, including connection outage probability (COP), average transmission number, secrecy outage probability (SOP) and effective secrecy throughput (EST). Connection outage occurs when the legitimate receiver (Bob) cannot decode the transmitted codewords, and secrecy outage occurs when one or several of the eavesdroppers (Eve1, ..., EveM) cannot be confused by secrecy redundancy after the k^{th} transmission.

We first considered the COP after k transmissions, denoted by $P_e(k)$. The COP is defined as the probability that a connection outage occurs; that is, the mutual information after the k^{th} transmission, $I_B(k)$, is less than the codeword rate R_B,

$$\begin{aligned} P_e(k) &= \Pr\{I_B(k) < R_B\} \\ &= \Pr\{\ln\left(1 + \sum_{i=1}^{k} S_B \left| h_B(i) \right|^2\right) < R_B\} \\ &= \Pr\left\{\sum_{i=1}^{k} \left| h_B(i) \right|^2 < \frac{e^{R_B} - 1}{S_B}\right\} \end{aligned}. \tag{3}$$

We know that 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. Denote the decoding threshold of the main channel by $\Theta_B = \left(e^{R_B} - 1\right) / S_B$, then

$$\begin{aligned} P_e(k) &= \mathcal{F}_{\chi^2}\left[2\Theta_B, 2k\right] \\ &= \gamma_{\text{r}}\left(k, \Theta_B\right) \end{aligned}, \tag{4}$$

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

The average transmission number $\bar{N}$ is determined by the main channel, which is equal to the expectation of the actual transmission number, N,

$$\begin{aligned} \bar{N} = \mathbb{E}[N] &= 1 + \sum_{k=1}^{K-1} P_e(k) \\ &= 1 + \sum_{k=1}^{K-1} \gamma_{\mathrm{r}}\left(k, \Theta_B\right) \end{aligned}. \tag{5}$$

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 Eve1 or ... or EveM after k transmissions. As passive receivers, Eve1, ..., EveM only receive messages when retransmissions are requested by Bob. When the number of transmissions in the main channel is N,

$$\begin{aligned} P_s(k) &= \sum_{i=1}^{k} \Pr\{N = i\} \cdot \Pr\left\{ I_{E,1}(i) > R_E \bigcup I_{E,2}(i) > R_E \bigcup \cdots \bigcup I_{E,M}(i) > R_E \right\} \\ &= \sum_{i=1}^{k} \Pr\{N = i\} \cdot \left(1 - \Pr\{I_{E,1}(i) < R_E, I_{E,2}(i) < R_E, \ldots, I_{E,M}(i) < R_E\}\right) \end{aligned}, \tag{6}$$

where $I_{E,i}$ is the mutual information of the wiretap channel, $\Pr\{N = i\}$ is the probability that the i^{th} transmission occurs, and $\Pr\{N = i\} = P_e(i-1) - P_e(i)$. Assume that M wiretap channels are i.i.d. Gaussian block fading channels, $S_{E,m} = S_E$, $\Pr\{I_{E,m}(i) > R_E\} = \Pr\{I_E(i) > R_E\}, m = 1, \ldots, M$. Denote the decoding threshold of a wiretap channel by $\Theta_E = \left(e^{R_E} - 1\right)/S_E$. Then we define

$$\begin{aligned} \phi(i) &= \Pr\{I_{E,1}(i) < R_E, I_{E,2}(i) < R_E, \ldots, I_{E,M}(i) < R_E\} \\ &= \Pr\{I_{E,1}(i) < R_E\} \Pr\{I_{E,2}(i) < R_E\} \ldots \Pr\{I_{E,M}(i) < R_E\} \\ &= \left(\Pr\{I_E(i) < R_E\}\right)^M \\ &= \left(\Pr\left\{ \log_2\left(1 + \sum_{j=1}^{i} S_E \left|h_{E,m}(i)\right|^2\right) < R_E \right\}\right)^M \\ &= \left(\gamma_{\mathrm{r}}\left(i, \Theta_E\right)\right)^M \end{aligned}. \tag{7}$$

Hence, the SOP after K transmissions becomes

$$P_s(K) = \sum_{i=1}^{K} \Pr\{N = i\} \cdot (1 - \phi(i)). \tag{8}$$

It is well-known that an extremely small COP is the fundamental reliablity requirement in modern systems. We assume that under different latency requirements (i.e., different maximum transmission numbers K), a small $P_e(K)$ has to be assured. Thus we have $\sum_{i=1}^{K} \Pr\{N = i\} = 1$, then

$$\begin{aligned} P_s(K) &= \sum_{i=1}^{K} \Pr\{N = i\} - \sum_{i=1}^{K} \Pr\{N = i\} \cdot \phi(i) \\ &= 1 - \mathbb{E}[\phi(N)] \end{aligned}. \tag{9}$$

As N is an integer, $\phi(N)$ is also M^{th} power of the complementary CDF (CCDF) of a Poisson random variable. With a given R_E, the PDF and CDF are both well-known as a log-concave function of N. According to [28], its CCDF is also log-concave. In other words, $\ln \phi(N)$ is concave with respect to

N. Under the above assumption that a low $P_e(K)$ is assured under different K, $\sum_{i=1}^{K} \Pr\{N=i\} = 1$. According to Jenson's inequality, we have

$$\begin{aligned} \ln \phi\left(\mathbb{E}[N]\right) &\leq \mathbb{E}\left[\ln \phi(N)\right] \\ &= \sum_{i=1}^{K} \Pr\{N=i\} \cdot \ln \phi(N) \\ &= \sum_{i=1}^{K} \ln \phi(N)^{\Pr\{N=i\}} \\ &= \ln \prod_{i=1}^{K} \phi(i)^{\Pr\{N=i\}} \\ &\overset{(a)}{\leq} \ln \sum_{i=1}^{K} \Pr\{N=i\} \cdot \phi(i) \\ &= \ln \mathbb{E}\left[\phi(i)\right] \\ &= \ln\left(1 - P_s(K)\right) \end{aligned} , \tag{10}$$

where (a) is true, based on the general mean inequality, and $1 - P_s(K)$ and $\phi\left(\mathbb{E}[N]\right)$ are both positive. Thus,

$$P_s(K) \leq 1 - \phi\left(\mathbb{E}[N]\right). \tag{11}$$

Substituting Equation (7) into Equation (11), we approximate the SOP of the K^{th} transmission by its upper bound, as follows:

$$P_s(K) \simeq 1 - \left(\gamma_{\mathrm{r}}\left(K, \Theta_E\right)\right)^M. \tag{12}$$

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

Most related works have not considered the influence of SOP in secrecy throughput, but this has been found to be inaccurate [24]. Hence, we define the effective secrecy throughput (EST) of a secure HARQ-CC system as [26]

$$\eta_s = \frac{\mathbb{E}[R_s]}{\mathbb{E}[N]} = \frac{\left(R_B - R_E\right) \cdot \left(1 - P_e\right) \cdot \left(1 - P_s\right)}{\bar{N}}, \tag{13}$$

where $R_s = R_B - R_E$ indicates the maximum rate of each reliable and secure transmission, $\bar{N}$ is the average transmission number, and the COP and SOP are denoted by P_e and P_s, respectively. Based on the renewal–reward theorem [29,30], η_s in Equation (13) expresses the average reliable and secure transmission rate of each transmission. As this metric demonstrates the secrecy performance more comprehensively, we adapted the code rate and secrecy redundancy rate to enhance the performance with this criteria in the following section.

4. Rate Adaption in Secure HARQ-CC System

In this section, in order to improve the performance of secure transmission when multiple eavesdroppers exist and latency is limited, we optimized the code rate R_B and secrecy redundancy rate R_E to maximize the EST of HARQ-CC. Three cases were considered: When R_E is given, R_B is optimized by a parameterized closed-form solution, with and without a COP constraint. When R_B is given, R_E is optimized by a fix-point method, with and without an SOP constraint. Combining the above methods, we then solved the joint optimization of the rate pair (R_B, R_E) by an iterative algorithm with and without both COP and SOP constraints.

4.1. Optimization of Code Rate

In a secure HARQ-CC system, when the number of eavesdroppers is M, the maximum transmission number is K and the secrecy redundancy rate is given by $\tilde{R}_E$, we first considered the problem of how to determine the code rate which maximizes the EST:

$$\begin{array}{ll} \max\limits_{R_B} & \eta_s \\ s.t. & 0 \le \tilde{R}_E \le R_B \end{array}, \tag{14}$$

where P_e, P_s and η_s are obtained by Equations (4), (12) and (13), respectively. Now, we extended the parameterized closed-form solution [17] to solve this problem. Several HARQ schemes tell us the standard solution is to solve the equation $\mathrm{d}\eta_s/\mathrm{d}R_B = 0$ for the (globally) optimal rate point $\hat{R}_B$. Furthermore, $\mathrm{d}^2\eta_s/\mathrm{d}R_B^2|_{\hat{R}_B} < 0$ is required to guarantee a global maximum.

The basic idea of this solution method is to use the substitution $R_B = \ln(1 + S_B\Theta_B)$ for the rate in the numerator of the EST expression. S_B only occurs in the numerator once; hence, instead of considering the rate R_B, we focus on the threshold Θ_B in the optimization.

The EST expression for secure HARQ-CC is first parameterized with respect to Θ_B, according to

$$\eta_s = \frac{R_B - R_E}{\tilde{\bar{N}}(\Theta_B)} = \frac{\ln(1 + S_B\Theta_B) - \tilde{R}_E}{\tilde{\bar{N}}(\Theta_B)}, \tag{15}$$

where $\tilde{\bar{N}}(\Theta_B) \triangleq \bar{N}(\Theta_B)/(1 - P_e(\Theta_B))(1 - P_s(\Theta_B))$, and $P_s(\Theta_B)$ is also function of Θ_B, as S_E, R_E, M and K are given. Then, we take the derivative with respect to Θ_B,

$$\frac{\mathrm{d}\eta_s}{\mathrm{d}\Theta_B} = \frac{1}{\left(\tilde{\bar{N}}(\Theta_B)\right)^2}\left(\frac{S_B}{1 + S_B\Theta_B}\tilde{\bar{N}}(\Theta_B) - \tilde{\bar{N}}'(\Theta_B)\left(\ln\left(1 + S_B\hat{\Theta}_B\right) - \tilde{R}_E\right)\right). \tag{16}$$

Let $\mathrm{d}\eta_s/\mathrm{d}\Theta_B|_{\hat{\Theta}_B} = 0$, where $\hat{\Theta}_B$ is the optimal point, and divide both sides by $\hat{\Theta}_B$. Then, we have

$$\frac{1 + S_B\hat{\Theta}_B}{S_B\hat{\Theta}_B}\left(\ln\left(1 + S_B\hat{\Theta}_B\right) - \tilde{R}_E\right) = \frac{\tilde{\bar{N}}(\hat{\Theta}_B)}{\hat{\Theta}_B\tilde{\bar{N}}'(\hat{\Theta}_B)}, \tag{17}$$

where the $S_B\hat{\Theta}_B$-terms and $\hat{\Theta}_B$-terms are separated into different sides of Equation (17). We define

$$u \triangleq S_B\hat{\Theta}_B, \tag{18}$$

$$g(u) \triangleq (1 + u)\left(\ln(1 + u) - \tilde{R}_E\right)/u, \tag{19}$$

$$t(\hat{\Theta}_B) \triangleq \tilde{\bar{N}}(\hat{\Theta}_B)/\hat{\Theta}_B\tilde{\bar{N}}'(\hat{\Theta}_B). \tag{20}$$

Then, Equation (17) is given by $g(u) = t$. From Equation (19), this relationship becomes $1 + u = e^{t - \frac{t}{1+u} + \tilde{R}_E}$. Let $v = -\frac{t}{1+u}$, which is rewritten to $ve^v = -te^{-t-\tilde{R}_E}$, which is solved by $v = W_0\left(-te^{-t-\tilde{R}_E}\right)$ where $W_0(x)$ is the principal branch ($W_0(x) > -1$) of Lambert's W-function. Thus, we have $1 + S_B\hat{\Theta}_B = e^{t + W_0\left(-te^{-t-\tilde{R}_E}\right) - R_E}$.

Then, we solve the problem in Equation (14) by

$$S_B(\hat{\Theta}_B) = \frac{e^{t+W_0\left(-te^{-t-\tilde{R}_E}\right)+\tilde{R}_E}-1}{\hat{\Theta}_B}, \tag{21}$$

$$\hat{R}_B(\hat{\Theta}_B) = t + W_0\left(-te^{-t-\tilde{R}_E}\right) + \tilde{R}_E, \tag{22}$$

$$\eta_s(\hat{\Theta}_B) = \frac{R_B(\hat{\Theta}_B) - \tilde{R}_E}{\tilde{\tilde{N}}(\hat{\Theta}_B)}, \tag{23}$$

where $t(\hat{\Theta}_B) = \tilde{\tilde{N}}(\hat{\Theta}_B)/\hat{\Theta}_B\tilde{\tilde{N}}'(\hat{\Theta}_B)$. We see that all equations are expressed only in terms of the parameter $\hat{\Theta}_B$. With the given S_B, the optimal $\hat{R}_B(\hat{\Theta}_B)$ and $\eta_s(\hat{\Theta}_B)$ can therefore be obtained.

As $g(u)$, defined in Equation (19), can be expanded by $\ln(1+u) \simeq u - u^2/2 + O(u^3)$, we give the low and high SNR asymptotes as follows:

Remark 1. *As $S_B \to 0$ for finite M, the problem in Equation (14) is solved by*

$$S_B(\hat{\Theta}_B) = \frac{t-1+\sqrt{(t-1)^2+2\tilde{R}_E}}{\hat{\Theta}_B}, \tag{24}$$

$$\hat{R}_B(\hat{\Theta}_B) = \ln\left(t+\sqrt{(t-1)^2+2\tilde{R}_E}\right), \tag{25}$$

$$\eta_s(\hat{\Theta}_B) = \frac{\ln\left(t+\sqrt{(t-1)^2+2\tilde{R}_E}\right) - \tilde{R}_E}{\tilde{\tilde{N}}(\hat{\Theta}_B)}, \tag{26}$$

where $t(\hat{\Theta}_B) = \tilde{\tilde{N}}(\hat{\Theta}_B)/\hat{\Theta}_B\tilde{\tilde{N}}'(\hat{\Theta}_B)$.

Proof. When $S_B \to 0$, we have $g(u) \simeq 1 + u/2 - \tilde{R}_E/u$. By $g(u) = t$, $u = t - 1 + \sqrt{(t-1)^2 + 2\tilde{R}_E}$, our solutions then become Equations (24)–(26), as $u = S_B\hat{\Theta}_B$, $R_B = \ln(1+u)$, and $\eta_s = (R_B - \tilde{R}_E)/\tilde{\tilde{N}}$. □

Remark 2. *As $S_B \to \infty$ for finite M, the problem in Equation (14) is solved by*

$$S_B(\hat{\Theta}_B) = \frac{e^{t+\tilde{R}_E}}{\hat{\Theta}_B}, \tag{27}$$

$$\hat{R}_B(\hat{\Theta}_B) = t, \tag{28}$$

$$\eta_s(\hat{\Theta}_B) = \frac{t - \tilde{R}_E}{\tilde{\tilde{N}}(\hat{\Theta}_B)}, \tag{29}$$

where $t(\hat{\Theta}_B) = \tilde{\tilde{N}}(\hat{\Theta}_B)/\hat{\Theta}_B\tilde{\tilde{N}}'(\hat{\Theta}_B)$.

Proof. When $S_B \to \infty$, $g(u) \simeq \ln(1+u)$. By $g(u) = t$, we have $u = e^{t+\tilde{R}_E} - 1$. Then, Equations (27)–(29) can be achieved. □

High reliability is the fundamental requirement in a modern wireless communication system. Hence, we continue to consider the problem in Equation (14) with the following COP constraint:

$$\begin{aligned} \max_{R_B} \quad & \eta_s \\ s.t. \quad & P_e \le P_e^\star \\ & 0 \le \tilde{R}_E \le R_B \end{aligned}, \tag{30}$$

where $P_e^\star$ denotes the target COP. According to Equation (4), P_e increases monotonically with increasing R_B. Hence, we know the COP constraint requires $R_B \leq R_B^\star$, where

$$R_B^\star = \ln\left[1 + \frac{S_B}{2}\mathcal{F}_{\chi^2}^{-1}[P_e^\star, 2K]\right], \tag{31}$$

in which $\mathcal{F}_{\chi^2}^{-1}[\cdot]$ is the inverse function of the CDF of the chi-squared distribution.

As the solution of Equation (14) requires $\mathrm{d}\eta_s/\mathrm{d}R_B|_{\hat{R}_B} = 0$ and $\mathrm{d}^2\eta_s/\mathrm{d}R_B^2|_{\hat{R}_B} < 0$, (30) can be solved by:

$$R_B^\dagger = \min\left[\hat{R}_B(\hat{\Theta}_B), R_B^\star\right], \tag{32}$$

where the optimal point $R_B^\dagger$ is always the maximum point in the feasible set of R_B.

4.2. Optimization of Secrecy Redundancy Rate

When the number of eavesdroppers is M, the maximum transmission number is K and code rate is given by $\tilde{R}_B$, we consider the problem of how to determine the secrecy redundancy rate which maximizes the EST:

$$\begin{aligned} \max_{R_E} \quad & \eta_s \\ s.t. \quad & 0 \leq R_E \leq \tilde{R}_B \end{aligned}, \tag{33}$$

where η_s is obtained by Equation (13). With the given $\tilde{R}_B$, the decoding threshold of main channel becomes $\tilde{\Theta}_B = e^{\tilde{R}_B - 1}/S_B$. According to Equation (4),

$$\tilde{P}_e = \gamma_{\mathrm{r}}\left(K, \tilde{\Theta}_B\right). \tag{34}$$

Thus, the EST of HARQ-CC becomes

$$\eta_s = \frac{\left(1 - \tilde{P}_e\right)}{\bar{N}} \cdot \left(\tilde{R}_B - R_E\right) \cdot \left(1 - P_s\right), \tag{35}$$

where $\tilde{P}_e$ and $\bar{N}$ are both determined, and P_s is given in Equation (6) and approximated in Equation (12).

Proposition 1. *η_s is a log-concave function on $0 \leq R_E \leq \tilde{R}_B$, with existing maximum value.*

Proof. Take the natural logarithm of both sides of Equation (35),

$$\ln\eta_s = \ln\left(1 - \tilde{P}_e\right) - \ln\bar{N} + \ln\left(\tilde{R}_B - R_E\right) + \ln\left(1 - P_s\right), \tag{36}$$

where the first two parts in the RHS of Equation (36) are determined. In the third part, $\ln\left(\tilde{R}_B - R_E\right)$ is a composition function $f = \ln\left(g\left(R_E\right)\right)$ on $0 \leq R_E \leq \tilde{R}_B$, and $g\left(R_E\right) = \tilde{R}_B - R_E$. $g\left(R_E\right)$ is obviously concave. Based on the convexity-preserving properties, $\ln\left(\tilde{R}_B - R_E\right)$ is still concave on $0 \leq R_E \leq \tilde{R}_B$. Finally, as $1 - P_s$ is the M^{th} power of the CDF of a chi-squared distribution, which is logarithmic concave, $\ln\left(1 - P_s\right)$ is concave. Therefore, η_s is logarithmic concave with maximum value [31]. □

Therefore, the log-concave optimization problem given in Equation (33) can be converted to the following concave one:

$$\begin{aligned} \max_{R_E} \quad & \ln\eta_s \\ s.t. \quad & 0 \leq R_E \leq R_B \end{aligned}. \tag{37}$$

Based on the above analysis, we know that if the optimal point $\hat{R}_E$ satisfies $\mathrm{d}\ln\eta_s/\mathrm{d}R_E|_{\hat{R}_E}=0$, then $\ln\eta_s$ and η_s both have their maximum value at this value. From Equation (35),

$$\begin{aligned}\frac{\mathrm{d}\eta_s}{\mathrm{d}R_E} &= \frac{\mathrm{d}}{\mathrm{d}R_E}\left(\ln\left(1-\tilde{P}_e\right)-\ln\bar{N}+\ln\left(\tilde{R}_B-R_E\right)+\ln\left(1-P_s\right)\right)\\ &= -\frac{1}{\tilde{R}_B-R_E}-\frac{1}{1-P_s}\cdot\frac{\mathrm{d}P_s}{\mathrm{d}R_E}\end{aligned}, \tag{38}$$

where P_s is approximated by Equation (12) and its first derivative is

$$\frac{\mathrm{d}P_s}{\mathrm{d}R_E}\simeq-\frac{M\Theta_E^{\bar{N}-1}e^{R_E-\Theta_E}\left(\gamma_{\mathrm{r}}\left(\bar{N},\Theta_E\right)\right)^{M-1}}{S_E\Gamma(\bar{N})}. \tag{39}$$

Substituting Equations (12) and (39) into Equation (38) and letting $\mathrm{d}\eta_s/\mathrm{d}R_E=0$, we have the following fixed-point equation of the approximated $\hat{R}_E$:

$$\hat{R}_E\simeq\tilde{R}_B-\frac{S_E\gamma\left(\bar{N},\hat{\Theta}_E(\hat{R}_E)\right)e^{\hat{\Theta}_E(\hat{R}_E)}}{Me^{\hat{R}_E}\left(\hat{\Theta}_E(\hat{R}_E)\right)^{\bar{N}-1}}, \tag{40}$$

where $\hat{\Theta}_E(\hat{R}_E)=\left(e^{\hat{R}_E}-1\right)/S_E$. Some classical techniques, such as the fixed-point iterative method, are suitable for solving the above equation.

Remark 3. *As $S_E\to 0$, we obtain $\hat{R}_E=0$.*

Proof. Since $\gamma(s,x)\to\Gamma(s)$ if $x\to\infty$, when $S_E\to 0$, we have $\gamma_{\mathrm{r}}\left(\bar{N},\Theta_E\right)\to 1$. Hence, from Equation (12), $P_s\to 0$ and Equation (35) become

$$\eta_s=\frac{1-\tilde{P}_e}{\bar{N}}\cdot\left(\tilde{R}_B-R_E\right). \tag{41}$$

It is easy to find that the maximum value of η_s, $\frac{(1-\tilde{P}_e)\cdot\tilde{R}_B}{\bar{N}}$, is obtained when $R_E=0$. □

Remark 4. *As $S_E\to\infty$, $\hat{R}_E$ can be obtained by solving the fixed-point equation,*

$$\hat{R}_E=\tilde{R}_B-\frac{e^{\hat{R}_E}-1}{M\cdot e^{\hat{R}_E}\cdot\bar{N}}. \tag{42}$$

Proof. If $S_E\to\infty$, $\hat{\Theta}_E\to 0$. Applying $\frac{\gamma(s,x)}{x^s}\to\frac{1}{s}$ when $x\to 0$, we have

$$\lim_{\hat{\Theta}_E\to 0}\frac{\gamma\left(\bar{N},\Theta_E\right)}{\left(\hat{\Theta}_E\right)^{\bar{N}}}=\frac{1}{\bar{N}}. \tag{43}$$

Substituting Equation (43) into Equation (40), Equation (42) can be obtained. □

When the SOP constraint is required (e.g., in some special application scenarios), the optimization problem of secrecy redundancy rate aiming to enhance the EST becomes:

$$\begin{aligned}\max_{R_E}\quad & \eta_s\\ s.t.\quad & P_s\le P_s^{\star}\\ & 0\le R_E\le\tilde{R}_B\end{aligned}, \tag{44}$$

where $P_s^\star$ denotes the target SOP. According to Equation (12), P_s decreases monotonically with increasing R_E. Hence, we know the SOP constraint requires $R_E \geq R_E^\star$, and

$$R_E^\star = \ln\left[1 + \frac{S_E}{2}\mathcal{F}_{\chi^2}^{-1}\left[(1-P_s^\star)^{\frac{1}{M}}, 2K\right]\right], \tag{45}$$

where $\mathcal{F}_{\chi^2}^{-1}[\cdot]$ is the same inverse function of the CDF of the chi-squared distribution as in Equation (31).

Since EST in Equation (35) has been proven to be log-concave on R_E and $\mathrm{d}\ln\eta_s/\mathrm{d}R_E|_{\hat{R}_E} = 0$, Equation (44) can be solved by

$$R_E^\dagger = \max\left[\hat{R}_E, R_E^\star\right], \tag{46}$$

where the optimal point $R_E^\dagger$ is always the maximum point in the feasible set of R_E.

4.3. Optimization of the Rate Pair (R_B, R_E)

In this part, we discuss a more general problem, which optimizes both the code rate and secrecy redundancy rate—that is, the rate pair (R_B, R_E)—with the EST criteria. When multiple eavesdroppers and limited retransmission number are still considered, this optimization problem is given by

$$\begin{aligned} \max_{R_B, R_E} \quad & \eta_s \\ s.t. \quad & 0 \leq R_E \leq R_B \end{aligned}, \tag{47}$$

where η_s is obtained by Equation (13), P_e and P_s are given by Equations (4) and (12), respectively. As the expression of η_s is extremely complicated and its concavity is difficult to prove, we proposed an iterative algorithm to determine the rate pair (R_B, R_E).

In brief, the optimization problem in Equation (47) can be tackled by iteratively adapting R_B and R_E separately until the EST gain denoted by δ is no greater than ϵ, where ϵ is a preassigned small positive real number (e.g., 10^{-3}). Specifically, it is first assumed that $\delta = \eta_s^{(1)} - \eta_s^{(0)} > \epsilon$, where $\eta_s^{(0)}$ and $\eta_s^{(1)}$ denote the optimal EST before and after each iteration, respectively. Here, we initialize them as $\eta_s^{(0)} = 0$ and $\delta = 1$. The optimal rates are initialized as $\hat{R}_B = 0$ and $\hat{R}_E = 0$. Next, using $\tilde{R}_E = \hat{R}_E$, we solve the optimization of R_B in Equation (14), while the optimal point $\hat{R}_B$ is obtained by Equations (21)–(23). Then, using $\tilde{R}_B = \hat{R}_B$, we solve the optimization of R_E in Equation (33), while the optimal point $\hat{R}_E$ is obtained by Equation (40). After this iteration, we computed the maximum EST, $\eta_s(\hat{R}_B, \hat{R}_E)$, by Equation (13) and set $\eta_s^{(1)} = \eta_s(\hat{R}_B, \hat{R}_E)$ to evaluate the EST gain by $\delta = \eta_s^{(1)} - \eta_s^{(0)}$. Simultaneously, $\eta_s^{(0)}$ is updated by $\eta_s^{(1)}$ for next iteration. The iterations continue if $\delta > \epsilon$; otherwise, the optimal rate pair $(\hat{R}_B, \hat{R}_E)$ is output. This algorithm giving the ϵ-suboptimal solution is summarized in Algorithm 1.

Algorithm 1 Iterative optimization of (R_B, R_E) for solving Equation(47).

Input: $\epsilon = 10^{-3}$, $\hat{R}_B = 0$, $\hat{R}_E = 0$, $\eta_s^{(0)} = 0$, $\delta = 1$;

1: **while** $\delta > \epsilon$ **do**
2: $\tilde{R}_E \Leftarrow \hat{R}_E$;
3: Compute $\hat{R}_B$ by Equations (21)–(23)
4: $\tilde{R}_B \Leftarrow \hat{R}_B$
5: Compute $\hat{R}_E$ by Equation (40)
6: Compute $\eta_s(\hat{R}_B, \hat{R}_E)$ by Equation (13)
7: $\eta_s^{(1)} \Leftarrow \eta_s(\hat{R}_B, \hat{R}_E)$
8: $\delta \Leftarrow \eta_s^{(1)} - \eta_s^{(0)}$
9: $\eta_s^{(0)} \Leftarrow \eta_s^{(1)}$
10: **end while**

Output: $(\hat{R}_B, \hat{R}_E)$;

Then, we reconsider Equation (47) when COP and SOP constraints are both required. The optimization becomes:

$$\begin{aligned} \max_{R_B,R_E} \quad & \eta_s \\ s.t. \quad & P_e \le P_e^\star \\ & P_s \le P_s^\star \\ & 0 \le R_E \le R_B \end{aligned}, \tag{48}$$

where $P_e^\star$ and $P_s^\star$ denote the target COP and SOP, respectively. This problem can be solved by a modified version of Algorithm 1, in which $\hat{R}_B$ and $\hat{R}_E$ are replaced by $R_B^\dagger$ and $R_E^\dagger$, computing Equations (32) and (46). In other words, the optimal rate pair should be selected among its feasible set.

5. Numerical Results

In this section, a wireless HARQ-CC system with Alice, Bob and multiple eavesdroppers, Eve1, ..., EveM, were considered, as shown in Figure 1. Under this system model, some typical results were demonstrated to evaluate the security performance. These related performance metrics include SOP, EST and optimal rate, with a given number of eavesdropper M and maximum transmission number K.

5.1. SOP Results

In Figure 2, we plot the SOP curves versus R_E for different S_E, which are determined by both the main and wiretap channels. The parameters were set as $S_B = 20$ dB, $R_B = 5$, $K = 4$, $M = 2$ and $S_E = 0$ dB, 5 dB, 10 dB. Theoretical and approximated P_s were obtained by Equations (6) and (12), respectively. First, we found that the simulation curves precisely match those of theoretical P_s, while their differences from the approximated P_s were limited. Then, SOP monotonically decreases with increasing R_E, which means that security will be enhanced by more secrecy redundancy. Furthermore, it should be pointed out that, in order to maintain the same SOP value, a larger R_E is required when S_E increases. In other words, although the wiretap channel is better, we need more secrecy redundancy to ensure the same level of security.

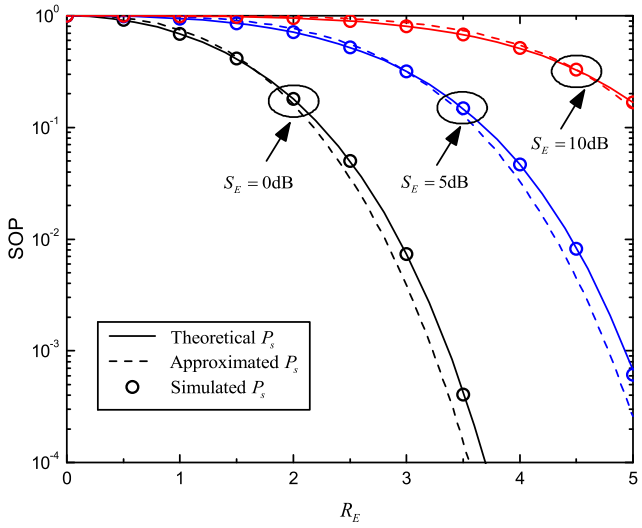

Figure 2. Secrecy outage probability (SOP) versus R_E for different average received signal-to-noise ratio (SNR) of wiretap channel with multiple eavesdroppers; $S_E \in \{0\text{dB}, 5\text{dB}, 10\text{dB}\}$, $S_B = 20\text{dB}$, $R_B = 5$, $K = 4$ and $M = 2$.

Figure 3 shows the SOP versus M for different S_E. For all curves, $S_B = 20$ dB, $R_B = 5$, $R_E = 3$, $K = 4$ and $S_E = 0$ dB, 5 dB, 10 dB. Theoretical and approximated P_s are also obtained by Equations (6) and (12); their differences are also limited, considering the use of logarithmic co-ordinate. SOP slowly rises with increasing M, which means that secrecy performance worsens when more eavesdroppers exist. On the other hand, when S_E increases, SOP with fixed M increases sharply. This means the condition of wiretap channel has more influence on the security.

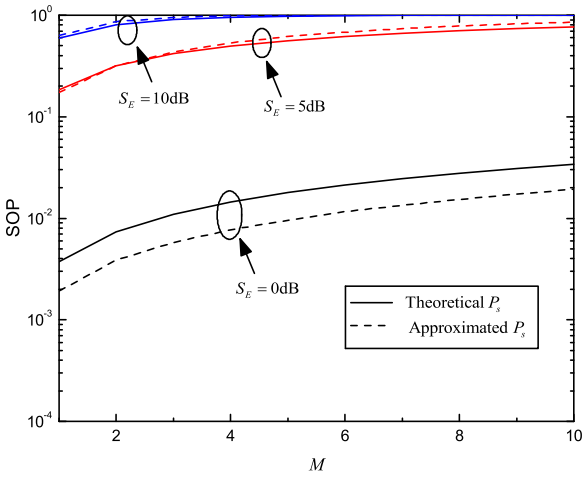

Figure 3. SOP versus M for different average received SNR of wiretap channel with multiple eavesdroppers; $S_E \in \{0 \text{ dB}, 5 \text{ dB}, 10 \text{ dB}\}$, $S_B = 20$ dB, $R_B = 5$, $R_E = 3$ and $K = 4$.

5.2. Optimization Results of Code Rate

Figure 4 shows the EST curves versus R_B for different S_E where the maximum ESTs are marked with and without the COP constraint. Parameters are set as $S_B = 20$ dB, $\tilde{R}_E = 1.5$, $M = 2$, $K = 4$ and $S_E = 0$ dB, 5 dB, 10 dB. Target COP is $P_e^\star = 10^{-4}$ when it is considered. Theoretical and approximated η_s curves are generated according to P_s and the approximated P_s, respectively. It can be observed that the difference between the theoretical and approximated η_s is limited, especially the maximum value. EST curves increase monotonically to the maximum point with increasing R_B, and then decrease monotonically. Hence, their slopes are positive when R_B is less than its optimal value $\hat{R}_B$, and negative when $R_B > \hat{R}_B$. The maximum $\eta_s(\hat{R}_B)$, using the parameterized close-form solution in Equations (21)–(23), are plotted in Figure 4. These results well match the maximum η_s and maximum approximated η_s without COP constraint. Considering the COP constraint $P_e < P_e^\star$, we state the feasible set $R_B \leq R_B^\star$. The corresponding maximum EST values, $\eta_s(R_B^\dagger)$, are also plotted, in which $R_B^\dagger$ equals the minimum of $\hat{R}_B$ and $R_B^\star$.

In Figure 5, we plot the EST versus R_B for different M. For all curves, $S_B = 20$ dB, $S_E = 0$ dB, $\tilde{R}_E = 1.5$ and $K = 4$. The target COP is still $P_e^\star = 10^{-4}$. Theoretical and approximated η_s also match well. $\eta_s(\hat{R}_B)$ and $\eta_s(R_B^\dagger)$ illustrate maximum ESTs without and with the COP constraint, respectively; the differences between their maximum and optimized values are all limited. Then, it is critical to point out that, all these η_s decrease obviously with increasing M. Similarly to SOP, more eavesdroppers worsen secrecy performance, including the EST.

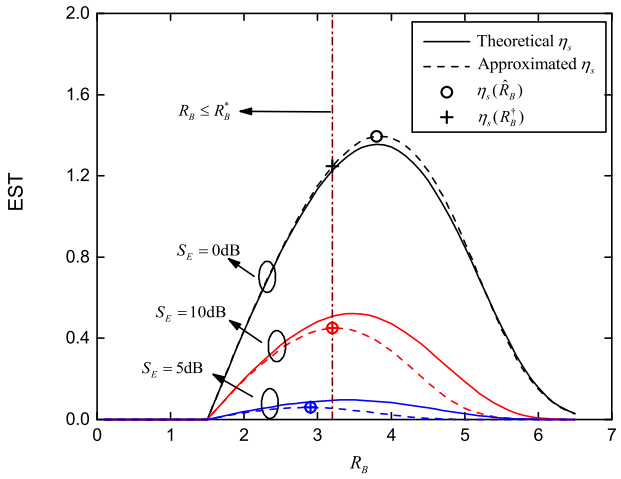

Figure 4. Effective secrecy throughput (EST) versus R_B for different average received SNR of wiretap channel and multiple eavesdroppers, with and without the COP constraint; $S_E \in \{0\text{ dB}, 5\text{ dB}, 10\text{ dB}\}$, $P_e^\star = 10^{-4}$, $S_B = 20$ dB, $\tilde{R}_E = 1.5$, $M = 2$ and $K = 4$.

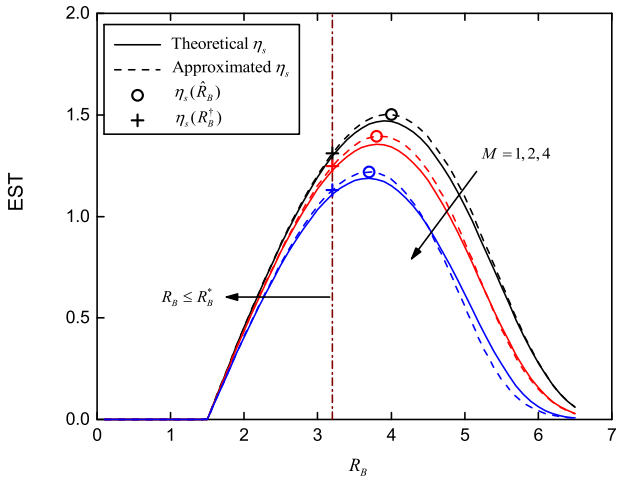

Figure 5. EST versus R_B for different number of eavesdroppers, with and without the COP constraint; $M \in \{1, 2, 4\}$, $S_B = 20$ dB, $S_E = 0$ dB, $P_e^\star = 10^{-4}$, $\tilde{R}_E = 1.5$ and $K = 4$.

5.3. Optimization Results of Secrecy Redundancy Rate

In Figure 6, we plot the EST curves versus R_E, as well as maximum ESTs corresponding to calculated optimal R_E with and without the SOP constraint. The channel conditions are $S_B = 20$ dB, $S_E = 0$ dB, 5 dB and 10 dB. The SOP constraint is $P_s^\star \le 10^{-1}$, when considered. The other parameters are set as $\tilde{R}_B = 3$, $K = 4$ and $M = 2$. Compared with the theoretical η_s, we verified that our approximated η_s is relatively accurate. The maximum ESTs without SOP constraint (i.e., $\eta_s(\hat{R}_E)$), are obtained by the fixed-point method in Equation (40). They precisely match the maximum value of the approximated η_s curves. When $P_s^\star$ is involved, we also state the feasible set, $R_E \ge R_E^\star$. The solutions $\eta_s(R_E^\dagger)$ computed by Equation (46) are plotted. It is worth noting that, $\eta_s(R_E^\dagger) = \eta_s(\hat{R}_E) = \eta_s(R_E^\star)$ for $S_E = 0$ dB, $\eta_s(R_E^\dagger) = \eta_s(\hat{R}_E)$ for $S_E = 5$ dB, and no feasible solution arrives for $S_E = 10$ dB, under the given $P_s^\star$.

Figure 7 shows the EST versus R_E for different number of eavesdroppers with and without the SOP constraint, and corresponding optimized ESTs. The channel conditions and maximum transmission number are same as the parameters in Figure 6. The SOP constraint is $P_s^\star = 10^{-1}$. The three groups of EST curves are obtained with $M = 1, 2, 4$, respectively. With an increasing M, we found that the optimal R_E rises and maximum EST reduces, which indicates that in order to meet the SOP requirement, we need an increased secrecy redundancy when more eavesdroppers exist; thus EST decreases.

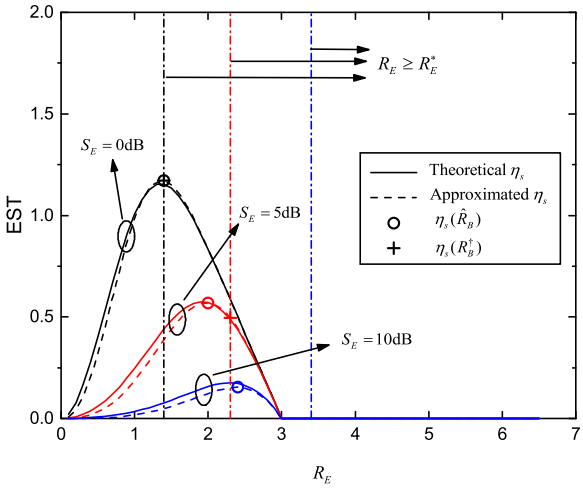

Figure 6. EST versus R_E for different average received SNR of wiretap channel and multiple eavesdroppers, with and without the SOP constraint; $S_E \in \{0\text{ dB}, 5\text{ dB}, 10\text{ dB}\}$, $P_s^\star = 10^{-1}$, $S_B = 20$ dB, $\tilde{R}_B = 3$, $K = 4$ and $M = 2$.

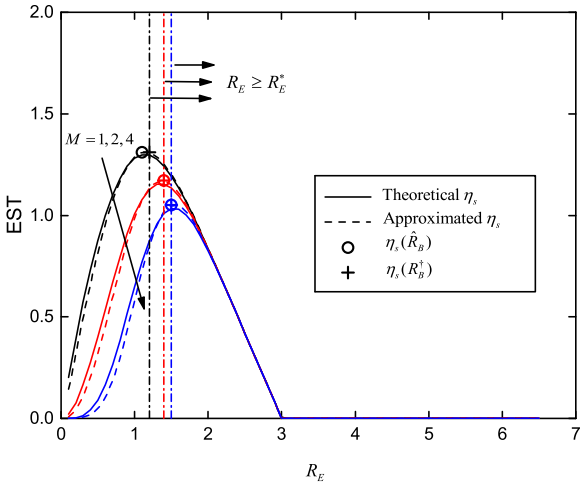

Figure 7. EST versus R_E for different number of eavesdroppers, with and without the SOP constraint; $M \in \{1, 2, 4\}$, $S_B = 20$ dB, $S_E = 0$ dB, $P_s^\star = 10^{-1}$, $\tilde{R}_B = 3$ and $K = 4$.

5.4. Optimization Results of the Rate Pair (R_B, R_E)

Figure 8 depicts the EST versus R_B and R_E for multiple eavesdroppers, without COP and SOP constraint. For simplicity, only the approximated EST is plotted here, while its accuracy was verified by Figures 4–7. The maximum EST is also marked, which was obtained by Algorithm 1. We observed that

the optimization is solved precisely, which confirms the effectiveness of Algorithm 1. In our simulation, we also found that the iteration number is small (only about four iterations were needed).

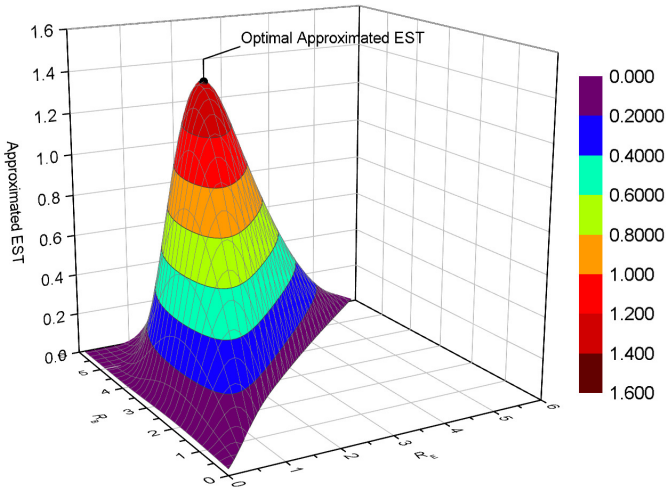

Figure 8. EST versus (R_B, R_E) for multiple eavesdroppers, without COP and SOP constraint; $S_B = 20$ dB, $S_E = 0$ dB, $M = 2$, and $K = 4$.

Finally, we give the surface of the EST versus R_B and R_E with COP and SOP constraints in Figure 9. The same parameters as Figure 8 are configured here, except for $P_e^\star = 10^{-4}$ and $P_s^\star = 10^{-1}$. The optimal EST is located at the maximum value of the approximated EST, which proves that our solution for Equation (48) works well. COP and SOP constraints, in fact, define a 2-dimensional feasible space for rate adaption.

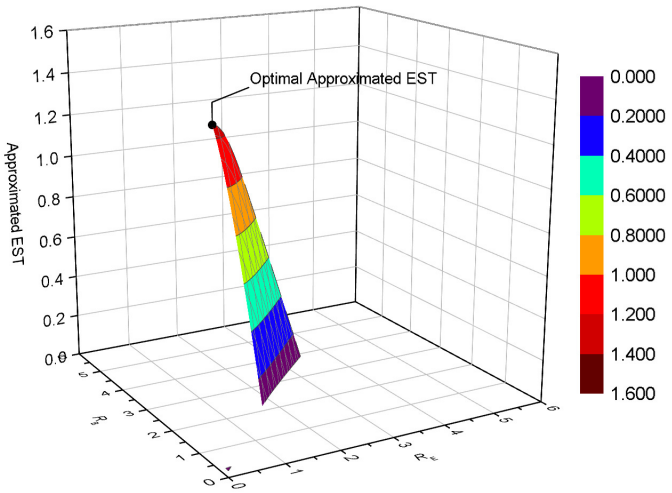

Figure 9. EST versus (R_B, R_E) for multiple eavesdroppers, with COP and SOP constraints; $S_B = 20$ dB, $S_E = 0$ dB, $P_e^\star = 10^{-4}$, $P_s^\star = 10^{-1}$, $M = 2$, and $K = 4$.

6. Conclusions

In this paper, we discussed the rate adaption of secure transmissions in HARQ-CC system, with multiple eavesdroppers and limited latency. We first presented some critical secrecy performance metrics, including COP, SOP and EST. Then, three optimization problems were derived using a

parameterized closed-form solution, a fixed-point method and an iterative algorithm, respectively. Finally, numerical and simulated results demonstrated that our proposed methods improved secrecy performance efficiently by optimizing code rate, secrecy redundancy rate and both of them paired. We also concluded that more eavesdroppers worsen the secrecy performance, but channel condition plays a more significant role.

Author Contributions: Funding acquisition, Y.W. and S.Y.; investigation, J.Z. and P.Y.; methodology, Y.W.; software, J.Z.; supervision, H.Y.; writing—original draft, Y.W.; writing—review and editing, S.Y., P.Y. and H.Y. All authors have read and agreed to the published version of the manuscript.

Funding: 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).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
2. Wynner, A.D. The wire-tap channel. *Bell. Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
3. Csiszar, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [CrossRef]
4. Leung-Yan-Cheong, S.; Hellman, M. The gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [CrossRef]
5. Barros, J.; Rodrigues M.R.D. Secrecy Capacity of Wireless Channels. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Seattle, WA, USA, 9–14 July 2006; pp. 356–360.
6. Xiao, K.; Li, W.; Kadoch, M.; Li, C. On the secrecy capacity of 5G mmWave small cell networks. *IEEE Wirel. Commun.* **2018**, *25*, 47–51. [CrossRef]
7. Yuan, C.; Tao, X.; Li, N.; Ni, W.; Liu, R.; Zhang, P. Analysis on secrecy capacity of cooperative non-orthogonal multiple access with proactive jamming. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2682–2696. [CrossRef]
8. Ahmed, M.; Bai, L. Secrecy capacity of artificial noise aided secure communication in MIMO Rician channels. *IEEE Access* **2018**, *6*, 7921–7929. [CrossRef]
9. Mao, L.; Li, Y.; Li, T.; Gao, M.; Zhang, H. Security Region Analysis with Artificial Noise Based on Secrecy Outage Probability. In Proceedings of the IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 336–340.
10. Chen, Y.; Ji, X.; Huang, K.; Li, B.; Kang, X. Minimizing secrecy outage probability in D2D enabled cellular networks: Access control with power optimization. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3231. [CrossRef]
11. Zheng, T.; Wang, H.; Liu, F.; Moon, H.F. Outage constrained secrecy throughput maximization for DF relay networks. *IEEE Trans. Commun.* **2015**, *63*, 1741–1755. [CrossRef]
12. Monteiro, M.E.P.; Rebelatto, J.L.; Souza, R.D.; Brante, G. Maximum secrecy throughput of transmit antenna selection with eavesdropper outage constraints. *IEEE Trans. Commun.* **2015**, *63*, 1741–1755. [CrossRef]
13. Zhou, F.; Li, Z.; Cheng, J.; Li, Q.; Si, J. Robust AN-Aided Beamforming and Power Splitting Design for Secure MISO Cognitive Radio With SWIPT. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 2450–2464. [CrossRef]
14. Liu, S.; Hong, Y.; Vierbo, E. Guaranteeing Positive Secrecy Capacity for MIMOME Wiretap Channels With Finite-Rate Feedback Using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 4193–4203. [CrossRef]
15. Wang, S.; Xu, X.; Huang K.; Ji, X.; Chen, Y.; Jin L. Artificial noise aided hybrid analog-digital beamforming for secure transmission in MIMO millimeter wave relay systems. *IEEE Access* **2019**, *7*, 28597–28606. [CrossRef]
16. Zou, Y.; Zhu, J.; Wang, X. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw.* **2015**, *29*, 42–48. [CrossRef]
17. Larsson, P.; Rasmussen, L.K.; Skoglund, M. Throughput analysis of ARQ schemes in Gaussian block fading channels. *IEEE Trans. Commun.* **2014**, *62*, 2569–2588. [CrossRef]
18. Makki, B.; Svensson, T.; Caire, G.; Zorzi, M. Fast HARQ over finite blocklength codes: A technique for low-latency reliable communication. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 194–209. [CrossRef]
19. Wu, Y.; Olawoyin, A.L.; Zhang, N.; Yang, H. The analysis of secure HARQ with chase combining over block fading channel. *China Commun.* **2016**, *13*, 82–88. [CrossRef]

20. Tang, X.; Liu, R.; Spasojevic, P. On the throughput of secure hybrid-arq protocols for gaussian block-fading channels. *IEEE Trans. Inf. Theory.* **2009**, *55*, 1575–1591. [CrossRef]
21. Tomasin, S. Secure HARQ with multiple encoding over block fading channels: channel set characterization and outage analysis. *IEEE Trans. Inf. Forensic Secur.* **2014**, *9*, 1708–1719. [CrossRef]
22. Mheich, Z.;Treust, M.L.; Alberge, F.; Duhamel, P.; Szczecinski, L. Rate-adaptive secure HARQ protocol for block-fading channels. In Proceedings of the 22nd European Sinal Processing Conference (EUSIPCO), Lisbon, Portugal, 1–5 September 2014; pp. 830–834.
23. Treust, M.L.; Szczecinski, L.; Labeau, F. Rate Adaptation for Secure HARQ Protocols. *IEEE Trans. Inf. Forensic Secur.* **2018**, *13*, 2981–2994. [CrossRef]
24. Guan, X.; Cai, Y.; Yang, W. On the Reliability-Security Tradeoff and Secrecy Throughput in Cooperative ARQ. *IEEE Commun. Lett.* **2014**, *18*, 479–482. [CrossRef]
25. Yan, S.; Yang, N.; Geraci, G. Optimization of Code Rates in SISOME Wiretap Channels. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 6377–6388. [CrossRef]
26. Wu, Y.; Yin, S.; Zhou, J.; Yang, P.; Yang, H. Quasi-Concave Optimization of Secrecy Redundancy Rate in HARQ-CC System *Sci. China Inf. Sci.* **2020**, *63*, 122303. [CrossRef]
27. Corless, R.; Gonnet, G.; Hare, D.; Jeffrey, D.; Knuth, D. On the Lambert W function. *Adv. Comput. Math.* **1996**, *5*, 329–359. [CrossRef]
28. Bagnoli, M.; Bergstrom, T. Log-concave probability and its applications. *Adv. Comput. Math.* **1996**, *5*, 329–359.
29. Zorzi, R.; Rao, R. On the use of renewal theory in the analysis of ARQ protocols. *IEEE Trans. Commun.* **2005**, *26*, 445–469. [CrossRef]
30. Caire, G.; Tuninetti, D. The Throughput of Hybrid-ARQ Protocols for the Gaussian Collision Channel. *IEEE Trans. Inf. Theory* **2001**, *47*, 1971–1988. [CrossRef]
31. Steven, B.; Lieven, V. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004; pp. 104–108.