Towards Robust Key Extraction from Multipath Wireless Channels

Youssef El Hajj Shehadeh, Omar Alfandi, and Dieter Hogrefe
Institute of Computer Science, University of Goettingen, Germany
E-mail: {shehadeh, alfandi, hogrefe}@informatik.uni-goettingen.de

Abstract: **This paper tackles the problem of generating shared secret keys based on the physical characteristics of the wireless channel. We propose intelligent quantization mechanisms for key generation, achieving high secret bits generation rate. Moreover, some practical issues affecting the performance of the key generation mechanism are deeply investigated. Mainly, we investigate the effects of delay and mobility on the performance and we enhance the key generation mechanism accordingly. As a result, this paper presents a framework towards robust key generation from multipath wireless channels.**

Index Terms: **Physical-layer security, key generation, multipath channel, intelligent quantization, practical issues.**

I. Introduction

WIRELESS communications have encountered a considerable improvement and have integrated human life through various applications, mainly by the widespread of mobile Ad hoc and sensor networks. But due to the broadcast nature of wireless communications, security remains a major concern in many applications. Actually, traditional security protocols rely mainly on cryptography and hashing functions, and other mathematical properties to fulfill their goals [1].

Yet, these security protocols are difficult to implement in some applications. In fact, one of the main requirements of communication security is the distribution of secret keys between communicating nodes. Some traditional solutions consider Public Key Infrastructure (PKI) mechanisms for key exchange [1] (e.g. Diffie Hellman) in the presence of a Certification Authority (CA). But PKI mechanisms are only computationally secure and require high computational complexity. In addition, the requirement of having a CA makes these solutions unpractical in some scenarios, mainly in Ad hoc and sensor networks.

Other solutions consider key predistribution schemes (see for example [2]). However, key predistribution schemes lack scalability which makes them inappropriate especially in case of large-scale sensor deployments or mobility. As a result, there have been recently many efforts to find other ways to secure wireless communications.

In optical communications, quantum cryptography [3] has been largely investigated as a security solution based on the uncertainty principle in quantum physics. As for wireless communications, the wireless multipath channel has appeared recently to be a candidate. In deed, a lot of attention is being given to the physical layer of wireless communication. Interestingly, it has been found that the multipath phenomenon in wireless communication provides a sort of randomness and diversity that can be leveraged in extracting secret keys [4, 5, 6, 7, 8, 9, 10]. Actually, many real world measurements have shown that in Time Division Duplex (TDD) wireless communications, the multipath channel forms a reciprocal common source of randomness for any two communicating nodes; such that other nodes separated by distances greater than the order of a wavelength observe different multipath channels. This is mainly due to the fact that in rich scattering environments, channel gains and phases vary rapidly in space. In other words, this means that an eavesdropper which is located few wavelengths away from both communicating nodes (call them Alice and Bob) will observe independent channel coefficients [11]. Thus, Alice and Bob can leverage their common secret reciprocal channel gains to generate a suitable shared-key for their communication.

In this paper, we investigate secret key generation from wireless multipath channels. We first analyze the main origin of error in case of direct quantization of channel taps, by deriving the probability of error formulation. We then propose two intelligent adaptive quantization mechanisms for key generation achieving low error rates; and consequently, we derive optimal quantization parameters achieving a high secret bit extraction rate. We further propose some possible improvements to increase the secret bit generation rate. After that, we tackle some practical issues that affect the performance of key extraction from wireless channels. Mainly, we discuss enhancing the robustness of key generation against delay between the channel observations and against mobility.

The rest of this paper is organized as follows. In Section II, we overview some of the related work. Section III presents the general system model, gives an overview of the wireless multipath channel, and then describes shortly the channel estimation procedure and the key agreement protocol. In section IV, we present our proposed intelligent quantization and key agreement mechanisms, compare them and discuss some further improvements. After that, in section V, we investigate some practical issues affecting the performance of physical-layer key generation, mainly delay and mobility. Consequently, we introduce some modifications to the considered key generation mechanism to ensure robustness against such practical issues. Finally, in Section VI, we study the effect of mobility on the overall key generation rate, before concluding the paper in Section VII.

II. Related Work

From an information-theoretic point of view, many authors [12, 13] explore the possibility of generating secret keys from correlated sources of randomness. On the other hand, many efforts target extracting keys using of-the-shelf devices [6, 7,

14]. These are mainly based on quantizing the Received Signal Strength Indicator (RSSI) measurements. Moreover, to improve the key agreement performance, they propose an information reconciliation stage [15]. And finally, to strengthen the secrecy, some authors consider removing any correlation with the eavesdropper by a privacy amplification stage [16].

In [6], the authors have used a level crossing quantization algorithm and a heuristic log likelihood ratio estimate to achieve an improved secret key generation rate of 10 bits/sec. In [7], the authors have proposed a bit extraction framework and an adaptive quantization approach achieving key rates of 22 bits/sec at a bit disagreement rate of 2.2 percent. They have further proposed a more robust and enhanced bit extraction method in [14] achieving a rate of 40 bits/sec. These approaches emphasize the possibility of generating secret keys from the wireless channel. However, they are based on quantizing the RSS indicator under the hardware limitations of the considered of-the-shelf devices, and do not consider leveraging the whole channel response. Therefore, such RSSI-based methods are still far from what can be achieved in key extraction from multipath wireless channels [17].

Therefore, other efforts have investigated theoretical bit extraction mechanisms based on the whole channel response. For example, the authors in [8] considered leveraging multipath by quantizing different channel taps at the same time and then applied Low Density Parity Check (LDPC) error correcting codes. They have applied their approach on ITU channels revealing interesting results. While, in [9], the authors have targeted mitigating error instead of correcting it and losing privacy, through smart quantization approaches. On the other hand, the authors in [18] have investigated theoretical bounds on the mutual information and derived the optimal coherence times and transmitted bandwidths that optimize the secret key generation rate. Moreover, they have investigated different quantization and public discussion approaches. Particularly, they have compared per sample coded, block coded and Trellis coded public discussion and showed that Trellis coding techniques can provide higher efficiency of secret bit extraction.

In this paper, we first propose intelligent quantization mechanisms achieving high reliability and we derive the optimal quantization parameters achieving high secret bit extraction rate. Moreover, we investigate some practical issues affecting the performance of key generation from wireless channels. To the best of our knowledge, there have been no work done analyzing the effect of delay, channel decorrelation and mobility on the performance and how to mitigate such problems. In this paper, we consider such practical issues and provide countermeasures. As a result, this paper provides a framework towards a robust key generation mechanism from multipath wireless channels.

III. System Model

A. General System Model

In this section, we describe the general system model which is formed mainly of two communicating nodes Alice(Node 1) and Bob(Node 2) and an eavesdropper (Eve) as shown in Fig. 1. We suppose that Alice and Bob are using the same frequency band and that Eve is sufficiently separated so that its channel observations are completely uncorrelated from those of Bob and Alice. Moreover, due to the reciprocity principle, the two channels $\mathbf{h_1}$ and $\mathbf{h_2}$ are equivalent so that they can be leveraged in extracting a secret key.

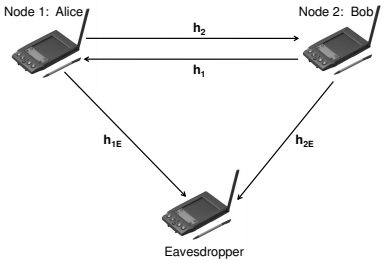


Fig. 1. A wireless communication scenario consisting of two legitimate communicating nodes and an eavesdropper.

B. Time-varying multipath channel

As for the channel, we suppose that it is a multipath fading channel which can be modeled as a combination of different channel impulses having different amplitudes and delays. In addition, due to the mobility of the communicating nodes and/or that of the reflecting clusters, the channel is varying with time. In other words, the channel impulse response at time instant t can be expressed as

$$h(t,\tau) = \sum_{l=0}^{L-1} h_l(t)\delta(\tau - \tau_l), \tag{1}$$

where δ is the unit impulse function, L is the length of the channel (number of taps), while $h_l(t)$ and τ_l represent the complex gain and delay of the $(l+1)^{th}$ channel tap at time instant t.

In this case, the channel taps can be considered independent from each other and can be quantized separately thus leveraging multipath to increase the number of secret bits generated [4, 8, 9]. Moreover, the uniform phase distribution [11] of the channel taps encourages the idea of phase quantization to generate secret keys.

It is important to note that the variation of the channel with time can have an important influence on the performance of a key extraction mechanism. In fact, channel variation influences negatively the channel estimation procedure. However, it has been found that the channel variation can be modeled through mathematical functions. Indeed, Basis Expansion Modeling (BEM) [19] has been largely investigated to model channel variation during short periods where the channel is highly correlated. Yet, it is necessary to find the time-spaced autocorrelation function as it determines the channel correlation as a function of time-shift Δt. For example, if a channel estimate is acquired at time t, the autocorrelation function determines the correlation between this estimate, and the channel at some time instant $t + \Delta t$ in the future. The normalized autocorrelation function of a Rayleigh fading channel with motion at a constant velocity is expressed as a zeroth-order Bessel function of the first kind [11]:

$$R(\Delta t) = J_0(2\pi f_D \Delta t), \tag{2}$$

where f_D is in this case the maximum Doppler spread due to mobility and can be expressed as : $f_D = \frac{v \cdot f}{c}$. v is here the speed of the mobile node and c the speed of light; while f is the transmission frequency.

In our case, it is necessary to perform the channel estimation at both nodes as fast as possible to avoid any decorrelation between the channel estimates at the two nodes. However, due to some practical issues, it is difficult to obtain channel estimates at the same time instant. Therefore, we analyze in this paper the effect of delay between the channel estimates and we investigate enhancing the robustness of the key generation mechanism accordingly.

Moreover, the phase of the channel taps is very sensitive to time synchronization and frequency offset. Indeed, a small residual frequency offset might lead to a considerable variation in the estimated phase of the channel taps and would result in a disagreement between the extracted bits. However, in this work we assume perfect time and frequency synchronization and leave these issues to be handled in future work.

C. Channel Estimation

Considering an Orthogonal Frequency Division Multiplexing (OFDM) system, the estimated channel coefficients in the frequency domain can be obtained as [19]

$$\widehat{\mathbf{H}} = \mathbf{H} + \mathbf{n_G}, \tag{3}$$

where $\mathbf{n_G}$ is the added white Gaussian noise vector which can be different at the two nodes; and $\mathbf{H}$ is a vector of N channel coefficients in the frequency domain with N being the Fast Fourier Transform (FFT) size. These channel coefficients can be expressed (taking out the time index t) as

$$H_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{L-1} h_l \exp\left(\frac{-j2\pi kl}{N}\right) \tag{4}$$

A direct approach that comes first in mind is quantizing these coefficients directly. But as they are correlated, we tend to transform them to the time domain where we get the uncorrelated channel taps. So, in our approach, we first estimate the H_k's and then by Fourier transform we obtain the h_l's:

$$\widehat{\mathbf{h}} = \mathbf{h} + \mathbf{z}, \tag{5}$$

where $\mathbf{z}$ is here the equivalent Gaussian noise in the time domain.

Hence, each of the legitimate nodes will observe a noised estimate of the channel:

$$\mathbf{h_1} = \mathbf{h} + \mathbf{z_1},\ and\ \mathbf{h_2} = \mathbf{h} + \mathbf{z_2}, \tag{6}$$

where $\mathbf{z_1}$ and $\mathbf{z_2}$ are added white Gaussian noise at the two nodes. In the case of complex Gaussian channel gains [11], the maximum number of secret bits that can be generated is upper bounded by the mutual information between the two observed channel vectors [8]:

$$N_k = I(\mathbf{h_1}, \mathbf{h_2}) = \sum_{i=0}^{i=L-1} \log_2(1 + TNR_i \cdot \frac{1}{2 + 1/TNR_i}), \tag{7}$$

where TNR_i is the Tap power to Noise Ratio for channel tap i.

We note here also that the use of N channel coefficients in the frequency domain to find the time domain ones leads to a gain of TNR = N [17].

D. Key Agreement Protocol

We have seen that it is only required that both communicating nodes estimate their common channel to be able to generate a secret key. It is also very important to perform this estimation in a very short period, especially in mobile scenarios where the channel response varies rapidly. Therefore, we suppose a simple shared-key generation protocol consisting mainly of channel estimation, public discussion, secret bit generation and finally key agreement and verification.

Considering, without loss of generality, that Node 1 is the leading node and Node 2 is the follower, we summarize the key extraction and agreement protocol in the following steps:

1. **Channel estimation phase:** Nodes 1 & 2 exchange pilot OFDM symbols (probe packets) for the purpose of channel estimation.
2. **Public discussion phase:** Nodes exchange parameters (ex. TNRs, Tap Indexes,...) related to the key generation mechanism over the public insecure channel. The purpose of this exchange is to minimize the probability of disagreement without any loss of secrecy. In Sections IV. and V., we describe more explicitly the parameters to be exchanged during the public discussion phase according to the proposed key generation mechanism.
3. **Extraction phase:** Nodes proceed in quantizing channel taps according to the key generation mechanism (see Section IV).
4. **Verification phase:** Nodes verify agreement on derived key (sending hash values, encrypted nonces...)

IV. Channel Quantization

In this section, we present the proposed channel quantization and bit extraction approaches. But first, we present the direct approach consisting of direct quantization of all channel taps. We discuss why this approach leads to a high error rate implying the need of error correcting codes, information reconciliation and consequently privacy amplification.

A. Direct Quantization

The direct approach consists of directly quantizing the phases of the obtained channel taps through a normal Phase Shift Keying (PSK) demodulation procedure.

In Fig. 2 , we show a plot of a large number of channel realizations over the complex plane and their noisy estimates. Considering particularly the values at the border regions (four regions in this case), we can see clearly that they are the most prone to error. Thus, an intelligent quantization approach should either avoid quantizing these values (using guard intervals separating the different quantization regions), or shift the random channel gains to be concentrated around the constellation points (secure phase shifting approach).

B. Quantization with Guard Intervals (GI)

As we have seen above, it is obvious that the high error rate is mainly due to the channel values close to the border regions.

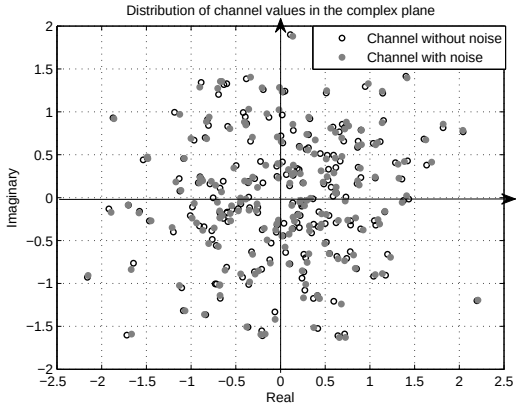


Fig. 2. A distribution of some channel realizations and their noisy estimates over the complex plane.

Therefore, we separate the quantization regions by small boundary regions mitigating the channel values that may cause a disagreement between the two communicating nodes. And as we will proceed in quantizing the phase of the obtained channel values, we define the boundary regions by guard phase intervals such that if the channel tap phase lies in one of these intervals, it is simply discarded.

From a security point of view, one may think how can each node inform the other that a channel tap should be discarded without any loss of secrecy. In fact, as the quantization regions are equiprobable, so are the boundary regions. In this case, any node can just announce during the public discussion phase which channel taps to be quantized or which to be discarded. In our approach, the leader node first announces its accepted channel taps by sending the corresponding indexes and so does the follower back. Thus, they agree on the channel taps to be used in the secret bits extraction process.

As for the performance, it is clear that larger boundary regions leads to a lower probability of bit disagreement while causing also a lower number of bits extracted as channel taps are more likely to be discarded. Thus, a performance-efficiency trade-off can be made in this case. Therefore, we consider a certain target probability of key disagreement and aim at extracting the maximum number of secret bits. In particular, we consider a target disagreement *per channel tap* less than 10^{-3} and we seek the optimal guard angle and quantization level achieving the maximum number of secret bits.

In Appendix I.A, we derive the probability of disagreement as a function of the guard angle β, the quantization level M, and the tap-to-noise ratio TNR as:

$$P_{GI} = \frac{1}{\pi/M - \beta/2} \cdot \int_{\theta=0}^{\theta=\pi/M-\beta/2} P_\theta(\beta, M, \sigma) d\theta, \qquad (8)$$

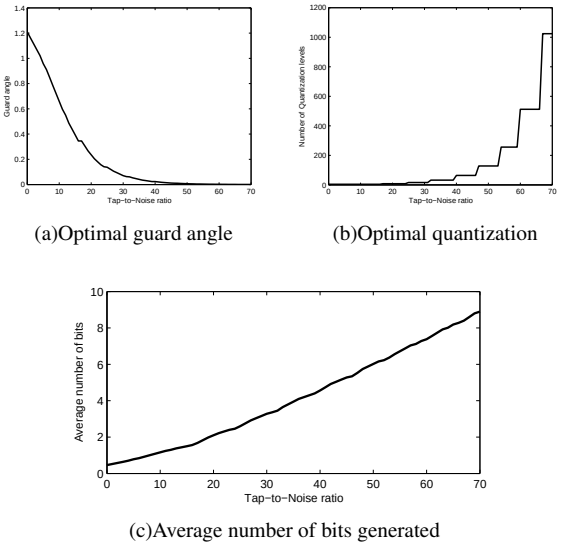
where P_θ is given by:

$$P_\theta = \frac{1}{2} \cdot [1 - \mathrm{erf}(\frac{1}{\sqrt{2}\sigma} \tan(\frac{\pi}{M} - \theta + \frac{\beta}{2}))], \qquad (9)$$

On the other hand, the average number of bits generated per channel tap depends also directly on β and M and can be found to be upper bounded by:

$$N_{av} \leq (1 - \frac{\beta \cdot M}{2\pi}) \cdot \log_2(M), \qquad (10)$$

From (8), we proceed in computing the probability of error in function of TNR for different values of β and M. Then, by considering the threshold probability of error of 10^{-3} per channel tap, we find the optimal parameters achieving the highest number of secret bits generated as shown in Fig. 3.



(a)Optimal guard angle (b)Optimal quantization

(c)Average number of bits generated

Fig. 3. Optimal guard angle (a), number of quantization levels (b), and average number of bits generated per one channel tap (c) as a function of TNR for a probability of error < 0.001, Guard Intervals (GI) method.

As a result, the public discussion phase would include exchanging the measured TNR values and the indexes of the channel taps. It is clear here that this exchange has no drawbacks on the secrecy of the derived key as the transmission of the TNR values does not decrease the entropy of the phases of the channel taps which have a random distribution [11].

C. Quantization with Phase Shifting (PS)

From (10), we can deduce that the guard intervals mechanism is not optimal in the sense of the efficiency of key extraction. In fact, in this approach, channel values lying in the guard intervals are simply ignored and not included in the quantization process. This leads to a decrease in the average number of secret bits extracted by a factor equal to $\beta M/2\pi$.

Therefore, to achieve a high efficiency of key extraction, the whole channel response should be considered. In other words, no channel taps with sufficient TNR should be ignored. Therefore, we propose a new approach to mitigate errors in channel quantization. It is mainly based on shifting the phases of the channel taps synchronously approaching the demodulation constellation. The idea is mainly to convert the problem into a normal demodulation problem where the channel values are spread around the constellation points rather than being randomly scattered. Hence, a direct quantization can be performed without the need for guard intervals.

To clarify this procedure, lets consider h_1 as a 1-tap channel estimate at Node 1 and h_2 as a 1-tap channel estimate at Node 2. In this approach, Node 1 first quantizes its channel tap value by a proper PSK demodulation and then sends during the public discussion phase, the phase difference $\mu = \theta_1 - \hat{\theta}$ to the other node, where θ_1 is the phase of h_1 as estimated at Node 1 and $\hat{\theta}$ is the phase of the obtained constellation point after PSK demodulation.

We suppose always that a reliable channel exists for the transmission of μ to Node 2. Consequently, Node 2 corrects its own estimated channel tap phase as:

$$\theta_2' = \theta_2 - \mu = \theta_2 - \theta_1 + \hat{\theta}, \tag{11}$$

where θ_2 is the phase of the corresponding channel tap h_2 as estimated by Node 2.

We can also write (11) as:

$$\theta_2' = \Delta\theta + \hat{\theta}, \tag{12}$$

where $\Delta\theta = \theta_2 - \theta_1$ represents the combined effect of noise.

From a security point of view, one may think how secure is this approach and if it causes any loss of secrecy. In fact, as the phases of the channel taps are random and uniformly distributed, then the transmission of a phase shift over the public channel does not reveal any information about the corresponding phase. This provides an eavesdropper only with the information that the phase of the channel tap is μ away from a constellation point. But since the constellation points are equiprobable, no additional information is provided to the eavesdropper. Hence, the public discussion phase would consist of transmitting the phase shifts, measured TNR values and indexes of the channel taps to be quantized, i.e. those with sufficient TNR.

As for the performance, an error only occurs in the key extraction process if $|\Delta\theta|$ is large enough, i.e. if $|\Delta\theta| > \pi/M$. In Appendix I.B, we derive the probability of disagreement for quantizing one channel tap as a function of the tap-to-noise power ratio and the number of quantization levels M for two cases: high TNR regime and low TNR regime.

Based on this formulation, we develop as in the GI mechanism, an adaptive quantization algorithm where the number of quantization levels varies depending on the tap-to-noise power ratio. In fact, we target achieving a certain probability of error per channel tap and seek the maximum number of quantization levels. Thus by considering a probability of disagreement per channel tap less than 10^{-3}, we obtain the **optimal** number of quantization levels as a function of TNR as shown in Fig. 4.

D. Simulation Results

Our system follows the 802.11n standard [20]. In particular, we consider a 20 MHz bandwidth divided over 64 subcarriers and we consider TDD communication. The duration of each OFDM symbol is $3.2\mu s$ in addition to a cyclic prefix up to $1.6\mu s$. As for the channel model, we test our algorithms on one of the defined channel models by IEEE 802.11 Task Group n TGn [21]; particularly, we use the Model F which is defined as a large space indoor or outdoor channel model. We consider in our simulations a Single Input Single Output (SISO) channel and we test our algorithms in terms of the number of secret bits generated in a single channel observation. Further, we express the results of our algorithms in terms of the probability of disagreement and average number of generated bits as a function of SNR, where SNR stands here for the received signal-to-noise ratio. In fact, as we have already mentioned, there is an efficiency-performance trade-off. Hence, we target a certain probability of disagreement in the key generation, i.e. the probability that there is no error in any bit extracted. Particularly, we target a probability of error *per one channel* tap to be below 10^{-3}.

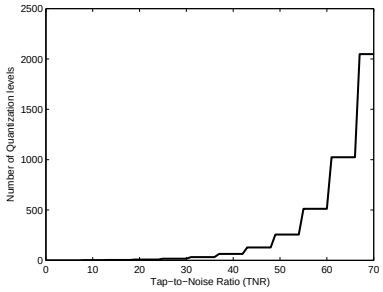


Fig. 4. Optimal number of quantization levels as a function of TNR for a probability of error per channel tap < 0.001, PS approach.

In Fig. 5, we trace the probability of disagreement as a function of SNR for the direct quantization approach, the guard-intervals approach and the phase shifting one. For the direct quantization approach, we observe a high probability of disagreement which makes it a non-reliable approach. As for the guard-intervals and the phase shifting methods, we observe a much lower probability of disagreement in the order of 10^{-2} and 10^{-3} respectively.

Further, in Fig. 6, we compare the average number of secret bits extracted by the phase shifting method as a function of SNR with that of the guard intervals method. It is obvious here that the PS mechanism performs better than the guard intervals one and yields a larger number of secret bits extracted. For example, for an SNR higher than 40dB, PS leads to the extraction of more than 90 secret bits compared to 60 for the GI approach. We also compare the maximum and minimum number of bits generated. Interestingly, the GI method shows a much bigger deviation from the average where the minimum number of generated secret bits is always equal to zero. This is due to the fact that in the guard-intervals key extraction method, many channel taps lying in the guard intervals are being simply ignored.

E. Further Improvements

As we have seen through the previous sections, the performance of the key extraction methods depend on the channel tap-to-noise ratio. Indeed, in our adaptive quantization approach, the number of quantization levels (consequently number of secret bits) depends on the TNR. Hence, enhancing the TNR of the channel taps is important for the key generation procedure. One of the possible solutions proposed is to average multiple channel observations in the time domain.

On the other hand, we have seen in Section III. C that the sampling of the channel in the frequency domain and then the transfer to the time domain leads to a gain in TNR = N. In ad-

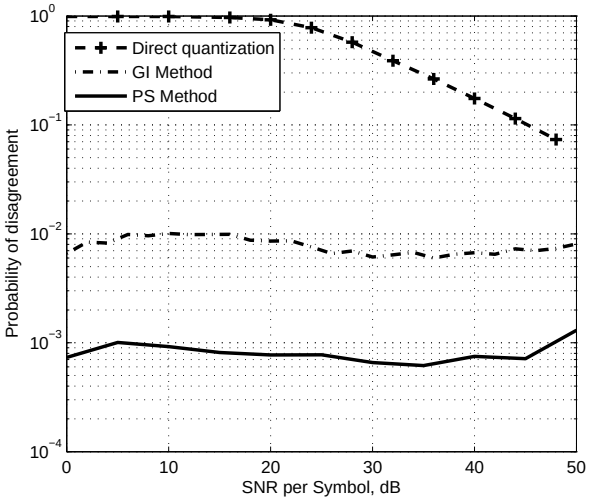


Fig. 5. Probability of disagreement as a function of SNR for the two approaches, N=64.

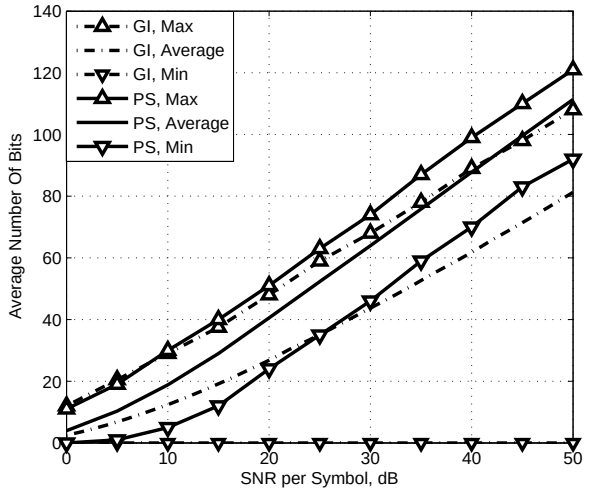


Fig. 6. Average, maximum, and minimum number of bits generated as a function of SNR, N=64.

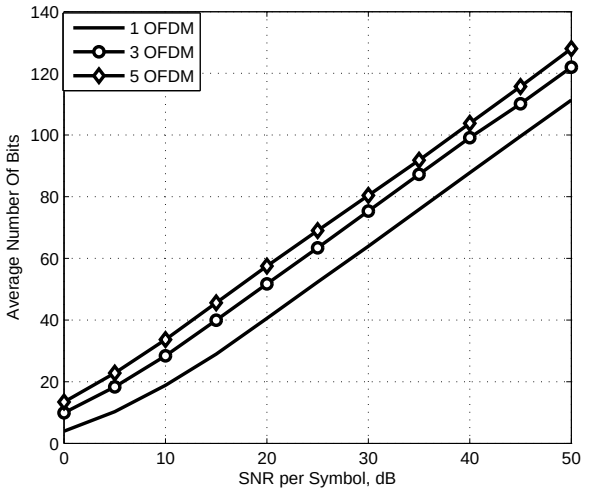


Fig. 7. Average number of bits generated by averaging over multiple OFDM symbols as a function of SNR, N=64.

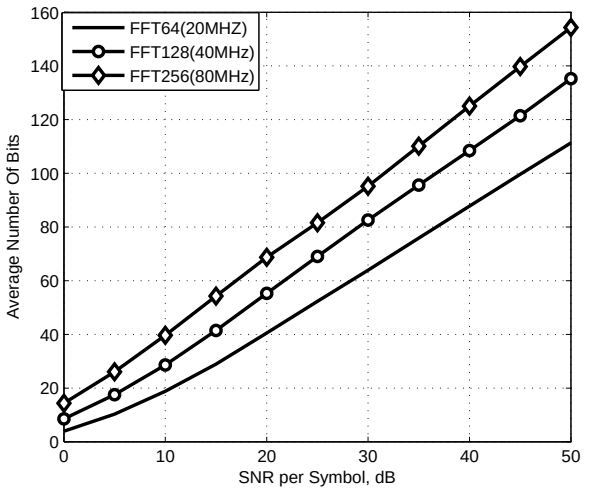


Fig. 8. Average number of bits generated as a function of SNR for various FFT sizes.

dition, higher sampling rates enables more channel taps to be considered. Therefore, the use of higher FFT sizes and bandwidths may also lead to a higher secret bits extraction rate.

In Fig. 7, we show the average number of secret bits extracted by the phase shifting method by averaging over multiple OFDM symbols. In this case, the communicating nodes send multiple pilot OFDM symbols for the purpose of channel estimation rather than sending only one OFDM symbol, thus obtaining an average over multiple channel observations. We observe here that the higher the number of OFDM symbols used, the higher the number of secret bits extracted. Comparing the case of 5 OFDM symbols sent by each node to that of 1 OFDM symbol, we can observe an improvement of approximately 7 dB.

Finally, in Fig. 8, we show the results for various FFT sizes (64, 128 and 256) and bandwidths (20MHz, 40MHz, and 80MHz respectively). We observe that higher FFT sizes and larger bandwidths leads to a higher number of secret bits extracted as predicted in section III. C. In fact, better TNRs are obtained for higher FFTs since the TNR is proportional to the FFT size. Moreover, higher sampling rates enable more channel taps (which are non-resolvable at lower sampling rates) to be taken into account leading to a higher number of secret bits extracted.

V. Improving Robustness

In this section, we first study the effect of delay between the channel estimates on the performance of the key generation mechanism. Based on the results, we propose a modification to the key extraction mechanism to mitigate the performance degradation due to delay. After that, we investigate the effect of channel variation and decorrelation due to mobility on the performance and improve our proposed key generation mechanism accordingly.

A. Robustness to Delay

A.1 **Impact of Delay**

As mentioned before in the key agreement protocol, it is important that the channel estimation occurs at the two nodes in a short period. Otherwise, the variation of the channel results in different obtained channel estimates at the two nodes. However, the delay between channel estimates is hard to avoid. There are many reasons that might result in delaying the channel estimation at the other node. Mainly: transmission delay, transmit-to-receive-switch delay in addition to other protocol related factors.

To study the effect of delay on the performance, we vary the delay between the channel estimates from a range of 5 (perfect synchronization) to $250\mu s$. Fig. 9 shows the probability of disagreement as a function of the delay between both channel estimates for an SNR of 30dB. Observing the solid line, we can see clearly that as the delay between the channel estimates increases, the probability of disagreement also increases significantly. This is mainly due to the varying nature of the channel.

However, for such considered delays the channel should still be highly correlated. In fact, the coherence time (for an autocorrelation > 0.75), normally approximated as: $\tau_C = \frac{1}{2\pi f_D}$, is here in the order of few milliseconds while the delay is in the order of microseconds. This means that it is possible to correct the channel gains and mitigate the phase variation. In the following section, we propose a modification to the secret bit extraction mechanism mitigating the effect of the variation of the channel gains during the coherence period.

A.2 **3-Way PS Mechanism**

In this section, we improve the robustness of the key generation mechanism against delay between the channel estimates. As discussed above, during the considered delays the channel is highly correlated. Hence, it is possible to correct the phases of the channel taps and remove the effect of channel variation.

To accomplish this task, we model the variation of the channel according to a BEM as discussed in Section III. B. Particularly, we model the channel variation as a polynomial of the first order, i.e. a linear modeling, since the normalized Doppler spread is relatively small in this case [19]. Yet, this requires two channel estimates at different time instants to compute the modeling coefficients. Thus, we modify our agreement protocol to be a 3-way channel estimation mechanism: Node 1 transmits a pilot symbol, Node 2 transmits back also a pilot symbol and finally Node 1 retransmits another. In this case, Node 2 would obtain two channel estimates at instants t_1 and t_3 that can be used to obtain the modeling coefficients. As a result, Node 2 can now use the modeling function to calculate an estimate of the channel gains at the same instant t_2 when Node 1 would have obtained a channel estimate; i.e. applying a linear modeling, Node 2 can calculate an estimate of $h(t_2)$ using the following equation:

$$\hat{h}(t_2) = h(t_1) + \frac{t_2 - t_1}{t_3 - t_1} \cdot (h(t_3) - h(t_1)), \qquad (13)$$

We test this algorithm on the same system as before and for the different values of delay between the consecutive channel estimates. The dotted line in Fig. 9 shows the probability of disagreement as a function of delay for the 3-way mechanism. We can see clearly that the 3-way PS mechanism is more robust to delay between the channel estimates. We obtain a probability of disagreement in the order of 10^{-3} as intended in our algorithm optimization while achieving an average number of 67 secret bits generated from a single channel observation.

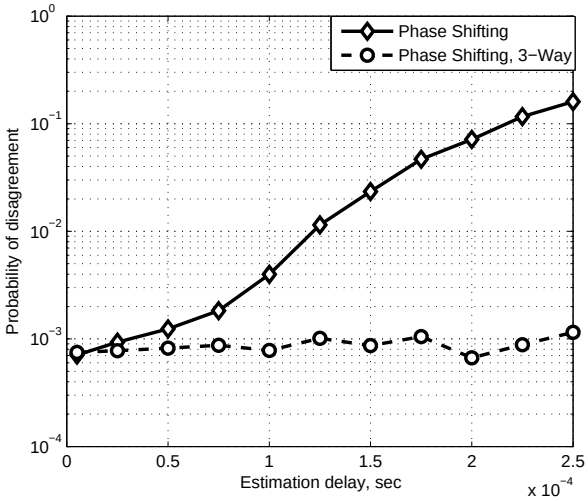


Fig. 9. Probability of disagreement as a function of the delay between the channel estimates, SNR=30dB, N=64.

B. Robustness to Mobility

B.1 **Effect of Mobility**

In the discussion above, we have only considered the case of low mobility to study the effect of delay between the channel estimates. However, the variation of the channel leading to the degradation of performance in case of delay is mainly due to the mobility of the communicating nodes and/or reflecting clusters. Hence, it is interesting to study the effect of mobility on the performance of the key extraction mechanism.

In fact, the channel variation can be partially corrected by the 3-way mechanism presented above. However, higher mobility leads on one hand to a faster decorrelation of the channel such that the channel estimates obtained at the two nodes are affected by a partial decorrelation in addition to the phase variation. And on the other hand, it leads to a bigger error in the polynomial modeling procedure (we note here that this error might be corrected by using multiple channel estimates and applying higher BEMs; however, this is out of the scope of this study).

Fig. 10 shows the probability of disagreement as a function of Doppler spread for an SNR of 30dB and a delay between the channel estimates of $250\mu s$. The solid line corresponds to the 3-way mechanism discussed above. We observe clearly that higher mobility leads to a significant increase in the probability of disagreement.

B.2 **Mobility-Resilient 3-Way PS Mechanism**

In this section, we propose a mobility-resilience enhancement to the 3-way phase-shifting mechanism to mitigate the effect of channel decorrelation and the modeling error due to mobility. The idea is to approximate the channel decorrelation and deviation from the linear model as an added noise. However, it is

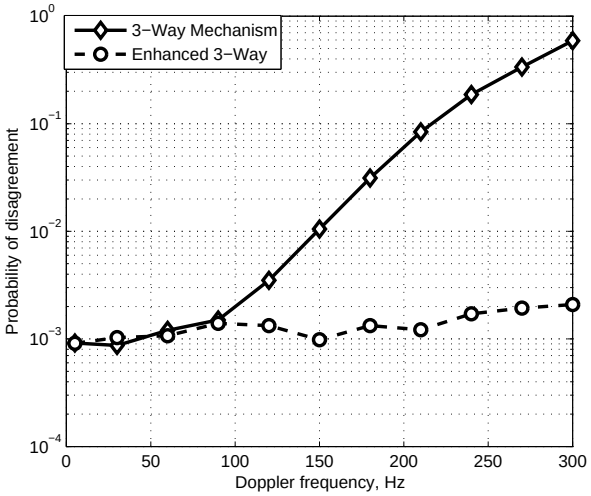


Fig. 10. Probability of disagreement as a function of the Doppler spread ($250\mu s$ delay), SNR=30dB, N=64.

difficult to calculate the exact value of this noise. Therefore, we approximate it as an added Gaussian noise with a variance expressed in function of the normalized Doppler spread ν_D as:

$$\sigma_D^2 = \frac{3}{2} \cdot (\frac{3}{2} - 2 \cdot J_0(2\pi\nu_D) + \frac{1}{2} \cdot J_0(4\pi\nu_D)), \qquad (14)$$

The dotted line in Fig.10 shows the probability of disagreement by using the Mobility-Resilient 3-way PS mechanism. We observe that this mechanism mitigates the error due to mobility and achieves the aimed probability of disagreement in the order of 10^{-3}.

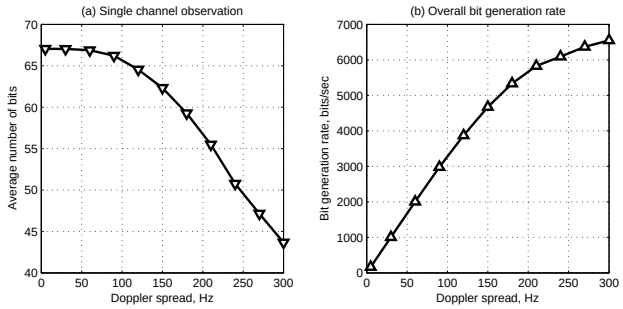


Fig. 11. Average number of secret bits generated from a single channel observation (a), and overall secret bit generation rate (b), as a function of the Doppler spread ($250\mu s$ delay), SNR=30dB, N=64.

In Fig. 11(a), we plot the average number of secret bits generated as a function of the Doppler spread using the Mobility-Resilient 3-way mechanism. We can observe that mobility has a negative effect on the number of secret bits generated from a single channel observation, as it decreases from 67 secret bits for a Doppler frequency of 5 Hz to less than 45 secret bits for a Doppler frequency of 300 Hz. This is mainly due to the decorrelation of the channel which leads to more noisy estimates.

VI. Effect of Mobility on Overall Performance

As we have seen above, mobility and consequently channel variation have a negative effect on the performance of the key extraction mechanism corresponding to a single channel observation. However, the effect of mobility on the overall performance, i.e. the key generation rate (measured in sbits(secret bits)/sec) is not clear yet. Therefore, one may still ask: Is mobility an advantage or a disadvantage for the key generation procedure?

To answer this question, we investigate the overall performance as a function of the Doppler spread. We should note here that higher mobility means faster decorrelation of the channel. On one hand, this signifies a lower average number of bits generated from a single channel observation due to the decorrelation problem discussed above. On the other hand, this means a faster observation of an uncorrelated channel, i.e. faster re-use of the channel to extract secret bits. Actually, it has been found that the channel decorrelates completely after an interval approximately greater than: $\frac{2}{f_D}$. Therefore, after this interval it is possible to get new independent channel estimates and apply the key generation mechanism to obtain a new set of secret bits.

In Fig. 11(b), the secret bits generation rate in sbits/sec as a function of the Doppler spread is plotted. We observe that the secret bits generation rate increases as a function of mobility. In particular, it increases from 167.5 sbits/sec to 6793 sbits/sec for an increase of the Doppler spread from 5 to 300 Hz. We can deduce from this graph that mobility is an advantage to the key generation procedure and permits a higher secret bits generation rate.

VII. Conclusion

In this paper, we have investigated key generation based on the wireless multipath channel. We proposed two intelligent mechanisms for shared-key generation based on mitigating error in the quantization of the channel taps either through guard intervals (GI method) or by shifting the phases of the channel taps synchronously (PS method). Moreover, we derived the optimal quantization parameters as a function of SNR achieving highest efficiency under a certain performance constraint. We also discussed the possibilities of further enhancements by averaging over multiple OFDM symbols and using higher FFT sizes. Through simulations, the proposed PS mechanism showed a high efficiency of secret bits extraction with more than 90 bits extracted per single channel realization in a typical SISO outdoor channel model.

In addition to that, we investigated some practical issues that might affect the performance and reliability of key generation from the multiptah wireless channel. Mainly, we investigated the effects of delay between the channel estimates and mobility on the performance. After discussing the effect of delay, we proposed a 3-way extraction procedure. It is mainly based on modeling the channel variation by a linear function during a small time window. After that, we investigated the effect of mobility and improved the key generation mechanism accordingly.

The established Mobility-Resilient 3-Way PS mechanism resulted in a lower average number of secret bits generated from a "single" channel observation as function of the Doppler spread. Yet, it was proved that mobility is in fact an advantage to the key generation process due to the faster decorrelation of the channel permitting a faster re-keying. The results obtained through simulations showed that the overall secret bit generation rate in-

creases as a function of mobility despite the lower average number of secret bits generated per a single channel realization.

As for future work, we will investigate applying more efficient encoding techniques like joint encoding and applying powerful error correcting codes to further improve the key generation rate. It would be also very interesting to consider synchronization and frequency offset issues and test our algorithm through real implementations and investigate key refreshment rate in real scenarios.

APPENDICES

I. Derivation of the Probability of Error

A. GI Mechanism

Lets consider h_1 as the channel estimate at Node 1 and h_2 as the channel estimate at Node 2. By considering only one tap, equation (6), can be written as

$$h_2 = h_1 + z_2 - z_1 = h_1 + z', \tag{15}$$

where in this case h_1 is considered normalized, and z_1, z_2 are the independent added white Gaussian noises at both nodes which are supposed to be of equal power $\sigma^2 = 1/TNR$. Then, z' is the equivalent noise of power $2 \times \sigma^2$.

Let θ_1, θ_2 be the phases of h_1 and h_2, respectively and let ϕ be the phase of z'. Then the probability of error can be expressed as the probability that θ_1 and θ_2 are in two different quantization regions.

As θ_1 is uniformly distributed, this can be reduced to calculating the probability of error given that θ_1 is in the first region. In other words, for a guard phase of β and M quantization levels, it is the probability that $\theta_2 > \pi/M + \beta/2$ or $\theta_2 < -\pi/M - \beta/2$ given that $\theta_1 \in$ [(-$\pi/M + \beta/2$) ($\pi/M - \beta/2$)]. This can be also approximated (for large TNR) as the probability of $\theta_2 > \pi/M + \beta/2$ given that $\theta_1 \in$ [0 ($\pi/M - \beta/2$)].

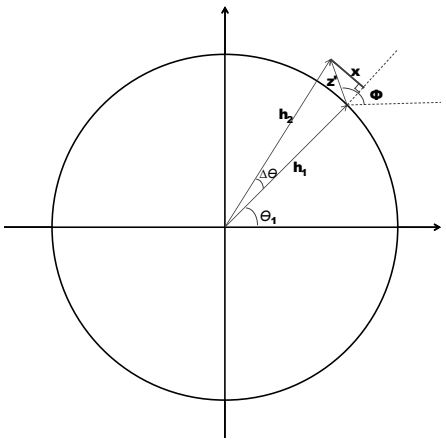


Fig. 12. Geometrical representation of the noisy channel estimates.

From Fig. 12, and for high TNR, one can write:

$$\tan(\Delta\theta) \approx \frac{x}{|h_1|} = \frac{|z'|\sin(\phi - \theta_1)}{|h_1|}, \tag{16}$$

where $\Delta\theta$ is the phase difference due to noise, ϕ is the phase of the equivalent noise z', and θ_1 is the phase of h_1.

As z' follows $CN(0, 2\sigma^2)$ distribution, and as ϕ and θ_1 are uniformly distributed and independent, then $x = |z'|\sin(\phi - \theta_1)$ follows $N(0, \sigma^2)$ distribution. We also note that $|h_1| \approx 1$ as it is normalized in this case.

Consequently, we can write the probability of error as a function of θ_1 as

$$\begin{aligned} P_{\theta_1} &= P(\theta_2 > \frac{\pi}{M} + \frac{\beta}{2}) \\ &= P(\Delta\theta > \frac{\pi}{M} + \frac{\beta}{2} - \theta_1) \\ &= P(\tan(\Delta\theta) > \tan(\frac{\pi}{M} + \frac{\beta}{2} - \theta_1)), \end{aligned} \tag{17}$$

where β being always the guard phase, and M the number of quantization levels.
By replacing $\tan(\Delta\theta)$ by x, we obtain:

$$P_{\theta_1} = P(x > \tan(\frac{\pi}{M} + \frac{\beta}{2} - \theta_1)), \tag{18}$$

which can be written in the form of the Error function:

$$P_{\theta_1} = \frac{1}{2} \cdot [1 - \mathrm{erf}(\frac{1}{\sqrt{2}\sigma}\tan(\frac{\pi}{M} - \theta_1 + \frac{\beta}{2}))], \tag{19}$$

Finally the total probability of error can be found by integrating over the (reduced) range of θ_1:

$$P_{GI} = \frac{1}{\pi/M - \beta/2} \cdot \int_{\theta=0}^{\theta=\pi/M-\beta/2} P_\theta(\beta, M, \sigma)d\theta, \tag{20}$$

B. PS Mechanism

From eq.(12), we deduce that an error occurs using the PS mechanism if $|\Delta\theta|$ is large enough, i.e. if $|\Delta\theta| > \pi/M$. Based on this result, we can derive the probability of error in quantizing a channel tap as a function of TNR and M. However, in this case, we tend to use two different approximations in the high TNR regime and the lower TNR regime.

B.1 High TNR regime

For the case of a high TNR, we use a similar derivation as above and find that:

$$\begin{aligned} P_{PS} &= P(|\Delta\theta| > \frac{\pi}{M}) \\ &= P(\tan(|\Delta\theta|) > \tan(\frac{\pi}{M})), \end{aligned} \tag{21}$$

Again, by replacing $\tan(\Delta\theta)$ by x, we obtain:

$$P_{PS_{High}} = P(|x| > \tan(\frac{\pi}{M})), \tag{22}$$

which can be written in the form of the Error function:

$$P_{PS_{High}} = 1 - \mathrm{erf}(\frac{1}{\sqrt{2}\sigma}\tan(\frac{\pi}{M})), \tag{23}$$

B.2 Low TNR Regime

As for the low TNR regime, the approximation made in (16) becomes inaccurate. Therefore, we follow a different procedure. First of all, we tend to assume in this case that the least quantization precision is used, i.e. $M = 2$. This means that an error occurs in the quantization process if $|\Delta\theta| > \pi/2$; or in other words if $\cos(\Delta\theta) < 0$. Based on this result, we can derive the probability of error in function of TNR and M.

Lets start first by expressing $\cos(\Delta\theta)$ in terms of $\cos(\theta_i)$ for $i = 1, 2$ using the following trigonometric equation:

$$\cos(\Delta\theta) = \cos(\theta_2) \cdot \cos(\theta_1) + \sin(\theta_2) \cdot \sin(\theta_1), \tag{24}$$

where $\cos(\theta_i)$ and $\sin(\theta_i)$ in this case can be expressed as:

$$\cos(\theta_i) = \frac{|h| + |z_i| \cdot \cos(\phi - \theta_i)}{|h_i|}, \tag{25}$$

$$\sin(\theta_i) = \frac{|z_i| \cdot \sin(\phi - \theta_i)}{|h_i|}, \tag{26}$$

Based on these expressions, and after some mathematical derivations, we obtain then an expression of the probability of error as:

$$P_{PS_{Low}} = P(x < \frac{-y \cdot z}{1 + t} - 1), \tag{27}$$

where x, y, z, and t are here i.i.d Gaussian random variables of variance = $\sigma^2/2$.

Finally, using the Error function we can write:

$$P_{PS_{Low}} = \frac{1}{2}[1 + \cdot \oint \oint \oint \operatorname{erf}(\frac{1}{\sigma} \cdot (-1 - \frac{y \cdot z}{1 + t})) \cdot P_y \cdot P_z \cdot P_t dy dz dt], \tag{28}$$

Acknowledgment

The authors would like to thank gratefully the esteemed reviewers for their helpful comments and feedback that helped a lot in improving the quality and clarity of this paper.

REFERENCES

[1] R. Oppliger, *Contemporary Cryptography*, Artech House, Inc., Norwood, MA, 2005.

[2] H. Chan, A. Perrig, D. Song, "Random key predistribution schemes for sensor networks," *Proc. of the 2003 IEEE Symposium on Security and Privacy*, May 2003, pp.197.

[3] C. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *J. of Cryptol.*, 1992.

[4] Y. El Hajj Shehadeh, O. Alfandi, K.Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," *IEEE WTS '11*, New York, NY, April 2011.

[5] M. Bloch, J. Barros, M. Rodrigues, and SW, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[6] S. Mathur, W. Trappe, N. Mandayam, C. ye, and A. Reznik, "Radio-Telepathy: extracting a secret key from an unauthenticated wireless channel," *Mobicom '08*, San Francisco, USA, September 2008.

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

[8] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of ITU channels," *IEEE VTC'07*, Baltimore, MD, October 2007, pp. 2030-2034.

[9] J. Wallace and R. Sharma, "Automatic Secret Keys from Reciprocal MIMO Wireless Channels: Measurement and Analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381-392, Sep. 2010.

[10] J. Wallace, C. Chen and M. Jensen, "Key generation exploiting MIMO channel evolution: algorithms and theoretical limits," *3rd European Conference on Antennas and Propagation, EuCAP 2009,* Berlin, March 2009, pp. 1499-1503.

[11] A. Goldsmith, *Wireless Communications*, Cambridge University Press, New York, NY, USA, 2005.

[12] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. on Inf. Theory*, vol. 39, no. 4, pp. 733-742, 1993.

[13] R. Ahlswde, and I. Csiszar, "Common randomness in information theory and cryptography- Part I: Secret sharing," *IEEE Trans. on Inf. Theory*, vol. 39, no. 4, pp. 1121-1132, 1993.

[14] J. Croft, N. Patwari, and S.K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," *Proc. of IPSN '10*, p. 70, 2010.

[15] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," *Advances in Cryptology Proc.- Eurocrypt '93*, vol. 765, pp. 410-423, 1994.

[16] C. Bennett, G. Brassard, and J.M. Robert, "Privacy amplification by public discussion," *SIAM K. Comput.*, vol. 17, no. 2, pp. 210-229, 1988.

[17] Y. Liu, S. Member, S. C. Draper, A. M. Sayeed, and S. Member, "A Secret Key Generation System Based on Multipath Channel Randomness : RSSI vs CSI," arXiv:1107.3534v1.

[18] R. Wilson and D. Tse, "Channel Identification : Secret Sharing using Reciprocity in Ultrawideband Channels," in *IEEE Transactions on Information Forensics and Security*, vol.2, no. 3, pp. 364-375, 2007.

[19] Y. EL Hajj Shehadeh and S. Sezginer, "Fast Varying Channel Estimation in Downlink LTE Systems," *Proc. of IEEE PIMRC'10*, Istanbul, September 2010, pp. 608-613.

[20] IEEE-SA, "IEEE 802.11n 2009 Amendment 5 Enhancements for Higher Throughput," 29 October 2009.

[21] V. Erceg et al., "TGn Channel Models", IEEE 802.11-03/940r4, January 2004.