Tsinghua Science and Technology

Volume 23 | Issue 2 Article 4

2018

Achievable Secrecy Rate Region of Two-Way Communication with Secret Key Feedback

Tao Li
the Department of Electronic Engineering, State Key Laboratory on Microwave and Digital Communications, and National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China.

Shidong Zhou
the Department of Electronic Engineering and State Key Laboratory on Microwave and Digital Communications, Tsinghua University, Beijing 100084, China.

Recommended Citation

Tao Li, Shidong Zhou. Achievable Secrecy Rate Region of Two-Way Communication with Secret Key Feedback. Tsinghua Science and Technology 2018, 23(2): 126-134.

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 02/09 pp126–134
DOI: 10.26599 / TST.2018.9010058
Volume 23, Number 2, April 2018

Achievable Secrecy Rate Region of Two-Way Communication with Secret Key Feedback

Tao Li and Shidong Zhou*

Abstract: This paper investigates the achievable secrecy rate region of the Gaussian two-way wiretap channel, which describes the simultaneous secure two-way transmission of a confidential message. Through adjusting the time-sharing factor and the rate at which the random secret key is fed back, the allocation and optimization for the secrecy rates of two-way communication are achieved. Under peak and average power constraints, the achievable secrecy rate regions of the two-way communication are derived respectively.

Key words: physical layer security; two-way communication; feed back; one-time-pad; random secret key; secrecy rate region

1 Introduction

Wireless communication is inherently insecure because of the broadcast nature of the wireless medium. Many works are devoted to improving the secrecy capacity. For example, Hero[1] exploited space-time block coding to achieve a low probability of interception. Beamforming is used to achieve secure communication[2–4]. Furthermore, an artificial noise injection strategy to improve the secrecy is suggested by Goel and Negi[5, 6].

All scenarios mentioned above deal with one-way communication. However, there are many two-way communication scenarios, e.g., satellite communications and cellular networks. The secrecy in two-way communication is also very important. Because of the differences in power, received interference, and the channel to eavesdropper, the secrecy capacities of both directions in two-way communication are asymmetric. Sometimes, the terminal with smaller secrecy capacity needs a greater secrecy rate to send the confidential message. For example, in cellular networks, the secrecy capacity from the base station to the legitimate user is usually greater than the uplink one, as the base station has advantages in terms of the antenna numbers and transmitting power. Thereby, the uplink secrecy rate from the legitimate user needs to be analyzed.

In this case, the feedback channel can be used to improve the secrecy rate of the feedforward channel, and vice versa. For example, feedback may increase the secrecy capacity of a point-to-point memoryless channel[7]. Inspired by this, the impact of feedback on secret communications is investigated. There are mainly three types of feedback.

(1) The feedback symbols are used to jam the eavesdropper whose channel will become more noisy[8–11].

(2) The signals fed back are used to encrypt the confidential message in the feedforward channel[12–14].

(3) The secure feedback link is used to increase the secrecy of two-way communication. For example, it is used to securely send back a random secret key to the legitimate transmitter to enhance the secrecy capacity[15, 16]. Moreover, the channel output symbols received by the legitimate receiver are fed back to generate the shared

• Tao Li is with the Department of Electronic Engineering, State Key Laboratory on Microwave and Digital Communications, and National Laboratory for Information Science and Technology, Tsinghua University, Beijing 100084, China. E-mail: litao09@tsinghua.org.cn.

• Shidong Zhou is with the Department of Electronic Engineering and State Key Laboratory on Microwave and Digital Communications, Tsinghua University, Beijing 100084, China. E-mail: zhousd@tsinghua.edu.cn.

* To whom correspondence should be addressed.

Manuscript received: 2016-11-15; revised: 2016-12-07; accepted: 2016-12-12

secret key through a secure feedback link[17]. Then, the secret key is used to encrypt the confidential message by one-time-pad coding scheme[18]. In Ref. [19], not only the secure feedback link is used to send back the random secret key, but also the causal channel state information, which is available to both the legitimate transmitter and the legitimate receiver, is used to generate the shared secret key.

We follow the work of Ardestanizadeh et al.[16], because the secure feedback link model is easy to achieve secret transmission. This model separates the forward and backward channels, making the two channels independent. The independence is suitable for the two-way secure communications over orthogonal channels such as different frequency bands or time slots. Due to the length of this paper, only the problem exploiting time division duplexing between the forward channel and the backward channel is investigated.

Via[20] investigated the time and power allocation problem for the Gaussian wiretap channel with secure feedback. In this paper, time sharing is exploited between feedback and forward channels; a random secret key is fed back securely to Alice from Bob, which is used to encrypt Alice's confidential message in a one-time-pad manner. The optimal power allocation and time-sharing factor are given to maximize the secrecy capacity from Alice to Bob.

However, Via[20] only considered the one-way secure communication, but the secrecy rates of both directions must be investigated in two-way secure communication. It is hoped that the secrecy rates of both directions can be greater, but it is a contradiction. There is a tradeoff between the two secrecy rates, which is demonstrated as the secrecy rate region of two-way communication. In Ref. [21], the authors investigated the achievable secrecy rate region of two-way communication under the peak power constraint in the parallel multiple-carrier system, but the problem regarding how to achieve an optimal achievable secrecy rate region was not researched.

In this paper, the achievable secrecy rate region of the two-way secure communication on the single carrier is investigated, under peak and average power constraints, respectively. One of the two legitimate terminals not only feeds back the random secret key but also sends the confidential message to the other one, thus the two-way secure communication is achieved.

The major contributions of this paper are as follows. (1) We give the criterion for judging which terminal feeds back the random secret key to the other terminal so that the achievable secrecy rate region is optimal. (2) The time-sharing factor for the two legitimate terminals and the rate of the random secret key are calculated. (3) The achievable secrecy rate region is derived.

The rest of this paper is organized as follows. The system model is stated in Section 2. We solve the achievable secrecy rate region under the peak power constraint in Section 3 and the question of achievable secrecy rate region under the average power constraint is investigated in Section 4. Section 5 concludes the paper.

2 Scenario and System Model

In Fig. 1, Alice and Bob are legitimate terminal users forming a bidirectional secure communication, Eve is a passive eavesdropper. Hence, this is a Gaussian wiretap channel.

C_{AB} and C_{AE} are the channel capacities from Alice to Bob and that from Alice to Eve, respectively. Similarly, C_{BA} and C_{BE} are the channel capacities from Bob to Alice and that from Bob to Eve, respectively.

$C_{S,AB}$ and $R_{S,AB}$ are the secrecy capacity and secrecy rate from Alice to Bob, respectively. Likewise, $C_{S,BA}$ and $R_{S,BA}$ are the secrecy capacity and secrecy rate from Bob to Alice, respectively. The time duration of one frame is T, and the scheme of time sharing is adopted. Alice communicates securely to Bob during $[0,\ t_1]$, and Bob communicates securely to Alice during $[t_1, T]$, where $t_2 = T - t_1$. Alice and Bob can send confidential messages to each other against the eavesdropper Eve with their own secrecy capacities. Furthermore, both Alice and Bob can also feed back the secret key securely to each other with its secrecy capacity, the one who receives the secret key encrypts its confidential message by a one-time-pad coding scheme; thus, its secrecy rate is enhanced.

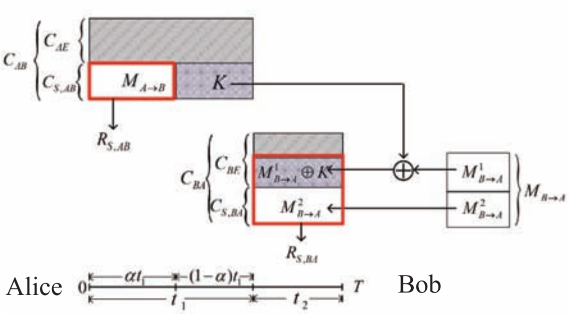

Fig. 1 Two-way communication with secure feedback.

3 Achievable Secrecy Rate Region Under the Peak Power Constraint

3.1 Achievable secrecy rate region under the peak power constraint when Alice feeds the secret key back to Bob

Assume that the secrecy capacity $C_{S,BA}$ is smaller than the rate of confidential message $M_{B\to A}$ which Bob sends to Alice. Thus, the confidential message $M_{B\to A}$ cannot be sent securely with Bob's secrecy capacity completely, leading to the leakage of the confidential message to the eavesdropper. But the secrecy capacity $C_{S,AB}$ of Alice is greater than the rate of confidential message $M_{A\to B}$ sent to Bob from Alice, which means that Alice has a redundant ability to feed the secret key back to Bob confidentially with its secrecy capacity $C_{S,AB}$.

Let $\alpha \in [0,1]$, Alice sends the confidential message $M_{A\to B}$ to Bob with its secrecy capacity $C_{S,AB}$ during the interval $[0,\alpha t_1]$, and the random secret key K to Bob with $C_{S,AB}$ during the interval $[\alpha t_1, t_1]$. During $[t_1, T]$, the confidential message $M_{B\to A}$ is split into two parts, namely $M^1_{B\to A}$ and $M^2_{B\to A}$. In addition, $M^2_{B\to A}$ can be sent confidentially with the secrecy capacity $C_{S,BA}$ of Bob. Since $M^1_{B\to A}$ is the part which is beyond the secrecy capacity $C_{S,BA}$, it cannot be sent securely. Then $M^1_{B\to A}$ is encrypted by the random secret key K which is fed back securely with $C_{S,AB}$. Alice sends the random secret key K to Bob for encrypting the same amount of $M^1_{B\to A}$, and the total rate of $M^1_{B\to A}$ and $M^2_{B\to A}$ cannot exceed the channel capacity from Bob to Alice. Then, the secrecy rates of Alice and Bob with given $\alpha^\star$ and $t_1^\star$ are

$$\begin{aligned}&R^\star_{S,AB} = \frac{\alpha^\star t_1^\star C_{S,AB}}{T},\\&R^\star_{S,BA} = \min\left(\frac{(1-\alpha^\star)t_1^\star C_{S,AB} + (T-t_1^\star)C_{S,BA}}{T},\right.\\&\left.\frac{(T-t_1^\star)C_{BA}}{T}\right)\end{aligned} \tag{1}$$

To derive the secrecy rate region of the two-way communication in this case, the secrecy rate $R_{S,BA}$ from Bob to Alice is first given. Then, we can solve the maximum of the secrecy rate $R_{S,AB}$ from Alice to Bob,

$$\begin{aligned}&\max_{\alpha,t_1} \frac{\alpha t_1 C_{S,AB}}{T},\\&\text{s.t. } \min\left(\frac{(1-\alpha)t_1 C_{S,AB} + (T-t_1)C_{S,BA}}{T},\right.\\&\left.\frac{(T-t_1)C_{BA}}{T}\right) \geqslant R_{S,BA},\\&\alpha \leqslant 1,\\&0 \leqslant t_1 \leqslant T\end{aligned} \tag{2}$$

which is equivalent to

$$\begin{aligned}&\max_{\alpha,t_1} \frac{\alpha t_1 C_{S,AB}}{T},\\&\text{s.t. } \frac{(1-\alpha)t_1 C_{S,AB} + (T-t_1)C_{S,BA}}{T} \geqslant R_{S,BA}\\&\frac{(T-t_1)C_{BA}}{T} \geqslant R_{S,BA},\\&\alpha \leqslant 1,\\&0 \leqslant t_1 \leqslant T\end{aligned} \tag{3}$$

Lemma 1 The primal problem in Formula (3) is not a convex optimization problem, but can be converted to a convex optimization problem.

Proof Let the rate of the random secret key fed back to Bob be $(1-\alpha)t_1 C_{S,AB}/T = R_K$, then $\alpha t_1 C_{S,AB}/T = t_1 C_{S,AB}/T - R_K$. The primal problem is equivalent to

$$\begin{aligned}&\max_{t_1,R_K} \frac{t_1 C_{S,AB}}{T} - R_K,\\&\text{s.t. } R_K + \left(1-\frac{t_1}{T}\right)C_{S,BA} \geqslant R_{S,BA},\\&\left(1-\frac{t_1}{T}\right)C_{BA} \geqslant R_{S,BA},\\&R_K \geqslant 0,\\&0 \leqslant t_1 \leqslant T\end{aligned} \tag{4}$$

It is a linear program problem, also a convex optimization problem. Hence, it can be solved by the KKT condition[22]. ■

If $C_{S,AB} < C_{S,BA}$, $(1-\alpha)t_1 C_{S,AB} < (1-\alpha)t_1 C_{S,BA}$, meaning the total amount of the confidential message encrypted by the fed back secret key from Alice is smaller than that sent with the secrecy capacity of Bob during the same interval $[\alpha t_1, t_1]$. So, to make the achievable secrecy rate region greater when Alice feeds the secret key back to Bob than when Bob feeds the secret key back to Alice, $C_{S,AB} \geqslant C_{S,BA}$ is the sufficient and necessary condition for Alice to feed the secret key back to Bob. Then convex optimization problem in Formula (4) can be solved by the KKT condition, the achievable secrecy rate region in the case is as follows:

$$R_{S,AB} = C_{S,AB} + \tfrac{C_{S,BA}-C_{S,AB}-C_{BA}}{C_{BA}} R_{S,BA} \tag{5}$$

3.2 Achievable secrecy rate region under the peak power constraint when Bob feeds the secret key back to Alice

If the roles of Alice and Bob exchange, Bob has the redundant ability to send the random secret key to Alice confidentially. Also, Alice uses the secret key to encrypt part of the confidential message which is beyond the secrecy capacity of Alice. Therefore, $C_{S,AB} < C_{S,BA}$ is the sufficient and necessary condition for Bob to feed the secret key back to Alice. Hence, the achievable secrecy rate region in this case is as follows:

$$R_{S,BA} = C_{S,BA} + \frac{C_{S,AB} - C_{S,BA} - C_{AB}}{C_{AB}} R_{S,AB} \qquad (6)$$

3.3 Achievable secrecy rate region of two-way communication

Considering the secrecy rate regions of Eqs. (5) and (6), the achievable secrecy rate region of the two-way communication by the feedback of secret key is as follows.

If $C_{S,AB} \geqslant C_{S,BA}$, according to Section 3.1, we exploit the scheme that Alice feeds the secret key back to Bob, within which the achievable secrecy rate region of the two-way communication is achieved, as shown in Fig. 2. The secrecy rate from Bob to Alice has been improved, which exceeds the secrecy capacity of Bob.

If $C_{S,AB} < C_{S,BA}$, according to Section 3.2, we exploit the scheme that Bob feeds the secret key back to Alice, within which the achievable secrecy rate region of the two-way communication is achieved, as shown in Fig. 3. The secrecy rate from Alice to Bob has been improved, which exceeds the secrecy capacity of Alice.

In other words, if one of the two legitimate terminals has greater secrecy capacity than the other, it feeds the random secret key back to the other legitimate terminal. The achievable secrecy rate region will be greater.

3.4 Numerical results

3.4.1 Boundary of the secrecy rate region

If $C_{S,AB} \geqslant C_{S,BA}$, the regime that Alice feeds the random secret key back to Bob can realize the achievable secrecy rate region. The parameters that make Alice and Bob work at the boundary of the achievable secrecy rate region are as follows,

$$\alpha = 1 - \frac{R_{S,BA}(C_{BA} - C_{S,BA})}{C_{S,AB}(C_{BA} - R_{S,BA})},$$
$$t_1 = (1 - \frac{R_{S,BA}}{C_{BA}})T \qquad (7)$$

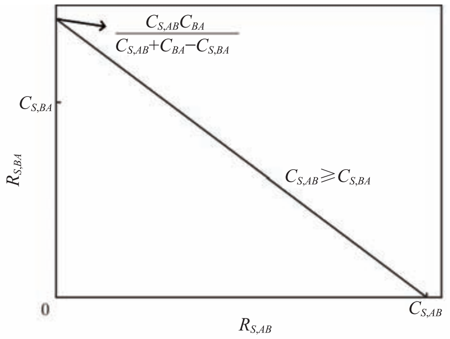
$\frac{C_{S,AB}C_{BA}}{C_{S,AB}+C_{BA}-C_{S,BA}}$
$C_{S,BA}$
$R_{S,BA}$
$C_{S,AB} \geqslant C_{S,BA}$
0
$C_{S,AB}$
$R_{S,AB}$

Fig. 2 Achievable secrecy rate region under the peak power constraint when Alice feeds the secret key back to Bob.

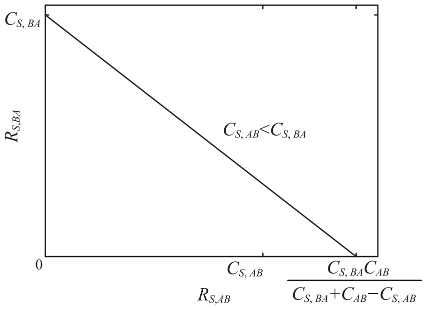

Fig. 3 Achievable secrecy rate region under the peak power constraint when Bob feeds the secret key back to Alice.

Figure 4 is used to demonstrate how Alice and Bob work at the boundary of the secrecy rate region. Assume that $C_{S,AB}$ = 4 bit·s^{-1}·Hz^{-1}, $C_{S,BA}$ = 2 bit·s^{-1}·Hz^{-1}, C_{AB}=5 bit·s^{-1}·Hz^{-1}, C_{BA}=3 bit·s^{-1}·Hz^{-1}, and T=1 s.

As the secrecy rate $R_{S,BA}$ from Bob to Alice increases, the time t_1 and the proportion α both decrease monotonously. Eventually, α goes to zero, which means that time t_1 is used to send the secret key from Alice to Bob. However, the time $(1-\alpha)t_1$ for Alice to securely feed the secret key back to Bob increases.

In other words, to increase $R_{S,BA}$, the time t_2 for Bob to transmit and $(1-\alpha)t_1$ for Alice to feed back the secret key both need to increase, but the time αt_1 for Alice to send the confidential message should be reduced. It is shown that the secrecy rate $R_{S,AB}$ is inversely proportional to the secrecy rate $R_{S,BA}$ linearly in Eq. (5).

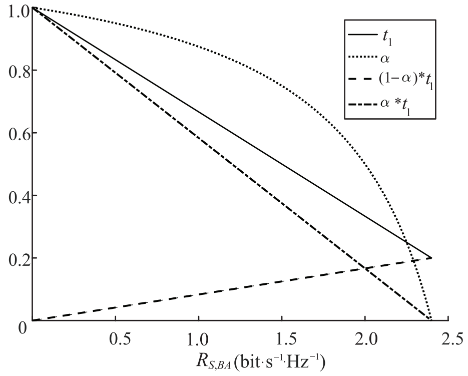

Fig. 4 Parameters for working at the boundary of the achievable secrecy rate region under the peak power constraint.

3.4.2 Relation of the secrecy rate to the secrecy capacity

When $C_{S,AB} \geqslant C_{S,BA}$, the regime that Alice feeds the random secret key back to Bob can reach the achievable secrecy rate region, and it is impossible for $R_{S,AB}$ to exceed $C_{S,AB}$. Given $R_{S,AB}$, according to Eq. (5), we have

$$R_{S,BA} = \frac{(C_{S,AB} - R_{S,AB})C_{BA}}{C_{S,AB} + C_{BA} - C_{S,BA}} \tag{8}$$

Figure 5 demonstrates the relation of secrecy rate $R_{S,BA}$ and secrecy capacities, i.e., $C_{S,AB}$ and $C_{S,BA}$, given $R_{S,AB}$ =0 bit·s^{-1}·Hz^{-1}, meaning Alice does not send its confidential message, only feeds the secret key back to Bob. Assume that $C_{S,AB}$ =10 bit·s^{-1}·Hz^{-1}, $C_{S,BA}$ =2 bit·s^{-1}·Hz^{-1}, C_{BA} =4 bit·s^{-1}·Hz^{-1}, and T =1 s.

As $C_{S,AB}$ and $C_{S,BA}$ increase, $R_{S,BA}$ will increase gradually. When $C_{S,AB}$ approaches infinity, $R_{S,BA}$ will get close to C_{BA}, no matter how large $C_{S,AB}$ is, i.e., no matter how much Alice feeds the random secret key back to Bob securely, the secrecy rate $R_{S,BA}$ will not exceed the channel capacity C_{BA}. When $C_{S,AB} = C_{S,BA}$, the cooperation of Alice and Bob is not necessary. If the secrecy rate of one direction needs to be improved, only the time for transmitting should be increased.

4 Achievable Secrecy Rate region Under the Average Power Constraint

4.1 Achievable secrecy rate region under the average power constraint when Alice feeds the secret key back to Bob

As above, the achievable secrecy rate region of the two-way communication with secure feedback of the secret key under the peak power constraint is investigated. Then, the same question under the constraint of average power will be considered.

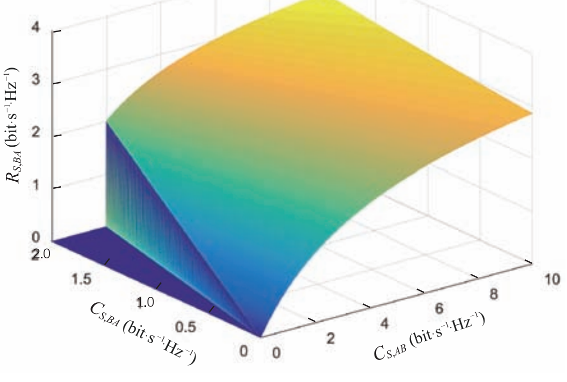

Fig. 5 Secrecy rate as a function of secrecy capacities.

In the new case, the instantaneous power of Bob or Alice is up to the time they work, so the instantaneous power is a function of the time one terminal works, as well as the channel capacities and secrecy capacities in the scenario.

The system model in the new case is the same as the aforementioned case. Assume that the channels among all the terminals are additive white Gaussian noise channels with complex Gaussian noise of zero mean and the variances of the noise for Alice, Bob, and Eve are σ_A^2, σ_B^2, and σ_E^2, respectively. Furthermore, g_{AB} and g_{AE} are the link gains from Alice to Bob and Eve, respectively. Similarly, g_{BA} and g_{BE} are the link gains from Bob to Alice and Eve, respectively. The total energy of Alice and Bob in a frame is $P_{Amax}T$ and $P_{Bmax}T$, respectively. So, the instantaneous power of Alice is $P_{Amax}T/(T-t_2)$ and $P_{Bmax}T/t_2$ for Bob. Then, the instantaneous secrecy capacity from Alice to Bob is[23]

$$C_{S,AB}(t_2) = [C_{AB}(t_2) - C_{AE}(t_2)]^+ = \\ \left[\log_2\left(1+\frac{P_{Amax}Tg_{AB}}{\sigma_B^2(T-t_2)}\right) - \log_2\left(1+\frac{P_{Amax}Tg_{AE}}{\sigma_E^2(T-t_2)}\right)\right]^+ = \\ \log_2\left(1+\frac{P_{Amax}T\left[\frac{\sigma_E^2}{\sigma_B^2}g_{AB}-g_{AE}\right]^+}{\sigma_E^2(T-t_2)+P_{A\max}Tg_{AE}}\right) \tag{9}$$

where $C_{AB}(t_2)$ and $C_{AE}(t_2)$ are the instantaneous channel capacities from Alice to Bob and Eve, respectively. Similarly, the instantaneous secrecy capacity from Bob to Alice is

$$C_{S,BA}(t_2) = [C_{BA}(t_2) - C_{BE}(t_2)]^+ = \\ \left[\log_2\left(1+\frac{P_{Bmax}Tg_{BA}}{\sigma_A^2 t_2}\right) - \log_2\left(1+\frac{P_{Bmax}Tg_{BE}}{\sigma_E^2 t_2}\right)\right]^+ = \\ \log_2\left(1+\frac{P_{Bmax}T\left[\frac{\sigma_E^2}{\sigma_A^2}g_{BA}-g_{BE}\right]^+}{\sigma_E^2 t_2+P_{Bmax}Tg_{BE}}\right) \tag{10}$$

where $C_{BA}(t_2)$ and $C_{BE}(t_2)$ are the instantaneous channel capacities from Bob to Alice and Eve, respectively. Similar to that described previously, Alice sends back the secret key to Bob with the secrecy capacity $C_{S,AB}$, and Bob encrypts its confidential message with the received secret key. The instantaneous secrecy rate from Bob to Alice is

$$R_{S,BA}(t_2) = \min(t_2C_{BA}(t_2)/T, t_2C_{S,BA}(t_2)/T + \\ (1-\alpha)(T-t_2)C_{S,AB}(t_2)/T) \tag{11}$$

Given the secrecy rate $R^*_{S,AB}$ from Alice to Bob, the maximal secrecy rate from Bob to Alice $R^{opt}_{S,BA}$ can be derived and the achievable secrecy rate region under the constraint of average power is obtained. Thus, the optimization question is as follows:

$$\begin{aligned} \max_{\alpha,t_2} & \min\left(t_2 C_{BA}\left(t_2\right)/T\ , t_2 C_{S,BA}\left(t_2\right)/T + \right. \\ & \left. (1-\alpha)\left(T-t_2\right) C_{S,AB}\left(t_2\right)/T\right), \\ \text{s.t.}\quad & R^*_{S,AB} \leqslant \alpha\left(T-t_2\right) C_{SAB}\left(t_2\right)/T, \\ & 0 \leqslant \alpha \leqslant 1, \\ & 0 \leqslant t_2 \leqslant T \end{aligned} \tag{12}$$

Lemma 2 The primal problem in Formula (12) is not a convex optimization problem, but can be converted to a convex optimization problem.

Proof $t_2 C_{BA}\left(t_2\right) = t_2 \log_2\left(1+\frac{P_{B\max} T g_{BA}}{\sigma_A^2 t_2}\right)$ and $t_2 C_{S,BA}\left(t_2\right) = t_2\left[\log_2\left(1+\frac{P_{B\max} T g_{BA}}{\sigma_A^2 t_2}\right) - \log_2\left(1+\frac{P_{B\max} T g_{BE}}{\sigma_E^2 t_2}\right)\right]^+$ are all concave functions of t_2, and $t_1 C_{S,AB}\left(t_1\right) = t_1\left[\log_2\left(1+\frac{P_{Amax} T g_{AB}}{\sigma_B^2\ t_1}\right) - \log_2\left(1+\frac{P_{Amax} T g_{AE}}{\sigma_E^2 t_1}\right)\right]^+$ is a concave functions of t_1[22]. Let $R_K = (1-\alpha)\left(T-t_2\right) C_{S,AB}\left(t_2\right)/T = (1-\alpha) t_1 C_{S,AB}\left(t_1\right)/T$. Then, $\alpha\left(T-t_2\right) C_{S,AB}\left(t_2\right)/T = t_1 C_{S,AB}\left(t_1\right)/T - R_K$, thus, it is a concave function of $\left(t_1, R_K\right)$. Therefore, the primal objective problem is equivalent to

$$\begin{aligned} \max_{t_1,t_2,R_K}\ & \min\left(t_2 C_{BA}\left(t_2\right)/T, t_2 C_{S,BA}\left(t_2\right)/T + R_K\right), \\ \text{s.t.}\quad & R_{S,AB} \leqslant t_1 C_{S,AB}\left(t_1\right)/T - R_K, \\ & t_1 \geqslant 0, \\ & t_2 \geqslant 0, \\ & t_1 + t_2 \leqslant T, \\ & R_K \geqslant 0 \end{aligned} \tag{13}$$

Because the pointwise infimum of a set of concave functions is a concave function, so

$$\min\left(t_2 C_{BA}\left(t_2\right)/T, t_2 C_{S,BA}\left(t_2\right)/T + R_K\right) \tag{14}$$

is a concave function of $\left(t_2, R_K\right)$. So the new objective problem in Formula (13) is a convex optimization problem, which has the unique extreme point. ■

The problem has the unique extreme point and the optimal solution can be derived by the CVX. We propose Algorithm 1 for the objective question, and the achievable secrecy rate region of Section 4.1 is derived.

The feasible set of the problem in Formula (13) is $\{t_2 : 0 \leqslant t_2 \leqslant T, \left(T-t_2\right) C_{S,AB}\left(t_2\right)/T \geqslant R^*_{S,AB}\}$, where $\left(T-t_2\right) C_{S,AB}\left(t_2\right)$ is decreasing function of t_2, so $R^*_{S,AB} \leqslant C_{S,AB}(0)$. Assuming that $t_2 = \beta(R^*_{S,AB})$, let $\left(T-\beta\left(R^*_{S,AB}\right)\right) C_{S,AB}\left(\beta\left(R^*_{S,AB}\right)\right)/T = R^*_{S,AB}$. If $R^*_{S,AB}$ is given, to satisfy $\left(T-t_2\right) C_{S,AB}\left(t_2\right)/T \geqslant R^*_{S,AB}$, t_2 should satisfy $0 \leqslant t_2 \leqslant \beta(R^*_{S,AB})$. Let $f\left(t_2\right) = t_2 C_{BA}\left(t_2\right)/T$ and $g\left(t_2\right) = t_2 C_{S,BA}\left(t_2\right)/T + \left(T-t_2\right) C_{S,AB}\left(t_2\right)/T - R^*_{S,AB}$.

Algorithm 1 The method for solving the achievable secrecy rate region under average power constrant

```
Step 1. Select $R^*_{S,AB}$ satisfying $R^*_{S,AB} \leqslant C_{S,AB}(0)$ ;
Step 2. Solve $(T-\beta) C_{S,AB}(\beta)/T = R^*_{S,AB}$ with bisection method, we can get $\beta(R^*_{S,AB})$ ;
Step 3. Solve $g(t_2) - f(t_2) = 0$, with bisection method, we can get $t_2 = d$ ;
Step 4.
if $d \geqslant \beta(R^*_{S,AB})$ then
    the optimal value $t_2^* = \beta(R^*_{S,AB})$, and go to step 7 ;
end if
Step 5. Calculate the extreme point $c$ of $g(t_2)$,
if $g'(0) \leqslant 0$ then
    $c = 0$, end step 5;
else
    if $g'(T) \geqslant 0$ then
        $c = T$, end step 5;
    else
        let $c$ equal the solution of the equation $g'(t_2) = 0$, end step 5;
    end if
end if
Step 6. According to the relations of $c$, $d$, $\beta(R^*_{S,AB})$, get the optimal value of $t_2$
if $c \leqslant d$ then
    $t_2^* = d$, end step 6;
else
    if $c \geqslant \beta\left(R^*_{S,AB}\right)$ then
        $t_2^* = \beta\left(R^*_{S,AB}\right)$, end step 6;
    else
        $t_2^* = c$, end step 6;
    end if
end if
Step 7. Calculate
    $R^{opt}_{S,BA} = \min\left\{t_2^* C_{BA}\left(t_2^*\right)/T, t_2^* C_{S,BA}\left(t_2^*\right)/T + \left(T-t_2^*\right) C_{S,AB}\left(t_2^*\right)/T - R^*_{S,AB}\right\}$
Step 8. Calculate the optimal scale
    $\alpha^* = \frac{R^*_{S,AB}}{(T-t_2^*) C_{S,AB}(t_2^*)}$
Step 9. Return to step 1;
```

4.2 Achievable secrecy rate region under the average power constraint when Bob feeds the secret key back to Alice

The instantaneous secrecy rate from Bob to Alice is

$$R_{S,BA}\left(t_1\right) = \alpha(T-t_1) C_{S,BA}\left(t_1\right)/T \tag{15}$$

where α is the proportion of t_2 for Bob to feed the secret key back to Alice, and

$$C_{S,BA}\left(t_1\right) = \\ \left[C_{BA}\left(t_1\right) - C_{BE}\left(t_1\right)\right]^+ =$$

$$\left[\log_2\left(1+\frac{P_{Bmax}Tg_{BA}}{\sigma_A^2(T-t_1)}\right)-\log_2\left(1+\frac{P_{Bmax}Tg_{BE}}{\sigma_E^2(T-t_1)}\right)\right]^+=$$
$$\log_2\left(1+\frac{P_{Bmax}T}{\sigma_E^2(T-t_1)+P_{Bmax}Tg_{BE}}\left[\left(\frac{\sigma_E^2}{\sigma_A^2}g_{BA}-g_{BE}\right)\right]^+\right) \tag{16}$$

The instantaneous secrecy rate from Alice to Bob is

$$R_{S,AB}(t_1)=\min(t_1C_{AB}(t_1)/T\ ,(t_1C_{S,AB}(t_1)/T+$$
$$(1-\alpha)(T-t_1)C_{S,BA}(t_1)/T) \tag{17}$$

where

$$C_{S,AB}(t_1)=$$
$$[C_{AB}(t_1)-C_{AE}(t_1)]^+=$$
$$\left[\log_2\left(1+\frac{P_{Amax}Tg_{AB}}{\sigma_B^2\,t_1}\right)-\log_2\left(1+\frac{P_{Amax}Tg_{AE}}{\sigma_E^2\,t_1}\right)\right]^+=$$
$$\log_2\left(1+\frac{P_{Amax}T}{\sigma_E^2\,t_1+P_{Amax}Tg_{AE}}\left[\frac{\sigma_E^2}{\sigma_B^2}g_{AB}-g_{AE}\right]^+\right) \tag{18}$$

Given the secrecy rate $R_{S,BA}$ from Bob to Alice, and maximizing the secrecy rate $R_{S,AB}(t_1)$; then, the achievable secrecy rate region under the constraint of average power is achieved. So, the optimization question is as follows:

$$\begin{aligned}\max_{\alpha,t_1}&\min(t_1C_{AB}(t_1)/T\ ,t_1C_{S,AB}(t_1)/T+\\&(1-\alpha)(T-t_1)C_{S,BA}(t_1)/T),\\\text{s.t.}\quad&R_{S,BA}\leqslant\alpha(T-t_1)C_{S,BA}(t_1)/T,\\&0\leqslant\alpha\leqslant1,\\&0\leqslant t_1\leqslant T\end{aligned} \tag{19}$$

With Algorithm 1 proposed above, the achievable secrecy rate region of Section 4.2 can be achieved.

4.3 Achievable secrecy rate region under the average power constraint

Finally, the achievable secrecy rate region under the average power constraint is the convex hull of the union set for the two secrecy rate regions in Sections 4.1 and 4.2.

Assume that P_{Amax}= 12 W, P_{Bmax} = 10 W, T = 1 s, g_{AB}= 1, g_{BA} = 1, g_{AE} = 0.05, g_{BE} = 0.1, σ_A^2= 1, σ_B^2 = 1, and σ_E^2 = 1. In Fig. 6, the red curve is the convex hull of the union set for the two secrecy rate regions. From Fig. 6, it is shown that each of the two schemes under the average power constraint has its own secrecy rate region, respectively. Furthermore, the union set of the two secrecy rate regions is achievable, as well as the convex hull of the union set.

From Fig. 6, there exists an intersection between the curves of the two secrecy rate regions. There is a very small difference between the union set of the two secrecy rate regions and its convex hull, which can be neglected. To reduce the complexity, it is thought that the achievable secrecy rate region of the two-way communication is the union set of the two secrecy rate regions under the average power constraint.

Figure 7 demonstrates the secrecy rate regions of the two schemes under the average power constraint, when P_{Amax} = 12 W, P_{Bmax}= 10 W, T=1 s, g_{AB} = 1, g_{BA} = 1, g_{AE} = 0.05, g_{BE} = 0.25, σ_A^2= 1, σ_B^2 = 1, and σ_E^2= 1. Figure 7 shows the union set of the two secrecy rate regions is the greater one of the two regions, which is convex, so the greater one is the convex hull of the union set. Also, the achievable secrecy rate region under the average power constraint in this case is the greater one.

So, it is observed that, when the secrecy performance of the two terminals in the two-way communication is approximated, there will exist an intersection between the curves of the two secrecy rate regions. When the secrecy performance of the two terminals has a greater difference, then the union set of the two secrecy rate regions is the

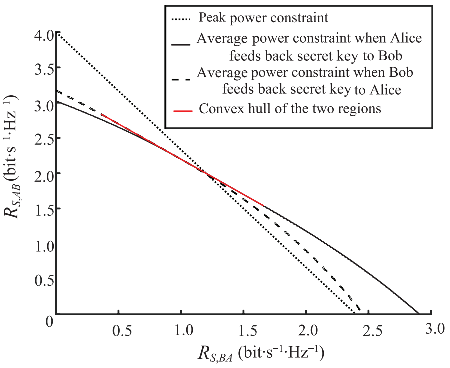

Fig. 6 The achievable secrecy rate region under peak power and average power constraints.

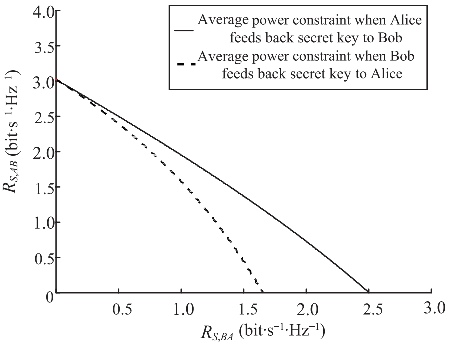

Fig. 7 The achievable secrecy rate region under average power constraints.

greater of the two regions.

4.4 Numerical results

We demonstrate the numerical results for the case when Alice feeds the secret key back to Bob. Assume that $P_{Amax} = 12$ W, P_{Bmax} = 10 W, $T = 1$ s, g_{AB} = 1, g_{BA}= 1, g_{AE}= 0.05, g_{BE} = 0.1, σ_A^2= 1, σ_B^2= 1, and σ_E^2= 1.

The achievable secrecy rate region under the average power constraint is illustrated in Fig. 7, where $R_{S,AB}$ is a decreasing function of $R_{S,BA}$, and the curve is nonlinear.

From Fig. 8, it is found that as $R_{S,BA}$ increases, the curves of the parameters t_1 and α can be divided into three stages.

At the first stage, the proportion α remains constant at 1, implying that the duration of time $[0, t_1]$ is used to send Alice's confidential message and Alice does not feed the secret key back to Bob. Through reducing the duration of time $[0, t_1]$, i.e., increasing the time t_2, the secrecy rate $R_{S,BA}$ grows without the need for any random secret key, so $(1-\alpha)\,t_1$ for Alice to feed the secret key back to Bob is 0.

At the second stage, the time t_1 when Alice communicates securely to Bob remains fixed. To maintain the increasing secrecy rate $R_{S,BA}$, the proportion α of t_1 for Alice to send the confidential message must be decreased, which leads to the increase of time $(1-\alpha)t_1$ for Alice to feed back the secret key. At this stage, to make $R_{S,BA}$ grow, the unique way is to increase the amount of the random secret key fed back.

At the third stage, as $R_{S,BA}$ increases, t_1 and α both decrease, and α decreases faster, inducing that the time αt_1 reduces faster than t_1, so $(1-\alpha)t_1$ can increase slowly at this stage. Eventually α drops to zero, meaning the duration of time $[0, t_1]$ is spent on feeding the secret key.

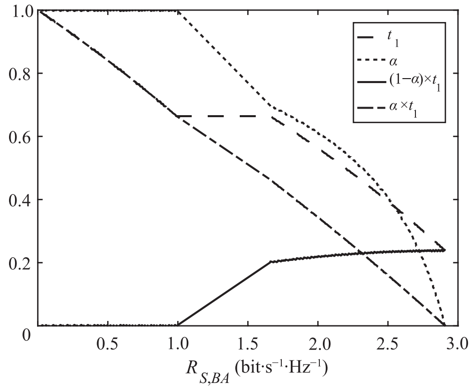

Fig. 8 Parameters for working at the boundary of the achievable secrecy rate region under the average power constraint when Alice feeds the secret key back to Bob.

To make $R_{S,BA}$ increase, the time $(1-\alpha)t_1$ should increase to feed more of the random secret key. Meanwhile, the time t_2 for Bob to securely transmit the message must increase.

5 Conclusion

The secrecy rate region of two-way communication is studied with secure feedback in this paper. Under peak and average power constraints, the achievable secrecy rate regions of the two-way secure communication are obtained. The time sharing factor and the rate of the random secret key are also derived.

Under the peak power constraint, the relation of secrecy rate and secrecy capacity is analyzed. Under the average power constraint, an algorithm for the problem of achievable secrecy rate region is proposed.

Acknowledgment

This work was supported in part by the National High-Tech Research and Development (863) Program (No. ss2015AA011306), the National key Basic Research and Development (973) Program of China (No. 2012CB316000), the Science Fund for Creative Research Groups of NSFC (No. 61321061), and Tsinghua University Initiative Scientific Research (No. 2015Z02-3). We would like to thank the reviewers for their valuable comments.

References

[1] A. Hero, Secure space-time communication, *IEEE Transactions on Information Theory*, vol. 49, no 12, pp.3235–3249, 2003.

[2] Z. Li, W. Trappe, and R. Yates, Secret communication via multiantenna transmission, presented at 41st Annual Conference on Informance Sciences and System, Baltimore, MD, USA, 2007.

[3] S. Shafiee and S. Ulukus, Achievable rates in Gaussian MISO channels with secrecy constraints, presented at IEEE International Symposium on Information Theory, Nice, France, 2007.

[4] S. Shafiee, N. Liu, and S. Ulukus, Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel, *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, 2009.

[5] R. Negi and S. Goel, Secret communication using artificial noise, presented at IEEE 62nd Vehicular Technology Conference, Dallas, TX, USA, 2005.

[6] S. Goel and R. Negi, Guaranteeing secrecy using artificial noise, *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[7] S. K. Leung-Yan-Cheong, Multi-user and wiretap channels including feedback, Ph D dissertation, Stanford, CA, USA:

Stanford Univ., 1976.

[8] B. Yang, W. Wang, Q. Yin, and J. Fan, Secret wireless communication with public feedback by common randomness, *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 269−272, 2014.

[9] E. Tekin and A. Yener, The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming, *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735−2751, 2007.

[10] L. Lai, H. E. Gamal, and H. V. Poor, The wiretap channel with feedback: Encryption over the channel, *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059−5067, 2008.

[11] L. Lai, H. E. Gamal, and H. V. Poor, Secrecy capacity of the wiretap channel with noisy feedback, arXiv preprint, arXiv: 0710.0865, 2007.

[12] G. T. Amariucai and S. Wei, Feedback-based collaborative secrecy encoding over binary symmetric channels, *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5248−5266, 2012.

[13] T. T. Kim and H. V. Poor, Secure communications with insecure feedback: Breaking the high-SNR ceiling, *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3700−3711, 2010.

[14] X. He and A. Yener, The role of feedback in two-way secure cocmmunication, *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8115–8130, 2013.

[15] D. Gunduz, D. R. Brown, and H. V. Poor, Secret communication with feedback, presented at IEEE International Symposium on Information Theory and Its Applications, Auckland, New Zealand, 2008.

[16] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. H. Kim, Wiretap channel with secure rate-limited feedback, *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5353−5361, 2009.

[17] R. Ahlswede and N. Cai, Transmission identification and common randomness capacities for wire-tap channels with secure feedback from the decoder, in *General Theory of Information Transfer and Combinatorics*. Springer, 2006, pp. 258–275.

[18] C. E. Shannon, Communication theory of secrecy systems, *Bell Syst.Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[19] A. Cohen and A. Cohen, Wiretap channel with causal state information and secure rate-limited feedback, *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1192−1203, 2016.

[20] J. Via, Time and power allocation for the gaussian wiretap channel with feedback of secret keys, presented at IEEE 16th International Workshop on Signal Processing Advances in Wireless Communication (SPAWC), Stockholm, Sweden, 2015.

[21] T. Li, J. Zhao, and S. Zhou, Secrecy rate region of independent parallel multiple-carrier two-way secure communications with secure feedback, presented at IEEE International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2015.

[22] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[23] S. K. Leung-Yan-Cheong and M. E. Hellman, The Gaussian wiretap channel, *IEEE Transaction on Information Theory*, vol. 24, no. 4, pp. 451−456, 1978.

Shidong Zhou received the BS and MS degrees in wireless communications from Southeast University, Nanjing, China, in 1991 and 1994, respectively, and the PhD degree in communication and information systems from Tsinghua University, Beijing, China, in 1998. From 1999 to 2001, he was in charge of several projects in the China 3G Mobile Communication R&D Project. He is currently a professor at Tsinghua University. His research interests are wireless and mobile communications.

Tao Li received the BS and MS degrees in communication engineering from PLA University of Science and Technology, Nanjing, China, in 2003 and 2008, respectively, and is currently pursuing the PhD degree with the Department of Electronic Engineering, Tsinghua University. His research interests are signal processing and wireless communications.