Channel Secondary Random Process for Robust Secret Key Generation

Ahmed Badawy*†, Tamer Khattab†, Tarek ElFouly‡, Carla-Fabiana Chiasserini *, Amr Mohamed‡ and Daniele Trinchero*
*Politecnico di Torino, DET. (ahmed.badawy, daniele.trinchero, chiasserini@polito.it)
†Qatar University, Electrical Engineering Dept. (tkhattab@qu.edu.qa)
‡Qatar University, Computer Engineering Dept. (tarekfouly,amrm@qu.edu.qa)

***Abstract*—The broadcast nature of wireless communications imposes the risk of information leakage to adversarial users or unauthorized receivers. Therefore, information security between intended users remains a challenging issue. Most of the current physical layer security techniques exploit channel randomness as a common source between two legitimate nodes to extract a secret key. In this paper, we propose a new simple technique to generate the secret key. Specifically, we exploit the estimated channel to generate a secondary random process (SRP) that is common between the two legitimate nodes. We compare the estimated channel gain and phase to a preset threshold. The moving differences between the locations at which the estimated channel gain and phase exceed the threshold are the realization of our SRP. We simulate an orthogonal frequency division multiplexing (OFDM) system and show that our proposed technique provides a drastic improvement in the key bit mismatch rate (BMR) between the legitimate nodes when compared to the techniques that exploit the estimated channel gain or phase directly. In addition to that, the secret key generated through our technique is longer than that generated by conventional techniques.**

***Index Terms*—Physical layer security, Secret key generation, Bit mismatch rate, Channel estimation, OFDM systems.**

I. INTRODUCTION

Orthogonal frequency division multiplexing (OFDM) is a multi-carrier modulation scheme that has been widely adopted in many wireless communication system such as Long Term Evolution (LTE) systems [1]. It provides many advantages over the single-carrier modulation schemes, including : high data rate, immunity to selective fading, resilience to inter-symbol interference and higher spectrum efficiency [2].

As in any wireless communication system, security of OFDM wireless system is a critical issue. Currently, security relies on cryptographic techniques and protocols that lie at the upper layers of the wireless network. One main drawback of these solutions is the necessity of a complex key management scheme in the case of symmetric ciphers and high computational complexity in the case of asymmetric ciphers. On the other hand, physical layer security relies on the randomness of the communication channel and has a much lower computational complexity.

Within the paradigm of physical layer security, typically a physical layer specific characteristic is used as key generator to guarantee information hiding from eavesdroppers. Such techniques are based on channel reciprocity assumption. When two antennas communicate by radiating the same signal through a linear and isotropic channel, the received signals by each antenna will be identical. This is due to the reciprocity of the radiating and receiving antenna pattern [3], [4].

In [5]–[8], channel measurements were exploited to solve the problem of secret key generation (SKG). In [5] the authors observed that the maximum size of the generated secret key mainly depends on the mutual information between the channel estimates at the two legitimate nodes. They also derived an expression for the mutual information for a general multipath channel. The most common feature of the channel characteristics that is widely used is channel gain, mainly because of its ease of implementation [7], [9]. Others exploit the channel phase to generate the secret key as in [10], [11]. Unlike channel gain, channel phase is uniformly distributed in narrowband fading channels. The authors in [10] were able to generate a *long* key as compared to the conventional cryptographic techniques from the estimated channel phase, while in [11], they extend their system to the use of relay nodes. Exploiting the channel estimates to generate a secret key has also been investigated under multiple antenna scenarios [12] and relaying scenarios [13].

In [9], [14], the authors presented a popular technique to extract a secret key that is based on level crossing of the estimated channel gain. The main advantage of their level crossing techniques is that it achieves a low bit mismatch rate (BMR) between the key generated at the legitimate nodes. The authors studied the channel probing rate effect on the secret key rate for different doppler shifts. They found that secret key rate increases as the probing rate increases and saturates at 20 KHz probing rate for the worst case doppler shift they assumed. The smaller the doppler shift the smaller the probing rate required to saturate the secret key rate. In [7], the authors observed that as the carrier frequency increases, the probing rate should increase to achieve a suitable key rate. This is mainly because the channel temporal variation increases at higher carrier frequencies.

One main advantage of exploiting channel estimates to generate the secret key is its high key generation rate. However, a main drawback of exploiting the channel reciprocity to generate secret keys is that the additive white Gaussian noise (AWGN) at both receivers affects the reciprocity of the channel measurements [15]. This drawback causes the BMR between the legitimate nodes to rise, which affects the operation of the

SKG based on channel estimates at low and medium signal to noise ratio (SNR) scenarios.

In this paper, we propose a robust technique to generate the secret key which we apply on the estimated channel gain only, channel phase only and combined gain and phase, which enhances the performance of the SKG system at low and medium SNR levels. In our technique, the estimated channel is considered our primary random process, from which we derive a secondary random process (SRP) that is then used to generate the secret key. The primary random process, which is either the estimated channel gain or phase, is compared to a preset threshold. The locations of the realizations at which the primary random process exceeds the threshold are stored. The moving increments, which is the difference between each two adjacent locations, are the realizations of our SRP. Those realizations are then used to generate the secret key. Our proposed technique improves the BMR drastically and achieves a longer key length than the conventional techniques.

The rest of this paper is organized as follows: In Section II the system model is presented. Related existing techniques are addressed in Section III. Our proposed channel SRP for SKG technique is presented in Section IV. We evaluate the performance of our solution in Section V. The paper is then concluded in Section VI.

II. System Model

We assume that there exist two legitimate nodes, named Alice and Bob, trying to secure a communicating link, and that each of them used OFDM for transmission/reception. In particular, consider an OFDM system where each OFDM symbol consists of N orthogonal subcarriers. After modulating the input serial data streams, a serial to parallel converter converts serial data symbols to N parallel streams, resulting in $X[k]$ for $k = 0, 1, ..., N-1$. We assume that N_p pilots are inserted for the measurement of channel conditions yielding X_p for $p = 1, ..., N_p$. The vector $X[k]$ is then used as input to an N-point Inverse Fast Fourier Transform (IFFT). The time domain signal is now:

$$x[n] = IFFT\{X[k]\} \qquad n = 0, 1, 2, N-1. \quad (1)$$

A guard interval of length N_g, also known as cyclic prefix is appended according to:

$$x_f[n] = \begin{cases} x[n+N], & n = N_g, -Ng+1, ..., -1, \\ x[n], & n = 0, 1, .., N-1. \end{cases} \quad (2)$$

$x_f[n]$ is then passed through a parallel to serial converter and digital to analog converter, which is then transmitted to the other node. The received signal, as exchanged between Alice and Bob, can be given by:

$$y_f^A = x_f^B[n] \otimes h[n] + w_A[n], \quad (3)$$

$$y_f^B = x_f^A[n] \otimes h[n] + w_B[n], \quad (4)$$

where x_f^B is the transmitted signal from Bob to Alice, x_f^A is the transmitted signal from Alice to Bob, h is a random process that describes the wireless channel between Alice and Bob and w_A and w_B are the additive white Gaussian noise (AWGN) at Alice and Bob's receivers, respectively. Note that the pilots, also known as training signals or reference signal, within x_f^A and x_f^B are identical. The guard interval is then removed from the received signal yielding $y[n] = y_f[n]$ for $n = 0, 1, ..., N-1$. $y[n]$ is then passed through an N-point FFT yielding the frequency domain signal $Y[k] = FFT\{y[n]\}$ $k = 0, 1, ..., N-1$. The pilots, whose locations are already known, are then extracted from $Y[k]$ yielding Y_p, where $p = 1, ..., N_p$. Note that the signal exchange between Alice and Bob is performed during the coherence time of the channel.

For simplicity, we estimate the channel through the least squares (LS) estimator in the frequency domain. The LS estimator minimizes the squared error as [16]:

$$\hat{H} = \arg\min ||Y_p - X_p H||. \quad (5)$$

The estimated channel at both Alice and Bob can be given by:

$$\hat{H}_{LS}^A = \left(X_p^H X_p\right)^{-1} X_p^H Y_p^A, \quad (6)$$

$$\hat{H}_{LS}^B = \left(X_p^H X_p\right)^{-1} X_p^H Y_p^B, \quad (7)$$

where $(.)^H$ denotes the Hermitian operation. The estimated channel at the pilot locations are then interpolated to estimate the channel across the entire OFDM symbol. The estimated channel gains at Alice and Bob $|\hat{H}_{LS}^A|$ and $|\hat{H}_{LS}^B|$ as well as the phases, which are the angles of $\hat{H}_{LS}^A$ and $\hat{H}_{LS}^B$, are the common sources of randomness which are typically used to generate the secret key and from which we will derive our SRP.

In our adversary model, we assume that an eavesdropper (Eve) can listen to all the communications between the two trusted communicating nodes (Alice) and (Bob). However, Eve can estimate the channel between itself and both Alice and Bob. Eve can not be within a few wavelength near to either Alice or Bob, which ensures that her estimated channel between either of them is independent of that between Alice and Bob. We assume that Eve is a passive adversary.

III. Existing Techniques

The most typical steps employed in SKG techniques are presented in Figure 1. In the first step, Alice and Bob exchange beacon signals, from which each estimates the physical layer characteristics that are used as common source of randomness. In our case, they estimate the channel gain or phase. The channel measurements are then quantized and converted into stream of bits. This is followed by an information reconciliation as well as a privacy amplification step to be applied at the two streams of bits.

Although uniform quantization is easy to implement, increasing the quantization bit number dramatically degrades the performance of the technique since the BMR between the Alice and Bob increases. In [8], an encoding algorithm is proposed to tackle this problem where each uniformly quantized value is encoded with multiple values. It is worth noting that a lower BMR after the quantization step leads to a longer key, which increases the technique's efficiency.

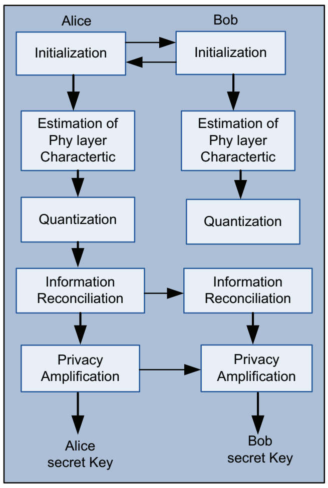

Fig. 1: Typical steps for SKG

Another popular technique to address the BMR is presented in [9], [14]. Their solution is based on level crossing of the estimated channel gain. They first use the statistics of the estimated channel gain to compute two thresholds (q_+ and q_-). Alice determines the locations of her estimated channel gain, which is stored in a vector L_A, that are above q_+ or below q_- for a duration of m successive estimates. Alice then sends those locations to Bob. Bob then compares his estimated channel gain at the locations in L_A to determine L_B at which the estimated channel gain are higher than q_+ or below q_- for a duration of $m-1$ successive estimates. Bob's estimated locations L_B, which is a subset of L_A are sent back to Alice. The channel estimates at the locations L_B at both Alice and Bob are then quantized and converted into bitstreams. The main difference between the level crossing technique and the traditional techniques is that the information reconciliation step is performed before the quantization and the bitstream generation. This leads to a much better BMR but at the cost of much shorter key length. To address this drawback, the authors of [9], [14] have proposed to increase the propping rate of the channel.

IV. Proposed SRP Technique

We propose a simple SKG technique exploiting, *indirectly*, the estimated channel. Our technique can be applied on the channel gain only, phase only or a combination of the channel gain and phase as we will show later. It is assumed that Alice and Bob have exchanged signals within the coherence time of the channel. They then have estimated the channel using (7). They applied an interpolation technique on their channel estimates at the pilot locations to estimate the channel across the entire OFDM symbol. It is worth noting that our technique is not exclusive to OFDM systems, rather it can be applied on the estimated channel in presence of any other system.

A. Creating a secondary random process

Due to the reciprocity of the channel, the channel estimates at Alice and Bob, $\hat{H}^A_{LS}$ and $\hat{H}^B_{LS}$, are supposed to be identical. However, because of the AWGN added at the two receivers, $\hat{H}^A_{LS}$ and $\hat{H}^B_{LS}$ are not identical. To address the BMR issue explained earlier, we generate a *secondary* random process from the channel estimates. This SRP is then used as common source of randomness to generate the secret key. The steps which can be applied on the estimated channel gain or phase, are reported below. The steps are reported for the channel gain and apply similarly to the phase. For simplicity, we limit the description below to the case in which they are applied to the estimated channel gain. The steps to generate our SRP are:

1) Both Alice and Bob use their estimated channel gain to estimate a threshold (γ_g) as:
$$\gamma^A_g = E[|\hat{H}^A_{LS}|] + \alpha std(|\hat{H}^A_{LS}|) \tag{8}$$
$$\gamma^B_g = E[|\hat{H}^B_{LS}|] + \alpha std(|\hat{H}^B_{LS}|), \tag{9}$$
where $E[.]$ is the mean operation, $std(.)$ is the standard deviation operation and α is a design parameter $\in [-1 : 1]$.
2) Both Alice and Bob compare their channel gain, recursively to the preset threshold γ_g.
3) If the channel estimate is higher than the preset threshold, the location, i.e, the index (x-axis) is stored in a vector S initialized to all zeros. Both Alice and Bob estimate their vectors as S^A_g and S^B_g.
4) Both Alice and Bob then estimate the moving increment of their estimated locations J^A_g and J^B_g for channel gain, which are computed as:
$$J^A_g[i] = S^A_g[i+1] - S^A_g[i], \quad i = 1, ..., N-1, \tag{10}$$
$$J^B_g[i] = S^B_g[i+1] - S^B_g[i], \quad i = 1, ..., N-1. \tag{11}$$

The realizations in the vectors J^A_g and J^B_g constitute the realizations of our *secondary* random process. In other words, we have created two SRPs, one for the channel gain and another for the channel phase. These SRPs are considered our new common sources of randomness which are then used by Alice and Bob to generate the secret key. In V, we provide an example of our SRP. Alice and Bob can use SRP extracted from channel gain only, channel phase only or a combination of the two for the SKG.

B. Quantization

Now that we have our *secondary* common sources of randomness estimated at both Alice and Bob, the next step is to convert them into a bit stream suitable for the SKG. The most popular technique for quantization is the uniform quantization. In the uniform quantization, the spaces along the x-axis is uniformly distributed. Similarly for the spaces in the y-axis, i.e., the estimated *secondary* common source of randomness. When using n_q bits as the number of quantization bits, there will exist 2^{n_q} levels to quantize the common sources of randomness. The quantized decimal valued are then converted into bits.

C. Information Reconciliation and Privacy Amplification

The generated bit streams at Alice and Bob might have some discrepancy, particularly at very low SNR levels. This is due to several reasons such as interference, noise and hardware limitations. A reconciliation protocol such as the one presented in [17] will be used to minimize the discrepancy. Both Alice and Bob first permute their bit streams in the same way. Then they divide the permuted bit stream into small blocks. Alice then sends permutations and parities of each block to Bob. Bob compares the received parity information with the ones he already processed. In case of a parity mismatch, Bob changes his bits in this block to match the received ones.

Although information reconciliation protocol leaks minimum information, the eavesdropper can still use this leaked information to guess the rest of the secret key. Privacy amplification solves this issue by reducing the length of the output bit stream. The generated bit stream is shorter in length but higher in entropy. To do so, both Alice and Bob apply a universal hash function selected randomly from a set of hash functions known by both Alice and Bob. Alice sends the number of the selected hash function to Bob so that Bob can use the same hash function.

Our SKG technique is summarized in Algorithm 1 for the channel gain. It is assumed that Alice and Bob have already estimated the channel. Same steps can be applied to the channel phase.

V. Performance Evaluation

To evaluate the performance of our technique, we simulate an entire OFDM system and estimate the channel using the LS estimator. Table I summarizes our simulation parameters for the subsequent figures. We simulate the conventional channel gain and phase techniques, level crossing technique, and proposed SRP technique for channel gain only and for channel phase only. Then we obtain the combined SRP by concatenating bitstreams from SRP channel gain and phase.

TABLE I: Simulation parameters

Parameter	Value
No. of subcarriers	1024
No. of FFT point	1024
Subcarrier spacing	15 KHz
Number of pilots	16.7%=171
Cyclic prefix length	25%=256
Modulation scheme	QPSK
Channel type	Rayleigh
Doppler shift	100 Hz
Chan. Estimation	LS
Interpolation type	Linear
α	-0.2
m for Level crossing	4
n_q	8 bits
Number of iterations	10000

Algorithm 1 Proposed SRP SKG Technique for Channel Gain

Step 1: Creating secondary random process
Alice and Bob estimate their thresholds using (8) and (9).
Both Alice and Bob apply the following steps on $|\hat{H}^A_{LS}|$ and $|\hat{H}^A_{LS}|$.
for i = *1: length(*$|\hat{H}^A_{LS}|$*)* **do**
  if $|\hat{H}_{LS}| > \gamma_g$ **then**
    $S[i] = i$
  else
    $S[i] = 0$
  end if
end for
Both Alice and Bob estimate $J^A_g = S^A_g[i+1] - S^A_g[i]$ and $J^B_g = S^B_g[i+1] - S^B_g[i]$.
Step 2: Uniform Quantization
Alice and Bob use n_q to quantize J^A_g and J^B_g.
Alice and Bon convert their quantized values into bit-streams.
Step 3: Information Reconciliation
Alice and Bob permute the bit stream and divide them into small blocks.
Alice sends the permutation and parities to Bob.
Bob compares the received parity information with his own.
In case of mismatch, Bob corrects his bits accordingly.
Step 4: Privacy Amplification
Alice sends the number of the hash function to Bob.
Alice and Bob apply the hash function to the bit stream.

Our combined vectors are given by:

$$J^A_c = [J^A_g[1], J^A_p[1], J^A_g[2], J^A_p[2], ..., J^A_g[N], J^A_p[N]], \quad (12)$$
$$J^B_c = [J^B_g[1], J^B_p[1], J^B_g[2], J^B_p[2], ..., J^B_g[N], J^B_p[N]]. \quad (13)$$

To show the effect of our proposed SRP technique on the BMR, we simulate all techniques up to the quantization and bitstream generation step. For a fair comparison, the level crossing technique is simulated without the information reconciliation step. In other words, channel estimates at the locations L_A at both Alice and Bob are quantized and converted into bitstreams.

A. SRP

In Figure 2-(a), we plot the estimated channel gain at both Alice and Bob, for SNR = 20 dB and the thresholds estimated from (8) and (9). We then follow the steps in Section IV-A to estimate J^A_g and J^B_g and plot them in Figure 2-(b). Our SRP is similar to a Gaussian random process with linearly increasing variance.

B. BMR

We plot the BMR between the secret keys generated at Alice and Bob for all the techniques in Figure 3. Our proposed SRP techniques drastically improve the BMR achieving a BMR that is ranging from 10-15% at low and high SNR levels to 25% at medium SNR levels less than that of the conventional channel gain and phase. In addition to that our proposed SRP is

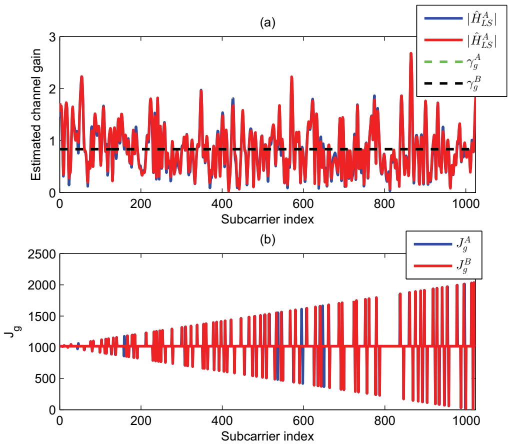

Fig. 2: (a) Estimated channel gain at Alice and Bob with γ_g^A and γ_g^B and (b) our estimated J_A and J_B.

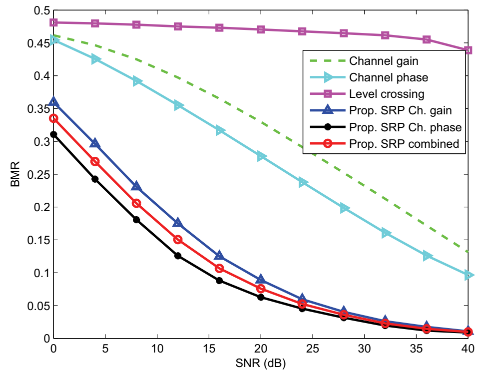

Fig. 3: BMR as a function of SNR for our scheme vs. existing techniques.

achieving a BMR that is ranging from 12% at low SNR levels to 40% at medium and high SNR levels less than that of the level crossing technique. It is worth noting that on average the worst BMR achieved is 0.5 which is equivalent to random guessing. The level crossing is performing worst achieving the highest BMR, which indicates that the strength of the level crossing algorithm derives from the information reconciliation step. The combined SRP technique achieves a BMR that is average between the SRP channel gain and phase. Also, as expected, as the SNR increases, the BMR for all techniques improves.

C. Entropy

Entropy is a measure of level of randomness of the generated key. For example, for our SRP channel gain, the entropy of a secret key generated from Alice's estimated channel gain is defined as $\mathcal{H}(J_g^A) = \log\left(1/f(J_g^A)\right)$ with $f(.)$ denoting the probability mass function. The average entropy is then $E[\mathcal{H}(J_g^A)]$. As expected from Figure 2-(b), the average entropy of our SRP secret key will be less than that of the channel gain. We plot the achieved average entropy of all techniques in Figure 4. Our SRP channel gain and phase exhibit less entropy than all other techniques. That was the motivation behind proposing combined SRP technique - than our benchmark techniques. Also, it is worth nothing that the combined SRP technique does not increase the complexity of the system since both channel gain and phase can be calculated from the channel estimates. In addition to that, it only requires a simple concatenation operation.

D. Key Length

Figure 5 shows the simulated key length of all techniques normalized to the length of the secret key generated through the conventional channel gain technique. Our proposed SRP channel gain and phase is achieving approximately the same key length as of that of the channel gain and phase techniques,

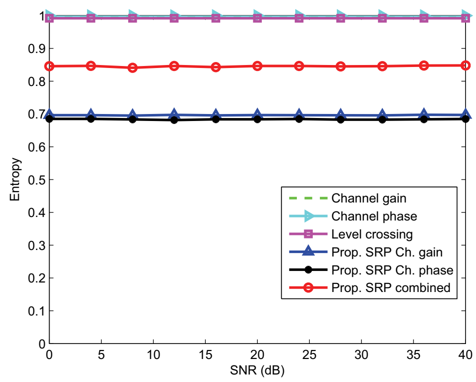

Fig. 4: Entropy as a function of SNR for our scheme vs. existing techniques.

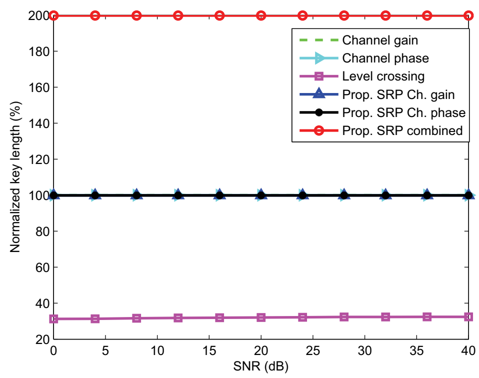

Fig. 5: Normalized key length as a function of SNR for our scheme vs. existing techniques.

while SRP combined is achieving twice that length. On the contrary, the level crossing technique is performing the worst achieving a normalized key length of 30%. This implies that for the level crossing rate technique to achieve a reasonable key length, the frequency of channel propping should increase which decreases the throughput of the system.

E. Secrecy Rate

Since our generated SRPs are independent and identically distributed (i.i.d.), our secret key rate after the information reconciliation and privacy amplification exhibit the same results presented in [18]. For example, the upper and lower bounds for the channel gain SRP are given by:

$$R_g^U(J_g^A; J_g^B||J_g^E) \leq \min\left[I(J_g^A; J_g^B), I(J_g^A; J_g^B|J_g^E)\right], \quad (14)$$

$$\begin{aligned} R_g^L(J_g^A; J_g^B||J_g^E) \geq \max[&I(J_g^B; J_g^A) \\ &- I(J_g^E; J_g^A), I(J_g^A; J_g^B) - I(J_g^E; J_g^B)], \end{aligned} \quad (15)$$

where $I(J_g^A; J_g^B)$ is the mutual information between J_g^A and J_g^B and $I(J_g^A; J_g^B|J_g^E)$ is the mutual information between J_g^A and J_g^B given J_g^E for the eavesdropper Eve. The supremum of the secret key rate is considered the secret key capacity C_g:

$$\begin{aligned} C_g &= \max_{P_{J_g^A}} S(J_g^A; J_g^B||J_g^E) \\ &\leq \min\left[\max_{P_{J_g^A}} I(J_g^A; J_g^B), \max_{P_{J_g^A}} I(J_g^A; J_g^B|J_g^E)\right] \end{aligned} \quad (16)$$

where $P_{J_g^A}$ is the probability density function of J_g^A.

VI. Conclusion

We proposed a simple yet robust technique to extract a secret key from a secondary random process that is derived from the channel estimates. We showed that our SRP technique can be applied on the channel gain only, channel phase only as well as a combination of the two. We simulated our technique using a complete OFDM system and compared its performance to existing techniques. Our SPR techniques provided a drastic improve in the BMR, and achieved comparable entropy and a much longer key length in the case of the combined SRPs. In addition, our SRP solution is easy to implement and does not increase the complexity of the system.

Acknowledgment

This research was made possible by NPRP 5-559-2-227 grant from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] 3GPP, "The 3rd generation partnership project, url = http://www.3gpp.org."

[2] T. Hwang, C. Yang, G. Wu, S. Li, and G. Li, "Ofdm and its wireless applications: A survey," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 4, pp. 1673–1694, May 2009.

[3] C. A. Balanis, *Antenna theory: analysis and design*. John Wiley & Sons, 2012.

[4] G. Smith, "A direct derivation of a single-antenna reciprocity relation for the time domain," *Antennas and Propagation, IEEE Transactions on*, vol. 52, no. 6, pp. 1568–1577, 2004.

[5] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, 2007.

[6] 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*, ser. CCS '07, 2007, pp. 401–410.

[7] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM Workshop on Wireless Security*, ser. WiSe '06, 2006, pp. 33–42.

[8] J. Zhang, S. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–5.

[9] 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*, ser. MobiCom '08, 2008, pp. 128–139.

[10] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207 – 212, 1996. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1051200496900238

[11] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 9, pp. 1666–1674, October 2012.

[12] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 3, pp. 381–392, Sept 2010.

[13] H. Zhou, L. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 3, pp. 476–488, March 2014.

[14] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, June 2010.

[15] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, 2010.

[16] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1993.

[17] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion." Springer-Verlag, 1994, pp. 410–423.

[18] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, 1993.