Key Generation in Two-Way Relay Wireless Channels

Heng Zhou[1], Lauren Huie[2] and Lifeng Lai[1]

[1]Department of Electrical & Computer Engineering, Worcester Polytechnic Institute,
Worcester, MA, 01609, USA. Email: {hzhou3,llai}@wpi.edu
[2]Air Force Research Lab, Information Directorate, Rome, NY, 13441, USA. Email: Lauren.Huie@rl.af.mil

***Abstract*—Most of the existing work on key generation from wireless fading channels requires a direct wireless link between legitimate users so that they can obtain correlated observations from the common wireless link. This paper studies the key generation problem in the two-way relay channel, in which there is no direct channel between the key generating terminals. We propose an effective key generation scheme that achieves a substantially larger key rate than that of a direct channel mimic approach. Unlike existing schemes, there is no need for the key generating terminals to obtain correlated observations in our scheme. We then extend our study to the case of a relay with multiple antennas. For this scenario, we derive the optimal power allocation at the relay that maximizes the key rate achieved using our protocol.**

***Index Terms*—Information-theoretic security, key generation, two-way relay channel**

I. Introduction

The idea of exploiting wireless fading channels for generating information theoretically secure secret keys has received considerable attentions recently [1]–[3]. In this line of work, two terminals, namely Alice and Bob, first obtain noisy estimates of the common fading channel gain between them, and then employ the celebrated key generation via public discussion approach [4], [5] to generate secret keys from these correlated estimates. In a nutshell, in all these work, the common direct channel connecting these two terminals provides a valuable common random source required for generating secret keys using the approach proposed in [4], [5].

In certain applications, however, two terminals might be far away from each other, and hence there is no direct channel between them. The two-way relay channel, in which two terminals are connected through a relay, is a basic setup that models this scenario. The key generation from two-way relay channel problem was considered in [6], which proposed several interesting schemes to circumvent the issue that there is no direct channel to provide the necessary common randomness. The basic idea of these schemes is to create a virtual direct link from which these two terminals can obtain channel estimates and then apply the approach in [4], [5]. For example, in the amplify forward (AF) scheme discussed in [6], Alice transmits a training signal to the relay, which then sends a scaled version of the received noisy signal to Bob. From the received signal, Bob can obtain an estimate of the product of two channel gains: the one from Alice to the relay, and the one from the relay to Bob. Similarly, by asking Bob to send a training signal and the relay to re-sends its received noisy signal, Alice can obtain an estimate of the product of these two channel gains. Hence the product of the two channel gains can serve as the common randomness for the secret key generation, since both Alice and Bob successfully obtain estimates of it. Although these schemes overcome the issue of no direct channel, there are some potential challenges, especially in the multiple antennas case. First, when the relay re-sends the received signal, which contains the information about the channel gain, Eve can also obtain a noisy copy. Hence Eve can obtain partial information about the common randomness used for the key generation, which will potentially reduce the key rate. Second, it is difficult to evaluate the key rates of the schemes proposed in [6] since the probability distribution function (pdf) of the estimate of the virtual channel gain (the product of two physical channel gains) is complicated and Eve has partial information about the common randomness used for the key generation. Third, multiple antennas in the relay are not efficiently used in [6], in particular only one effective channel gain of a randomly selected channel is used.

In this paper, we propose a new scheme for the key generation in the two-way relay channel by adopting a scheme proposed in our recent work [7]. Instead of trying to mimic a direct channel as done in [6], in the proposed scheme, the two terminals involved do not need to obtain correlated estimates. Instead, the relay first establishes a pairwise key with Alice using the physical channel linking it and Alice. Similarly, the relay and Bob can establish a pairwise key using the channel linking them. Then the relay broadcasts the xor of these two pairwise keys to both Alice and Bob. Alice and Bob can then decode both keys and pick the one with a smaller size as the final key. The advantages of this approach are: 1) Eve does not obtain any information about the channel gains used for the key generation, hence our scheme obtains a much higher key rate; 2) It is very easy to evaluate the key rate of the proposed scheme; and 3) Our scheme can be easily extended to multiple antenna case, and the key rate scales linearly with the number

The work of H. Zhou and L. Lai was supported by the National Science Foundation CAREER Award under Grant CCF-13-18980, the National Science Foundation under Grant CNS-13-21223, and Air Force Research Lab, Information Directorate.

of antennas. Furthermore, we investigate the optimal power allocation problem that maximizes the resulting key rate for the multiple antenna case.

The remainder of the paper is organized as follows. In Section II, we introduce the model studied in this paper. In Section III, we discuss the proposed scheme in detail. Simulation results are presented in Section IV. Concluding remarks are given in Section V.

II. Model

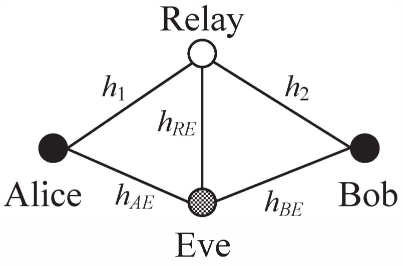

Fig. 1: Model of two-way relaying system.

In this section, we introduce the key generation through two-way relay model considered in this paper. Fig. 1 shows the simplest model of two-way relaying system that consists of Alice, Bob, a single antenna relay (the case of multiple-antenna relay will be discussed in Section III-B) and Eve. There exists a wireless channel between every pair of terminals in the system except between Alice and Bob. Alice and Bob would like to establish a secret key such that Eve has no knowledge about the generated key. All legitimate terminals can transmit over the wireless channel. We assume that Alice, Bob and the relay are half-duplex nodes.

More specifically, if Alice transmits signal x_A in a given channel use, the relay and Eve will receive

$$y_R = h_{AR}x_A + n_R, \tag{1}$$
$$y_E = h_{AE}x_A + n_E, \tag{2}$$

in which h_{AR} is the fading coefficient of the channel from Alice to the relay, n_R is zero mean Gaussian noise with variance σ^2 at the relay, h_{AE} is the channel gain between Alice and Eve, and n_E is the noise at Eve. h_{AR} and n_R are both random variables and independent of each other. No part in the system knows the value of h_{AR} a priori, but all parts know its distribution. Noise in all channels is independently and identically distributed.

Similarly, when Bob sends x_B, the relay and Eve receive

$$y_R = h_{BR}x_B + n_R, \tag{3}$$
$$y_E = h_{BE}x_B + n_E, \tag{4}$$

in which h_{BR} is the fading coefficient of the channel from Bob to the relay, h_{BE} is the channel gain between Bob and Eve. When the relay broadcasts x_R, the received signals are

$$y_A = h_{RA}x_R + n_A, \tag{5}$$
$$y_B = h_{RB}x_R + n_B, \tag{6}$$
$$y_E = h_{RE}x_R + n_E, \tag{7}$$

in which h_{RA}, h_{RB} and h_{RE} are the channel gains from the relay to Alice, to Bob and to Eve respectively, while n_A and n_B are zero mean Gaussian noise with variance σ^2 at Alice and Bob respectively.

In this paper, we assume that all the channels are reciprocal, i.e., $h_{AR} = h_{RA}$ (we denote them collectively as h_1), $h_{BR} = h_{RB}$ (we denote them collectively as h_2), etc. But the scheme developed in this paper still works (with a different key) even if this assumption does not hold, as long as there is correlation between the forward and backward channel. Furthermore, we consider an ergodic block fading model for the wireless channel, which means that the channel gain remains constant for a period of T symbols and changes randomly to another independent value after the current period [8]. We assume $h_1 \sim \mathcal{N}(0, \sigma_1^2)$ and $h_2 \sim \mathcal{N}(0, \sigma_2^2)$. Similarly, our scheme still works if the distribution of the random channel gain changes.

Let $\mathbf{X}_A = (x_A(1), \ldots, x_A(M))'$, $\mathbf{X}_B = (x_B(1), \ldots, x_B(M))'$ and $\mathbf{X}_R = (x_R(1), \ldots, x_R(M))'$ be the signals transmitted by the terminals in M channel uses. Similarly, let $\mathbf{Y}_A$, $\mathbf{Y}_B$ and $\mathbf{Y}_R$ be signals received by the terminals over M channel uses. Since we assume that the legitimate users are half duplex, $y_A(i) = \phi$ if $x_A(i) \neq \phi$, in which ϕ denotes either no transmission or no signal. The same thing holds for the relay and Bob. We have a total power constraint for the legitimate terminals, namely

$$\frac{1}{M}\mathbb{E}\{\mathbf{X}'_A\mathbf{X}_A + \mathbf{X}'_B\mathbf{X}_B + \mathbf{X}'_R\mathbf{X}_R\} \leq P_T. \tag{8}$$

In addition to the wireless channels, we assume that there is a public channel in which all legitimate users can exchange messages. However, all messages exchanged through this public channel will be overheard by Eve. We denote all messages transmitted in the public channel as $\mathbf{F}$. Both Alice and Bob need to generate a key using the information transmitted and received from wireless channels and the public channel. Let f_A and f_B be the key generation functions at Alice and Bob respectively, namely $K_A = f_A(\mathbf{X}_A, \mathbf{Y}_A, \mathbf{F})$ and $K_B = f_B(\mathbf{X}_B, \mathbf{Y}_B, \mathbf{F})$. A key rate R is said to be achievable if, for any $\epsilon > 0$, there exists a scheme such that

$$\tfrac{1}{M}H(K_A) > R - \epsilon, \tag{9}$$
$$P\{K_A \neq K_B\} < \epsilon, \tag{10}$$
$$\tfrac{1}{M}I(K_A; \mathbf{Y}_E, \mathbf{F}) < \epsilon, \tag{11}$$
$$\tfrac{1}{M}\log|\mathcal{K}_A| < \tfrac{1}{M}H(K_A) + \epsilon, \tag{12}$$

with $|\mathcal{K}_A|$ being the size of the key's alphabet. Here (10) implies that the keys generated at Alice and Bob are the same with a high probability (and hence we will use K to denote the generated key), (11) implies that the eavesdropper learns limited amount of information about the generated key, while (12) implies that the key is nearly uniformly generated.

III. Key Generation Algorithms

A. Single Antenna Case

Algorithm 1 shows the proposed key generation scheme, which is adapted from our recent work [7]. The time frame of Algorithm 1 is shown in Fig. 2. We divide each fading block into three slots each with duration $T_0 = T/3$. Supposing Alice sends training sequence with power P_A, Bob with power P_B and the relay with power P_R, then the energy of each training sequence is $\|\mathbf{S}_A\|^2 = T_0 P_A = TP_A/3, \|\mathbf{S}_B\|^2 = T_0 P_B = TP_B/3$ and $\|\mathbf{S}_R\|^2 = T_0 P = TP_R/3$, and the total power constraint (8) reduces to

$$\frac{1}{3}(P_A + P_B + P_R) \leq P_T.$$

Algorithm 1: Key Generation Algorithm for One Antenna

Step 1: Channel Estimation:

1) Alice sends a known sequence $\mathbf{S}_A$ with power P_A through channel h_1 to the relay. The relay receives $\mathbf{Y}_R^{(1)}$ from which it obtains estimate $\tilde{h}_{1,R}$.
2) Bob sends a known sequence $\mathbf{S}_B$ with power P_B through channel h_2 to the relay. The relay receives $\mathbf{Y}_R^{(2)}$ from which it obtains estimate $\tilde{h}_{2,R}$.
3) The relay broadcasts a known sequence $\mathbf{S}_R$ with power P_R to Alice and Bob. Alice receives $\mathbf{Y}_A$ from which she obtains estimate $\tilde{h}_{1,A}$; Bob receives $\mathbf{Y}_B$ from which he obtains estimate $\tilde{h}_{2,B}$.

Step 2: Key Agreement:

1) Alice and the relay agree on a pairwise key K_1 using the correlated estimation pair $(\tilde{h}_{1,R}, \tilde{h}_{1,A})$.
2) Bob and the relay agree on a pairwise key K_2 using the correlated estimation pair $(\tilde{h}_{2,R}, \tilde{h}_{2,B})$.
3) The relay broadcasts $K_1 \oplus K_2$. Then Alice and Bob can obtain both K_1 and K_2. They choose the one with a smaller size as the common secret key.

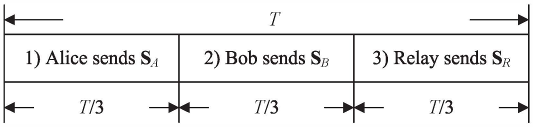
T
1) Alice sends $\mathbf{S}_A$
2) Bob sends $\mathbf{S}_B$
3) Relay sends $\mathbf{S}_R$
T/3
T/3
T/3

Fig. 2: Time frame for one antenna.

For channel h_1, at the end of the training phase, the relay and Alice receive

$$\mathbf{Y}_R^{(1)} = h_1 \mathbf{S}_A + \mathbf{N}_R^{(1)}, \tag{13}$$

$$\mathbf{Y}_A = h_1 \mathbf{S}_R + \mathbf{N}_A, \tag{14}$$

respectively. From these observations, the relay and Alice obtain the following estimates

$$\tilde{h}_{1,R} = \frac{\mathbf{S}'_A}{\|\mathbf{S}_A\|^2}\mathbf{Y}_R^{(1)} = h_1 + \frac{\mathbf{S}'_A}{\|\mathbf{S}_A\|^2}\mathbf{N}_R^{(1)}, \tag{15}$$

$$\tilde{h}_{1,A} = \frac{\mathbf{S}'_R}{\|\mathbf{S}_R\|^2}\mathbf{Y}_A = h_1 + \frac{\mathbf{S}'_R}{\|\mathbf{S}_R\|^2}\mathbf{N}_A. \tag{16}$$

Eve also receives faded training sequences. But since the channel fadings to her are independent of h_1 [8], the received signals are independent of the above correlated estimates. Using the result from [4], the relay and Alice can establish a pairwise key K_1 with a rate:

$$\frac{1}{T} I(\tilde{h}_{1,A}; \tilde{h}_{1,R}). \tag{17}$$

Note that scalar $\tilde{h}_{1,A}$ and $\tilde{h}_{1,R}$ are two correlated Gaussian variables with zero mean, and that variances $\mathrm{Var}(\tilde{h}_{1,A}) = \sigma_1^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2} = \sigma_1^2 + \frac{\sigma^2}{T_\bullet P_R}$, $\mathrm{Var}(\tilde{h}_{1,R}) = \sigma_1^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2} = \sigma_1^2 + \frac{\sigma^2}{T_\bullet P_A}$. These facts will be useful for deriving explicit expression of mutual information in (17) since $I(\tilde{h}_{1,A}; \tilde{h}_{1,R}) = -\frac{1}{2}\log(1 - \rho_1^2)$ where ρ_1 is the correlation coefficient between $\tilde{h}_{1,A}$ and $\tilde{h}_{1,R}$.

Similarly, for channel h_2, through sending training sequences to each other, the relay and Bob obtain estimates $\tilde{h}_{2,R}$ and $\tilde{h}_{2,B}$ respectively. They can then establish a common key K_2 with rate

$$\frac{1}{T} I(\tilde{h}_{2,B}; \tilde{h}_{2,R}). \tag{18}$$

When the relay broadcasts $K_1 \oplus K_2$ in the public channel to both Alice and Bob, the system can be viewed as a one-time pad [9] where the longer key is used to perfectly protect the shorter key. Alice and Bob can know both K_1 and K_2 by the XOR operation on the received $K_1 \oplus K_2$ signal. Eve will also obtain $K_1 \oplus K_2$, but she learns nothing about the shorter key from $K_1 \oplus K_2$ since it is protected by the longer key via the one-time pad operation. As a result, Alice and Bob both choose the shorter key as the common secret key. Hence the key rate is:

$$R_{co} = \frac{1}{T}\min\{I(\tilde{h}_{1,A}; \tilde{h}_{1,R}), I(\tilde{h}_{2,B}; \tilde{h}_{2,R})\}. \tag{19}$$

Following similar arguments in [3], one can easily show that Eve obtains a limited amount of the key information.

B. Multiple Antennas Case with Optimal Power Allocation

The aforementioned key generation algorithm for one antenna can be easily extended to the multiple antennas case. Supposing there are N antennas at the relay, similar to the one antenna case, we assume that the channel gain between the i-th antenna and Alice conforms to $\mathcal{N}(0, \sigma_{1,i}^2)$ distribution, the channel gain between the i-th antenna and Bob conforms to $\mathcal{N}(0, \sigma_{2,i}^2)$ distribution, $i = 1, \ldots, N$, and the noise in each channel is Gaussian with zero mean and variance σ^2. We summarize our protocol in Algorithm 2.

The time frame of our key generation algorithm for a relay with multiple antennas is shown in Fig. 3. The length of each training sequence T_0 is now set to be $T/(N+2)$. Denoting the transmission power of training sequence of Alice as P_A, Bob as P_B, and antenna i in the relay as $P_i, i = 1, \ldots, N$, the total power constraint (8) is now

$$\frac{1}{N+2}\left(P_A + P_B + \sum_{i=1}^{N} P_i\right) \leq P_T. \tag{20}$$

Algorithm 2: Key Generation for Two-Way Relay with Multiple Antennas

Step 1: Channel Estimation:

1) Alice broadcasts a known sequence $\mathbf{S}_A$ with power P_A to all antennas in the relay, from which each antenna obtains an estimate $\tilde{h}_{A,i,R}, i = 1, \ldots, N$. Here the subscript A represents the estimate regarding channel gain at Alice's side, i represents the antenna index and R means that this estimate is obtained by the relay.
2) Bob broadcasts a known sequence $\mathbf{S}_B$ with power P_B to all antennas in the relay, from which each antenna obtains an estimate $\tilde{h}_{B,i,R}$. The notation is defined in the same way as above.
3) For each $i = 1, \ldots, N$, the relay broadcasts a known sequence $\mathbf{S}_{R,i}$ with power P_i from antenna i to Alice and Bob, from which Alice and Bob obtains estimates $\tilde{h}_{A,i,A}$ and $\tilde{h}_{B,i,B}$, respectively.

Step 2: Key Agreement:

1) Alice and the relay agree on common keys $K_{A,i}$'s according to the pairs of estimates $(\tilde{h}_{A,i,A}, \tilde{h}_{A,i,R})$, $i = 1, \ldots, N$, using the same method described in Algorithm 1.
2) Bob and the relay agree on common keys $K_{B,i}$'s according to the pairs of estimates $(\tilde{h}_{B,i,B}, \tilde{h}_{B,i,R})$, $i = 1, \ldots, N$.
3) The relay concatenates $K_{A,i}$'s into $K_A = (K_{A,1}, K_{A,2}, \ldots, K_{A,N})$ and $K_{B,i}$'s into $K_B = (K_{B,1}, K_{B,2}, \ldots, K_{B,N})$ and broadcasts $K_A \oplus K_B$ to Alice and Bob. From K_A and K_B, Alice and Bob choose the one with the smaller size as the final common secret key.

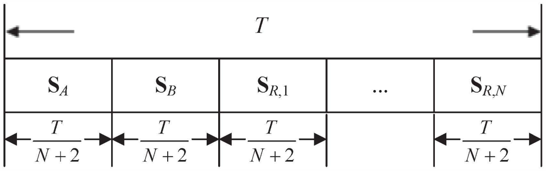

Fig. 3: Time frame for two-way relay with multiple antennas.

Accordingly, the key rate for Algorithm 2 is

$$R_{co,N} = \frac{1}{T} \min\{I_1, I_2\}, \tag{21}$$

where

$$I_1 = \sum_{i=1}^{N} I(\tilde{h}_{A,i,A}; \tilde{h}_{A,i,R}), \tag{22}$$

$$I_2 = \sum_{i=1}^{N} I(\tilde{h}_{B,i,B}; \tilde{h}_{B,i,R}), \tag{23}$$

in which $I(\tilde{h}_{A,i,A}; \tilde{h}_{A,i,R})$ can be expressed explicitly as

$$-\frac{1}{2} \log \left(1 - \frac{1}{\left(1 + \frac{\sigma^2}{\sigma_{1,i}^2 P_A T_0}\right)\left(1 + \frac{\sigma^2}{\sigma_{1,i}^2 P_i T_0}\right)} \right).$$

$I(\tilde{h}_{B,1,B}; \tilde{h}_{B,1,R})$ has a similar expression, which can be obtained by replacing P_A by P_B, and $\sigma_{1,i}^2$ by $\sigma_{2,i}^2$.

The total power constraint (20) can be rewritten as

$$\sum_{i=1}^{N} P_i \leq (N+2)P_T - P_A - P_B \triangleq P. \tag{24}$$

Given P_A and P_B, under the above requirement that the sum of transmission powers $\sum_{i=1}^{N} P_i$ of the relay be under a specified value P, the key rate (21) depends on the power used for each antenna. In the following, we will maximize the key rate by optimizing the power allocated to each antenna. In particular, we have the following optimization problem:

$$\begin{array}{ll} \text{maximize} & \min\{I_1, I_2\} \\ \text{subject to} & \sum_{i=1}^{N} P_i \leq P, P_i \geq 0, i = 1, \ldots, N. \end{array} \tag{25}$$

To simplify the notation, in the following derivation and results, we will ignore the constant $1/2$ before each mutual information term.

The objective function in (25) contains a `min` operation, which makes it challenging. To solve this max-min optimization problem, we transform (25) into an equivalent optimization problem [10]:

$$\begin{array}{ll} \text{maximize} & z \\ \text{subject to} & z \leq I_1, z \leq I_2, \\ & \sum_{i=1}^{N} P_i \leq P, \\ & z \geq 0, P_i \geq 0, i = 1, \ldots, N. \end{array} \tag{26}$$

The Lagrangian of problem (26) is

$$\mathcal{L} = z + \lambda_1(I_1 - z) + \lambda_2(I_2 - z) + \lambda_3 \left(P - \sum_{i=1}^{N} P_i \right). \tag{27}$$

Then the KKT conditions are

$$\frac{\partial \mathcal{L}}{\partial z} \leq 0, \quad z \geq 0, \quad z\frac{\partial \mathcal{L}}{\partial z} = 0, \tag{28}$$

$$\frac{\partial \mathcal{L}}{\partial P_i} \leq 0, \quad P_i \geq 0, \quad P_i\frac{\partial \mathcal{L}}{\partial P_i} = 0, \tag{29}$$

$$z \leq I_1, \quad \lambda_1 \geq 0, \quad \lambda_1(z - I_1) = 0, \tag{30}$$

$$z \leq I_2, \quad \lambda_2 \geq 0, \quad \lambda_2(z - I_2) = 0, \tag{31}$$

$$\sum_{i=1}^{N} P_i \leq P, \quad \lambda_3 \geq 0, \quad \lambda_3 \left(\sum_{i=1}^{N} P_i - P \right) = 0. \tag{32}$$

Since the objective function is linear and therefore concave, I_1, I_2 is concave so $z - I_1, z - I_2$ is convex, and the constraint

$\sum_{i=1}^{N} P_i \leq P$ is also linear, the necessary KKT conditions are sufficient.

By analyzing these KKT conditions, we know that $\lambda_1 + \lambda_2 = 1$ and $\sum_{i=1}^{N} P_i = P$. In the following, we discuss different cases of values of λ_1 and λ_2.

1) Case 1: If $\lambda_1 \neq 0$ and $\lambda_2 = 0$, then $I_1 \leq I_2$, so $\min\{I_1, I_2\} = I_1$ and therefore the original optimization problem (25) reduces to

$$\begin{aligned} &\text{maximize} && I_1 \\ &\text{subject to} && \sum_{i=1}^{N} P_i = P, \\ &&& P_i \geq 0, i = 1, \ldots, N. \end{aligned} \tag{33}$$

This is an optimization problem with nonnegativity constraints. Again we can employ KKT conditions to solve it. Similar to (26), I_1 is concave with regard to $P_i, i = 1, \ldots, N$, and the constraint is linear so here KKT conditions are sufficient too. It can be verified that its solution satisfies KKT conditions (28-32) of the problem (26), so it is also the solution of (26). The optimal solution is

$$P_i = \left(\frac{-P_A + \sqrt{P_A^2 + \frac{4P_A}{\mu}}}{2} - \frac{\sigma^2}{\sigma_{1,i}^2 T_0} \right)^+, \tag{34}$$

$i = 1, \ldots, N$, where the function $(x)^+ = \max\{0, x\}$,.

If we know the number N' of P_i's that are strictly positive, we have

$$\begin{aligned} P_i &= \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \frac{1}{\sigma_{1,j}^2} - \frac{\sigma^2}{\sigma_{1,i}^2 T_0} && (35) \\ &= \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \left(\frac{1}{\sigma_{1,j}^2} - \frac{1}{\sigma_{1,i}^2} \right) && (36) \end{aligned}$$

for those i satisfying $P_i > 0$.

2) Case 2: If $\lambda_1 = 0$ and $\lambda_2 \neq 0$, then it is certain $I_2 \leq I_1$ and the original optimization problem (25) turns to

$$\begin{aligned} &\text{maximize} && I_2 \\ &\text{subject to} && \sum_{i=1}^{N} P_i = P, \\ &&& P_i \geq 0, i = 1, \ldots, N. \end{aligned} \tag{37}$$

Similar to Case 1, we can solve this optimization problem under nonnegativity constraints by KKT. Specifically, the optimal points P_i's are

$$P_i = \left(\frac{-P_B + \sqrt{P_B^2 + \frac{4P_B}{\mu}}}{2} - \frac{\sigma^2}{\sigma_{2,i}^2 T_0} \right)^+ \tag{38}$$

or, for those strictly positive P_i's

$$P_i = \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \left(\frac{1}{\sigma_{2,j}^2} - \frac{1}{\sigma_{2,i}^2} \right) \tag{39}$$

where N' is the number of P_i's having positive optimal values.

3) Case 3: If $\lambda_1 \neq 0$ and $\lambda_2 \neq 0$ at the same time, it follows $I_1 = I_2$, and the original optimization problem (25) becomes

$$\begin{aligned} &\text{maximize} && I_1 \\ &\text{subject to} && I_1 = I_2, \\ &&& \sum_{i=1}^{N} P_i = P. \end{aligned} \tag{40}$$

This is an optimization problem with equality constraints and we can use Lagrange multiplier method to handle it. But due to the complexity of formulas involved, there is no closed-form solution to (40). One needs to resort to a numerical method to solve it.

Note that these three cases are not mutually exclusive. Therefore, after obtaining the solutions to these three cases, we should compare the resulting values of key rate for each case and pick out the largest one as the final optimal key rate. In addition, we should check necessary conditions $I_1 \leq I_2$ for Case 1 and $I_2 \leq I_1$ for Case 2. If any one of them does not hold, the corresponding optimal points obtained are invalid and should be discarded.

IV. Simulation Results

In this section, we present various simulation results to illustrate the analytical results derived in this paper. In this example, we assume that there are $N = 5$ antennas in the two-way relay. The variances $\sigma_{1,i}^2$ and $\sigma_{2,i}^2, i = 1, \ldots, N$, used in the simulation are listed in the TABLE I. Other parameters used in the simulation are: the variance of the channel noise $\sigma^2 = 1$; the transmission powers of Alice and Bob are $P_A = P_B = P_T$ (therefore, the relay's total power $P = \sum_{i=1}^{N} P_i = N P_T$); the channel coherence time $T = 14$. Note that in this case, we have $T_0 = \frac{T}{N+2} = 2$. Fig. 4 shows the key rate $R_{co,N}$ defined in (21) for the case of optimal power allocation described in Section III-B and the case of equal power allocation. The optimal power distribution when the relay's total power $P = NP_T = 13.5$ is listed in TABLE II. For the ease of comparison, simulation results for the equal power distribution are also included in the table. Since the results of Case 2 violate $I_2 \leq I_1$, it is discarded; so the optimal key rate is achieved for Case 1, i.e. $4.9681/(2T) = 0.1774$ nat.

Antenna #	1	2	3	4	5
$\sigma_{1,i}^2$	0.4	0.3	2	1	0.5
$\sigma_{2,i}^2$	0.28	3.8	3	2	5.5

TABLE I: Values of $\sigma_{1,i}^2$ and $\sigma_{2,i}^2, i = 1, \ldots, N$ used in generating Fig.4

From Fig. 4, we can see that for a low P_T, the gain due to the power optimization is considerable. But when P_T is large, the improvement brought by the power optimization is limited, which is also reflected in TABLE II. This phenomenon can be explained by examining (35). When P_T is large, the differences of P_i due to different values of $\sigma^2/(\sigma_{1,i}^2 T_0)$ become insignificant. As a consequence, the

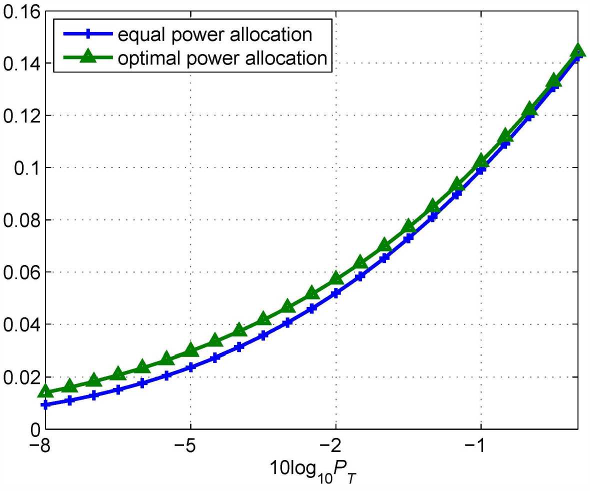

Fig. 4: Key rates of our algorithms vs. P_T.

	Equal Power Distribution	Case 1	Case 2	Case 3
P_1	2.7	2.3833	1.3993	13.2422
P_2	2.7	1.9667	3.0534	0
P_3	2.7	3.3833	3.0183	0.2578
P_4	2.7	3.1333	2.9350	0
P_5	2.7	2.6333	3.0941	0
I_1	4.9346	4.9681	4.9027	1.6046
I_2	9.5963	9.5598	9.6575	1.6046

TABLE II: Simulation results when the total power for relay $P = 13.5$

resulting mutual information would be close to those produced with equal power distribution. The same argument applies if T is sufficiently large in which $\sigma^2/(\sigma^2_{1,i}T_0)$ becomes very small, making the differences of P_i unnoticeable.

In the following, we compare the key rate of our algorithms with that of the AF with AN algorithm in [6] that deals with the multiple antennas case. The key rates of AF with AN algorithm is computed based on the k-nearest neighbor distances method in [11]. The variances of the fading coefficients of all channels are listed in TABLE III. Other simulation parameters are $\sigma^2 = 0.01, T = 308\ (T_0 = 44), P_A = P_B = P_T$. Fig. 5 illustrates the simulation results. This figure shows that our algorithm for the two-way relay with multiple antennas greatly outperforms the AF with AN algorithm, primarily because our scheme fully exploits the random channels associated with all antennas while the latter makes use of only one randomly selected antenna in the relay. In addition, our algorithm takes advantages of long training sequences which efficiently suppress the harmful effects of channel noise.

Antenna #	1	2	3	4	5
$\sigma^2_{1,i}$	0.004	0.015	0.02	0.01	0.025
$\sigma^2_{2,i}$	0.026	0.015	0.01	0.02	0.005

TABLE III: Values $\sigma^2_{1,i}$ and $\sigma^2_{2,i}, i = 1, \ldots, N$ used in generating Fig. 5

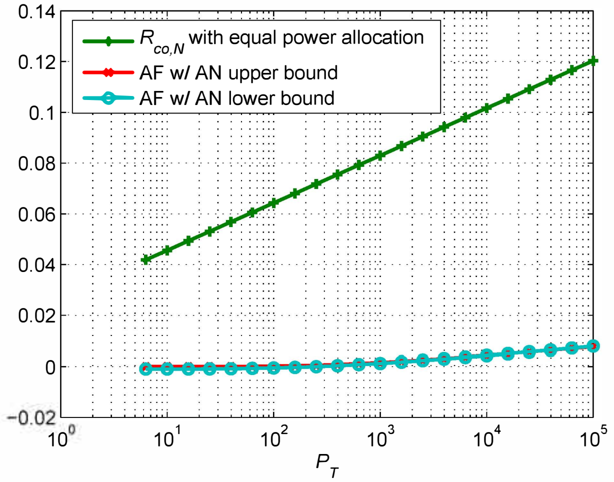

Fig. 5: Key rates vs. P_T in the sequence version.

V. Conclusion

We have considered the key generation problem in the two-way relay wireless channel in which there is no direct link between Alice and Bob. We have proposed an effective key generation scheme that achieves a substantially larger key rate than that of a direct channel mimic approach. Unlike existing schemes, there is no need for the key generating terminals to obtain correlated observations in our scheme. We have also extended the study to the case in which the relay has multiple antennas. We have characterized the optimal power allocation scheme at the relay that maximizes the key rate of the proposed scheme.

References

[1] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Trans. Inform. Forensics and Security*, vol. 2, pp. 364–375, Sep. 2007.

[2] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inform. Forensics and Security*, vol. 5, pp. 240–254, Jun. 2010.

[3] L. Lai, Y. Liang, and H. V. Poor, "A unified frame work for key agreement over wireless fading channels," *IEEE Trans. Inform. Forensics and Security*, vol. 7, pp. 480–490, Apr. 2012.

[4] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, Jul. 1993.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May 1993.

[6] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying," *IEEE Trans. Inform. Forensics and Security*, vol. 6, pp. 650–660, Sep. 2011.

[7] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless network," *IEEE Journal on Selected Areas in Communications*, vol. 30, pp. 1578–1588, Sep. 2012.

[8] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, May 2005.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[10] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, seventh printing with corrections 2009 ed., 2004.

[11] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, p. 066138, Jun. 2004.