Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness

Tzu-Han Chou
Electrical and Computer Engineering
University of Wisconsin
Madison, WI 53706, USA
email: tchou2@wisc.edu

Akbar M. Sayeed
Electrical and Computer Engineering
University of Wisconsin
Madison, WI 53706, USA
email: akbar@engr.wisc.edu

Stark C. Draper
Electrical and Computer Engineering
University of Wisconsin
Madison, WI 53706, USA
email: sdraper@ece.wisc.edu

***Abstract*—We study secret key generation from reciprocal multipath wireless channels modeled as multiple parallel fading channels. We consider two channel characteristics that heavily impact secret key capacity: channel sparsity and correlation between main and eavesdropper's channels. We propose a model of channel sparsity where the fraction of subchannels with non-zero coefficients is specified by a sparsity parameter ρ. For sparse channels without eavesdroppers we show that at each transmitter SNR γ there is an optimal sparsity $0 \leq \rho_{\rm opt} \leq 1$ that yields the maximum secret key capacity.**

The reduction in secret key capacity due to eavesdropping is due to two sources. First is the overlap between the main and eavesdropper channels, i.e., the pattern of non-zero subchannels common to both. The second is the correlation between the channel coefficients of the overlapping channels. We propose a model that captures these two effects, and characterize the impact of each by studying achieveable secret key rates.

We show that when the power of the training signal is uniformly distributed over the non-vanishing channels, there is a cutoff SNR γ_c below which the secret key rate is zero, but non-zero (and increasing in γ) when $\gamma > \gamma_c$. We also show that in the low SNR regime, the optimal input signal is peaky (a non-uniform training signal) by which the secret key capacity is non-zero at all $\gamma > 0$.

I. Introduction

Secure transmission of private message over an open channel is a critical issue in wireless communication due to the broadcast nature of wireless. Two approaches to physical layer secure transmission have drawn much attention in recent years. One approach is transmission over the wiretap channel [1], [2]. The other approach, which we focus on in this paper, is secret key generation from correlated sources of randomness [3], [4].

Two issues arise in implementing key generation from common randomness. The first is the design of a protocol between legitimate users Alice and Bob so that the key can be generated secretly and reliably. When discussion over an error-free public channel (reconciliation) is allowed, [3], [4] show that though distributed source coding techniques [5] Alice and Bob can generate a common key at a non-zero rate while leaking negligible information to an eavesdropper Eve. The supremum of achievable secret key rates is the *secret key capacity*.

The second issue is identifying an accessible and appropriate source of correlated randomness. The channel coefficients due to multipath fading in wireless communication is a widely available source of randomness. We focus on the case where transmission is reciprocal, e.g., as in time-division duplexing in the same frequency band. In such a case, when the coherence time is sufficiently long, the reciprocity ensures that both users see the same channel (complex gains and delays). This source of common randomness appears particularly well suited to key generation as in rich scattering environments channel gains vary rapidly in space. Thus, an eavesdropper who is located a few wavelengths from either Alice or Bob will observe, more-or-less, uncorrelated channel gains, ensuring the secrecy of the key.

However, recent measurement campaigns [6] and theoretical work [7] demonstrate that wireless channels are often *sparse*. Such sparsity leads to increased correlation between Eve's observations and Alice's and Bob's, undercutting security guarantees, and reducing secret key capacity. The impact of channel sparsity on secret key capacity is the focus of this paper.

II. Background and prior work

In generating secret keys from channel randomness, sounding signals D_a^n and D_b^n must be transmitted by Alice and Bob, respectively, to excite the channel. Due to our assumption of a reciprocal channel law, we are in a symmetric setting, and the simplifying assumption of a single sounding signal $D_a^n = D_b^n = D^n$ can be made. The main difference from [3], [4] is the design of this sounding signal. In [8] we show the the secret key capacity of a memoryless channel $p_{X^n,Y^n,Z^n|D^n}(x^n, y^n, z^n|d^n) = \prod_{i=1}^n p_{X,Y,Z|D}(x_i, y_i, z_i|d_i)$ is

$$C_{\rm key} = \max_{P_D \in \Omega_D} |I(X;Y|D) - I(X;Z|D)|^+ \qquad (1)$$

where (i) $|x|^+ = \max\{x, 0\}$, (ii) X, Y, Z represent the observations of Alice, Bob and Eve, respectively, (iii) the maximization is taken over the input distribution that satisfies the power constraint $\Omega_D = \{P_D : E[|D|^2] \leq \mathcal{E}\}$.

Regarding previous work on secret key generation from multipath fading, [9], [10] consider straight quantization of the phase difference of channel outputs, but do not including the de-noising effect of the public discussion of [3], [4]. On the other hand, [9] applies coding to reduce the error probability while [10] analyzes the minimum energy required for key acquisition. Further, [11] considers ultrawideband channels where the amplitude of time delay channel serves as the source of randomness. Regarding generic Gaussian models, [12], [13] study key generation from jointly Gaussian sources where LDPC coding is used in [12] and [13] uses nested lattice codes and vector quantization for de-noising. Finally, [14] discusses the minimum energy per secret key bit and shows that the optimal input distribution P_D is peaky in the low SNR regime.

All this prior work is subject to the assumption that the eavesdropper channel is statistically independent of the main channel. Thus, the penalty term in (1), due to the correlated eavesdropper observation, is zero. On the other hand, in this paper, we propose models of channel sparsity and eavesdropper correlation and quantify the impact on secret key capacity.

III. Modeling of main and eavesdropper channels

Consider a wireless system consisting of n independent parallel fading channels. To generate a secret key from a reciprocal wireless channel, Alice and Bob each send a training sequence through the channel. Suppose the channel is static over two uses of the channel. The channel outputs on i-th subchannel are

$$\begin{aligned} X(i) &= h_a(i)d(i) + N_a(i) \\ Y(i) &= h_b(i)d(i) + N_b(i) \\ Z_1(i) &= h_{e_1}(i)d(i) + N_{e_1}(i) \\ Z_2(i) &= h_{e_2}(i)d(i) + N_{e_2}(i) \end{aligned}$$

where $X(i)$, $Y(i)$, $i = 1, \cdots, n$, are the channel outputs for Alice and Bob, respectively. The channel coefficient of the ith subchannel is $h_a(i) = h_b(i) = h(i)$ and $d(i)$ is the training symbol transmitted over that subchannel.

Eve has two observations $Z_1(i)$, $Z_2(i)$ corresponding to the respective channel outputs when Alice and Bob send training symbols. Finally, N_a, N_b, N_{e_j}, for $j = 1, 2$ are independent and identically distributed (i.i.d.) random variables $\mathcal{CN}\left(0, \sigma_n^2\right)$ corresponding to observation noise.

Based on the correlated observations of X and Y, the number of key bits that Alice and Bob can generate while keeping Eve in the dark depends on how much information about h Eve can deduce based on her observations Z_1, Z_2 and the public message.

A. Modelling channel sparsity

For channels that exhibits sparsity, the physical paths are clustered in a fractional dimension represented by the basis functions (e.g., time delays) [7]. Among n subchannels, let ρn subchannels have non-vanishing independent channel coefficients. Let $\mathcal{S}_{ab} = \{i : E[|h(i)|^2] > 0\}$ denotes the *sparsity pattern* (SP) of the main channel where $|\mathcal{S}_{ab}| = \rho n$. $\mathcal{S}_{ae_1}$ and $\mathcal{S}_{ae_2}$ are defined similarly for Eve's channels and $|\mathcal{S}_{ae_1}| = |\mathcal{S}_{ae_2}| = \rho n$ for the same parameter ρ. We assume that $\Pr[i \in \mathcal{S}_{av}] = \rho$ for all i where i is the index of a particular sub-channel.

B. Correlation between sparsity patterns

We introduce parameters q_1, q_2 to characterize the overlap between the sparsity patterns of the main and eavesdropper channels. In particular

$$\begin{aligned} \Pr(i \in \mathcal{S}_{ae_1} | i \in \mathcal{S}_{ab}) &= q_1 & \text{(2a)} \\ \Pr(i \in \mathcal{S}_{ae_2} | i \in \mathcal{S}_{ab}) &= q_2 & \text{(2b)} \end{aligned}$$

for all $1 \leq i \leq n$.

C. Correlation between channel coefficients

We model the correlation between overlapped channel coefficients as

$$\begin{aligned} h_{e_1} &= \lambda_1 h + \sqrt{1-\lambda_1^2}\hat{h}_{e_1} \ , & \text{(3a)} \\ h_{e_2} &= \lambda_2 h + \sqrt{1-\lambda_2^2}\hat{h}_{e_2} \ . & \text{(3b)} \end{aligned}$$

where h, $\hat{h}_{e_1}$, $\hat{h}_{e_2}$ are i.i.d. $\mathcal{CN}\left(0, \sigma^2\right)$. Eve's channel coefficients consist of two parts: one perfectly correlated with the main channel h and another that is uncorrelated with h. The correlation coefficient between h_{e_1} (resp. h_{e_2}) and h is

$$\frac{E[h_{e_j} h^*]}{\sqrt{E[|h_{e_j}|^2] E[|h|^2]}} = \lambda_j \ , \quad \text{for } j = 1, 2.$$

where $0 \leq \lambda_1 \leq 1$ (resp. λ_2). To simplify the problem, we assume that for all subchannels $i \in \mathcal{S}_{ab} \cap \mathcal{S}_{ae_j}$, $h(i)$ and $h_{e_j}(i)$ have the same λ_j for $j = 1, 2$.

We now express the channel coefficients in matrix form

$$\begin{bmatrix} h_a \\ h_b \\ h_{e_1} \\ h_{e_2} \end{bmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ \lambda_1 & \sqrt{1-\lambda_1^2} & 0 \\ \lambda_2 & 0 & \sqrt{1-\lambda_2^2} \end{pmatrix}}_{\mathbf{A}} \begin{bmatrix} h \\ \hat{h}_{e_1} \\ \hat{h}_{e_2} \end{bmatrix} .$$

For a deterministic input training symbol $D = d$ (i.e., $D = d$ with probability one), the channel outputs are

$$\begin{bmatrix} X \\ Y \\ Z_1 \\ Z_2 \end{bmatrix} = d\mathbf{A} \begin{bmatrix} h \\ \hat{h}_{e_1} \\ \hat{h}_{e_2} \end{bmatrix} + \begin{bmatrix} N_a \\ N_b \\ N_{e_1} \\ N_{e_2} \end{bmatrix} \quad \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{K}_{xy\mathbf{z}}\right) \quad (4)$$

where

$$\begin{aligned} &\mathbf{K}_{xy\mathbf{z}} = \mathcal{E}\sigma^2 \mathbf{A}\mathbf{A}^H + \sigma_n^2 \mathbf{I} \\ &= \sigma_n^2 \begin{pmatrix} 1+\sigma^2\gamma & \sigma^2\gamma & \lambda_1\sigma^2\gamma & \lambda_2\sigma^2\gamma \\ \sigma^2\gamma & 1+\sigma^2\gamma & \lambda_1\sigma^2\gamma & \lambda_2\sigma^2\gamma \\ \lambda_1\sigma^2\gamma & \lambda_1\sigma^2\gamma & 1+\sigma^2\gamma & \lambda_1\lambda_2\sigma^2\gamma \\ \lambda_2\sigma^2\gamma & \lambda_2\sigma^2\gamma & \lambda_1\lambda_2\sigma^2\gamma & 1+\sigma^2\gamma \end{pmatrix} \end{aligned}$$

$\mathcal{E} = |d|^2$ is the training symbol power and $\gamma = \frac{\mathcal{E}}{\sigma_n^2}$ is the transmitted SNR.

IV. Secret Key Capacity of Parallel Fading Channels

To quantify the secret key capacity and the optimal input distribution, we first consider the secret key rate with deterministic training signaling and define following functions: $I_{ab}(\sigma^2\gamma) \triangleq I(X;Y|d)$, $I_{ae_j}(\sigma^2\gamma) \triangleq I(X;Z_j|d)$, for $j = 1, 2$, and $I_{ae_1e_2}(\sigma^2\gamma) \triangleq I(X;Z_1Z_2|d)$. For the Gaussian model in (4), these functions can be expressed in terms of λ_1, λ_2 and received SNR $\sigma^2\gamma$. The secret key capacity is found by optimizing over the input distribution P_D subject to power constraint. In most cases, Alice/Bob can learn the sparsity pattern of the main channel by an additional measurement [15] but not the sparsity patterns of Eve's channels. With $\mathcal{S}_{ab}$ information, the total training signal power is distributed to $|\mathcal{S}_{ab}| = \rho n$ dimensions so that the transmitted SNR in each non-vanishing dimension is increased by a factor $1/\rho$. Since there is no knowledge of Eve's sparsity patterns, the realization of $\mathcal{S}_{ae_1}$ and $\mathcal{S}_{ae_2}$ becomes the unknown *state* of the system. The achievable key rate per dimension is, averaging over all states,

$$\begin{aligned} R_{\text{key}}(\gamma) &= (1-q_1)(1-q_2)\rho I_{ab}\left(\frac{\sigma^2\gamma}{\rho}\right) \\ &\quad + q_1(1-q_2)\rho\left(I_{ab}\left(\frac{\sigma^2\gamma}{\rho}\right) - I_{ae_1}\left(\frac{\sigma^2\gamma}{\rho}\right)\right) \\ &\quad + (1-q_1)q_2\rho\left(I_{ab}\left(\frac{\sigma^2\gamma}{\rho}\right) - I_{ae_2}\left(\frac{\sigma^2\gamma}{\rho}\right)\right) \\ &\quad + q_1q_2\rho\left|I_{ab}\left(\frac{\sigma^2\gamma}{\rho}\right) - I_{ae_1e_2}\left(\frac{\sigma^2\gamma}{\rho}\right)\right|^+ . \end{aligned} \quad (5)$$

In the following, we first look the case without an eavesdropper to investigate the effect of channel sparsity. Two possible channel normalizations are discussed, $\sigma^2 = 1$ and $\sigma^2 = 1/\rho$. Each normalization corresponds to a way in which the sparse channel can be formed. In Sec. V we give examples to show that both cases are physically possible. In the first case, rich ($\rho = 1$) and sparse ($\rho < 1$) channels, respectively correspond to two physical channels with different delay spreads represented in a system with fixed signal bandwidth. The second case correspond to the same physical channel represented by signals with different bandwidths.

We then look at the case where there is an eavesdropper present and study the impact of channel coefficient correlation (λ_1, λ_2) and sparsity correlation (q_1, q_2). Finally, the optimal input distribution needed to find the secret key capacity is discussed.

A. Secret Key Capacity without Eavesdropper

1) Rich fading channels: Without the loss of generality, assume that in rich channels ($\rho = 1$), the power of each subchannel is normalized to $\sigma^2 = 1$. In [14] it is shown that for a deterministic signaling d, the achievable secret key function $R_{\text{key}}(\gamma) = I_{ab}(\gamma)$ is convex-up at low SNR and convex-down at high SNR. It also shows that for any γ, the capacity achieving input training signal with $E[|D|^2] \leq \mathcal{E}$ has distribution

$$P_D = \begin{cases} \mu^*, & D = d \\ 1-\mu^*, & D = 0 \end{cases} , \quad (6)$$

where $\mu^* = \min(1, \gamma/\gamma^*)$ and γ^* is the positive root of

$$I_{ab}(\gamma) = \gamma \cdot \frac{dI_{ab}(\gamma)}{d\gamma} , \quad (7)$$

which can be solved for numerically. When $\gamma \geq \gamma^*$, $\mu^* = 1$, the optimal input is deterministic and therefore has a uniform power distribution over n channels. When $\gamma < \gamma^*$, the optimal input is a type of peaky on-off signaling, cf. (6). The resulting secret key capacity per channel degree of freedom (DoF)

$$C_{\text{key}}(\gamma) = \mu^* I_{ab}\left(\frac{\gamma}{\mu^*}\right) \quad (8)$$

is a convex-down function.

2) Sparse channels: From the first term of (5), when $q_1 = q_2 = 0$, the achievable key rate for $\rho < 1$ is

$$R_{\text{key}}(\gamma) = \rho I_{ab}\left(\frac{\sigma^2\gamma}{\rho}\right) \quad (9)$$

Due to the convexity of $I_{ab}(\cdot)$ in low SNR, there is an optimal *operating sparsity* ρ_{opt} at which the deterministic signaling has the highest rate. To characterize ρ_{opt}, two channel normalization σ^2, which affect received SNR, are considered:

(i) Case $\sigma^2 = 1$: From the similarity between (9) and (8), we can get $\rho_{\text{opt}} = \min(1, \gamma/\gamma^*)$ where γ^* is the solution of (7). The signal with power distributing over the non-vanishing dimension ρn is equivalent to the peaky signal in (6) (where $\mu^* = \rho_{\text{opt}}$). Thus, the key rate that ρ_{opt} can achieved is the same as (8) and, therefore, is the secret key capacity. Fig. 1(a) shows $R_{\text{key}}(\gamma)$ for various ρ and the curve corresponding ρ_{opt}. Fig. 1(c) shows ρ_{opt} as function of SNR.

(ii) Case $\sigma^2 = 1/\rho$: This is the case that the total channel power is preserved when the channel DoF decreases. The optimal operating sparsity is obtained by maximizing (9)

$$\rho_{\text{opt}} = \arg\max_{0\leq\rho\leq1} \rho I_{ab}\left(\frac{\gamma}{\rho^2}\right).$$

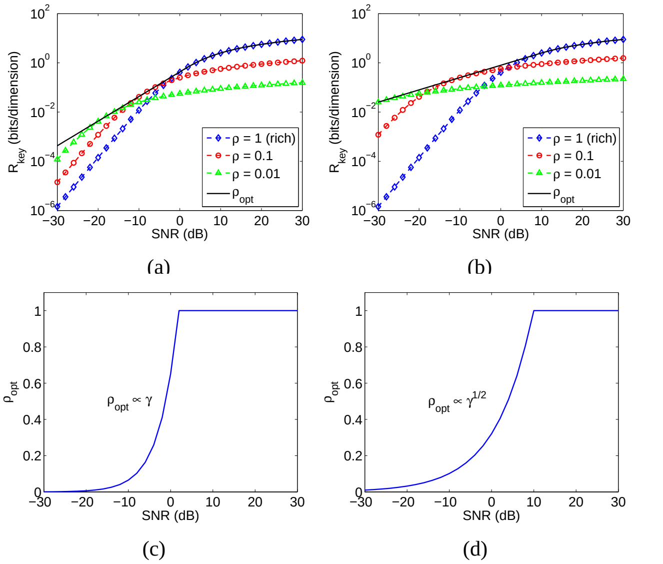
Take the derivative with respect to ρ to find the stationary point, we have

$$\rho_{\text{opt}} = \min\left(1, \left(\frac{\gamma}{\gamma^*}\right)^{\frac{1}{2}}\right) \quad (10)$$

where γ^* is the solution of the equation

$$I_{ab}(\gamma) = 2\gamma \cdot \frac{dI_{ab}(\gamma)}{d\gamma} . \quad (11)$$

Substituting into (9), the resulting secret key is convex-up function and is proportional to $\gamma^{1/2}$ for $\gamma < \gamma^*$. Fig. 1(b) and 1(d) show these results. Comparing with $\sigma^2 = 1$, the received SNR in this case is increased by $1/\rho$ due to the channel power conservation. ρ_{opt} in (10) is the optimal trade-off between the DoF ($\rho < 1$) and the received SNR



(a)

(b)

(c)

(d)

Fig. 1. Secret key rate of sparse channel. (a) R_{key} for $\sigma^2 = 1$ (b) R_{key} for $\sigma^2 = 1/\rho$ (c) ρ_{opt} for $\sigma^2 = 1$ (d) ρ_{opt} for $\sigma^2 = 1/\rho$

per DoF which consists of transmitted SNR ($\propto \gamma/\rho$) and channel power ($\propto 1/\rho$). The result is pronounced in low SNR (the power-limited regime). In Sec. V, we show that the sparse channel corresponding to $\sigma^2 = 1/\rho$ can be obtained by controlling signal bandwidth. Therefore, the secret key rate corresponding to ρ_{opt} (10) is achievable.

B. Secret key capacity with eavesdropper

1) Impact of channel coefficient correlation: Look the last term of (5) which captures the effect of channel coefficient correlation (λ_1, λ_2). This corresponds to the case that $\mathcal{S}_{ae_j}$, $j = 1, 2$, fully overlaps with $\mathcal{S}_{ab}$ (i.e.,$q_1 = q_2 = 1$). The loss term due to the presence of an eavesdropper can be approximated as

$$\rho I_{ae_1e_2}\left(\frac{\sigma^2\gamma}{\rho}\right) \approx \begin{cases} \rho\log\left(\frac{1-\lambda_1^2\lambda_2^2}{(1-\lambda_1^2)(1-\lambda_2^2)}\right), & \text{High SNR}\\ (\lambda_1^2+\lambda_2^2)\frac{(\sigma^2\gamma)^2}{\rho}, & \text{Low SNR}\end{cases}$$

Note that in high SNR, the loss is limited (it does not increase in γ) as long as λ_1 and λ_2 are both strictly less than one. This can be explained by looking (3) and (4), Eve has two types of noise regarding estimating h. One is the observation noise N_{e_j}, the other is the uncorrelated source $\hat{h}_{e_j}$. In high SNR, the N_{e_j} is negligible while $\hat{h}_{e_j}$ is amplified by the training symbol power. This limits the information about h that Eve can learn. We have secret key rate in both regimes

$$R_{\text{key}}(\gamma)\approx\begin{cases}\rho\left|\log\left(\frac{(1-\lambda_1^2)(1-\lambda_2^2)}{(1-\lambda_1^2\lambda_2^2)}\frac{\sigma^2\gamma}{2\rho}\right)\right|^+, & \text{High SNR}\\ \left|1-(\lambda_1^2+\lambda_2^2)\right|^+\frac{(\sigma^2\gamma)^2}{\rho}, & \text{Low SNR}\end{cases}$$

Fig. 2 shows the key rate in the presence of Eve when $\rho = 1$, $\sigma^2 = 1$ and $\lambda_1 = \lambda_2 = \lambda$. We can see that for large λ, there is a cutoff SNR γ_c so that $R_{\text{key}} = 0$ for $\gamma < \gamma_c$. The next proposition quantifies the relationship of λ_1, λ_2 and γ_c

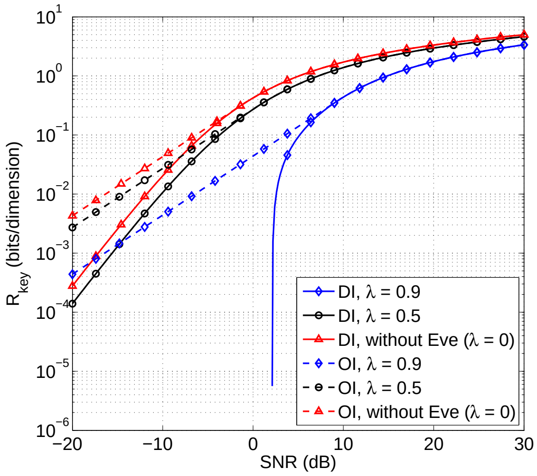


Fig. 2. Secret key rate with correlated eavesdropper. $(q_1, q_2) = (1, 1)$, $\rho = 1$, $\lambda_1 = \lambda_2 = \lambda$, $\sigma^2 = 1$. DI="Deterministic Input", OI="Optimal Input"

Proposition 1: When the total training signal power is uniformly distributed over the non-zero channels,

$$\gamma_c=\begin{cases}0, & \text{if } \lambda_1^2+\lambda_2^2\le 1\\ \frac{\rho}{\sigma^2}\left(\frac{\lambda_1\lambda_2}{\sqrt{(1-\lambda_1^2)(1-\lambda_2^2)}}-1\right), & \text{if } \lambda_1^2+\lambda_2^2>1\end{cases}.$$

The proof is by finding the root of $I_{ab}(\frac{\sigma^2\gamma}{\rho}) - I_{ae_1e_2}(\frac{\sigma^2\gamma}{\rho})$.

2) Impact of sparsity pattern correlation: From (5), R_{key} consists of four terms that correspond to the secret key rate in four different states. Different state have different level of secret key rate loss. Among the main channel DoF ρn, (q_1, q_2) captures the number of DoF in each state. Thus, the sparsity pattern correlation characterizes the effective DoF that Alice and Bob can exploit.

3) Optimal input distribution: From previous discussions, we know that when the channel power normalization is $\sigma^2 = 1$ the R_{key} is restricted if $\gamma < \gamma_c$. On the other hand, the peaky signaling (6) is the capacity achieving input distribution and the improvement is significant in the low SNR. It can be shown that each term of (5) is convex-up in the low SNR and convex-down in the high SNR. So the linear combination $R_{\text{key}}(\gamma)$ has the same property. In additional to $\mathcal{S}_{ab}$, if Alice/Bob know the parameters (λ_1, λ_2) and (q_1, q_2), they can find an optimal μ^*-peaky signaling by solving the optimization $\mu^* = \arg\max_\mu \mu R_{\text{key}}(\frac{\gamma}{\mu})$. Then μ^* is the root of an equation similar to (7) by replacing $I_{ab}(\cdot)$ with $R_{\text{key}}(\cdot)$ where γ, ρ, (λ_1, λ_2) and (q_1, q_2) are involved. Solving μ^* numerically, we get the non-zero secret key capacity for all $\gamma > 0$. Fig. 2 presents $R_{\text{key}}(\gamma)$ with optimal input signaling. In particular, when $\lambda_1^2 + \lambda_2^2 > 1$, using peaky training signal can achieve a non-zero $R_{\text{key}}(\gamma)$ for $\gamma < \gamma_c$.

For the case $\sigma^2 = 1/\rho$, as we have discussed before (and is detailed in Sec. V), we are able to control the sparsity ρ. The secret key capacity is achieved by operating the system with optimal ρ_{opt} (10). The optimal input power allocation is uniform over $\rho_{\text{opt}} n$ channels.

V. Discussion

We have discussed two power normalizations for sparse multipath channels: $\sigma^2 = 1$ and $\sigma^2 = 1/\rho$. We now provide a justification for these. The first represents channel sampling in frequency, as in an OFDM system, and sparsity corresponds to two different channels. The second represents channel sampling in delay, as in a spread-spectrum system, and sparsity corresponds to the same channel observed through different signal bandwidths.

Regarding the first case, $\sigma^2 = 1$, consider an OFDM system with a fixed bandwidth W, and a frequency selective fading channel whose frequency response can be modeled as

$$H(f) = \sum_{m=1}^{N_{path}} \beta_m e^{-j2\pi\tau_m f}$$

where N_{path} is the total number of paths, each path has an independent complex gain β_m and delay τ_m. Let $\tau_{\max}$ denote the channel delay spread. In this case, the channel coefficients for secret key generated are obtained by sampling $H(f)$ and each sample has the same variance

$$E[|H(f)|^2] = \sum_{m=1}^{N_{path}} E[|\beta_m|^2] = \sigma^2 = 1 \qquad (12)$$

In order to get independent channel samples, the samples must be separated by channel coherence bandwidth, $W_c \propto \frac{1}{\tau_{\max}}$. For a given system bandwidth W, the number of independent channel coefficients (DoF) is $N_{\text{ind}} = \frac{W}{W_c} \propto \tau_{\max}$.

In this case, a rich and a sparse channel correspond to two channels with different delay spreads: $\tau_{\max,\text{rich}} > \tau_{\max,\text{sparse}}$. Thus, we have the following interpretation for the sparsity parameter ρ

$$\frac{N_{\text{ind,sparse}}}{N_{\text{ind,rich}}} = \frac{\tau_{\max,\text{sparse}}}{\tau_{\max,\text{rich}}} = \rho < 1 \qquad (13)$$

From (12) and (13), the sparse channel has fewer DoF ($\rho < 1$) while it maintains the same channel power per DoF ($\sigma^2 = 1$). As a result the total channel power (in all DoF) is smaller for sparse channels.

Regarding the second case, $\sigma^2 = 1/\rho$, consider a spread-spectrum system (e.g, a CDMA system) with bandwidth W in which the independent channel coefficients are obtained by sampling the channel in the delay domain with a resolution $\Delta\tau = 1/W$. The sampled representation of the physical channel at this resolution is

$$H(f) = \sum_{m=1}^{N_{path}} \beta_m e^{-j2\pi\tau_m f} \approx \sum_{\ell=0}^{L-1} h_\ell e^{-j2\pi\frac{\ell}{W}f} \qquad (14)$$

where $L = \lceil \tau_{\max} W \rceil$ is the number of resolvable delays within the delay spread and h_ℓ's represent the sampled channel coefficients in the spread-spectrum. Each h_ℓ is related to the physical path gains as, $h_\ell \approx \sum_{\mathcal{S}_{\tau,l}} \beta_m$, and is thus the sum of all β_m whose delays located in the ℓ-th delay resolution bin $\mathcal{S}_{\tau,l} = \{m : \tau_m \in (l/W - 1/2W, l/W + 1/2W]\}$. Under the assumption of i.i.d. β_m, the h_ℓ's are also i.i.d. with power $\sigma_h^2 \propto 1/W$ since the number of paths in delay bin is proportional to $1/W$. From (12) and (14), we also have $L\sigma_h^2 = \sigma^2 = 1$.

In this case, a rich and a sparse channel correspond to the same physical channel sampled through different signal bandwidths: $W_{\text{rich}} > W_{\text{sparse}}$. We have the following interpretation for the sparsity parameter ρ

$$\frac{L_{\text{sparse}}}{L_{\text{rich}}} = \frac{W_{\text{sparse}}}{W_{\text{rich}}} = \rho < 1$$

which also reflects the ratio between the power in the sampled h_ℓ's in the two cases:

$$\frac{\sigma^2_{h,\text{sparse}}}{\sigma^2_{h,\text{rich}}} = \frac{W_{\text{rich}}}{W_{\text{sparse}}} = \frac{1}{\rho}$$

In this case, number of independent coefficients L (DoF) gets smaller for a sparse channel but the power per DoF gets amplified to keep the total channel power constant.

This case shows that we can transform a fixed physical channel into a sparse channel by changing the signal bandwidth. As a consequence, we have the ability to control the sparsity parameter ρ. Thus, the secret key rate curve corresponding to ρ_{opt} in Fig. 1(b) is achievable and, therefore, is the secret key capacity of the system.

References

[1] A.D. Wyner. The wire-tap channel. *The Bell Systems Technical Journal*, 54:1355–1387, 1975.

[2] I. Csiszár and J. Körner. Broadcast channels with confidential messages broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, 1978.

[3] U. M. Maurer. Secret key agreement by public discussion from common information. *Information Theory, IEEE Transactions on*, 39(3):733–742, 1993.

[4] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography part I: Secret sharing. *Information Theory, IEEE Transactions on*, 39(4):1121–1132, 1993.

[5] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *Information Theory, IEEE Transactions on*, 19(4):471–480, Jul 1973.

[6] S.S. Ghassemzadeh, R. Jana, C.W. Rice, W. Turin, and V. Tarokh. Measurement and modeling of an ultra-wide bandwidth indoor channel. *Communications, IEEE Transactions on*, 52(10):1786–1796, Oct. 2004.

[7] A. Sayeed. Sparse multipath wireless channels: Modeling and implications. In *Proc. ASAP*, 2006.

[8] T.-H. Chou, A. Sayeed, and S. Draper. Secret key generation from multipath randomness: Capacity and reliability. *in preparation*.

[9] A. A. Hassan, W. E. Stark, J. E. Hersheyc, and Sandeep Chennakeshu. Cryptographic key agreement for mobile radio. *Digital Signal Processing*, 6(4):207–212, 1996.

[10] A. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. In *ICASSP 2008. IEEE International Conference on*, pages 3013–3016, 2008.

[11] R. Wilson, D. Tse, and R. A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. *Information Forensics and Security, IEEE Transactions on*, 2(3):364–375, 2007.

[12] Chunxuan Ye, A. Reznik, and Y. Shah. Extracting secrecy from jointly gaussian random variables. In *Information Theory, 2006 IEEE International Symposium on*, pages 2593–2597, July 2006.

[13] S. Nitinawarat. Secret key generation for correlated gaussian sources. In *Proceedings of the 45th annual Allerton Conference*, 2007.

[14] T.-H. Chou, A. Sayeed, and S. Draper. Minimum energy per bit for secret key acquisition over multipath wireless channels. In *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 2009.

[15] W.U. Bajwa, A. Sayeed, and R. Nowak. Sparse multipath channels: Modeling and estimation. In *Digital Signal Processing Workshop*, pages 320–325, Jan. 2009.