The Role of Channel States in Secret Key Generation

Xiang He Aylin Yener

Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu yener@ee.psu.edu

***Abstract*—In this work, we investigate secret key generation from channel states. We point out, by means of a packet-delay-based attack, that observing its own channel states is not the only way an adversary can learn about the channel states of the legitimate communicating parties. The attack suggests that it is not secure to transmit data via the channel whose states generate secret keys. However, not using the channel at all would result in a waste of bandwidth. Hence, we propose using this channel to transmit the bits needed to reconcile the channel state estimates at the transmitter and the receiver. This is a necessary step in secret key generation that required a separate channel in previous work. Although the scheme proposed here in effect prohibits the use of an adaptive transmitter, we show, for the Rayleigh fading channel, that a decent key rate that outperforms existing schemes is obtained. This is due to the fact that collection of the channel state information and transmission of the reconciliation bits are performed concurrently rather than via time sharing.**

I. Introduction

Cryptography is the most widely used means of secure communication today. Yet, alternatives to securing communication links are of interest since the security guarantees offered by cryptography rely on the absence of known efficient attacks against these schemes. There are several alternatives proposed to date which use the physical medium to provide means to generate secret keys. In this work, we shall investigate one, which generates a secret key from the channel states of a wireless link [1].

The approach of generating a secret key from channel states is based on the following assumptions: Let $h_{i,j}$ denote the channel gain of a wireless communication link from node i to node j. Then:

1) $h_{i,j} \approx h_{j,i}$.
2) It is difficult for an eavesdropper to compute $h_{i,j}$ or $h_{j,i}$.

The first assumption is usually justified from the fact that the propagation of electromagnetic (EM) wave is reciprocal [1]. If the frequency and time at which node i transmits is close to the frequency and time at which node j transmits, then the channel gain observed by i should be close to that observed by node j.

The second assumption needs a closer examination. This assumption is usually justified from the experiment observation that in an environment with many reflecting surfaces for the EM wave, if the distance between the eavesdropper and node i, j is more than the wavelength of the EM wave, the channel state of the eavesdropper channel at a certain time instance is not highly correlated with $h_{i,j}$ and $h_{j,i}$ at the same time instance [1]–[4]. However, it should noted that observing its own channel states is not the only way that the eavesdropper can learn about $h_{i,j}, h_{j,i}$. Usually, the channel state estimates are not kept secret at the legitimate nodes since they are not the actual transmission data and are usually revealed to the users as diagnosis information. Later, we will see another example where the eavesdropper can learn the channel states $h_{i,j}, h_{j,i}$ by inspecting packet delays, which are also not kept secret in general. Finally, if the environment is relatively static, the eavesdropper can potentially measure the channel states of the environment beforehand as a function of the location of the communication parties. In this case, it is possible for the eavesdropper to determine the channel gains observed by node i and j from their locations, which can be identified, say, via satellites. To prevent these potential leaks, it is desirable for the communication environment to be constantly changing, so that it becomes *computationally challenging* for the eavesdropper to compute the propagation paths of EM waves. By the same token, the secret key is likely to be generated from the small-scale fluctuation of the channel states, which is more difficult for the eavesdropper to track than the large scale fluctuation of the channel states. Yet, this brings in another problem, namely the accuracy of the assumption on channel reciprocity. Recall that node i and j must generate the same secret key from the $h_{i,j}$ and $h_{j,i}$. When small scale fluctuations are considered, even a small difference in $h_{i,j}$ and $h_{j,i}$ can become problematic from the viewpoint of generating the common key. This can potentially lead to more communication overhead required to reconcile the difference between $h_{i,j}$ and $h_{j,i}$ and limit the secret-key rate.

The impact of this communication overhead has received relatively little attention in the past. In [2]–[4], the need to transmit these reconciliation bits was avoided by aggressively reducing the key rate. The motivation therein was to avoid the need to authenticate these bits. References [2], [3] proposed to use the channel states to generate secret key if their amplitude exceed certain thresholds for a consecutive period of channel uses. Reference [4] proposed to use the channel states to generate secret key if deep fading occurs. Clearly, if the

978-1-4244-8015-9/10/$26.00 ©2010 IEEE

adversary actively introduces deep fading, for example, by obscuring the antennas of legitimate communicating parties, this approach becomes problematic. In all these works, the generated secret key is short (128 -512 bits) and has to be used along with block ciphers to encrypt data streams, whose security again relies on the absence of known attacks. In [5], [6], it is assumed that $h_{i,j} = h_{j,i}$ exactly. In most previous work in key generation, see [7], [8] for example, the standard approach is to assume the existence of another public discussion link, which is then used to transmit the reconciliation bits. In [9] and [10], it is assumed that these bits are transmitted over a separate wiretap channel.

In this work, we investigate the secret key generation problem if the reconciliation bits are sent over the *same* communication link that provides the channel states for secret key generation. Doing so is motivated by three reasons: (1) The channel state usually fluctuates at a rate that is slower than the communication rate. Hence there is spare bandwidth that can be utilized to transmit these bits. (2) Previous efforts [7], [9], [10] require a separate communication link to transmit these communication overheads, which may not be available or desirable in practice. (3) As we will demonstrate in Section III, this excess bandwidth mentioned in (1) is not useful for transmitting information, even public data, due to the potential for compromised security of the communication link.

The main contribution of this work is to derive the achievable secret-key rate for the above scheme. We first model the communication link as a wiretap channel with causal side information at the transmitter and the receiver in Section II. In Section IV, we provide the proof of the achievable secret-key rate. In Section V, we evaluate this rate for the i.i.d. Rayleigh fading case and provide numerical results which show that the rate we derived compares favorably to alternative schemes.

II. System Model

In this section, we describe the channel we use to model the communication link. To make the problem tractable, we assume that the current channel state is estimated by the transmitter and the receiver before each use of the communication link. Hence, before each use of the link, the transmitter and the receiver has their own estimates of the current channel state (but not future channel states). The communication link, with an eavesdropper present, thus is modeled as wiretap channel with causal side information, as shown in Figure 1. In this model, node 1 wants to send a confidential message W to node 2 over n channel uses through a memoryless wiretap channel. The state of the wiretap channel is denoted by $\{R, S\}$. R is known by node 1 and S is known by node 2 up to the current channel use. Let X^n denote the signals transmitted by node 1. Y^n denotes the signals received by node 2. Z^n denotes the signals received by the eavesdropper. The channel description is given by:

$$\Pr(Y, Z|X, S, R) = \Pr(Z|X) \Pr(Y|X, Z, S, R) \quad (1)$$

The situation corresponds to the case that the side information available to the legitimate communicating parties *does not* include any channel state information of the eavesdropper, which models a practical system.

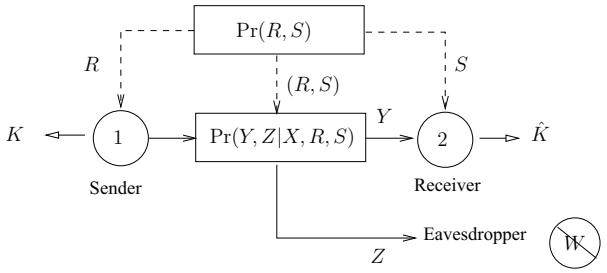

Fig. 1. Wiretap Channel with Causal Side Information

The channel states R and S are modeled as outputs from a i.i.d. random source. Hence we have:

$$\Pr(R^n, S^n) = \prod_{i=1}^{n} \Pr(R_i, S_i) \quad (2)$$

We also assume that given R^n and S^n, the randomness of the channel is independent from the random source. Hence we have:

$$\begin{aligned} &\Pr(Y^n, Z^n, X^n, R^n, S^n) \\ &= \Pr(X^n|R^n) \Pr(R^n, S^n) \Pr(Y^n, Z^n|X^n, R^n, S^n) \end{aligned} \quad (3)$$

The distribution $\Pr(X^n|R^n)$ in (3) is determined by the encoding function. Let f_i be the encoder of node 1 at the ith channel use. Let R^i denote the sequence of R from the first to the ith channel use. Let M_1 be the local randomness available to node 1. Then the encoder takes the following form:

$$X_i = f_i(M_1, R^i) \quad (4)$$

After n channel uses, node $i, i = 1, 2$ try to agree on a secret key. Let the key generated by node 1 and 2 be K and $\hat{K}$ respectively. Let the generation function of node 1 be $h_i, i = 1, 2$. Then

$$K = h_i(R^n, X^n, M_1), \quad \hat{K} = h_i(S^n, Y^n) \quad (5)$$

The secret-key rate is defined as

$$R_e = \lim_{n\to\infty} \frac{1}{n} H(K) \quad (6)$$

subject to the following two constraints:

$$\lim_{n\to\infty} \frac{1}{n} I(K; Z^n) = 0 \quad (7)$$

$$\lim_{n\to\infty} \Pr\left(K \neq \hat{K}\right) = 0 \quad (8)$$

III. An attack using packet delays

The attack scheme is shown in Figure 2. For simplicity, we assume nodes 1 and 2 are connected by an on-off channel, whose state is denoted by $S \in \{0, 1\}$ and is known causally by both node 1 and 2. We assume each time $S = 1$, node 1 will transmit exactly one packet to node 2. When $S = 0$, node 2 will not be able to receive anything.

To demonstrate the effectiveness of the attack, we consider the setting where the adversary is *not able* to receive any signal transmitted by node 1 at all. Yet, we shall see, even in this scenario, it is still possible for the adversary to learn about the channel states if it can trigger a sequence of packets for node 1 to send to node 2 and examine the delay of these packets. The delay is defined as the difference between the time instance that a packet is transmitted by the adversary and the time instance that this packet arrives at the adversary. In this example, we assume the only uncertain component of the delay is the time period that the packet stay in the queue of node 1 waiting to be transmitted. In order not to overload the queue of node 1, the adversary needs to pace its speed of injecting packets. Here, we assume, upon receiving a packet back from node 2, the adversary immediately sends a new packet to node 1 to transmit. We assume the time it takes for the new packet to arrive at the queue of node 1 is small compared to the time it takes for node 1 and 2 to estimate the channel state S. Hence when the channel estimation is complete, the new packet is in the queue of node 1, ready to be transmitted. Let the delay of packet i be denoted by t_i. We also assume that node 1 happen to receive no other packets that are not originated from the adversary during this period. We observe that

$$t_i - t_{i-1} \tag{9}$$

approximates the time period that packet i stays in the queue after packet $i-1$ is sent. Let $t_i - t_{i-1} = k$. Then, the adversary can deduce that S takes values of k zeros during which packet i stays in the queue, followed by 1 during which packet i is transmitted. The adversary can use this side information to reduce the search space when it tries to guess the secret key.

The example here, of course, is over simplified compared to a real system. For example, the packet delay will be affected by more factors, like transmission delays and delays caused by other traffic unknown to the adversary. Yet, even in these more complicated scenarios, the delay information will not be entirely independent from the channel states.

The attack in this example can be avoided by not transmitting unauthorized packets over the channel whose states are used to generate secret key. However, in most current implementations, the physical layer is oblivious to the origin of a packet. This implies that to deploy schemes which generate secret key from channel states, it entails not just a simple modification of current system, but a careful re-examination of different layers of the system.

If this is too costly, then a more conservative alternative is that we do not transmit any packets over the channel whose state is used to generate secret key. This implies a waste of bandwidth. As mentioned in the introduction, usually the side information available to node 1 is not exactly the same as the side information available to node 2, and communication overhead is required to reconcile their side information in order for the two nodes to generate the same secret key. In previous works, this communication overhead is transmitted over a separate channel. In the next section, we investigate how to transmit it using the spare bandwidth of the channel whose state has been used for secret key generation.

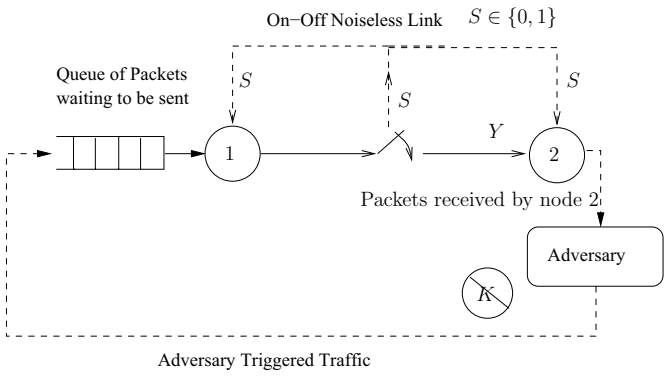

Fig. 2. Side Channel Attack

IV. Achievable Rate

In this section, we derive the achievable secret-key rate when the reconciliation bits are transmitted over the same channel whose states generate the secret key. The rate is given by the following theorem:

Theorem 1: For an auxiliary random variable U such that $U - R - S$ is a Markov chain, the following secret-key rate is achievable:

$$\max_{\Pr(X)} \left\{ I(U;S) + \alpha \left[I(X;Y|S) - I(X;Z) \right]^+ \right\} + \max_{\Pr(X)} (1-\alpha) \left[I(X;Y,S) - I(X;Z,R) \right]^+ \tag{10}$$

such that

$$I(U;R) - I(U;S) = \alpha I(X;Y|S) \tag{11}$$

for $0 \leq \alpha < 1$. Both terms in the achievable rate expression is maximized over the following joint distribution, although they may not share the same $\Pr(X)$:

$$\Pr(X) \Pr(R) \Pr(U|R) \Pr(S|R) \tag{12}$$

$$\Pr(Z|X) \Pr(Y|X,Z,R,S) \tag{13}$$

Remark 1: We explicitly choose a $\Pr(X)$ that is independent of R. This means the transmitter is *not* using the side information to increase the reliable transmission rate. This greatly simplifies the computation of equivocation. It should be noted that this choice can decrease the achievable rate significantly in some channels [11, Figure 4]. Yet, in the case of Gaussian i.i.d. Rayleigh fading channel, the rate loss caused by not using transmitter side information is known to be limited [12]. □

Proof: The proof is similar to [9]. The difference is that the side information S and R are not known non-causally to the communication parties as in [9]. Hence the communication has to be divided into several blocks.

We assume the communication spans over m blocks. Each block is composed of n channel uses. To simplify the notation,

we use $\mathbf{A}$ to denote the signal A within one block. We use $\bar{\mathbf{A}}$ to denote the first αn components of $\mathbf{A}$, and use $\tilde{\mathbf{A}}$ to denote the remaining $(1-\alpha)n$ components of $\mathbf{A}$. We also use the notation $\mathbf{A}_i$ to denote the signals $\mathbf{A}$ related to the ith block.

In each block, nodes 1 and 2 perform two tasks:

1) Collect channel state information and perform Wyner-Ziv coding.
2) Transmit the bin index produced by Wyner-Ziv encoder from the *previous* block.

We point out that since different blocks are entangled together, the eavesdropper can potentially obtain more information by processing all blocks jointly. The main trick is to show that the equivocation can still be computed in a block by block fashion if X is chosen to be independent from the transmitter side information R.

The codebook is constructed as follows: Let δ_n be a positive sequence such that $\lim_{n\to\infty}\delta_n = 0$ and $\lim_{n\to\infty} n\delta_n = \infty$.

1) Codebook for U, denoted by $\mathcal{C}_U$: Sample $2^{n(I(U;R)+\delta_n)}$ i.i.d. sequences from $\Pr(U)$.
2) Codebook $\mathcal{C}_X$, which will be used to transmit the Wyner-Ziv code bin index: Sample $2^{\alpha n(I(X;Y|S)-\delta_n)}$ i.i.d. sequences from $\Pr(X)$, each sequence has αn components.
3) Codebook $\mathcal{C}_W$, which will be used to transmit the wiretap code: Sample $2^{(1-\alpha)n(I(X;Y,S)-2\delta_n)}$ i.i.d. sequences from $\Pr(X)$, which can be a different distribution from the $\Pr(X)$ used to generate $\mathcal{C}_X$. Each sampled sequence has $(1-\alpha)n$ components.

We next describe the encoding scheme: First we need to define the encoders:

1) The source encoder: The encoder takes input R^n and finds the first sequence U^n which is jointly typical with R^n.
2) The Wyner-Ziv encoder: The sequences in $\mathcal{C}_U$ are divided into $2^{n(I(U;R)-I(U;S)+2\delta_n)}$ bins. Each bin has $2^{n(I(U;S)-\delta_n)}$ sequences. The encoder takes input U^n and output the index of the bin that contains U^n.
3) The secret key generator: We choose U such that
$$I(U;R) - I(U;S) + 2\delta_n = \alpha\left(I(X;Y|S) - \delta_n\right) \tag{14}$$
The sequences in $\mathcal{C}_U$ are divided into $2^{n(I(U;S)+\alpha[I(X;Y|S)-I(X;Z)]^+-\delta_n)}$ bins. Each bin has $2^{n\alpha(\min\{I(X;Y|S),I(X;Z)\}-\delta_n)}$ sequences. From (14), it can be verified that the total number of sequences of U^n remains as $2^{n(I(U;R)+\delta_n)}$. The encoder takes input U^n and outputs the index of the bin that contains U^n.
4) The wiretap encoder: The encoder is used only if $I(X;Y,S) > I(X;Z,R)$. The sequences in $\mathcal{C}_W$ are binned into $2^{(1-\alpha)n(I(X;Y,S)-I(X;Z,R)-\delta_n)}$ bins. Each bin contains $2^{(1-\alpha)n(I(X;Z,R)-\delta_n)}$ sequences. The encoder takes input w and outputs one sequence contained in the bin indexed by w, which is chosen according to a uniform distribution over all sequences in the bin.

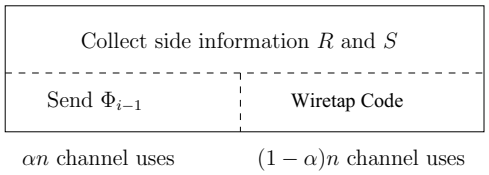

Fig. 3. Channel uses breakdown in a block

At the end of the ith block, node 1 encodes $\mathbf{R}_i$ into $\mathbf{U}_i$. It then uses the Wyner-Ziv encoder to encode $\mathbf{U}_i$ into the Wyner-Ziv bin index Φ_i. This index is then mapped to a sequence $\bar{\mathbf{X}}_{i+1}$ in $\mathcal{C}_X$, which is possible because of (14). The resulting $\bar{\mathbf{X}}_{i+1}$ is then transmitted during the first αn channel uses in the $(i+1)$th block.

If $\alpha < 1$ and $I(X;Y,S) > I(X;Z,R)$, in the remaining $(1-\alpha)n$ channel uses, node 1 randomly generate w_i uniformly distributed over $1, ..., 2^{(1-\alpha)n(I(X;Y,S)-I(X;Z,R)-\delta_n)}$ and encode it with the wiretap encoder. Node 1 then transmits the encoder output $\tilde{\mathbf{X}}_i$ in the remaining $(1-\alpha)n$ channel uses. The encoding scheme is summarized in Figure 3.

We next describe the decoding scheme: At the end of the ith block, node 2 receives $\mathbf{Y}_i, \mathbf{S}_i$. It then compute $\bar{\mathbf{X}}_i$ from them by finding a sequence in $\mathcal{C}_X$ which is jointly typical with $\bar{\mathbf{Y}}_i$ and $\bar{\mathbf{S}}_i$. The sequence $\bar{\mathbf{X}}_i$ determines Φ_{i-1}. Node 2 then looks into the sequences in $\mathcal{C}_U$, which are included in the bin indexed by Φ_{i-1} and find the first sequence that is jointly typical with $\mathbf{S}_{i-1}$. With high probability this sequence is $\mathbf{U}_{i-1}$.

If $\alpha < 1$, node 2 will also find the sequence in $\mathcal{C}_W$ that is jointly typical with $\tilde{\mathbf{Y}}_i$. With high probability, the sequence is $\tilde{\mathbf{X}}_i$.

We next describe the secret key generation process: From the description of the decoding procedure, at the end of the ith block, both node 1 and node 2 should know $\mathbf{U}_{i-1}$. It should also be able to deduce w_{i-1}, which is determined by $\tilde{\mathbf{X}}_{i-1}$. The secret key generated from $i-1$st block is denoted by k_{i-1} and is chosen as the output of the secret key generator a_{i-1}, along with w_{i-1} for $i-1 < m$. k_m is assumed to be 1.

We next compute the equivocation rate: We use the notation $\mathbf{A}_p^q$ to denote $\mathbf{A}_p, \mathbf{A}_{p+1}, ..., \mathbf{A}_q$ if $p < q$ and empty otherwise. Then the equivocation is given by:

$$H\left(k_1^m|\mathbf{Z}_1^m\right) = H\left(k_1^{m-1}|\mathbf{Z}_1^m\right) \tag{15}$$
$$= \sum_{i=1}^{m-1} H\left(k_i|\mathbf{Z}_1^i, \mathbf{Z}_{i+1}, \mathbf{Z}_{i+2}^m, k_{i+1}^m\right) \tag{16}$$

Each term inside the sum of (16) can be written as:

$$H\left(k_i|\mathbf{Z}_1^i, \mathbf{Z}_{i+1}, \mathbf{Z}_{i+2}^m, k_{i+1}^m\right) \tag{17}$$
$$\geq H\left(k_i|\mathbf{Z}_1^i, \bar{\mathbf{X}}_i, \mathbf{Z}_{i+1}, \mathbf{Z}_{i+2}^m, k_{i+1}^m\right) \tag{18}$$
$$= H\left(k_i|\bar{\mathbf{X}}_i, \tilde{\mathbf{Z}}_i, \mathbf{Z}_{i+1}, \mathbf{Z}_{i+2}^m, k_{i+1}^m\right) \tag{19}$$
$$= H\left(k_i|\tilde{\mathbf{Z}}_i, \mathbf{Z}_{i+1}, \mathbf{Z}_{i+2}^m, k_{i+1}^m\right) \tag{20}$$
$$\geq H\left(k_i|\tilde{\mathbf{Z}}_i, \mathbf{Z}_{i+1}, \mathbf{R}_{i+1}, \mathbf{Z}_{i+2}^m, k_{i+1}^m\right) \tag{21}$$

$$=H\left(k_i|\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) \quad (22)$$

$$=H\left(a_i|\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) + H\left(w_i|a_i,\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) \quad (23)$$

In (19), we use the following Markov chain:

$$k_i - \left\{\bar{\mathbf{X}}_i,\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{Z}_{i+2}^m,k_{i+1}^m\right\} - \left\{\mathbf{Z}_1^{i-1},\bar{\mathbf{Z}}_i\right\} \quad (24)$$

Note that this chain holds because we are considering the channel factorization (1), which implies that given $\bar{\mathbf{X}}_i$, the random variable $\bar{\mathbf{Z}}_i$ is independent from $\mathbf{R}_i$, from which we generate α_i.

Equation (20) is due to the fact that k_i, $\tilde{\mathbf{Z}}_i$, $\mathbf{Z}_{i+1}$, $\mathbf{Z}_{i+2}^m$, k_{i+1}^m are independent from $\bar{\mathbf{X}}_i$. This is because we choose $\bar{\mathbf{X}}_i$ to be independent from $\mathbf{R}_i$, from which we generate a_i.

In (22), we use the following Markov chain:

$$k_i - \left\{\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right\} - \left\{\mathbf{Z}_{i+2}^m,k_{i+1}^m\right\} \quad (25)$$

This is in part because k_{i+1} is generated from $\mathbf{R}_{i+1}$, $\mathbf{Z}_{i+2}^m$ is related to k_i only through R_{i+1}.

For the first term in (23), we have:

$$H\left(a_i|\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) \quad (26)$$

$$=H\left(a_i|\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) \quad (27)$$

$$=H\left(a_i|\mathbf{Z}_{i+1}\right)=H\left(a_i|\bar{\mathbf{Z}}_{i+1}\right) \quad (28)$$

Equation (28) is due to the fact that $\mathbf{R}_{i+1}$ is independent from α_i and $\mathbf{Z}_{i+1}$. This, again is because we choose $\mathbf{X}_i$ to be independent from $\mathbf{R}_i$, from which we generate a_i.

For the second term in (23), we have:

$$H\left(w_i|a_i,\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) \quad (29)$$

$$\geq H\left(w_i|\mathbf{R}_i,a_i,\tilde{\mathbf{Z}}_i,\mathbf{Z}_{i+1},\mathbf{R}_{i+1}\right) \quad (30)$$

$$=H\left(w_i|\mathbf{R}_i,\tilde{\mathbf{Z}}_i\right)=H\left(w_i|\tilde{\mathbf{R}}_i,\tilde{\mathbf{Z}}_i\right) \quad (31)$$

Equation (28) can be written as:

$$H\left(a_i|\bar{\mathbf{Z}}_{i+1}\right)\geq H\left(a_i|\bar{\mathbf{Z}}_{i+1}\right)-H\left(a_i|\mathbf{U}_i,\bar{\mathbf{Z}}_{i+1}\right) \quad (32)$$

$$=I\left(\mathbf{U}_i;a_i|\bar{\mathbf{Z}}_{i+1}\right) \quad (33)$$

$$=H\left(\mathbf{U}_i|\bar{\mathbf{Z}}_{i+1}\right)-H\left(\mathbf{U}_i|a_i,\bar{\mathbf{Z}}_{i+1}\right) \quad (34)$$

$$\geq H\left(\mathbf{U}_i,\Phi_i|\bar{\mathbf{Z}}_{i+1}\right)-\alpha n\varepsilon \quad (35)$$

$$=H\left(\mathbf{U}_i|\Phi_i,\bar{\mathbf{Z}}_{i+1}\right)+H\left(\Phi_i|\bar{\mathbf{Z}}_{i+1}\right)-\alpha n\varepsilon \quad (36)$$

$$=H\left(\mathbf{U}_i|\Phi_i\right)+H\left(\Phi_i|\bar{\mathbf{Z}}_{i+1}\right)-\alpha n\varepsilon \quad (37)$$

In particular, (35) is based on [9, Lemma 4]. Then as shown by [9, Lemma 3], we have:

$$\lim_{n\to\infty}\frac{1}{n}H\left(\mathbf{U}_i|\Phi_i\right)=I\left(U;S\right) \quad (38)$$

$$\lim_{n\to\infty}\frac{1}{n}H\left(\Phi_i|\bar{\mathbf{Z}}_{i+1}\right)\geq\alpha[I\left(X;Y|S\right)-I\left(X;Z\right)]^+ \quad (39)$$

Using the standard arguments for the wiretap channel [13], it can be shown that (31) is lower bounded by:

$$H\left(\tilde{\mathbf{X}}_i\right)-I\left(\tilde{\mathbf{X}}_i;\tilde{\mathbf{R}}_i,\tilde{\mathbf{Z}}_i\right) \quad (40)$$

And we have:

$$\lim_{n\to\infty}\frac{1}{n}H\left(\tilde{\mathbf{X}}_i\right)=(1-\alpha)\,I\left(X;Y,S\right) \quad (41)$$

$$\lim_{n\to\infty}\frac{1}{n}I\left(\tilde{\mathbf{X}}_i;\tilde{\mathbf{R}}_i,\tilde{\mathbf{Z}}_i\right)=(1-\alpha)\,I\left(X;Z,R\right) \quad (42)$$

By letting $m,n\to\infty$, we have the theorem. ■

V. Rayleigh Fading

The Rayleigh fading channel model is determined by the following equations:

$$R=T+N_R \qquad S=T \quad (43)$$

$$Y=TX+N_Y \qquad Z=\{QX,Q\} \quad (44)$$

where T is the channel state of the main channel. Q is the channel state of the eavesdropper channel. T,N_R,N_Y,Q are all zero mean independent complex Gaussian random variables. Without loss of generality, we assume T, Q and N_Y has unit variance. The variance of N_R is given by σ_R^2.

Remark 2: We explicitly assume the eavesdropper observes zero additive noise in (44) because in a real system, it is difficult to estimate the average received SNR of the eavesdropper. We also assume in (44), the eavesdropper has perfect knowledge of its channel state Q. □

We choose $\Pr(X)$ as a complex Gaussian distribution with zero mean and variance P. Define $Z'=QX$. Then (10) is found to be:

$$I\left(U;S\right) \quad (45)$$

We can choose $\alpha=1$ and write (11) as:

$$I\left(U;R\right)-I\left(U;S\right)=I\left(X;Y|S\right) \quad (46)$$

Define A, such that

$$A=I(X;Y|S)=\mathrm{E}\left[\log_2\left(1+|S|^2P\right)\right] \quad (47)$$

where the expectation is over the random variable S.

For $I(U;R)$ and $I(U;S)$, we obtain:

$$I\left(U;R\right)=\log_2\pi e\left(1+\sigma_R^2+\sigma_U^2\right)-\log_2\pi e\sigma_U^2 \quad (48)$$

$$I\left(U;S\right)=\log_2\pi e\left(1+\sigma_R^2+\sigma_U^2\right)-\log_2\pi e\left(\sigma_R^2+\sigma_U^2\right) \quad (49)$$

Let A denote the right hand side of (47), and choose σ_U^2 such that $I(U;R)-I(U;S)=A$. Then the achievable rate is:

$$I\left(U;S\right)=\log_2\left(1+\frac{1-2^{-A}}{\sigma_R^2}\right) \quad (50)$$

We next compare this secret-key rate with the following time sharing scheme: The legitimate communication parties spend $(1-\alpha)n$ channel uses collect channel states, and the remaining αn channel uses transmitting the communication overhead require to reconcile their side information. During these αn channel uses, the legitimate communicating parties do not collect channel states.

Let the rate of the channel code during the remaining αn channel uses be R_0. Note that here, during the remaining αn channel uses, we allow the transmitter to be adaptive in rate

and power to the channel states it observed, R. Hence R_0 is greater than A. Also, we ignore the transmission power consumption required to estimate the channel states. Hence the average power constraints of the channel code during the remaining αn channel uses is P/α.

Following the same derivation in [9], the secret-key rate achieved by this time sharing scheme is given by $(1-\alpha)I(U;S)$, subject to the constraint:

$$(1-\alpha)(I(U;R)-I(U;S)) = \alpha R_0 \tag{51}$$

It is difficult to evaluate R_0, since the transmitter side information R is not a deterministic function of the channel state S [14]. However, we can give S to the transmitter as genie information and derive an upper bound for R_0, which leads to an upper bound on the secret-key rate achievable using this time sharing scheme. We denote this upper bound of R_0 with $\bar{R}_0$, which is given by [12]:

$$\bar{R}_0 = \int_0^{+\infty} \log_2\left(1+|t|P\left(t\right)\right) f_{|S|^2}\left(t\right) dt \tag{52}$$

where $f_{|S|^2}(t)$ is the P.D.F. of $|S|^2$. $P(t)$ is the non-negative power allocation function subject to the constraint:

$$\int_0^{+\infty} P\left(t\right) f_{|S|^2}\left(t\right) dt = \frac{P}{\alpha} \tag{53}$$

It then follows from [12] that $\bar{R}_0$ is given by:

$$\bar{R}_0 = \frac{1}{\ln 2}\int_{\mu}^{+\infty} \frac{1}{t} e^{-t} dt \tag{54}$$

where $1/\mu$ is the water level given by:

$$\int_{\mu}^{+\infty} \left(\frac{1}{\mu}-\frac{1}{t}\right) e^{-t} dt = \frac{P}{\alpha} \tag{55}$$

For each possible time sharing factor α, we compute μ and the corresponding achievable secret-key rate. Then we optimize over α to maximize the secret-key rate.

The key rates achievable with these two schemes are compared in Figure 4. We observe that the achievable rate given by Theorem 1 is much larger than the rate given by the time sharing scheme, even though with the latter adaptive transmission is used.

VI. Conclusion

In this work, we have investigated the method of generating a secret key from channel states. An attack based on packet delays is provided to make the point that observing its channel state is not the only way that an adversary can learn about the channel states of the legitimate communicating parties, and it is not safe to use the channel whose states generate the secret key to transmit data. Hence, as an alternative, we have proposed to send over this channel the communication overhead required to reconcile the channel states learned by the transmitter and the receiver. We have derived the secret key generation rate for this scheme and evaluated the rate when the channel state is i.i.d. Rayleigh fading. We have shown from numerical results that the rate offered by the proposed scheme outperforms the existing key generation scheme.

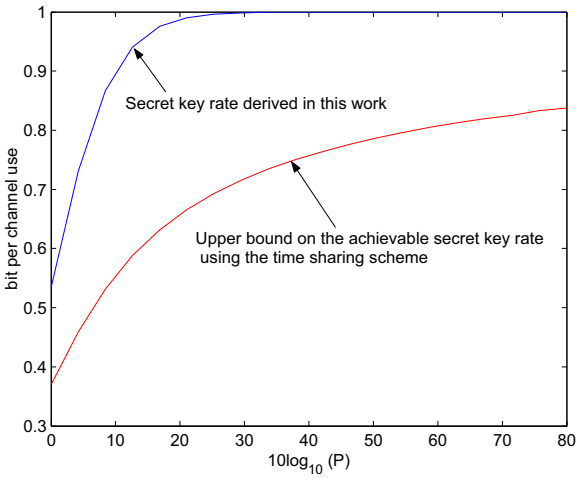

Fig. 4. Secret Key Rate, $\sigma_R^2 = 1$

References

[1] R. Wilson, D. Tse, and R. A. Scholtz. Channel Identification: Secret Sharing using Reciprocity in Ultrawideband Channels. *IEEE Transactions on Information Forensics and Security*, 2(3):364–375, September 2007.

[2] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust Key Generation from Signal Envelopes in Wireless Networks. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, October 2007.

[3] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, September 2008.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam. Information-theoretically Secret Key Generation for Fading Wireless Channels. Submitted to the IEEE Transactions on Information Forensics and Security, February, 2009, available online at http://arxiv.org/abs/0910.5027.

[5] A. Khisti, S. Diggavi, and G. Wornell. Secret Key Agrement Using Asymmetry in Channel State Knowledge. In *IEEE International Symposium on Information Theory*, June 2009.

[6] Y. K. Chia and A. El Gamal. Wiretap Channel with Causal State Information. Available online at http://arxiv.org/abs/1001.2327v2, January, 2010.

[7] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik. Secret Key Generation for a Pairwise Independent Network Model. In *IEEE International Symposium on Information Theory*, July 2008.

[8] S. Salimi, M. Salmasizadeh, and M. R. Aref. Rate Regions of Secret Key Sharing in a New Source Model. Available online at http://arxiv.org/abs/1004.0799, April, 2010.

[9] A. Khisti, S. Diggavi, and G. Wornell. Secret-Key Generation using Correlated Sources and Channels. Submitted to IEEE Transactions on Information Theory, June 2009, available online at http://arxiv.org/abs/0906.1835.

[10] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran. Secrecy via Sources and Channels - A Secret Key - Secret Message Rate Tradeoff Region. In *IEEE International Symposium on Information Theory*, July 2008.

[11] C. E. Shannon. Channels with Side Information at the Transmitter. *IBM Journal of Research and Development*, 2(4):289–293, 1958.

[12] A. J. Goldsmith and P. P. Varaiya. Capacity of Fading Channels with Channel Side Information. *IEEE Transactions on Information Theory*, 43(6):1986–1992, November 1997.

[13] I. Csiszár and J. Körner. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[14] G. Caire and S. Shamai. On the Capacity of some Channels with Channel State Information. *IEEE Transactions on Information Theory*, 45(6):2007–2019, September 1999.