Secret Key Generation through OFDM Multipath Channel

Yanpei Liu
Electrical and Computer Engineering
University of Wisconsin
Madison, Wisconsin 53706, USA
yliu73@wisc.edu

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

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

Abstract—We analyze the fundamental limits of key generation and describe an implementation based on error correcting codes. We show that key extraction based on channel coefficients significantly outperforms key extraction based on received signal strength indicators (RSSI). The development in this paper is based on an IEEE 802.11a orthogonal frequency-division multiplexing (OFDM) model and we demonstrate that it is feasible to use the sampled channel coefficients in OFDM as the key source. The key extraction problem is cast as a Slepian-Wolf coding and decoding problem. We construct regular and irregular forms of binary and non-binary low-density parity check (LDPC) codes to prototype our key extraction.

Index Terms—Common randomness, secret key generation, OFDM channel, LDPC codes, Slepian-Wolf decoder

I. INTRODUCTION

Current wireless communication security protocols are largely based on public key cryptography, such as Wired Equivalent Privacy (WEP), Extensible Authentication Protocol (EAP) and Wi-Fi Protected Access (WPA). However, the security of these techniques have been of great concern in recent years. For example, an attacker can cause a denial-of-service attack in a network equipped with WPA [1]. Also, recent research show that public key cryptography consumes a significant amount of computing resources and power. This places a significant load on the resources of circuitry of small-scale, especially battery-powered networks [2].

The encryption method we propose makes use of the inherent channel randomness shared by two users Alice and Bob [2]–[4]. This method generates a secret key from dependent randomness observed by Alice and Bob. As the channel is inherently random, the key generated herein is inherently random, which is superior to the one generated by computational cryptography. The key generation method is based on the channel coefficients under multipath propagation of wireless channel and security relies on three fundamental radio propagation properties induced by multipath: reciprocity of radio propagation, as well as temporal and spatial channel variations.

• Reciprocity of Radio Propagation: The electromagnetic wave propagation is identical in both directions: the propagation from Alice to Bob is identical to the one from Bob to Alice. To be more specific, the multipath channel coefficients over a certain time scale are identical in both Alice and Bob’s observations [2], [3].

• Temporal Channel Variation: The channel between Alice and Bob changes whenever one of them moves or whenever there are moving scattering objects in this channel.

• Spatial Channel Variation: Once the channel is set up, Alice and Bob uniquely characterize this channel. If multipath is rich, an eavesdropper (Eve) in another location which is even a few wavelengths away from either of them observes a distinct channel.

A. System Overview

We consider a system with the model shown in Figure. 1 and the operation of the system is summarized as follows. Alice and Bob perform a two-way channel estimation: Alice sends a training signal to Bob and Bob sends a training signal to Alice in consecutive time slots. Alice obtains measurements of the channel coefficients from her observation as does Bob. Ideally, their observations are identical, but only correlated in practice because of the asymmetric observation caused by noise, interference or observation errors. We then need a reconciliation process. In the reconciliation process, Alice sends Bob a public message based on her observation which
she uses to describe her observation. The public message from Alice must not reveal too much information to the public. Based on the public message received and his own observation, Bob can determine with high probability what Alice’s observation is.

B. Related Work

There are many current research works on different secret key generation techniques that explore multipath randomness. For the method based on RSSI, when the channel is over-static, key bits may contain long runs of 0’s and 1’s, which make it susceptible to potential attackers. In [5], an adaptive quantizer is proposed to address the problem caused by the over-static channel. They incorporate the Discrete Cosine Transform (DCT) transform to remove the redundancy caused by long runs of 0’s and 1’s. Universal hash functions (UHFs) are used in [4] to amplify the randomness by extracting the maximum possible amount of entropy. In quantizer design, a good quantizer should not only maximize the mutual information between Alice and Bob’s bit sequences, but also reveal limited information to the eavesdropper. An algorithm is proposed in [6, 7] to find such a quantizer, inspired from [8, 9]. Fundamental limits to key generation for multipath randomness are studied in [10], including the minimum energy required to generate a finite-length key with a specified probability of error in key acquisition. The analysis is further extended in [11] to sparse multipath channels which exhibit high correlations.

C. Notation

Unless otherwise specified, we use upper case letters, e.g., $X$ to denote a random variable and bold letters, e.g., $\mathbf{X}$ to denote a random vector: $x$ and $\mathbf{x}$ are the respective realizations. If $X$ is a complex random variable, we use $\Re(X)$ and $\Im(x)$ to denote its real and imaginary part, respectively. In particular, we denote a complex Gaussian random variable $X$ with mean $m$, variance $\sigma^2$, and with real and imaginary parts independent and identically distributed as $X \sim \mathcal{CN}(m, \sigma^2)$.

D. Paper Outline

The rest of the paper is organized as follows. In Section II we provide necessary background on OFDM. In Section III we define our measurement model and discuss some discoveries in secret key capacity calculation. In Section IV we explain the use and introduce the design of our Slepian-Wolf LDPC codes. In Section V we provide simulation results of OFDM model and LDPC codes under typical Wi-Fi parameter settings. We conclude the paper in Section VI.

II. FUNDAMENTAL BACKGROUND

A. OFDM Background

In this section, we introduce the OFDM model and study the sampled channel coefficients from which the key bits are extracted. Since we extract the keys from sampled channel coefficients, we use “sampled channel coefficients” and “channel coefficients” interchangeably. The OFDM model we use follows closely to [12].

1) OFDM Channel Model: Consider an OFDM system with $M$ frequency tones. The received signal $r(t)$ in an OFDM communication system can be demodulated at $n^{th}$ tone by match-filtering with the Fourier basis function $\phi_n(t)$ [12]:

\[ r_n = \langle r(t), \phi_n(t) \rangle = H_n s_n + w_n, \]

where $\langle r(t), \phi_n(t) \rangle$ is defined as $\int_0^\infty r(t)\phi_n^*(t)dt$. We term $H_n$ the frequency domain channel coefficient at $n^{th}$ tone and $w_n$ is a complex white Gaussian noise with variance $\sigma_n^2$. In our setup, Alice and Bob send sounding signal to each other and for simplicity we assume the sounding signal has amplitude $s_n = 1$. $H_n$ is the frequency domain channel coefficient at $n^{th}$ tone and it can be represented as:

\[ H_n = \sum_{k=0}^{N_p} \beta_k e^{-j2\pi \tau_k n \Delta f} \]

where $N_p$ is the total number of transmission paths and $\tau_k \in [0, \tau_{max}]$ is the path delay of the $k^{th}$ path. The variable $\beta_k$ is the complex path gain associated with the $k^{th}$ path and it can be modeled as a complex-valued random variable due to the randomness of its phase. The variable $h_{\ell}$ is the sampled or time domain channel coefficient associated with the $\ell^{th}$ resolvable delay bin. The inequality (a) comes from the fact that each $h_{\ell}$ approximately equals to the sum of $\beta_k$’s that are within the $\ell^{th}$ resolvable bin [12]. The parameter $L \approx [\tau_{max} W]$ is the degree of freedom (DoF). The inequality (b) comes from the fact that the last $M - L$ sample channel coefficients are approximately equal to zero. They are not exactly zero due to the spread of tails of sinc functions in the first $L$ bins [12].

As we can see from (2), frequency domain channel coefficients are related to time domain coefficients through Discrete Fourier Transform (DFT). The DFT can be viewed as the decorrelator which decorrelates the $M$ frequency channel coefficients into $L$ approximately independent sampled channel coefficients. This approximation is asymptotically exact as $T$ becomes large where the DFT vectors become the eigenfunctions of Toeplitz matrices [13]. We assume the time domain coefficients are perfectly independent in the remaining parts of the paper, unless otherwise specified.

2) Signal to Noise Ratio: When multipath is rich, i.e., $N_p$ is large, $H_n$ can be well modeled as $\mathcal{CN}(0, \sigma_{H_n}^2)$ due to the central limit theorem (CLT). From (1), we define the per-tone SNR in frequency domain as:

\[ SNR_f = \frac{E[H_n^2]}{E[w_n^2]} = \frac{\sigma_{H_n}^2}{\sigma_n^2}. \]
Because the DFT is unitary transform, Parseval’s theorem states that:
\[
\sum_{n=0}^{M-1} |H_n|^2 \approx \sum_{\ell=0}^{M-1} |h_{\ell}|^2 \approx \sum_{\ell=0}^{L-1} |h_{\ell}|^2,
\]
(4)
where the approximation follows from the approximation in (2). Let \(\sigma_h(\ell)^2\) denote the variance of the \(\ell^{th}\) sampled channel coefficient. We have the following relationship between the variance of frequency domain channel coefficients and sampled coefficients:
\[
\sum_{\ell=0}^{L-1} \sigma_h(\ell)^2 = \sum_{\ell=0}^{L-1} E[h_{\ell}^2] \approx \sum_{n=0}^{M-1} E[H_n^2] = M\sigma_H^2,
\]
(5)
Therefore, the SNR in the time domain is related to the SNR in the frequency domain as:
\[
\sum_{\ell=0}^{L-1} \text{SNR}_r(\ell) \approx M \cdot \text{SNR}_f,
\]
(6)
where \(\text{SNR}_r(\ell)\) is the time domain SNR at the \(\ell^{th}\) sampled channel coefficient. If we assume sampled channel coefficients to have equal variance, the SNR in time domain reduces to:
\[
\text{SNR}_r = \text{SNR}_s(\ell) \approx \frac{M}{L} \text{SNR}_f.
\]
(7)

### III. Secret Key Capacity

In this section, we introduce the measurement model and compare two secret key extraction methods.

#### A. Measurement Model and Capacity from Channel Coefficients

From (1), we model Alice and Bob’s measurements as:
\[
H_{A,n} = H_n + w_{A,n}
\]
\[
H_{B,n} = H_n + w_{B,n},
\]
(8)
respectively where \(w_{A,n}, w_{B,n} \sim \mathcal{CN}(0, \sigma_n^2)\) are independent sources of noise. We can also consider the time domain observation as:
\[
h_{A,\ell} = \Re(h_{A,\ell}) + j\Im(h_{A,\ell}) = h_{\ell} + n_{A,\ell}
\]
\[
h_{B,\ell} = \Re(h_{B,\ell}) + j\Im(h_{B,\ell}) = h_{\ell} + n_{B,\ell},
\]
(9)
where \(h_{\ell} \sim \mathcal{CN}(0, \sigma_h(\ell)^2)\) is the sampled channel coefficient and \(n_{A,\ell}, n_{A,\ell} \sim \mathcal{CN}(0, \sigma_n^2)\) are the noises. The correlation coefficient in \(\ell^{th}\) sampled channel coefficient is given as:
\[
\rho_r(\ell) = \frac{\sigma_h(\ell)^2}{\sigma_h(\ell)^2 + \sigma_n^2} = \frac{\text{SNR}_r(\ell)}{1 + \text{SNR}_r(\ell)}.
\]
(10)

Note that the correlation coefficient \(\rho_r(\ell)\) between \(h_{A,\ell}\) and \(h_{B,\ell}\) is equal to the correlation coefficient between \(\Re(h_{A,\ell})\) and \(\Re(h_{B,\ell})\) or equivalently equal to that between \(\Im(h_{A,\ell})\) and \(\Im(h_{B,\ell})\). With the correlation coefficient defined above, the mutual information between Alice and Bob at sampled coefficient domain is represented by:
\[
I(A;B) \approx \sum_{\ell=0}^{L-1} -\log \left[ 1 - \left( \frac{\text{SNR}_r(\ell)}{1 + \text{SNR}_r(\ell)} \right)^2 \right],
\]
(11)
and the secret key capacity is given by:
\[
C \approx \frac{1}{2M} \sum_{\ell=0}^{L-1} -\log \left[ 1 - \left( \frac{\text{SNR}_r(\ell)}{1 + \text{SNR}_r(\ell)} \right)^2 \right],
\]
(12)
Note that the mutual information between Alice and Bob at a particular sampled channel coefficient consists of the sum of mutual information between real and imaginary parts of that coefficient and the total number of observation symbol is \(2M\). If we assume sampled coefficients to have equal variance, \(\rho_r(\ell)\) does not depend on \(\ell\) and the secret key capacity reduces to:
\[
C \approx \frac{L}{2M} \log \left[ 1 - \left( \frac{\text{SNR}_r}{1 + \text{SNR}_r(\ell)} \right)^2 \right].
\]
(13)

We comment that if we have access to the statistics of frequency domain coefficients, the secret key capacity between Alice and Bob can be equivalently calculated from frequency domain channel coefficients. To do this, we perform eigenvalue decomposition (EVD) on the correlation matrix of frequency domain coefficients thus completely decorrelate those frequency domain coefficients into independent entities and the mutual information is the sum of the mutual information of these entities. The secret key capacity is then the total mutual information normalized by \(2M\). However, we may not be able to do this in the actual operation of the system because the training between Alice and Bob may only occur few times before they have enough statistics of frequency domain coefficients unless it is an available prior.

#### B. Compared with RSSI-Based Approach

In this section we study the secret key capacity under an idealized model wherein all sampled channel coefficients have the same variance. We let \(h_{A,\ell}, h_{B,\ell}\) be \(\mathcal{CN}(0, \sigma^2)\) where \(\sigma^2 = \sigma_h^2 + \sigma_n^2\). Note that \(\Re(h_{A,\ell}), \Re(h_{B,\ell})\) have correlation coefficient \(\rho_r\) which does not depend on \(\ell\) and \(\Im(h_{A,\ell}), \Im(h_{B,\ell})\) also have the same correlation coefficient \(\rho_r\). The secret key capacity between Alice and Bob now reduces to (13). We show in this section that secret key extraction based on channel coefficients is superior to the one based on RSSI.

The secret key capacity obtained from sampled channel coefficients can be calculated using (13). To calculate the secret key capacity between RSSIs, let \(R_A\) and \(R_B\) denote the RSSI received by Alice and Bob respectively. In an OFDM
system, the RSSI typically takes the form [14]:

\[
R_A = \sum_{\ell=0}^{L-1} |h_{A,\ell}|^2 = \sum_{\ell=0}^{L-1} |\Re(h_{A,\ell})|^2 + \sum_{\ell=0}^{L-1} |\Im(h_{A,\ell})|^2 = 2L-1 X_{A,\ell}^2,
\]

\[
R_B = \sum_{\ell=0}^{L-1} |h_{B,\ell}|^2 = \sum_{\ell=0}^{L-1} |\Re(h_{B,\ell})|^2 + \sum_{\ell=0}^{L-1} |\Im(h_{B,\ell})|^2 = 2L-1 X_{B,\ell}^2,
\]

where \(X_{A,\ell}\) and \(X_{B,\ell}\) are \(\mathcal{N}(0, \frac{\sigma^2}{2})\) Gaussian random variables with correlation coefficient \(\rho_{\tau}\). Both \(R_A\) and \(R_B\) are non-standard chi-square distributed random variables with \(2L\) degree of freedom. However, as we are only interested in \(I(R_A; R_B)\) and since \(I(R_A; R_B)\) equals to \(I(aR_A; aR_B)\) with \(a\) being a non-zero constant, we can normalize \(X_{A,\ell}\) and \(X_{B,\ell}\) by the variance so that both \(R_A\) and \(R_B\) are standard chi-square distributed random variables with \(2L\) degree of freedom. The secret key capacity is then given by:

\[
C_{RSSI} = \frac{1}{2M} I(R_A; R_B).
\]  

The joint density function of two standard chi-square random variables can be found in [15] and it is used to numerically calculate the mutual information \(I(R_A; R_B)\).

When \(L\) is large, \(R_A\) and \(R_B\) can be well approximated as Gaussian random variables due to the central limit theorem (CLT). With the variance normalization, \(E[X_{A,\ell}^2] = 1\), \(E[X_{A,\ell}^4] = 3\), and \(Var[X_{A,\ell}] = 2\), \(R_A\) and \(R_B\) are both \(\mathcal{N}(2L, 4L)\) random variables. The mutual information between RSSIs under Gaussian approximation can be calculated as:

\[
I(R_A, R_B) = \frac{1}{2} \log \left( \frac{1}{1 - \rho_{\tau}^2} \right),
\]

and the secret key capacity is given by:

\[
C_{RSSI} = \frac{1}{4M} \log \left( \frac{1}{1 - \rho_{\tau}^2} \right).
\]

Observe from (17) that the secret key capacity does not depend on \(L\). In other words, at a given \(SNR_{\ell}\), while the capacity between coefficients increases linearly with \(L\) as shown in equation (13), the capacity between RSSIs stays the same. This is because there is only one single RSSI value regardless of the number of observations. In Fig. 2, we compare the capacity obtained from channel coefficients and from RSSIs for \(L = 2, 5\) and 10 with \(M = 10\). The secret key capacity between the channel coefficients is calculated using (13) and that between RSSIs is calculated both using numerical (15) and Gaussian approximation (17). We first note that the secret key capacity obtained from the channel coefficients increases with \(L\), whereas that based on RSSI stays constant. Furthermore, Gaussian approximation is quite accurate, even when \(L\) is rather small.

In this section we prototype a key reconciliation system based on LDPC codes. Alice initiates the reconciliation process by sending Bob the syndrome \(S\) which is the index of the bin her quantized observation \(X\) belongs to. Her sequence \(X\) is obtained by quantizing the real and imaginary parts of sampled channel coefficients \(h_{A,\ell}, \ell = 0, 1, \ldots, L - 1\) she observes. Since Alice may observe multiple copies of \(h_{A,\ell}\), we assume \(X\) has length \(N\). Then based on the received bin index and his own observation \(Y\), Bob tries to find the most correlated sequence \(\hat{X}\) which is in the same bin indexed by \(S\). This problem can be best expressed as a decoding-with-side-information problem as shown in Fig. 3. After decoding, if Bob’s decoded result is equal to Alice’s observation, a secret key can be extracted and the process terminates.

Under binary quantization, \(X \in \{0, 1\}^N\), \(Y \in \mathcal{Y}^N\) and \(S \in \{0, 1\}^{N(1-R)}\) where \(R\) is the rate of the underlying LDPC code. The Slepian-Wolf theorem [16] says that the syndrome decoding succeeds with error probability approaching 0 as \(N\) approaches infinity, given the condition that \(1 - R > \frac{1}{2} H(X|Y)\). Note that \(R\) has the unit \(bits\ per\ sampled\ coefficient\) and a scaling of \(\frac{1}{L}\) is needed to convert to \(bits\ per\ frequency\ domain\ coefficient\) which secret key capacity is
based upon.

We construct regular LDPC codes using a code generating engine [17] and we build irregular LDPC codes using density evolution [18]. To meet the requirement of 4-level quantization, we also design a non-binary LDPC code in $GF(4)$. To implement our 4-ary codes we combine two binary LDPC codes and augment these two corresponding factor graphs by extra factor nodes that encode the mapping from 4-ary variables to binary variables. The decoding algorithm runs belief propagation (BP) on this augmented factor graph.

V. SIMULATION RESULTS

In this section we provide simulation results and discussion for the theoretical models proposed in previous sections.

A. OFDM Simulation Results

We first show the simulation result of an IEEE 802.11a channel. We simulate the frequency and sampled channel coefficients and their correlation matrices. Then we numerically compute the empirical secret key capacity between Alice and Bob based on our simulated frequency and time domain channel coefficients under different channel environment.

1) Channel Coefficients Simulation: An 802.11a OFDM channel with rich multipath typically has the following key parameters [19]:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Tones ($M$)</td>
<td>52</td>
</tr>
<tr>
<td>Signal Bandwidth ($W$)</td>
<td>20 MHz</td>
</tr>
<tr>
<td>Signal Duration ($T_s$)</td>
<td>3.2 µs</td>
</tr>
<tr>
<td>Carrier Frequency Spacing ($\Delta f$)</td>
<td>312.5 kHz</td>
</tr>
<tr>
<td>Center Carrier Frequency ($F_c$)</td>
<td>5.18 GHz</td>
</tr>
</tbody>
</table>

We consider $N_p = 300$ multipath and assume the 52 tones all have the same $SNR_f$ (3). For simplicity, we choose the maximum delay spread $\tau_{max}$ to be 650 ns so that the degree of freedom (DoF) $L \approx \lceil \tau_{max} W \rceil = 13$. We reduce the redundancy in the $M = 52$ frequency domain channel coefficients by using the IDFT transform to obtain 13 approximately independent sampled channel coefficients. Note that these coefficients will not have the same variance as was ideally assumed in Section III-B. We perform $10^5$ independent channel realizations and the sets of complex path gain $\beta_k$'s are independent across realizations. We construct the contour plots of correlation matrices of frequency domain channel coefficients and sampled channel coefficients as shown in Fig. 4. The plot shows how frequency domain coefficients are correlated with each other and how sampled coefficients are correlated with each other.

2) Secret Key Capacity Simulation: We can characterize the secret key capacity between Alice and Bob in two different ways: one from the sampled channel coefficients using (12) and one from the frequency domain channel coefficients. We calculate it from the frequency domain channel coefficients. Recall that we have simulated the empirical correlation matrix of frequency domain coefficients, we can perform eigenvalue decomposition (EVD) on this correlation matrix to decorrelate the frequency domain coefficients. Note that this requires the actual statistics of frequency domain coefficients which may not be obtainable in actual operation of our system. Fig. 5 provides the secret key capacity drawn from frequency domain channel coefficients where we plot it under $L = 1, 13$ and 52 versus $SNR_f$.

Simulation in Fig. 5 suggest that there is no single optimal OFDM channel which has the best secret key capacity under any $SNR_f$: under low $SNR_f$, one would like to have fewer degree of freedom; under high $SNR_f$, one would like to have more degree of freedom.

B. Slepian-Wolf Decoding

There are basically two ways for an error correcting code to reconcile their measured channel coefficients. If they both quantize their channel coefficients and obtain two quantized sequences, we call this hard decoding process. On the other hand, if only Alice quantizes her channel coefficients and Bob keeps his unquantized coefficients, we call this soft decoding process. In soft decoding process, the decoder has access to Bob’s full unquantized channel coefficients which improves
We study channel randomness and propose a practical system that can be used to generate secret keys based on channel randomness. We investigate the secret key capacity shared by two end-users and conclude that channel-coefficients-based approach is superior to RSSI-based approach in the sense that the former gives higher secret key capacity. The simulation show that it is feasible to work on sampled channel coefficients. Regular and Irregular LDPC codes with the Slepian-Wolf decoding structure are designed to reconcile the two users to help them establish the same observation.

VI. CONCLUSION

We study channel randomness and propose a practical system that can be used to generate secret keys based on channel randomness. We investigate the secret key capacity shared by two end-users and conclude that channel-coefficients-based approach is superior to RSSI-based approach in the sense that the former gives higher secret key capacity. The simulation show that it is feasible to work on sampled channel coefficients. Regular and Irregular LDPC codes with the Slepian-Wolf decoding structure are designed to reconcile the two users to help them establish the same observation.

REFERENCES