Secret Key Generation in the Two-Way Relay Channel With Active Attackers

Heng Zhou, Lauren M. Huie, *Member, IEEE*, and Lifeng Lai, *Member, IEEE*

***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 also investigate the effects of an active attacker on the proposed key generation protocol. We characterize the optimal attacker's strategy that minimizes the key rate of the proposed scheme. Furthermore, we establish the maximal attacker's power under which our scheme can still achieve a nonzero key rate.**

***Index Terms*— Active attack, 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 attention recently [2]–[11]. 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 [12], [13] to generate secret keys from these correlated estimates. In a nutshell, in all these works, the common direct channel connecting these two terminals provides a valuable common random source required for generating secret keys using the approach proposed in [12] and [13].

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 the two-way relay channel problem was considered in [14], 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 [12] and [13]. For example, in the amplify forward (AF) scheme discussed in [14], Alice transmits a training sequence 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 sequence and the relay to re-send its received noisy signal, Alice can obtain an estimate of the product of these two channel gains. Hence the product of these 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 [14] 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 [14], 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 [15]. Instead of trying to mimic a direct channel as done in [14], in the proposed scheme, the two terminals involved do not need to obtain correlated estimates. Instead, the relay first establishes a pair-wise key with Alice using the physical channel linking it and Alice. Similarly, the relay and Bob can establish a pair-wise key using the channel linking them. Then the relay broadcasts the XOR of these two pair-wise 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 of antennas.

The second main contribution of the paper is to consider the active attacker scenario. In most of the existing work on the key generation using wireless channels, Eve is assumed to

Manuscript received September 23, 2013; revised November 13, 2013; accepted January 5, 2014. Date of publication January 17, 2014; date of current version February 12, 2014. The work of H. Zhou and L. Lai was supported in part by the National Science Foundation under CAREER Award CCF-13-18980, in part by NSF under Grant CNS-13-21223, in part by the Air Force Research Laboratory Information Directorate, and in part by Qatar National Research Fund under Grant NPRP-5-559-2-227. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Kui Ren.

H. Zhou and L. Lai are with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA (e-mail: hzhou3@wpi.edu; llai@wpi.edu).

L. M. Huie is with the Air Force Research Laboratory, Information Directorate, Rome, NY 13441 USA (e-mail: lauren.huie@us.af.mil).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2014.2301233

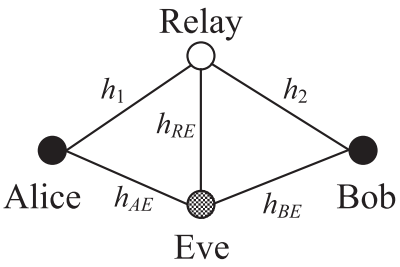


Fig. 1. Model of two-way relaying system.

be a passive listener. In practice, Eve might be active and try to send attack signals to interrupt the key generation process. In this paper, we assume that Eve's goal is to send attack signals to minimize the key rate of the proposed scheme. The effects of an active attacker are twofold: 1) Eve can corrupt signals received by legitimate nodes, and hence reduce the correlations between the signals observed by legitimate users; and 2) By controlling the signals observed by the legitimate users, Eve has partial information about the observations used for the key generation. Both of these two effects will decrease the key rate. In this paper, we characterize Eve's optimal attack strategy (including the optimal input distribution and optimal power allocation) and characterize the corresponding key rate achieved using our scheme under this worst case scenario. We note that we derive these results for a generic value of Eve's power. Our result characterizes the maximum attacker's power under which we can still achieve a non-zero key rate.

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 for the case of a passive eavesdropper in detail. We then extend our study to the case of an active attacker in Section IV. Simulation results are presented in Section V. Concluding remarks are given in Section VI.

II. Model

In this section, we introduce the key generation through the two-way relay model considered in this paper. Fig. 1 shows the simplest model of the 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 four terminals can transmit over the wireless channel (hence, Eve is an active attacker). We assume that Alice, Bob and the relay are half-duplex nodes, while the attacker is a full-duplex node. In this paper, we assume that the goal of the attacker is to minimize the key rate generated by Alice and Bob from the wireless channel. The attacker can receive a noisy version of the signal transmitted by the legitimate terminals. In addition, it can send signals to contaminate the signal transmitted by the legitimate users.

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

$$y_R = h_{AR}x_A + z_1 + n_R, \tag{1}$$

$$y_E = h_{AE}x_A + n_E, \tag{2}$$

in which h_{AR} is the fading coefficient of the channel from Alice to the relay, z_1 is the attack signal that arrives at 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.[1] No part of the system knows the value of h_{AR} a priori, but all parts know its distribution. The noise in all channels is independently and identically distributed. We note that what really matters from the attacker's perspective is the signal z_1 that arrives at the relay. In this paper, we assume that the eavesdropper knows its channel state to the legitimate receiver (hence giving the attacker extra ability), and can hence control its output signal to the legitimate receiver to achieve its attacking goal by mitigating the impact of its channel on the output signal. Hence, we did not assume any particular fading model from the attacker and legitimate user. In the following, we will characterize the optimal distribution of the optimal arriving attack signal.

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

$$y_R = h_{BR}x_B + z_2 + n_R, \tag{3}$$

$$y_E = h_{BE}x_B + n_E, \tag{4}$$

in which h_{BR} is the fading coefficient of the channel from Bob to the relay, z_2 is the attack signal that arrives at relay, h_{BE} is the channel gain between Bob and Eve. The signal model when the relay broadcasts x_R is similar.

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 rate) 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 [16]. 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 $\mathbf{X}_A = (x_A(1), \ldots, x_A(M))'$, $\mathbf{X}_B = (x_B(1), \ldots, x_B(M))'$, $\mathbf{X}_R = (x_R(1), \ldots, x_R(M))'$, and $\mathbf{Z}_i = (z_i(1), \ldots, z_i(M))'$ be the signals transmitted by the terminals in M channel uses. Similarly, let $\mathbf{Y}_A$, $\mathbf{Y}_B$, $\mathbf{Y}_R$, $\mathbf{Y}_E$ 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

$$\frac{1}{M}\mathbb{E}\{\mathbf{X}_A'\mathbf{X}_A + \mathbf{X}_B'\mathbf{X}_B + \mathbf{X}_R'\mathbf{X}_R\} \leq P_T. \tag{5}$$

[1]This assumption generally holds as long as the distance between Eve and the legitimate users are half-wavelength away from each other (please see reference [16]). Our scheme can be modified to fit the scenario in which this assumption does not hold. The modifications are described in Section IV. Note that in Section IV, the attacker is active and can control the random observations at the legitimate users. Hence, in this case, the observations at the legitimate users and Eve are indeed correlated. Furthermore, in this case, the correlation is controlled the Eve. Our scheme can still generate a secret key with a nonzero secret key rate under this situation.

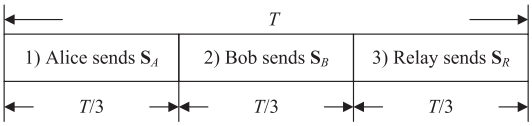


Fig. 2. Time frame for one antenna.

Similarly, we assume that the attacker has an average power constraint

$$\frac{1}{M}\mathbb{E}\{\mathbf{Z}_1'\mathbf{Z}_1 + \mathbf{Z}_2'\mathbf{Z}_2 + \mathbf{Z}_3'\mathbf{Z}_3\} \le P_E. \tag{6}$$

In addition to the wireless channels, we assume that there is a public channel in which all legitimate users can exchange messages.[2] 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

$$P\{K_A \neq K_B\} < \epsilon, \tag{7}$$

$$\tfrac{1}{M} I(K_A; \mathbf{Z}_i, i = 1, 2, 3, \mathbf{Y}_E, \mathbf{F}) < \epsilon, \tag{8}$$

$$\tfrac{1}{M} H(K_A) > R - \epsilon, \tag{9}$$

$$\tfrac{1}{M} \log |\mathcal{K}_A| < \tfrac{1}{M} H(K_A) + \epsilon, \tag{10}$$

with $|\mathcal{K}_A|$ being the size of the key's alphabet. Here (7) 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), (8) implies that the eavesdropper learns limited amount of information about the generated key, while (10) implies that the key is nearly uniformly generated.

III. Key Generation Algorithms With a Passive Attacker

In this section, we study the case in which the attacker is passive, i.e., $\mathbf{Z}_i = \boldsymbol{\phi}, i = 1, 2, 3$. This section will provide the necessary background for the general case with active attackers, which will be discussed in Section IV.

A. Single Antenna Case

Algorithm 1 shows the proposed key generation scheme, which is adopted from our recent work [15]. Roughly speaking, in our scheme, Alice, Bob and the relay take turns to send training sequences. After the training stage, the terminals will generate pair-wise keys, and then the relay will send additional information to help Alice and Bob to establish a common key.

We now explain the steps in the algorithm in more detail. The time frame of Algorithm 1 is shown in Fig. 2. We divide each fading block into three slots each with duration T_0, and we set $T_0 = T/3$. Suppose Alice sends training sequence

[2]If the public channel is not available, the terminals can still establish a key. In particular, we can divide the time into two parts. The first part is used for channel training so that the terminals can obtain correlated observations. The second part can be used to transit the public discussion over the wireless channel. Since the capacity of the wireless channel is limited, the rate of the public discussion will also be limited. This will reduce the key rate. However, the impact will be limited if the available power is large enough or the channel coherence time is long enough.

Algorithm 1: Key Generation Algorithm with 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 the 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 the 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 the estimate $\tilde{h}_{1,A}$; Bob receives $\mathbf{Y}_B$ from which he obtains the 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.

with power P_A, Bob with power P_B and the relay with power P_R, then the training sequences transmitted by the legitimate users have the form $\mathbf{S}_A = \underbrace{(\sqrt{P_A}, \sqrt{P_A}, \ldots, \sqrt{P_A})'}_{T_0}, \mathbf{S}_B = \underbrace{(\sqrt{P_B}, \sqrt{P_B}, \ldots, \sqrt{P_B})'}_{T_0}, \mathbf{S}_R = \underbrace{(\sqrt{P_R}, \sqrt{P_R}, \ldots, \sqrt{P_R})'}_{T_0}$. Therefore, 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 (5) is equivalent to

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

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

$$\mathbf{Y}_R^{(1)} = h_1 \mathbf{S}_A + \mathbf{N}_R^{(1)}, \tag{11}$$

$$\mathbf{Y}_A = h_1 \mathbf{S}_R + \mathbf{N}_A, \tag{12}$$

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

$$\tilde{h}_{1,R} = \frac{\mathbf{S}_A'}{\|\mathbf{S}_A\|^2}\mathbf{Y}_R^{(1)} = h_1 + \frac{\mathbf{S}_A'}{\|\mathbf{S}_A\|^2}\mathbf{N}_R^{(1)}, \tag{13}$$

$$\tilde{h}_{1,A} = \frac{\mathbf{S}_R'}{\|\mathbf{S}_R\|^2}\mathbf{Y}_A = h_1 + \frac{\mathbf{S}_R'}{\|\mathbf{S}_R\|^2}\mathbf{N}_A. \tag{14}$$

Eve also receives

$$\mathbf{Y}_E^{(1)} = h_{AE}\mathbf{S}_A + \mathbf{N}_E^{(1)},$$

$$\mathbf{Y}_E^{(3)} = h_{RE}\mathbf{S}_R + \mathbf{N}_E^{(3)}. \tag{15}$$

However, since h_{AE} and h_{RE} are independent of h_1 [16], $\mathbf{Y}_E^{(1)}$ and $\mathbf{Y}_E^{(3)}$ are independent of the correlated estimations $(\tilde{h}_{1,R}, \tilde{h}_{1,A})$. Using the result from [12], the relay and Alice can establish a pairwise key K_1 with a rate:

$$\frac{1}{T} I(\tilde{h}_{1,A}; \tilde{h}_{1,R}). \tag{16}$$

To generate a uniformly distributed key with the rate in (16), one needs to employ the Slepian-Wolf coding [12] to send helper information from Alice to Bob through the public channel in order to reconciliate the effects of noise in their channel estimates. Somewhat remarkably, the helper data, although observable to Eve, does not leak any information about the generated key to Eve. More specifically, for every N symbol times, which is as large as a number of blocks of symbol times, Alice has $m = \lfloor N/T \rfloor$ observations of the random variable $\tilde{h}_{1,A}$, where $\lfloor \cdot \rfloor$ denotes the largest integer that is smaller than its argument. These observations are collected into a vector $\tilde{\mathbf{h}}_{1,A} = [\tilde{h}^{\Delta}_{1,A}(1), \cdots, \tilde{h}^{\Delta}_{1,A}(m)]^T$, where $\tilde{h}^{\Delta}_{1,A}(i)$ is a quantized version of $\tilde{h}_{1,A}(i)$ with quantization interval being Δ. $\tilde{h}^{\Delta}_{1,A}(i)$'s are independent of each other. Similarly, the relay has a vector of observations $\tilde{\mathbf{h}}_{1,R} = [\tilde{h}^{\Delta}_{1,R}(1), \cdots, \tilde{h}^{\Delta}_{1,R}(m)]^T$. Alice randomly divides the typical $\tilde{h}^{\Delta}_{1,A}$ sequences into non-overlapping bins, with each bin having $2^{mI(\tilde{h}^{\Delta}_{1,A};\tilde{h}^{\Delta}_{1,R})}$ typical $\tilde{h}^{\Delta}_{1,A}$ sequences. Hence, each sequence has two indices: bin number and index within the bin. Now, after observing the vector $\tilde{\mathbf{h}}_{1,A}$, Alice sets the key to be the index of this sequence within its bin. Alice then sends the bin number as the helper data to Bob through the public channel. That is, Alice needs to send $H(\tilde{h}^{\Delta}_{1,A}|\tilde{h}^{\Delta}_{1,R})$ bits of information through the public channel, where $H(X|Y)$ denotes the conditional entropy of X given Y. After combining the information observed from the public channel with $\tilde{\mathbf{h}}_{1,R}$, it can be shown that Bob can recover the value of $\tilde{\mathbf{h}}_{1,A}$ with the probability arbitrarily close to 1. Then Bob can recover the key. It can also be shown that the bin number and index within each bin are independent of each other. Hence, even though the eavesdropper can observe the bin number transmitted over the public channel, it learns no information about the generated key. Now, by letting the quantization level Δ go to zero, one achieve the key rate (16).

Similarly, for channel h_2, the relay and Bob receive

$$\mathbf{Y}_R^{(2)} = h_2 \mathbf{S}_B + \mathbf{N}_R^{(2)}, \tag{17}$$

$$\mathbf{Y}_B = h_2 \mathbf{S}_R + \mathbf{N}_B, \tag{18}$$

from which the relay and Bob obtain the following estimates

$$\tilde{h}_{2,R} = \frac{\mathbf{S}'_B}{\|\mathbf{S}_B\|^2}\mathbf{Y}_R^{(2)} = h_2 + \frac{\mathbf{S}'_B}{\|\mathbf{S}_B\|^2}\mathbf{N}_R^{(2)}, \tag{19}$$

$$\tilde{h}_{2,B} = \frac{\mathbf{S}'_R}{\|\mathbf{S}_R\|^2}\mathbf{Y}_B = h_2 + \frac{\mathbf{S}'_R}{\|\mathbf{S}_R\|^2}\mathbf{N}_B. \tag{20}$$

Eve receives, in addition to (15),

$$\mathbf{Y}_E^{(2)} = h_{BE}\mathbf{S}_B + \mathbf{N}_E^{(2)},$$

where h_{BE} is independent of h_2. Again, using the results from [12], the key rate of K_2 is

$$\frac{1}{T} I(\tilde{h}_{2,B}; \tilde{h}_{2,R}). \tag{21}$$

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 [17] where the longer key is the secret key used to protect secret transmission of the shorter key as a message. As the result, Alice and Bob can obtain both K_1 and K_2 by the XOR operation on the received $K_1 \oplus K_2$ signal. Eve also receives $K_1 \oplus K_2$. However, Eve 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. In this case, both Alice and Bob can choose the shorter key as the common secret key. Hence the key rate is:

$$R_{co} = \frac{1}{T}\min\{I(\tilde{h}_{1,A}; \tilde{h}_{1,R}), I(\tilde{h}_{2,B}; \tilde{h}_{2,R})\}. \tag{22}$$

Following similar steps in [4], one can easily show that Eve obtains a limited amount of the key information.

The scalars $\tilde{h}_{1,A}$ and $\tilde{h}_{1,R}$ are two correlated Gaussian variables with zero mean, thus we have [18]

$$I(\tilde{h}_{1,A}; \tilde{h}_{1,R}) = -\frac{1}{2}\log(1-\rho_1^2) \tag{23}$$

where ρ_1 is the correlation coefficient of $\tilde{h}_{1,A}$ and $\tilde{h}_{1,R}$. It is easy to check that the covariance $\mathrm{cov}(\tilde{h}_{1,A}, \tilde{h}_{1,R}) = \sigma_1^2$, variances $\mathrm{Var}(\tilde{h}_{1,A}) = \sigma_1^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2} = \sigma_1^2 + \frac{\sigma^2}{T_0 P_R}$, $\mathrm{Var}(\tilde{h}_{1,R}) = \sigma_1^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2} = \sigma_1^2 + \frac{\sigma^2}{T_0 P_A}$, and

$$\begin{aligned}\rho_1^2 &= \frac{\mathrm{cov}^2(\tilde{h}_{1,A}, \tilde{h}_{1,R})}{\mathrm{Var}(\tilde{h}_{1,A})\mathrm{Var}(\tilde{h}_{1,R})} \\ &= \frac{1}{\left(1+\frac{\sigma^2}{\sigma_1^2 T_0 P_A}\right)\left(1+\frac{\sigma^2}{\sigma_1^2 T_0 P_R}\right)}.\end{aligned} \tag{24}$$

Similarly,

$$I(\tilde{h}_{2,B}; \tilde{h}_{2,R}) = -\frac{1}{2}\log(1-\rho_2^2) \tag{25}$$

where ρ_2 is the correlation coefficient of $\tilde{h}_{2,B}$ and $\tilde{h}_{2,R}$. We have $\mathrm{cov}(\tilde{h}_{2,B}, \tilde{h}_{2,R}) = \sigma_2^2$, $\mathrm{Var}(\tilde{h}_{2,B}) = \sigma_2^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2} = \sigma_2^2 + \frac{\sigma^2}{T_0 P_R}$, $\mathrm{Var}(\tilde{h}_{2,R}) = \sigma_2^2 + \frac{\sigma^2}{\|\mathbf{S}_B\|^2} = \sigma_2^2 + \frac{\sigma^2}{T_0 P_B}$, and

$$\rho_2^2 = \frac{1}{\left(1+\frac{\sigma^2}{\sigma_2^2 T_0 P_B}\right)\left(1+\frac{\sigma^2}{\sigma_2^2 T_0 P_R}\right)}. \tag{26}$$

B. Multiple Antennas Case With Optimal Power Allocation

The aforementioned key generation algorithm for a relay with one antenna can be easily extended to the case of multiple antennas. Suppose there are N antennas at the relay, 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

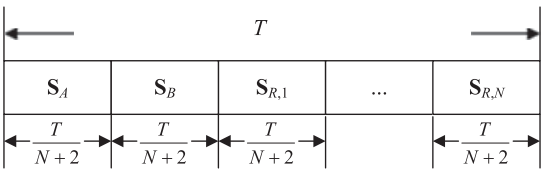


Fig. 3. Time frame for two-way relay with multiple antennas.

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 obtain 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.

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 (5) is now

$$\frac{1}{N+2}\left(P_A + P_B + \sum_{i=1}^{N} P_i\right) \leq P_T. \tag{27}$$

Accordingly, the key rate for Algorithm 2 is

$$R_{co,N} = \frac{1}{T}\min\{I_1, I_2\}, \tag{28}$$

where

$$I_1 = \sum_{i=1}^{N} I(\tilde{h}_{A,i,A}; \tilde{h}_{A,i,R}), \tag{29}$$

$$I_2 = \sum_{i=1}^{N} I(\tilde{h}_{B,i,B}; \tilde{h}_{B,i,R}), \tag{30}$$

in which $I(\tilde{h}_{A,i,A}; \tilde{h}_{A,i,R})$ and $I(\tilde{h}_{B,1,B}; \tilde{h}_{B,1,R})$ can be calculated using formulas (23), (24) and (25), (26):

$$I(\tilde{h}_{A,i,A}; \tilde{h}_{A,i,R}) = -\frac{1}{2}\log\left(1 - \frac{1}{\left(1 + \frac{\sigma^2}{\sigma_{1,i}^2 P_A T_0}\right)\left(1 + \frac{\sigma^2}{\sigma_{1,i}^2 P_i T_0}\right)}\right),$$

$$I(\tilde{h}_{B,i,B}; \tilde{h}_{B,i,R}) = -\frac{1}{2}\log\left(1 - \frac{1}{\left(1 + \frac{\sigma^2}{\sigma_{2,i}^2 P_B T_0}\right)\left(1 + \frac{\sigma^2}{\sigma_{2,i}^2 P_i T_0}\right)}\right).$$

The total power constraint (27) can be rewritten as

$$\sum_{i=1}^{N} P_i \leq (N+2)P_T - P_A - P_B \triangleq P. \tag{31}$$

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 is under a specified value P, the key rate (28) depends on the power used for each antenna. In the following, we solve the optimal power allocation problem to maximize the key rate.

Formally, the optimization problem is

$$\begin{aligned} &\text{maximize } \min\{I_1, I_2\} \\ &\text{subject to} \sum_{i=1}^{N} P_i \leq P, P_i \geq 0, \quad i = 1, \ldots, N. \end{aligned} \tag{32}$$

To simplify the notation, in the following derivation, we will ignore the constant $1/2$ before each mutual information term. Clearly, this will not affect the optimal power allocation scheme.

The objective function in (32) contains a `min` operation, which makes it challenging. To solve this max-min optimization problem, we transform (32) into an equivalent optimization problem [19]:

$$\begin{aligned} &\text{maximize } z \\ &\text{subject to } z \leq I_1, z \leq I_2, \\ &\sum_{i=1}^{N} P_i \leq P, \\ &z \geq 0, P_i \geq 0, \quad i = 1, \ldots, N. \end{aligned} \tag{33}$$

The Lagrangian of problem (33) is

$$\mathcal{L} = z + \lambda_1(I_1 - z) + \lambda_2(I_2 - z) + \lambda_3\left(P - \sum_{i=1}^{N} P_i\right). \tag{34}$$

Then the KKT conditions are

$$\frac{\partial \mathcal{L}}{\partial z} \leq 0, \quad z \geq 0, \quad z\frac{\partial \mathcal{L}}{\partial z} = 0, \tag{35}$$

$$\frac{\partial \mathcal{L}}{\partial P_i} \leq 0, \quad P_i \geq 0, \quad P_i\frac{\partial \mathcal{L}}{\partial P_i} = 0, \tag{36}$$

$$z \leq I_1, \quad \lambda_1 \geq 0, \quad \lambda_1(z - I_1) = 0, \tag{37}$$

$$z \leq I_2, \quad \lambda_2 \geq 0, \quad \lambda_2(z - I_2) = 0, \tag{38}$$

$$\sum_{i=1}^{N} P_i \leq P, \quad \lambda_3 \geq 0, \quad \lambda_3\left(\sum_{i=1}^{N} P_i - P\right) = 0. \tag{39}$$

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

We can calculate

$$\frac{\partial \mathcal{L}}{\partial z} = 1 - \lambda_1 - \lambda_2,$$

so from condition (35.i) (this notation means the first condition of (35)) we have

$$1 - \lambda_1 - \lambda_2 \le 0. \tag{40}$$

From the definition of I_1, I_2 in (29), (30), it is clear that I_1, I_2 are always positive, so if $z = 0$, from (37.iii) and (38.iii), it follows $\lambda_1 = \lambda_2 = 0$. But this violates (40), so $z \neq 0$ and from (35.iii) we get $\frac{\partial \mathcal{L}}{\partial z} = 1 - \lambda_1 - \lambda_2 = 0$, which implies

$$\lambda_1 + \lambda_2 = 1. \tag{41}$$

The partial derivative of I_1 with regard to P_i can be computed as follows:

$$\frac{\partial I_1}{\partial P_i} = \frac{P_A}{\left(P_i + \dfrac{\sigma^2}{\sigma_{1,i}^2 T_0}\right)\left(P_i + \dfrac{\sigma^2}{\sigma_{1,i}^2 T_0} + P_A\right)}, \tag{42}$$

which is always positive. Similarly we can compute $\frac{\partial I_2}{\partial P_i}$ and see that it is always positive as well.

We can then calculate

$$\frac{\partial \mathcal{L}}{\partial P_i} = \lambda_1 \frac{\partial I_1}{\partial P_i} + \lambda_2 \frac{\partial I_2}{\partial P_i} - \lambda_3. \tag{43}$$

From (36.i) and the analysis above, we know

$$\lambda_3 \ge \lambda_1 \frac{\partial I_1}{\partial P_i} + \lambda_2 \frac{\partial I_2}{\partial P_i} > 0. \tag{44}$$

Consequently, by (39.iii) we have

$$\sum_{i=1}^{N} P_i = P. \tag{45}$$

In the following, we discuss different cases of the values of λ_1 and λ_2. Note that we have already eliminated the possibility of $\lambda_1 = \lambda_2 = 0$. Also note that the following three cases are not mutually exclusive.

1) Case 1: If $\lambda_1 \neq 0$ and $\lambda_2 = 0$, then λ_1 must be 1 by (41). Next from (37.iii), $z = I_1$. But (38.i) implies

$$I_1 \le I_2, \tag{46}$$

so $\min\{I_1, I_2\} = I_1$ and the original optimization problem (32) reduces to

$$\begin{aligned} &\text{maximize } I_1 \\ &\text{subject to } \sum_{i=1}^{N} P_i = P, \\ &\qquad P_i \ge 0, \quad i = 1, \ldots, N. \end{aligned} \tag{47}$$

This is an optimization problem with nonnegativity constraints. Again we can employ KKT conditions to solve it. Similar to (33), 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. The Lagrangian and KKT conditions are [19]:

$$L = I_1 + \mu\left(P - \sum_{i=1}^{N} P_i\right), \tag{48}$$

$$\frac{\partial L}{\partial P_i} \le 0, \qquad P_i \ge 0, \qquad P_i \frac{\partial L}{\partial P_i} = 0, \tag{49}$$

$$\sum_{i=1}^{N} P_i = P. \tag{50}$$

It can be verified that the solution of KKT system (49-50) satisfies KKT conditions (35-39) of the problem (33), so they are also the solution of (33).

For those P_i's that are greater than zero, (49.iii) leads to

$$\frac{\partial L}{\partial P_i} = \frac{\partial I_1}{\partial P_i} - \mu = 0. \tag{51}$$

Letting

$$P_i + \frac{\sigma^2}{\sigma_{1,i}^2 T_0} = x_i, \tag{52}$$

it follows from (42) that

$$x_i = \frac{-P_A + \sqrt{P_A^2 + \frac{4P_A}{\mu}}}{2}, \tag{53}$$

from which we get

$$P_i = \frac{-P_A + \sqrt{P_A^2 + \frac{4P_A}{\mu}}}{2} - \frac{\sigma^2}{\sigma_{1,i}^2 T_0}. \tag{54}$$

Those P_i's in (54) are positive because this is what we proposed to do. For other P_i's which would be negative if we forcibly solve them according to (54), due to the requirement of nonnegativity in (49.ii), we set them to zeros. Therefore, we can collectively write

$$P_i = \left(\frac{-P_A + \sqrt{P_A^2 + \frac{4P_A}{\mu}}}{2} - \frac{\sigma^2}{\sigma_{1,i}^2 T_0}\right)^+ \tag{55}$$

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

If we know the number N' of P_i's that are strictly positive, based on condition (50) and the observation that x_i's in (53) are independent of i and are therefore all the same, we have

$$x_i = \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \frac{1}{\sigma_{1,j}^2},$$

$$\therefore P_i = \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \frac{1}{\sigma_{1,j}^2} - \frac{\sigma^2}{\sigma_{1,i}^2 T_0} \tag{56}$$

$$= \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \left(\frac{1}{\sigma_{1,j}^2} - \frac{1}{\sigma_{1,i}^2}\right) \tag{57}$$

for those i satisfying $P_i > 0$.

From the derived formulas, we observe that the optimal power distribution under the fixed total relay power constraint does not depend on the transmission power of Alice and Bob, i.e., P_A and P_B.

2) Case 2: If $\lambda_1 = 0$ and $\lambda_2 \neq 0$, then λ_2 must be 1 by (41). Next from (38.iii), $z = I_2$. But (37.i) implies

$$I_2 \leq I_1, \tag{58}$$

so $\min\{I_1, I_2\} = I_2$ and the original optimization problem (32) turns to

$$\begin{aligned} &\text{maximize } I_2 \\ &\text{subject to } \sum_{i=1}^{N} P_i = P, \\ &\qquad P_i \geq 0, i = 1, \ldots, N. \end{aligned} \tag{59}$$

Similar to Case 1, we can solve this optimization problem under nonnegativity constraints by KKT, and its solutions would be the solutions of KKT conditions (35-39). Following the same argument as that of Case 1, the optimal points P_i's are

$$P_i = \left(\frac{-P_B + \sqrt{P_B^2 + \frac{4P_B}{\mu}}}{2} - \frac{\sigma^2}{\sigma_{2,i}^2 T_0} \right)^+ \tag{60}$$

or, for those strictly positive P_i's

$$P_i = \frac{P}{N'} + \frac{\sigma^2}{N' T_0} \sum_{j=1}^{N'} \left(\frac{1}{\sigma_{2,j}^2} - \frac{1}{\sigma_{2,i}^2} \right) \tag{61}$$

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

3) Case 3: If $\lambda_1 \neq 0$ and $\lambda_2 \neq 0$ at the same time, from (37.iii) we have $z = I_1$ and in the same way we can obtain $z = I_2$. So in this case $I_1 = I_2$, and the original optimization problem (32) becomes

$$\begin{aligned} &\text{maximize } I_1 \\ &\text{subject to } I_1 = I_2, \\ &\qquad \sum_{i=1}^{N} P_i = P. \end{aligned} \tag{62}$$

This is an optimization problem with equality constraints. The Lagrangian is:

$$\begin{aligned} L &= I_1 + \mu_1 (I_2 - I_1) + \mu_2 \left(P - \sum_{i=1}^{N} P_i \right) \\ &= (1 - \mu_1) I_1 + \mu_1 I_2 + \mu_2 \left(P - \sum_{i=1}^{N} P_i \right). \end{aligned} \tag{63}$$

Using the Lagrange multiplier method, the partial derivative of L with respect to P_i is

$$\frac{\partial L}{\partial P_i} = (1 - \mu_1) \frac{\partial I_1}{\partial P_i} + \mu_1 \frac{\partial I_2}{\partial P_i} - \mu_2 = 0, \tag{64}$$

which, when combined with the equality conditions $I_1 = I_2$ and $P = \sum_{i=1}^{N} P_i$, forms a system whose solution is the same as that for (62). Setting $1 - \mu_1 = \lambda_1$ (therefore $\mu_1 = \lambda_2$) and $\mu_2 = \lambda_3$, it is clear that solution of (62) satisfies the KKT conditions (35-39) (cf. (43)). Due to the complexity of formulas involved, there is no closed-form solution to optimization problem (62). One needs to resort to a numerical method to solve it.

We have solved for the P_i's and obtained the optimal power distribution under a fixed total relay transmission power for three cases. Since these three cases are not mutually exclusive, after obtaining the solutions to three cases, we should compare the resulting values of each case and pick out the largest one as the final optimal result. In addition, we should check the necessary conditions (46) and (58); if they do not hold, the optimal points obtained are invalid and should be discarded. It is worth noting that the KKT conditions are essentially necessary so we are sure that at least one of the three cases will have valid solution that achieves optimality. So, if we find that solutions of Case 1&2 are both invalid, then there must be an array of nonnegative P_i's satisfying $I_1 = I_2$ and $P = \sum_{i=1}^{N} P_i$.

IV. Key Generation Algorithms With the Presence of an Active Attacker

In this section, we consider the active Eve case. The single antenna at the relay case will be discussed in detail. We will use the same protocol as in Section III, and characterize the attacker's optimal attack strategy. In particular, Eve will send attack signals $\mathbf{Z}_i \neq \phi, i = 1, 2, 3$. We will characterize the optimal distributions of $\mathbf{Z}_i$'s and the corresponding achievable key rate.

A. Optimal Attack Signal

Since Eve is active, when Alice sends the training sequence $\mathbf{S}_A$, the relay receives

$$\mathbf{Y}_R^{(1)} = h_1 \mathbf{S}_A + \mathbf{Z}_1 + \mathbf{N}_R^{(1)},$$

from which the relay calculates a scalar estimate of h_1

$$\tilde{h}_{1,R} = \frac{\mathbf{S}_A' \mathbf{Y}_R^{(1)}}{\|\mathbf{S}_A\|^2} = h_1 + \frac{\mathbf{S}_A' \mathbf{Z}_1}{\|\mathbf{S}_A\|^2} + \frac{\mathbf{S}_A' \mathbf{N}_R^{(1)}}{\|\mathbf{S}_A\|^2}. \tag{65}$$

If we denote $\frac{\mathbf{S}_A' \mathbf{Z}_1}{\|\mathbf{S}_A\|^2}$ as Γ_1 and $\frac{\mathbf{S}_A' \mathbf{N}_R^{(1)}}{\|\mathbf{S}_A\|^2}$ as $N_R^{(1)}$ which conforms to $\mathcal{N}(0, \frac{\sigma^2}{\|\mathbf{S}_A\|^2})$ distribution, (65) can be written as

$$\tilde{h}_{1,R} = h_1 + \Gamma_1 + N_R^{(1)}. \tag{66}$$

Similarly, when the relay sends the training sequence $\mathbf{S}_R$, Alice receives a tampered sequence

$$\mathbf{Y}_A = h_1 \mathbf{S}_R + \mathbf{Z}_3 + \mathbf{N}_A$$

and calculates a scalar estimate

$$\begin{aligned} \tilde{h}_{1,A} &= h_1 + \frac{\mathbf{S}_R' \mathbf{Z}_3}{\|\mathbf{S}_R\|^2} + \frac{\mathbf{S}_R' \mathbf{N}_A}{\|\mathbf{S}_R\|^2} \\ &\triangleq h_1 + \Gamma_3 + N_A \end{aligned} \tag{67}$$

where $N_A \sim \mathcal{N}(0, \frac{\sigma^2}{\|\mathbf{S}_R\|^2})$.

According to our protocol, Alice and the relay will generate a pair-wise key from $(\tilde{h}_{1,R}, \tilde{h}_{1,A})$. From (66) and (67), we observe that the estimates at Alice and the relay are partially controlled by Eve. Furthermore, Eve has partial information about the correlated estimates at Alice and the relay. The key generation problem under this setup hence is a key generation with side-information at Eve problem considered in [12]. An achievable key rate is [4]:

$$R_{s1} = [I(\tilde{h}_{1,A}; \tilde{h}_{1,R}) - I(\tilde{h}_{1,A}; \Gamma_1, \Gamma_3)]^+. \tag{68}$$

On the Bob-relay side, the effects of the attacker on the channel estimates can be formulated as

$$\tilde{h}_{2,R} = h_2 + \frac{\mathbf{S}_B'\mathbf{Z}_2}{\|\mathbf{S}_B\|^2} + \frac{\mathbf{S}_B'\mathbf{N}_R^{(2)}}{\|\mathbf{S}_B\|^2} \triangleq h_2 + \Gamma_2 + N_R^{(2)}, \tag{69}$$

$$\tilde{h}_{2,B} = h_2 + \frac{\mathbf{S}_R'\mathbf{Z}_3}{\|\mathbf{S}_R\|^2} + \frac{\mathbf{S}_R'\mathbf{N}_B}{\|\mathbf{S}_R\|^2} \triangleq h_2 + \Gamma_3 + N_B. \tag{70}$$

Again, in our protocol specified in Algorithm 1, the relay and Bob will establish a pair-wise key K_2 from $(\tilde{h}_{2,R}, \tilde{h}_{2,B})$. Similar to the case of K_1, the key rate of K_2 is

$$R_{s2} = [I(\tilde{h}_{2,B}; \tilde{h}_{2,R}) - I(\tilde{h}_{2,B}; \Gamma_2, \Gamma_3)]^+. \tag{71}$$

According to Algorithm 1, the final key rate of the two-way relaying system is

$$R_s = \frac{1}{T}\min\{R_{s1}, R_{s2}\}. \tag{72}$$

Clearly, Eve will choose her attack strategy to minimize the key rate, hence Eve will try to solve the following optimization problem

$$\begin{aligned} &\underset{\Gamma_1,\Gamma_2,\Gamma_3}{\text{minimize}} \ \min\{R_{s1}, R_{s2}\} \\ &\text{subject to (6)} \end{aligned} \tag{73}$$

where R_{s1} and R_{s2} depend on the distribution of $\Gamma_i, i = 1, 2, 3$. In the following, we will first characterize the optimal distribution of Γ_i's, then we will optimize over the power allocation for Eve.

We can use the result in Theorem 4.1 of [4] for the first step. Theorem 4.1 of [4] shows that, the minimal R_{s1} is achieved when (Γ_1, Γ_3) are zero mean jointly Gaussian random variables. In this case, the optimal attack signals are characterized by the variances and correlation coefficient. If Eve sends attack signal z_i with power $P_{Ei} = \mathbb{E}\{z_i^2\}, i = 1, 2, 3$, then for zero mean Gaussian random variables, $\text{Var}\{\Gamma_1\} \triangleq \sigma_1^2 = P_{E1}/\|\mathbf{S}_A\|^2$, $\text{Var}\{\Gamma_2\} \triangleq \sigma_2^2 = P_{E2}/\|\mathbf{S}_B\|^2$ and $\text{Var}\{\Gamma_3\} \triangleq \sigma_3^2 = P_{E3}/\|\mathbf{S}_R\|^2$. Theorem 4.1 of [4] says that the optimal correlation coefficient between Γ_1 and Γ_3 is given by

$$\rho_1 = \begin{cases} -\dfrac{\sigma_{h1}^2}{\sigma_1\sigma_3}, & \text{if } \sigma_{h1}^2 \le \sigma_1\sigma_3 \\ -1, & \text{otherwise,} \end{cases} \tag{74}$$

where σ_{h1}^2 is the variance of the Gaussian channel gain h_1, and the minimal R_{s1} is

$$\begin{aligned} R_{s1} &= \left[-\frac{1}{2}\log(2\pi e\sigma_{e1}^2) + h(h_1 + N_A)\right]^+ \\ &= \left[-\frac{1}{2}\log(2\pi e\sigma_{e1}^2) + \frac{1}{2}\log\left(2\pi e(\sigma_{h1}^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2})\right)\right]^+ \\ &= \left[\frac{1}{2}\log\left(\frac{\sigma_{h1}^2 + \sigma^2/\|\mathbf{S}_R\|^2}{\sigma_{e1}^2}\right)\right]^+ \end{aligned} \tag{75}$$

where

$$\sigma_{e1}^2 = \left(\sigma_{h1}^2 + \sigma_3^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2}\right) - \frac{(\sigma_{h1}^2 + \rho_1\sigma_1\sigma_3)^2}{\sigma_{h1}^2 + \sigma_1^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2}}. \tag{76}$$

Similarly, on the Bob-relay side, the minimal R_{s2} for the key between Bob and relay is achieved when (Γ_2, Γ_3) is jointly Gaussian with correlation coefficient

$$\rho_2 = \begin{cases} -\dfrac{\sigma_{h2}^2}{\sigma_2\sigma_3}, & \text{if } \sigma_{h2}^2 \le \sigma_2\sigma_3 \\ -1, & \text{otherwise,} \end{cases} \tag{77}$$

and the minimal

$$R_{s2} = \left[-\frac{1}{2}\log(2\pi e\sigma_{e2}^2) + h(h_2 + N_B)\right]^+ \tag{78}$$

$$= \left[\frac{1}{2}\log\left(\frac{\sigma_{h2}^2 + \sigma^2/\|\mathbf{S}_R\|^2}{\sigma_{e2}^2}\right)\right]^+ \tag{79}$$

where

$$\sigma_{e2}^2 = \left(\sigma_{h2}^2 + \sigma_3^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2}\right) - \frac{(\sigma_{h2}^2 + \rho_2\sigma_2\sigma_3)^2}{\sigma_{h2}^2 + \sigma_2^2 + \frac{\sigma^2}{\|\mathbf{S}_B\|^2}}. \tag{80}$$

To satisfy the structure above, the attacker can generate the attack signal $\mathbf{Z}_i, i = 1, 2, 3$ in the following order. Eve first generates $\mathbf{Z}_1$ using the Gaussian distribution. Then Eve produces $\mathbf{Z}_3$ from $\mathbf{Z}_1$ with the correlation coefficient ρ_1. Finally, Eve generates $\mathbf{Z}_2$ based on ρ_2 from $\mathbf{Z}_3$.

In the active attack case, the average power constraint for attacker (6) becomes

$$\frac{1}{3}(P_{E1} + P_{E2} + P_{E3}) \le P_E,$$

or equivalently

$$\frac{\sigma_1^2}{1/\|\mathbf{S}_A\|^2} + \frac{\sigma_2^2}{1/\|\mathbf{S}_B\|^2} + \frac{\sigma_3^2}{1/\|\mathbf{S}_R\|^2} \le 3P_E. \tag{81}$$

Clearly equation (81) represents an ellipsoid with nonnegative coordinates.

From the discussion above, the optimization problem in (73) can be simplified as

$$\begin{aligned} &\underset{\sigma_1,\sigma_2,\sigma_3}{\text{minimize}} \ \min\{R_{s1}(\sigma_1,\sigma_2,\sigma_3), R_{s2}(\sigma_1,\sigma_2,\sigma_3)\} \\ &\text{subject to (81)}, \sigma_i \ge 0, i = 1, 2, 3. \end{aligned} \tag{82}$$

Hence, characterizing the optimal attacker's strategy is simplified to finding the optimal power allocation strategy.

B. Effects of Active Attacks

Before we solve the optimization problem (82), we study the effects of active attacks. In particular, we would like to determine under which conditions, the attacker can make the key rate to be zero. From (75), we observe that there is an $(\cdot)^+$ operation in R_{s1}. As a result, the minimal possible value of R_{s1}, and in turn of R_s, is zero. If the σ_{e1}^2 is too large (because the attacker's power is too large), the logarithm inside $(\cdot)^+$ would be negative, leading to a zero key rate. We use the set $\{(\sigma_1, \sigma_2, \sigma_3) | R_s = 0\}$ to denote the set of $(\sigma_1, \sigma_2, \sigma_3)$ such that if the attacker uses these $(\sigma_1, \sigma_2, \sigma_3)$'s, the key rate of our protocol will be zero. We call this set the infeasible set, since it is infeasible for us to generate a key if the attacker's power is large enough to be in this set. Here, we will characterize the smallest attack power in the infeasible set, which is equivalent to the largest attacker's power that our protocol can tolerate.

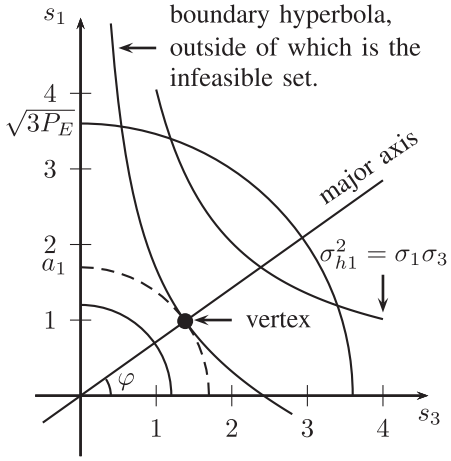


Fig. 4. The relations between the power constraint and the infeasible set. Two circles in the figure represent attacker's average power constraint. The one with a larger radius intersects with the infeasible set.

We will first focus on R_{s1}. From (75) and (76), we can see that R_{s1} is zero if and only if

$$\sigma_{e1}^2 \geq \sigma_{h1}^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2}, \tag{83}$$

or

$$\sigma_3^2 - \frac{(\sigma_{h1}^2 + \rho_1\sigma_1\sigma_3)^2}{\sigma_{h1}^2 + \sigma_1^2 + \sigma_A^2} \geq 0 \tag{84}$$

where $\sigma_A^2 = \frac{\sigma^2}{\|\mathbf{S}_A\|^2}$. Since σ_2 is not involved, it is clear that the minimal attacker power that makes $R_{s1} = 0$ is obtained when $\sigma_2 = 0$. According to (74), in the region of σ_3-σ_1 plane outside the hyperbola $\sigma_{h1}^2 = \sigma_1\sigma_3$ (upper right side of the curve), $\rho_1 = -(\sigma_{h1}^2/\sigma_1\sigma_3)$ and consequently the subtrahend of (84) vanishes. So the region outside this hyperbola is all contained in the infeasible set, resulting in a zero R_{s1}. On the other hand, in the region inside both this hyperbola and the ellipse representing average power constraint (81), $\rho_1 = -1$ and the boundary of the infeasible set can be written as

$$\sigma_3^2 = \frac{(\sigma_{h1}^2 - \sigma_1\sigma_3)^2}{\sigma_{h1}^2 + \sigma_1^2 + \sigma_A^2},$$

or

$$(\sigma_{h1}^2 + \sigma_A^2)\sigma_3^2 + 2\sigma_{h1}^2\sigma_1\sigma_3 - \sigma_{h1}^4 = 0. \tag{85}$$

To simplify the analysis, we scale coordinates to make the ellipsoid (81) a sphere, i.e., setting $s_1^2 = \|\mathbf{S}_A\|^2\sigma_1^2, s_2^2 = \|\mathbf{S}_B\|^2\sigma_2^2, s_3^2 = \|\mathbf{S}_R\|^2\sigma_3^2$. Then, (85) becomes

$$\begin{aligned}&\frac{(\sigma_{h1}^2 + \sigma_A^2)}{\|\mathbf{S}_R\|^2}s_3^2 + \frac{2\sigma_{h1}^2}{\|\mathbf{S}_A\|\|\mathbf{S}_R\|}s_1s_3 - \sigma_{h1}^4 \\ &\quad\triangleq A_{33}s_3^2 + 2A_{13}s_1s_3 + C = 0.\end{aligned} \tag{86}$$

This is the boundary hyperbola outside of which is the infeasible set. This hyperbola has its center located at the origin and rotates counter-clockwise by an angle φ where $0 < \varphi < \pi/4$. Fig. 4 illustrates the relationship between the power constraint and the infeasible set. In the spherical coordinates the attacker's power on s_3-s_1 plane is $s_1^2 + s_3^2$. It is obvious that the smallest value of it within the boundary hyperbola is achieved at the vertex shown in Fig. 4. With the aid of analytic geometry, it can be calculated that φ satisfies

$$k_1 \triangleq \tan(2\varphi) = \frac{2A_{13}}{A_{33}} = \frac{2\sigma_{h1}^2}{\sigma_{h1}^2 + \sigma_A^2}\frac{\|\mathbf{S}_R\|}{\|\mathbf{S}_A\|}. \tag{87}$$

In other words, k_1 is the reciprocal of the slope of an asymptote of the boundary hyperbola. The semi-major axis a_1, i.e., the distance from the vertex to the origin, satisfies

$$a_1^2 = \frac{\sigma_{h1}^4}{\lambda_1} \tag{88}$$

where λ_1 is the positive eigenvalue of characteristic equation $\lambda_1^2 - A_{33}\lambda_1 - A_{13}^2 = 0$, i.e.,

$$\frac{1}{2}\left(\frac{\sigma_{h1}^2 + \sigma_A^2}{\|\mathbf{S}_R\|^2} + \sqrt{\frac{(\sigma_{h1}^2 + \sigma_A^2)^2}{\|\mathbf{S}_R\|^4} + \frac{4\sigma_{h1}^4}{\|\mathbf{S}_A\|^2\|\mathbf{S}_R\|^2}}\right). \tag{89}$$

Therefore, we obtain the optimal point (s_3, s_1) which achieves the minimal attack power in the infeasible set satisfying:

$$s_3^2 = (a_1\cos\varphi)^2 = \frac{a_1^2}{2}\left(1 + \frac{1}{\sqrt{1+k_1^2}}\right), \tag{90}$$

$$s_1^2 = (a_1\sin\varphi)^2 = \frac{a_1^2}{2}\left(1 - \frac{1}{\sqrt{1+k_1^2}}\right). \tag{91}$$

The analytic results of the Bob-relay side take the same form; we only need to replace 1 in all subscripts from (87) to (91) with 2 and σ_A^2 with $\sigma_B^2 = \sigma^2/\|\mathbf{S}_B\|^2$. In summary, we have the following lemma.

Lemma 1: If the attacker's power satisfies the following condition

$$P_E \geq \frac{1}{3}\min\{a_1^2, a_2^2\}, \tag{92}$$

then the key rate $R_s = 0$. Furthermore, if $a_1^2 \leq a_2^2$, then the attacker should choose

$$\sigma_3^2 = \frac{a_1^2}{2\|\mathbf{S}_R\|^2}\left(1 + \frac{1}{\sqrt{1+k_1^2}}\right), \tag{93}$$

$$\sigma_1^2 = \frac{a_1^2}{2\|\mathbf{S}_A\|^2}\left(1 - \frac{1}{\sqrt{1+k_1^2}}\right). \tag{94}$$

If $a_1^2 > a_2^2$, the attacker should choose (σ_3^2, σ_2^2) using a similar formula as above.

C. Optimal Attack Power Allocation

If P_E is smaller than the upper bound (92), shown by the smaller circle in Fig. 4, our protocol achieves a nonzero key rate. In this case, we need to solve the optimization problem (82) to fully characterize the attacker's optimal attack strategy. Since the problem is a min-min problem, we can solve it by finding minimum values of R_{s1} and R_{s2} separately, and then choose the smaller one. In the following we will focus on finding the minimum value of R_{s1}, because the procedure for R_{s2} is similar.

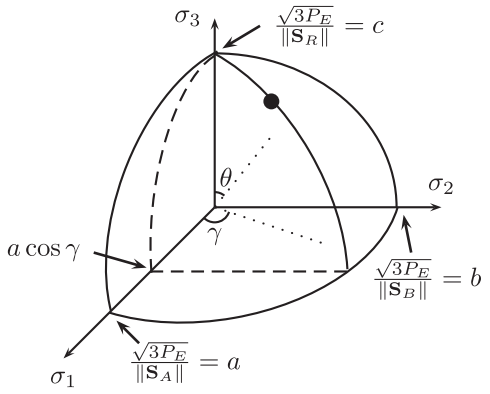


Fig. 5. Ellipsoid representing power constraint (81).

The attacker's power constraint ellipsoid determined by (81) is shown in Fig. 5. Using angular coordinates, we can express $\sigma_i, i = 1, 2, 3$ as follows:

$$\sigma_1 = a\cos\gamma\,\sin\theta, \tag{95}$$

$$\sigma_2 = b\sin\gamma\,\sin\theta, \tag{96}$$

$$\sigma_3 = c\cos\theta. \tag{97}$$

where $a = \sqrt{3P_E}/\|\mathbf{S}_A\|, b = \sqrt{3P_E}/\|\mathbf{S}_B\|, c = \sqrt{3P_E}/\|\mathbf{S}_R\|$ and $0 \le \theta, \gamma \le \frac{\pi}{2}$. Finding the optimal values of $\sigma_i, i = 1, 2, 3$ is equivalent to finding the optimal value of γ and θ.

To find the minimal R_{s1}, or the maximal σ_{e1}^2, which depends only on σ_1 and σ_3, we first fix γ, project the ellipsoidal section to the σ_1-σ_3 plane and find the optimal θ that maximizes σ_{e1}^2 under the given γ. Next we find the global minimal R_{s1} among all valid γ's and compare it with the global minimal R_{s2} derived using the same approach, to determine the final minimal R_s.

We know from (74) that the hyperbola $\sigma_{h1}^2 = \sigma_1\sigma_3$ determines the value of ρ_1. However, as shown in the analysis, this hyperbola is completely contained in the infeasible set. So for the region inside the projected ellipse, we know that $\rho_1 = -1$, and σ_{e1}^2 is determined by

$$\left(\sigma_{h1}^2 + \sigma_3^2 + \frac{\sigma^2}{\|\mathbf{S}_R\|^2}\right) - \frac{(\sigma_{h1}^2 - \sigma_1\sigma_3)^2}{\sigma_{h1}^2 + \sigma_1^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2}}. \tag{98}$$

It can be easily seen that, for a fixed σ_1, the larger the value of σ_3, the larger the value of σ_{e1}^2. As a result, the maximal value is achieved at the boundary of the ellipse (and therefore we only need to search for the maximum on the surface of the ellipsoid). Motivated by this observation, we next compute the maximal point on the ellipse.

Plugging the angularly parameterized σ_1 and σ_3 into (98) and differentiating it with respect to θ, the numerator of the derivative has the form

$$A\cos\Theta - B\sin\Theta - C \tag{99}$$

where

$$A = ac\sigma_{h1}^2\cos\gamma\left(\sigma_{h1}^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2} + \frac{a^2}{2}\cos^2\gamma\right) \tag{100}$$

$$= ac\sigma_{h1}^2\cos\gamma\left(\sigma_{h1}^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2}\right) + C, \tag{101}$$

$$B = \frac{a^2}{2}\cos^2\gamma\left[c^2\left(\sigma_{h1}^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2}\right) - \sigma_{h1}^4\right] + \frac{c^2}{2}\left(\sigma_{h1}^2 + \frac{\sigma^2}{\|\mathbf{S}_A\|^2}\right)^2, \tag{102}$$

$$C = \frac{a^3c}{2}\sigma_{h1}^2\cos^3\gamma, \tag{103}$$

and $\Theta = 2\theta$ that ranges from 0 to π. Note that A and C are both positive while B may be negative. The optimal value of θ can be found by setting (99) to zero.

Thus, (99) can be written as

$$\sqrt{A^2 + B^2}\sin(\alpha - \Theta) - C \tag{104}$$

where α satisfies $\tan\alpha = \frac{A}{B}$. Hence $0 < \alpha \le \frac{\pi}{2}$ if $B \ge 0$. However, if $B < 0$, $\frac{\pi}{2} < \alpha < \pi$, so $\alpha = \pi + \arctan A/B$.

From (101), we have $\sin\alpha = \frac{|\tan\alpha|}{\sqrt{1+\tan^2\alpha}} = \frac{A/|B|}{\sqrt{1+A^2/B^2}} = \frac{A}{A^2+B^2} \ge \frac{C}{A^2+B^2}$. Therefore, the equation

$$A\cos\Theta - B\sin\Theta - C = 0 \tag{105}$$

always has a unique solution

$$\Theta = \alpha - \arcsin\frac{C}{\sqrt{A^2 + B^2}}$$

for Θ in $[0, \pi]$. In summary, we have the following lemma regarding the optimal value of θ.

Lemma 2: For any $\gamma \in [0, \frac{\pi}{2}]$, the optimal value of θ that minimizes R_{s1} is

$$\theta = \begin{cases} \frac{1}{2}\left(\arctan\frac{A}{B} - \arcsin\frac{C}{\sqrt{A^2+B^2}}\right), & B \ge 0 \\ \frac{1}{2}\left(\pi + \arctan\frac{A}{B} - \arcsin\frac{C}{\sqrt{A^2+B^2}}\right), & B < 0. \end{cases} \tag{106}$$

Fig. 6 illustrates the relationship between α and Θ when B is positive and negative, respectively. From this figure, we can see that, when $B \ge 0$, the optimal point will have $\theta \le \frac{\pi}{4}$.

To find the maximal σ_{e2}^2, we need to project ellipsoidal section under angle γ to the σ_2-σ_3 plane (this is equivalent to setting σ_1 to zero), and then conduct the same analysis as above. The results are the same as in the σ_1-σ_3 plane, except for substituting b for a and $\sin\gamma$ for $\cos\gamma$ in formulas (100)-(103). Observe that regardless of whether Eve's average power P_E exceeds the upper bound (92), the covariance coefficients $\rho_i, i = 1, 2$, are always -1 when Eve generates optimal interference signal.

V. Simulation Results

In this section, we present various simulation results to illustrate the analytical results derived in this paper.

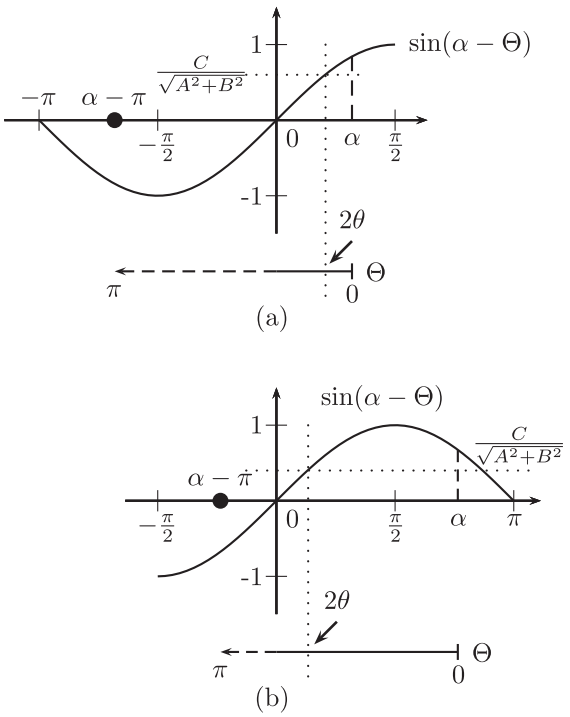


Fig. 6. Relations between α and Θ. (a) $B \geq 0, 0 < \alpha \leq \frac{\pi}{2}$. (b) $B < 0$, $\frac{\pi}{2} < \alpha < \pi$.

TABLE I
VALUES OF $\sigma_{1,i}^2$ AND $\sigma_{2,i}^2, i = 1, \ldots, N$ USED IN GENERATING FIG. 7

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

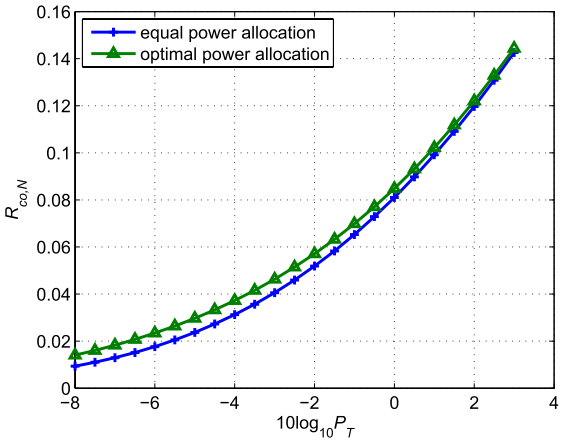


Fig. 7. Key rates of our algorithms versus P_T.

TABLE II
SIMULATION RESULTS WHEN THE TOTAL POWER FOR RELAY $P = 13.5$

	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 III
VALUES $\sigma_{1,i}^2$ AND $\sigma_{2,i}^2, i = 1, \ldots, N$ USED IN GENERATING FIGS. 8 AND 9

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

A. Simulations for the Passive Eavesdropper Case

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 $P = \sum_{i=1}^{N} P_i = NP_T$ (see (31), (45)); the channel coherence time $T = 14$. Note that in this case, we have $T_0 = \frac{T}{N+2} = 2$. Fig. 7 shows the key rate $R_{co,N}$ defined in (28) for the case of optimal power allocation described in Section III-B and for 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 ease of comparison, simulation results for the equal power distribution are also included in the table. Since the results of Case 2 violate (58), it is discarded; so the optimal key rate is achieved in Case 1, i.e. $4.9681/(2T) = 0.1774$ nat.

From Fig. 7, 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 performance improvement using the power optimization is limited, which is also reflected in Table II. This phenomenon can be explained by examining (56). When P_T is large, the difference between the individual P_i's due to the different values of $\sigma^2/\sigma_{1,i}^2 T_0$ is negligible. As a consequence, the resulting mutual information is close to that of equal power distribution. The same argument applies if T is sufficiently large in which $\sigma^2/\sigma_{1,i}^2 T_0$ becomes very small, making the differences of P_i negligible.

In the following, we compare the key rate of our algorithms with that of the AF with AN algorithm in [14] 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 [20]. The variances of the fading coefficients of all channels are listed in Table III. Other simulation parameters are $\sigma^2 = 0.01, P_A = P_B = P_T$. We consider two different scenarios. The first one, a scalar version, is carried out with a scalar training signal, namely, the length of all training sequences, T_0, is 1. This is the scheme used in [14]. The second one, a sequence version, is performed with $T = 308$, or $T_0 = 44$, to show the effects of the training sequences instead of a single training symbol against the channel noise. Fig. 8 shows the key rates in the scalar version and Fig. 9 illustrates the key rates in the sequence version. Both figures show that our algorithms for the two-way relay with multiple antennas greatly outperform the AF with AN algorithm, primarily because our scheme exploits the random channels associated with all antennas while the latter makes use of only one randomly selected antenna in the relay.

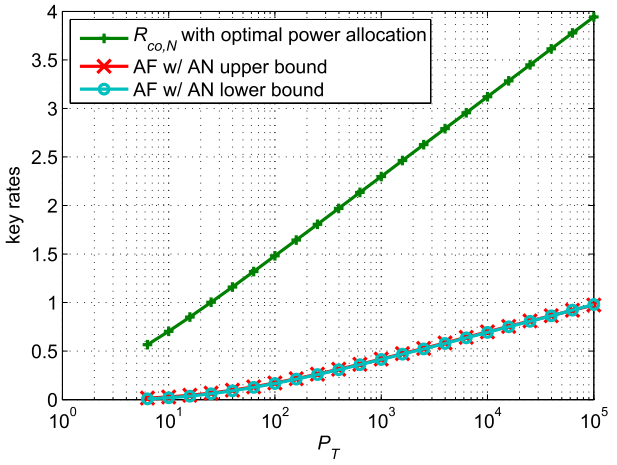


Fig. 8. Key rates versus P_T in the scalar version.

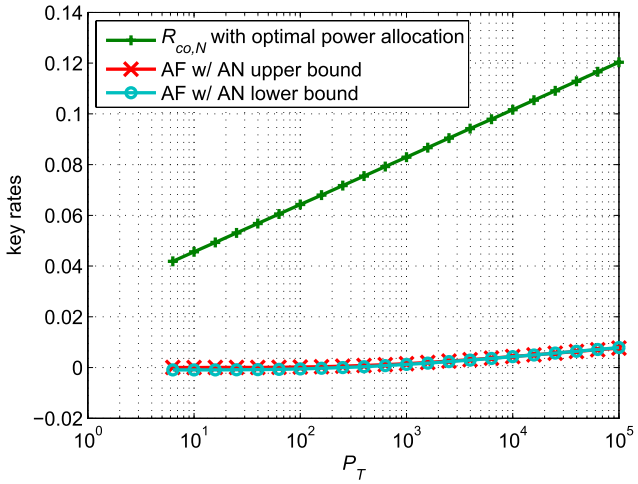


Fig. 9. Key rates versus P_T in the sequence version.

In addition, the key rates of our algorithms have a much better performance over AF with AN in the sequence version than in the scalar version, showing that the use of training sequences in our algorithms successfully suppress the harmful effects of channel noise (see, e.g., (23)).

B. Simulations for the Active Attacker Case

We compare the key rates of our protocol when the attacker employs optimal power allocation and equal power allocation. We also illustrate the smallest power in infeasible set, which is equivalent to the maximum attacker's power that our protocol can tolerate. If Eve's attacking power is distributed equally, i.e.,

$$\sigma_1^2\|\mathbf{S}_A\|^2 = \sigma_2^2\|\mathbf{S}_B\|^2 = \sigma_3^2\|\mathbf{S}_R\|^2 = P_E, \qquad (107)$$

we can solve each $\sigma_i, i = 1, 2, 3$, and calculate the key rate using formulas in Sec. IV. Here we let training sequence energies $\|\mathbf{S}_A\|^2$, $\|\mathbf{S}_B\|^2$ and $\|\mathbf{S}_R\|^2$ identically take values in a range from 1 to 10000. Other parameters are: average attacker's power P_E is 0.3333; $\sigma^2 = 0.1$; $\sigma_{h1}^2 = 0.3$; $\sigma_{h2}^2 = 0.5$ and $T = 99$. The minimal key rates R_s corresponding to these training energies are depicted in the upper subplot of Fig. 10. The lower subplot shows the minimal average power Eve uses

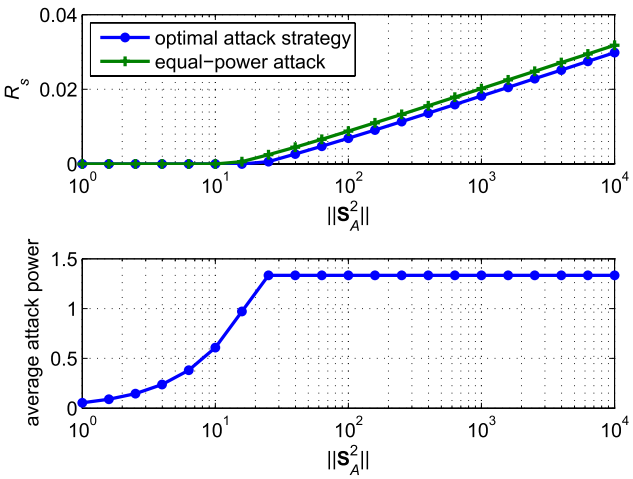


Fig. 10. Comparison of key rates under the optimal attack strategy and the equal power attack strategy versus the legitimate user's transmission power $\|\mathbf{S}_A\|^2 = \|\mathbf{S}_B\|^2 = \|\mathbf{S}_R\|^2$, as well as the minimal average attack power.

to achieve the corresponding key rate, which when $R_s = 0$, is $\min\{a_1^2, a_2^2\}/3$.

In Fig. 10, it is clear that the key rates with the optimized power allocation for the attacker is smaller than those under the equal power allocation. In addition, with an increased power of the legitimate users, the key rates increase.

VI. Conclusion

We have considered the key generation problem in the two-way relay 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 investigated the effects of an active attacker on the proposed key generation protocol. We have characterized the optimal attacker's strategy that minimizes the key rate of the proposed scheme and have established the maximal attacker's power under which our scheme can still achieve a non-zero key rate.

References

[1] H. Zhou, L. Huie, and L. Lai, "Key generation in two-way relay wireless channels," in *Proc. 17th Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2013, pp. 1–6.

[2] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[3] 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. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[4] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

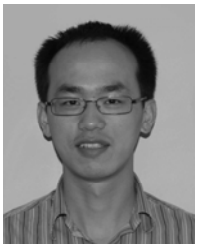
[5] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2518–2522.

[6] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, Las Vegas, NV, USA, Apr. 2008, pp. 3031–3016.

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.
[8] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared key generation in wireless networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1–9.
[9] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 1422–1430.
[10] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.
[11] A. Khisti, "Interactive secret key generation over reciprocal fading channels," in *Proc. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Oct. 2012, pp. 1–8.
[12] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[13] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
[14] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 650–660, Sep. 2011.
[15] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless network," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.
[16] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, May 2005.
[17] C. E. Shannon, "Communication theory of secrecy systems," *Bell. Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.
[19] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[20] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, p. 066138, Jun. 2004.

Heng Zhou received the B.E. degree from the Huazhong University of Science and Technology and the M.E. degree from the Nanjing University of Posts and Telecommunications. His research interests include information theory and information theoretic security.

Lauren M. Huie (S'05–M'11) received the B.S. degree in electrical engineering from the State University of New York at Binghamton in 2005, and the M.S. degree in electrical engineering from The Pennsylvania State University in 2007. She was a member of the Wireless Communications and Networking Laboratory. She received the Ph.D. degree from the State University of New York at Binghamton in 2013. Her current research interests include sensor networks, estimation and detection theory, and physical layer security. She is currently with the Air Force Research Laboratory Information Directorate, Rome, NY, USA.



Lifeng Lai (M'07) received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China, in 2001 and 2004, respectively, and the Ph.D. degree from The Ohio State University, Columbus, OH, USA, in 2007. He was a Postdoctoral Research Associate with Princeton University from 2007 to 2009, and was an Assistant Professor with the University of Arkansas, Little Rock, from 2009 to 2012. Since 2012, he has been an Assistant Professor with the Worcester Polytechnic Institute. His research interests include information theory, stochastic signal processing and their applications in wireless communications, security, and other related areas. He was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He is a corecipient of the Best Paper Award from the IEEE Global Communications Conference in 2008, the Best Paper Award from the IEEE Conference on Communications in 2011, and the Best Paper Award from the IEEE Smart Grid Communications in 2012. He received the National Science Foundation CAREER Award in 2011 and the Northrop Young Researcher Award in 2012. He served as a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS SPECIAL ISSUE ON SIGNAL PROCESSING TECHNIQUES FOR WIRELESS PHYSICAL LAYER SECURITY. He is currently serving as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.