Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers

Article *in* IEEE Transactions on Communications · March 2016

DOI: 10.1109/TCOMM.2016.2552165

CITATIONS
38

READS
135

4 authors:

Junqing Zhang
University of Liverpool
38 PUBLICATIONS **459** CITATIONS
SEE PROFILE

Alan Marshall
University of Liverpool
109 PUBLICATIONS **814** CITATIONS
SEE PROFILE

Roger Woods
Queen's University Belfast
244 PUBLICATIONS **1,574** CITATIONS
SEE PROFILE

Trung Q. Duong
Queen's University Belfast
395 PUBLICATIONS **7,915** CITATIONS
SEE PROFILE

Efficient Key Generation by Exploiting Randomness From Channel Responses of Individual OFDM Subcarriers

Junqing Zhang, Alan Marshall, *Senior Member, IEEE*, Roger Woods, *Senior Member, IEEE*, and Trung Q. Duong, *Senior Member, IEEE*

***Abstract*— Key generation from the randomness of wireless channels is a promising technique to establish a secret cryptographic key securely between legitimate users. This paper proposes a new approach to extract keys efficiently from the channel responses of individual orthogonal frequency-division multiplexing (OFDM) subcarriers. The efficiency is achieved by: 1) fully exploiting randomness from time and frequency domains and 2) improving the cross-correlation of the channel measurements. Through the theoretical modeling of the time and frequency autocorrelation relationship of the OFDM subcarrier's channel responses, we can obtain the optimal probing rate and use multiple uncorrelated subcarriers as random sources. We also study the effects of non-simultaneous measurements and noise on the cross-correlation of the channel measurements. We find that the cross-correlation is mainly impacted by noise effects in a slow fading channel and use a low-pass filter to reduce the key disagreement rate and extend the system's working signal-to-noise ratio range. The system is evaluated in terms of randomness, key generation rate, and key disagreement rate, verifying that it is feasible to extract randomness from both time and frequency domains of the OFDM subcarrier's channel responses.**

***Index Terms*— Physical layer security, key generation, OFDM, time and frequency autocorrelation, channel reciprocity.**

I. Introduction

THE BROADCAST nature of wireless communications allows all the users within range to hear the transmission, thus making it vulnerable to various active and passive attacks. Wireless network security and privacy thus has attracted many research interests [1]–[4]. In 5G networks, many new techniques have emerged, such as full-duplex communications [5], large-scale MIMO [6], etc. Physical layer security (PLS), which exploits channel characteristics to provide information-theoretic security for wireless communications, has been extensively researched for the protection of future 5G networks [7]. Key generation, an active research direction of PLS, automatically generates keys at each side of two legitimate users, Alice and Bob, from the randomness of their common wireless channel [8], [9]. This technique exploits unpredictable channel characteristics, which is information theoretically secure [10]. It is low complexity and does not require the aid of other nodes, thus representing a promising alternative to public key cryptography to establish keys for classical symmetric encryption.

Key generation system is evaluated in terms of key randomness, key generation rate (KGR), and key disagreement rate (KDR). Randomness is the most important feature for the key sequence as the key generated is used for encryption and/or authentication. A less random key will result in a smaller search space by brute force attacks thus compromising the security of the cryptographic system. KGR is an essential factor for the practical application of key generation system. It quantifies the number of key bits generated in each second, which can be given as

$$KGR = \frac{N_k}{T_k}, \tag{1}$$

where N_k is the number of keys and T_k is the time taken. Cryptography usually needs a key sequence with a certain length, e.g., advanced encryption standards (AES) requires a key length at least 128 bits, so a too low KGR will limit its application. KDR is the disagreement rate of the raw key bits quantized from the measurements, which is defined as

$$KDR = \frac{\sum_{i=1}^{N_k} |K^A(i) - K^B(i)|}{N_k}, \tag{2}$$

where K^A and K^B are the keys generated at Alice and Bob, respectively. The disagreement is corrected by information reconciliation techniques. A lower KDR can always decrease the reconciliation overhead and reveal less information during the public discussion. Therefore, an efficient key generation system should have a high KGR and small KDR with the premise of generating random keys. KGR can be improved by

Manuscript received August 27, 2015; revised January 26, 2016; accepted March 30, 2016. Date of publication April 7, 2016; date of current version June 14, 2016. This work was supported by the Queen's University Belfast university studentship, Newton Institutional Links Grant 172719890, Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22, and U.S.–Ireland R&D Partnership USI033 'WiPhyLoc8' grant involving Rice University (USA), University College Dublin (Ireland) and Queen's University Belfast (Northern Ireland). This paper was presented in part at the IEEE Global Communications Conference Workshop on Trusted Communications with Physical Layer Security, Austin, TX, USA, December 2014 and the IEEE International Conference on Acoustics, Speech and Signal Processing, Brisbane, Australia, April 2015. The associate editor coordinating the review of this paper and approving it for publication was J. Yuan.

J. Zhang, R. Woods, and T. Q. Duong are with the Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast BT3 9DT, U.K. (e-mail: jzhang20@qub.ac.uk; r.woods@qub.ac.uk; trung.q.duong@qub.ac.uk).

A. Marshall is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: alan.marshall@liverpool.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2016.2552165

leveraging fine-grained channel state information (CSI) and exploiting randomness fully from temporal, frequency, and spatial domains. KDR can be decreased by improving the signal cross-correlation. In the following of this introduction, we review key generation channel parameters, randomness exploitation from different domains, and measurement cross-correlation improvement.

Several practical and simulation systems have been reported for extracting keys from coarse-grained channel parameters, such as received signal strength (RSS) [11]–[18], channel phase in narrowband systems [19], [20], and deep fades of the signal envelop [21], etc. However, all of this work only extracts keys from a single dimension or a single frequency, which results in a low KGR and therefore limits their practical application. Although some research effort has attempted to improve the KGR by leveraging multi-antenna [14] and/or multi-bit quantization [16], it remains that these single-dimensional approaches lose much useful information.

Key generation from fine-grained CSI can achieve a higher KGR [22], [23]. A practical CSI-based key generation system was proposed to quantize channel responses in the frequency domain from all subcarriers in orthogonal frequency-division multiplexing (OFDM) systems [22], which may introduce redundancy and correlation between keys especially in a frequency flat fading channel. Later, another CSI-based key generation protocol called KEEP that uses a validation-recombination mechanism was designed [23]. However, it is difficult to reach an agreement in low signal-to-noise ratio (SNR) environments as even a single bit mismatch will result in a failure of the entire process and thereafter require a new validation-recombination process. In this paper, we also exploit channel randomness from CSI but in a different manner, i.e., by extracting keys from the channel responses of individual OFDM subcarriers over time. This provides a thorough theoretical modelling of the system and channel, and enables us to obtain the optimal probing rate and maximize the KGR, which will be discussed later.

The randomness in time, frequency, and spatial domains can be used for key extraction. While spatial randomness exploitation has been extensively analyzed in [24]–[28], this paper focuses on randomness extraction from time and frequency domains. The temporal randomness is the main random source for key generation as it can be easily introduced by the movement of the users and/or any objects within the communication environments [11]–[16], [25]. Frequency variation is another random source which currently receives less attention. Frequency diversity is intrinsically determined by the delay spread of multipath channel, which has been used for key generation in ultrawideband channel [29]. There has been research reported exploiting frequency diversity from RSS using channel hopping [17], [18], from channel measurements of multiple FM radios [30], or from CSI in IEEE 802.11 OFDM systems [22], [23]. However, a detailed theoretical modelling and analysis of the temporal and frequency correlation is missing, which restricts the capability to exploit the randomness of the channel.

The cross-correlation of the channel measurements of Alice and Bob is essential for the success of key generation. The statistical features of the same carrier frequency at each end are reciprocal, which is the basis of this type of key generation [13]. Most of the current commercial devices work in half-duplex mode, and the cross-correlation of the received signals measured at Alice and Bob are impacted by the non-simultaneous measurements (probing) and noise. Even when Alice and Bob measure the channel at the same frequency and time using full-duplex hardware,[1] the noise at each side will still be independent and uncorrelated as they reside in two different hardware platforms. Non-identical channel measurements introduce key disagreement, while a too high KDR may result in a failure of the entire key generation process. There has been research in compensating the non-simultaneous measurements using interpolation [15], [16] and suppressing the noise by filtering [11], [21], [22], [31]. However, the cross-correlation of the channel measurements has not yet been modelled theoretically, therefore, the design of the interpolation or filter algorithms are mainly empirical, resulting in a less effective improvement on the correlation.

In this paper, we propose a new efficient CSI-based key generation system by exploiting both the temporal and frequency randomness from channel responses of individual OFDM subcarriers. As part of the ongoing WiPhyLoc8 project [32], this paper aims to develop novel and practical approaches for wireless security. We carried out the analysis by considering a practical scenario, i.e., by incorporating an IEEE 802.11 OFDM transceiver model and a time-varying multipath channel model. This offers guidelines to implement a real key generation system in the testbed. Our contributions are:

- Efficient key generation from the channel responses of individual OFDM sucbarriers. By theoretically modelling the subcarrier's channel responses, it is demonstrated that they are fine-grained channel parameter which provides detailed channel properties in both time and frequency domains.
- By theoretically modelling the time and frequency auto-correlation relationship of OFDM subcarrier's channel responses, we can fully exploit the randomness of the channel in both time and frequency domains by obtaining the optimal probing rate and using multiple subcarriers as random source. Therefore, we can greatly improve the KGR while guaranteeing the randomness of the keys.
- By theoretically modelling the effects of non-simultaneous measurements and noise on the cross-correlation of the channel measurements, we found that noise plays a more dominant role in a slow fading channel and thereof employed a finite impulse response (FIR) low pass filter (LPF) to effectively target the high frequency components of the noise and significantly improve the correlation. The employment of LPF helps reduce the KDR and extend the working SNR range.

In previous work, we have analyzed the temporal variation of the OFDM subcarrier's channel response and verified its

[1] In full-duplex system, transceivers can work in different carrier frequencies, but their channel responses will be different and cannot be used for key generation.

application in key generation in [33] and used an LPF to improve the correlation of the measurements in [34]. In this paper, we considerably extend and complement this work by providing a theoretical and extensive modelling and analysis of the channel, time and frequency domains autocorrelation relationship, and cross-correlation of the channel measurements.

The rest of the paper is organized as follows. Section II describes OFDM channel model and the simulation model. Sections III and IV theoretically analyze the time and frequency autocorrelation relationship of the channel responses and channel measurements cross-correlation, respectively. The performance of our key generation system is evaluated in Section V. Section VI concludes the paper.

II. Channel Model

A. Multipath Channel

A dynamic multipath channel with lots of reflection, scattering, and refraction of the electromagnetic wave is an ideal random source for key generation. The channel impulse response (CIR) $h(\tau, t)$ of such a multipath channel can be written as

$$h(\tau, t) = \sum_{l=0}^{L-1} h(\tau_l, t)\delta(\tau - \tau_l), \tag{3}$$

where $h(\tau_l, t)$ and τ_l are the attenuation and delay of l^{th} channel tap, respectively, $\tau_l = lT$, and T is the sampling period of the system, L is the total number of the channel taps and $\delta(\cdot)$ is the Dirac delta function.

When there is rich scattering, the channel can be modelled as a *wide sense stationary uncorrelated scattering* (WSSUS) random process [35]. Under this model, the attenuation of each channel tap $h(\tau_l, t)$ is a WSS random process and the attenuations of any two taps with different delays, i.e., $h(\tau_l, t)$ and $h(\tau_j, t)$, are uncorrelated. Therefore, the temporal autocorrelation function (ACF) $r_h(\tau, \Delta t)$ is given by

$$r_h(\tau, \Delta t) = E\{h(\tau, t)^* h(\tau, t + \Delta t)\}. \tag{4}$$

The normalized temporal ACF of $h(\tau_l, t)$ can also be further defined as

$$R_h(\tau_l, \Delta t) = \frac{r_h(\tau_l, \Delta t)}{r_h(\tau_l, 0)}. \tag{5}$$

WSS is a common channel model and has been verified by experimental measurements for a rich scattering environment [36]. It is suitable to describe the channel correlation when the Doppler spread is fixed, i.e., the channel is always changing in the same rate. In real channels, this assumption may not be satisfied due to the uncontrolled movement of objects and thereof variable Doppler spread. Under this circumstance, the channel can be divided into small time frames and each frame can be approximated as a WSS random process [37].

B. OFDM Model

In OFDM systems, the transmitted signal consists of multiple OFDM symbols $x_q[m]$, which can be written as

$$x_q[m] = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} X_q[k] e^{j2\pi km/M}, \tag{6}$$

where $X_q[k]$ is the data modulated to the k^{th} subcarrier in q^{th} OFDM symbol in frequency domain at t_q, $x_q[m]$ is the m^{th} sample in q^{th} OFDM symbol in time domain, and M is the number of total subcarriers. In an OFDM system with BW Hz channel spacing and M evenly distributed subcarriers, the frequency of each subcarrier is given as

$$f_k = k\frac{BW}{M}, \tag{7}$$

where $BW = \frac{1}{T}$.

The transmitted signal $x_q[m]$ experiences the multipath effect and is affected by the noise. After synchronization, the received signal can be written as [38]

$$y_q[m] = \sum_{l=0}^{L-1} x_q[m - \varepsilon_q - l]h_q[l] + n_q[m], \tag{8}$$

where $n_q[m]$ is the additive Gaussian white noise (AWGN) and $n_q[m] \sim C\mathcal{N}(0, \sigma_n^2)$; ε_q is the time offset due to the imperfect synchronization and is determined by the synchronization algorithm, SNR, and the multipath effect; $h_q[l]$ is the discrete form of $h(\tau_l, t)$, and is assumed to remain unchanged during one OFDM symbol, which is a fair assumption in a slow fading environment.

When the synchronization time offset is small, the equivalent frequency domain value $Y_q[k]$ can be written as [38]

$$\begin{aligned} Y_q[k] &= \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} y_q[m] e^{-j2\pi km/M} \\ &= X_q[k]H_q[k]e^{-j2\pi k\varepsilon_q/M} + w_q[k], \end{aligned} \tag{9}$$

where

$$H_q[k] = \sum_{l=0}^{L-1} h_q[l] e^{-j2\pi kl/M}; \tag{10}$$

$$w_q[k] = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} n_q[m] e^{-j2\pi km/M}. \tag{11}$$

Least square (LS) channel estimation can get a noisy observation of the channel responses in OFDM systems, which can be given as

$$\widehat{H}_q[k] = \frac{Y_q[k]}{X_q[k]} = \widetilde{H}_q[k] + \widehat{w}_q[k], \tag{12}$$

where

$$\widetilde{H}_q[k] = H_q[k]e^{-j2\pi k\varepsilon_q/M}; \tag{13}$$

$$\widehat{w}_q[k] = \frac{w_q[k]}{X_q[k]}. \tag{14}$$

It can be calculated that

$$\sigma_{\widetilde{H}}^2 = \sigma_H^2 = \sum_{l=0}^{L-1} \sigma_{h_l}^2; \tag{15}$$

$$\sigma_{\widehat{w}}^2 = \sigma_w^2 = \sigma_n^2; \tag{16}$$

$$\sigma_{\widehat{H}}^2 = \sigma_H^2 + \sigma_w^2. \tag{17}$$

TABLE I
SIMULATION PARAMETERS

IEEE 802.11 OFDM channel spacing BW	20 MHz
Hardware sampling frequency $\frac{1}{T}$	20 MHz
Doppler spread f_d	6 Hz
Root mean square delay spread σ_τ	50 ns
Total sampling time	500 s

The above variances do not depend on the subcarrier index k which is omitted. Therefore, the channel responses of all the subcarriers will have the same SNR which can be given as

$$SNR_f = \frac{E\left[|\widetilde{H}_q[k]|^2\right]}{E\left[|\widehat{w}[k]|^2\right]} = \frac{\sigma_H^2}{\sigma_w^2}. \tag{18}$$

It should be noted that the mean square error (MSE) of LS channel estimation is inversely proportional to SNR [39], which is not as accurate as some other algorithms, e.g., minimum mean square error (MMSE) channel estimation. However, it is widely applied in commercial OFDM systems such as IEEE 802.11 OFDM. Therefore, in order to make the analysis in this paper more general, LS channel estimation is still adopted.

C. Simulation Model

A Matlab simulation model is implemented as an example for analysis. The transceiver is implemented according to the IEEE 802.11 OFDM protocol [40]. The statistical channel is modelled as a time-variant multipath fading channel [41] and a WSSUS random process. The average power of each channel tap follows an exponential-decay power delay profile and a Bell-shaped Doppler power spectrum [42], which is recommended by the IEEE working group. The normalized Doppler power spectral density (PSD) can be given as

$$S(f) = \frac{\sqrt{A}/(\pi f_d)}{1 + A(\frac{f}{f_d})^2}, \tag{19}$$

where A is a constant, e.g., in IEEE 802.11 channel, $A = 9$ and f_d is the Doppler spread, whose values were found to be up to approximately 6 Hz at a center frequency of 5.25 GHz and up to approximately 3 Hz at a center frequency of 2.4 GHz by experiments in indoor environment [42]. PSD and normalized temporal ACF form an IFFT pair. Therefore, the corresponding temporal ACF of the Bell-shaped Doppler spectrum can be given by

$$R(\Delta t) = e^{-\frac{2\pi f_d}{\sqrt{A}}\Delta t}. \tag{20}$$

For the simplicity of analysis, all the channel taps are modelled to have the same PSD.

The simulation parameters are shown in Table I. Unless otherwise specified, the results in this paper are based on the above simulation model and parameters. However, it is worth noting that our system and analyses work for other OFDM standards and multipath channels as well.

III. ANALYSIS OF TIME AND FREQUENCY AUTOCORRELATION

In a dynamic multipath environment, the signal experiences time-selective and frequency-selective fading. In order to generate a random key sequence, the sampled data should be uncorrelated. The correlation relationship of $H_q[k]$ can be characterized by the time and frequency ACF and given as [43]

$$\begin{aligned} r_H(\Delta f, \Delta t) &= E\{H_q[k]^* H_p[i]\} \\ &= \sum_{l=0}^{L-1} r_h(\tau_l, \Delta t) e^{-j2\pi \Delta f \tau_l}, \end{aligned} \tag{21}$$

and the normalized correlation function of $H_q[k]$ can be written as

$$\begin{aligned} R_H(\Delta f, \Delta t) &= \frac{r_H(\Delta f, \Delta t)}{r_H(0,0)} \\ &= \frac{\sum_{l=0}^{L-1} r_h(\tau_l, \Delta t) e^{-j2\pi \Delta f \tau_l}}{\sum_{l=0}^{L-1} r_h(\tau_l, 0)}, \end{aligned} \tag{22}$$

where $\Delta f = f_i - f_k = (i-k)\frac{BW}{M}$, $\Delta t = t_p - t_q$.

The time and frequency ACF of $\widetilde{H}_q[k]$ and $\widehat{w}_q[k]$ can be calculated as

$$r_{\widetilde{H}}(f_k, f_i, \Delta t) = r_H(\Delta f, \Delta t) E\{e^{j2\pi(k\varepsilon_q - i\varepsilon_p)/M}\}, \tag{23}$$

and

$$r_{\widehat{w}}(\Delta f, \Delta t) = r_w(\Delta f, \Delta t) = \delta(\Delta f)\delta(\Delta t)\sigma_w^2, \tag{24}$$

respectively.

Therefore, the time and frequency ACF of the channel estimation $\widehat{H}_q[k]$ can be given as

$$\begin{aligned} &r_{\widehat{H}}(f_k, f_i, \Delta t) \\ &\quad = r_{\widetilde{H}}(f_k, f_i, \Delta t) + r_{\widehat{w}}(\Delta f, \Delta t) \\ &\quad = r_H(\Delta f, \Delta t) E\{e^{j2\pi(k\varepsilon_q - i\varepsilon_p)/M}\} + r_w(\Delta f, \Delta t), \end{aligned} \tag{25}$$

and the normalized correlation function of $\widehat{H}_q[k]$ can be written as

$$\begin{aligned} &R_{\widehat{H}}(f_k, f_i, \Delta t) \\ &\quad = \frac{r_{\widehat{H}}(f_k, f_i, \Delta t)}{r_{\widehat{H}}(f_k, f_k, 0)} \\ &\quad = \frac{r_H(\Delta f, \Delta t) E\{e^{j2\pi(k\varepsilon_q - i\varepsilon_p)/M}\} + r_w(\Delta f, \Delta t)}{r_H(0,0) + r_w(0,0)} \\ &\quad = \frac{R_H(\Delta f, \Delta t) SNR_f E\{e^{j2\pi(k\varepsilon_q - i\varepsilon_p)/M}\} + \delta(\Delta f)\delta(\Delta t)}{1 + SNR_f}. \end{aligned} \tag{26}$$

A. Time Correlation

In a dynamic environment with random movement, the signal experiences time-selective fading, which is the main random source for key generation. The users harvest the entropy by probing the channel and getting the channel measurements. A smaller probing rate enjoys a higher KGR but compromises the randomness of the generated key sequence due to the correlation between the sampled data, while a larger probing rate results in a lower KGR and limits its

practical application. Key sequence is used in cryptographic applications and should be random. Optimal probing rate is defined as the minimum probing rate which can guarantee the randomness of the key sequence.

The channel variation in the time domain can be characterized by the temporal ACF. The channel coherence time can statistically approximate the time duration over which the CIR is essentially invariant and quantifies the similarity of the channel response [44]. It is usually defined by the time over which the coefficient of the temporal ACF is above 50%. The definition can be further extended to $X\%$ coherence time [45] and be used for all the random process, which is given as

$$R(T_c(X\%)) = X\%. \tag{27}$$

In this section, under the assumption that $h(\tau, t)$ is a WSSUS random process, we model the $R_{\widehat{H}}(f_k, \Delta t)$ and $R_H(f_k, \Delta t)$, and prove $\widehat{H}_q[k]$ and $H_q[k]$ are also WSS random processes. The WSS property guarantees that the data sampled by the same time interval Δt will have the same correlation relationship. Based on the temporal ACF, the optimal probing rate can be determined.

For the k^{th} subcarrier, the mean value of $H_q[k]$ is 0. The normalized temporal ACF of the $H_q[k]$ can be obtained by letting $\Delta f = 0$ in (22), which can be given as

$$\begin{aligned} R_H(0, \Delta t) &= \frac{\sum_{l=0}^{L-1} r_h(\tau_l, \Delta t)}{\sum_{l=0}^{L-1} r_h(\tau_l, 0)} \\ &= \frac{\sum_{l=0}^{L-1} (r_h(\tau_l, 0) \times R_h(\Delta t))}{\sum_{l=0}^{L-1} r_h(\tau_l, 0)} \\ &= R_h(\Delta t). \end{aligned} \tag{28}$$

The second equality holds because in this paper, all the channel taps have the same temporal ACF, i.e.,

$$R_h(\tau_l, \Delta t) = R_h(\Delta t), \quad l = 0, 1, \ldots, L-1. \tag{29}$$

As the mean value is a constant and ACF only depends on the time delay, $H_q[k]$ is a WSS random process.

The normalized temporal ACF of the imperfectly synchronized channel estimation can be calculated by letting $f_i = f_k$, i.e, $\Delta f = 0$, in (26) and written as

$$R_{\widehat{H}}(f_k, \Delta t) = \frac{R_H(0, \Delta t) SNR_f E\{e^{j2\pi k(\varepsilon_q - \varepsilon_p)/M}\} + \delta(\Delta t)}{1 + SNR_f}. \tag{30}$$

$R_{\widehat{H}}(f_k, \Delta t)$ is also only determined by Δt and irrelevant to the observation time, therefore, it is a WSS process.

Fig. 1 shows several results for $R_h(\tau_l, \Delta t)$, $R_H(f_k, \Delta t)$, and $R_{\widehat{H}}(f_k, \Delta t)$ from the simulation to validate the above analytic analysis. $R'_{\widehat{H}}(f_1, \Delta t)$ is calculated by letting $\varepsilon_q - \varepsilon_p = 0$ to show the reference ACF if perfect synchronization were achieved. Firstly, all the shown $R_h(\tau_l, \Delta t)$ and $R_H(f_k, \Delta t)$ values are equal, which matches the analytic expression (28). Secondly, $R_H(f_k, \Delta t)$ and $R_{\widehat{H}}(f_k, \Delta t)$ observed at t_1, match their counterparts at t_2 quite well, respectively, which validates that $H_q[k]$ and $\widehat{H}_q[k]$ are WSS random processes. Lastly, $R_{\widehat{H}}(f_k, \Delta t)$ observed at t_1 vary according to the subcarrier index k, which matches the analytical expression (30).

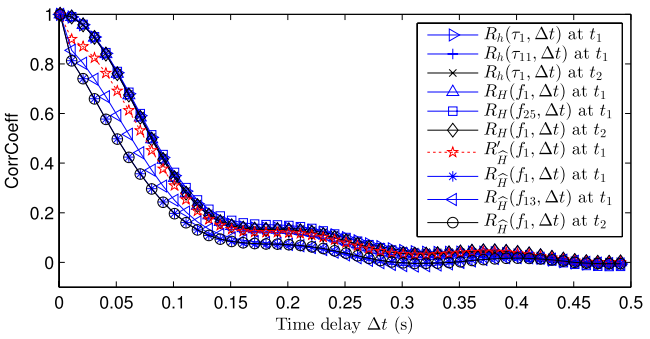

Fig. 1. Temporal ACFs. $SNR = 10$ dB. $R_h(\tau_l, \Delta t)$, $R_H(f_k, \Delta t)$ and $R_{\widehat{H}}(f_k, \Delta t)$ observed at t_1 and t_2. $t_2 = t_1 + 10$ s.

Previous key generation research has claimed that the probing rate should be larger than 50% coherence time in order to get a random key sequence. However, it has been observed that whenever the experiments were carried out, the authors usually chose the probing rate to be large enough to exceed the expected coherence time [22]. However, in this paper we calculate the $X\%$ coherence time $T_c(X\%)$ based on the temporal ACF of the random process, and use it as the probing rate to sample the channel. The optimal probing rate can then be found by evaluating the randomness of the key sequence sampled by different $T_c(X\%)$, which is a major difference from previous work. The detailed results for this procedure are presented in Section V-A1.

B. Frequency Correlation

In a multipath environment with rich scattering, the signal experiences frequency-selective fading, which is another valid random source that can be used for key generation. However, there will be correlation between adjacent frequencies. In this section, we exploit the frequency correlation relationship of the channel estimation $\widehat{H}_q[k]$.

The normalized frequency ACFs of $H_q[k]$ and $\widehat{H}_q[k]$ can be obtained by letting $\Delta t = 0$ in (22) and (26) and are written as

$$R_H(\Delta f, 0) = \frac{r_H(\Delta f, 0)}{r_H(0, 0)}, \tag{31}$$

and

$$R_{\widehat{H}}(f_k, f_i, 0) = \frac{R_H(\Delta f, 0) SNR_f E\{e^{j2\pi(k-i)\varepsilon_q/M}\} + \delta(\Delta f)}{1 + SNR_f}, \tag{32}$$

respectively, and shown in Fig. 2.

The frequency ACFs of $\widehat{H}_q[k]$ indicates that it is feasible to extract keys from multiple subcarriers that are separated by a certain frequency. This is verified by the randomness test and the detailed results are shown in Section V-A2.

IV. Analysis and Improvement of Measurements Cross-Correlation

In this section, we analyze the effects of non-simultaneous measurements and noise on the signal cross-correlation and improve the correlation by an FIR LPF. We consider

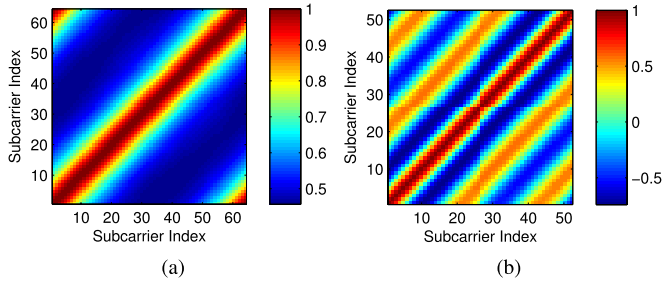

Fig. 2. Frequency ACFs, $\sigma_\tau = 50$ ns, $SNR = 10$ dB. (a) $R_H(\Delta f, 0)$; (b) $R_{\widehat{H}}(f_k, f_i, 0)$.

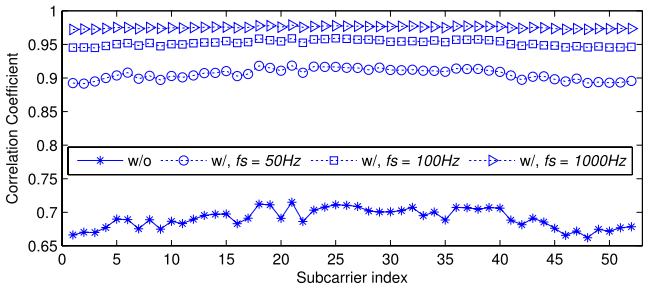

Fig. 3. $\rho(\widehat{H}_{t_A}^A[k], \widehat{H}_{t_B}^B[k])$ of all the subcarriers. $SNR = 6$ dB.

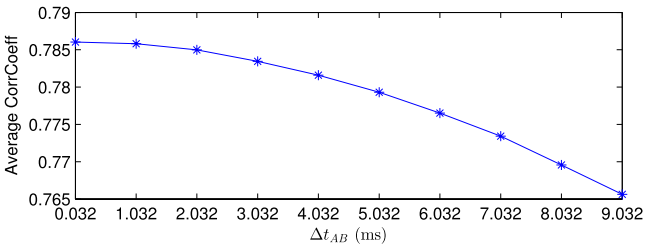

Fig. 4. The average correlation coefficient against Δt_{AB}. $SNR = 10$ dB.

half-duplex hardware to make our analysis more general. The estimated channel responses of Alice and Bob can be given as

$$\widehat{H}_{t_A}^A[k] = \widetilde{H}_{t_A}[k] + \widehat{w}_{t_A}^A[k]; \tag{33}$$

$$\widehat{H}_{t_B}^B[k] = \widetilde{H}_{t_B}[k] + \widehat{w}_{t_B}^B[k], \tag{34}$$

where t_A and t_B are the measurement time of Alice and Bob, respectively. The value $\Delta t_{AB} = |t_A - t_B|$ is deliberately kept as small as possible to ensure that $\widetilde{H}_{t_A}^A[k]$ and $\widetilde{H}_{t_B}^B[k]$ are highly correlated in a slow fading channel. The noises $\widehat{w}_{t_A}^A[k]$ and $\widehat{w}_{t_B}^B[k]$ reside in two hardware platforms and therefore are independent.

A. Cross-Correlation Relationship

Cross-correlation relationship describes the similarity between the measured channel responses of Alice and Bob. The covariance between $\widehat{H}_{t_A}^A[k]$ and $\widehat{H}_{t_B}^B[k]$ can be calculated as

$$cov(\widehat{H}_{t_A}^A[k], \widehat{H}_{t_B}^B[k]) = cov(H_{t_A}[k], H_{t_B}[k]) E\{e^{j2\pi \Delta\varepsilon' k/M}\}, \tag{35}$$

where $\Delta\varepsilon' = \varepsilon_{t_A} - \varepsilon_{t_B}$.

The correlation coefficient between $\widehat{H}_{t_A}^A[k]$ and $\widehat{H}_{t_B}^B[k]$ can be given as

$$\rho(\widehat{H}_{t_A}^A[k], \widehat{H}_{t_B}^B[k]) = \frac{cov(H_{t_A}[k], H_{t_B}[k]) E\{e^{j2\pi \Delta\varepsilon' k/M}\}}{\sigma_H^2 + \sigma_w^2}, \tag{36}$$

and the average correlation coefficient of all the subcarriers can be calculated by

$$\bar{\rho} = \frac{1}{M} \sum_{k=0}^{M-1} \rho(\widehat{H}_{t_A}^A[k], \widehat{H}_{t_B}^B[k]). \tag{37}$$

The cross-correlation coefficients of all the subcarriers are shown in Fig. 3 using SNR = 6 dB as an example. It may be observed that the cross-correlation coefficients are slightly different due to the imperfect synchronization at the receiver.

1) Effect of Non-Simultaneous Measurements: Although Alice and Bob do not measure the channel at the same time, the channel does not change much in a slow fading environment as long as Δt_{AB} is small enough. The average correlation coefficient against Δt_{AB} is shown in Fig. 4.

As may be observed from the figure, Δt_{AB} does not affect the average correlation coefficients much when it is small. This time resolution is easy to satisfy. For example, in a 20 MHz channel spacing IEEE 802.11 OFDM system, the sampling time difference between Alice and Bob can be configured in the order of 0.1 ms.

2) Effect of Noise: Noise is then the main factor that impacts the measurements. The frequency domain components of the $H_t[k]$ and $\widehat{H}_t[k]$ are shown in Fig. 5 (a) and Fig. 5 (b), respectively. As shown in (28), $H_t[k]$ has the same temporal ACF as the channel taps, therefore, their PSD $S(f)$ are the same as well. The main energy of $H_t[k]$ is then concentrated in $[0, f_d]$. This can also be observed from Fig. 5 (a). Therefore, an LPF can be designed to eliminate the high frequency components which flood $\widehat{H}_t[k]$.

3) Correlation Relationship Approximation: As the channel does not change much during Δt_{AB}, the correlation coefficient can be approximated to

$$\begin{aligned}\rho(\widehat{H}_{t_A}^A[k], \widehat{H}_{t_B}^B[k]) &\approx \frac{cov(H_{t_A}[k], H_{t_A}[k]) E\{e^{j2\pi \Delta\varepsilon' k/M}\}}{\sigma_H^2 + \sigma_w^2} \\ &= \frac{\sigma_H^2 E\{e^{j2\pi \Delta\varepsilon' k/M}\}}{\sigma_H^2 + \sigma_w^2} \\ &= \frac{SNR_f}{1 + SNR_f} E\{e^{j2\pi \Delta\varepsilon' k/M}\}. \end{aligned} \tag{38}$$

The cross-correlation coefficients are mainly determined by the SNR. We calculate the average correlation coefficients of all the subcarriers against SNR and show the results in Fig. 6. The theoretical curve is calculated by the analytical expression (38) which assumes perfect synchronization, i.e., $\Delta\varepsilon' = 0$. As may be observed from the figure, when SNR is low, the correlation coefficients exhibit large deviations from the theoretical ones. This is because in low SNR environments, there is a greater difference in the time offsets of Alice and Bob.

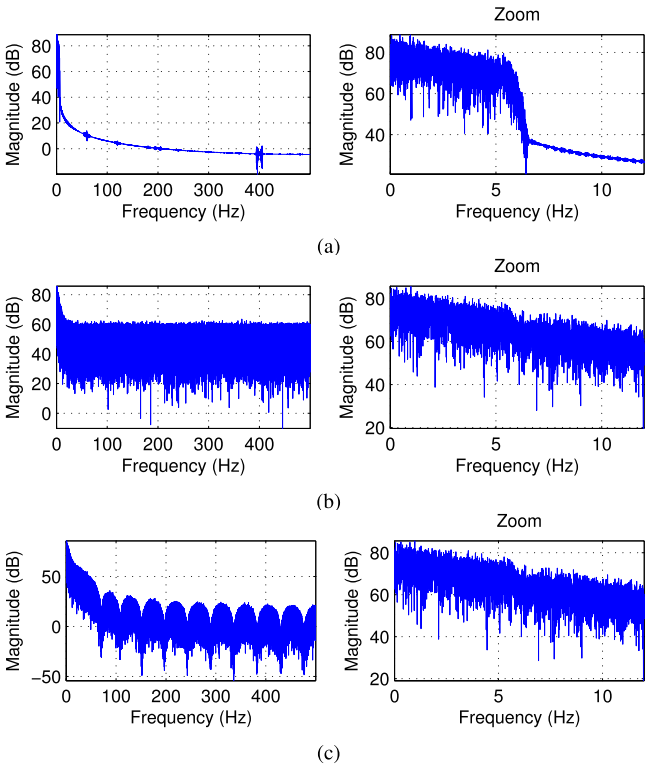

Fig. 5. Frequency domain analysis (magnitude), $SNR = 6$ dB, $f_d = 6$ Hz. The figures in the right panes are a zoom of the frequency. (a) $H_t[k]$; (b) $\widehat{H}_t[k]$; (c) Filtered $\widehat{H}_t[k]$.

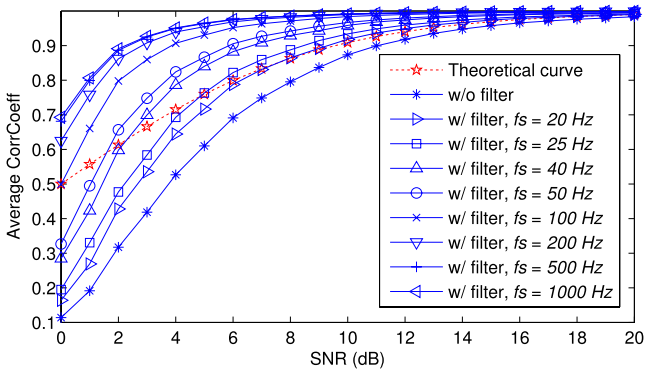

Fig. 6. The average correlation coefficient in different SNR environments under an LPF with different sampling frequency.

B. Measurements Correlation Improvement

An FIR LPF is proposed to effectively target the elimination of the noise and improve the SNR and correlation relationship. The parameters of the LPF are shown in Table II. As the main energy of the $H_t[k]$ is in the range of $[0, f_d]$, an LPF with a cutoff frequency f_c of f_d is designed to target elimination of the high frequency components of the noise. However, the estimation of the Doppler spread is difficult, thus f_c is fixed to $f_{d,max}$. Key generation has been conventionally aimed at slow fading environments so that $f_{d,max}$ is very small, e.g., 6 Hz in a Bell-shaped Doppler power spectrum model [42]. Therefore, keeping f_c to $f_{d,max}$ fixed will not greatly impact the performance.

TABLE II
PARAMETERS OF THE DESIGNED LPF

Cutoff frequency f_c	$f_{d,max}$
Filter order	20
Kaiser window length	21
Kaiser window β	3

The noise suppression effect of the LPF is shown in Fig. 5 (c); it may be observed that the high frequency components of the noise is largely eliminated. The improvement of the correlation relationship for all the subcarriers when $SNR = 6$ dB is shown in Fig. 3, from which it may be observed that all the subcarriers have quite similar correlation coefficients after filtering.

The performance of the LPF with varying sampling frequencies f_s in different SNR environments is shown in Fig. 6. It may be observed from the figure that the LPF produces a good improvement of the correlation, especially in low SNR environments. Ideally, a higher sampling frequency f_s is preferred due to its better improvement. However, when the channel changes slowly and the sampling frequency reaches some value, e.g., 200 Hz in Fig. 6, any further increase in the sampling frequency does not contribute much more to the sampling of the signal variation. Therefore, it is not necessary to use a very high sampling frequency because an optimal sampling frequency can be tuned to the signal variation. This could benefit the application of LPF in cost- and energy-sensitive devices as it can keep the overhead introduced by LPF as low as possible while achieving an acceptable performance.

The hardware cost for the filter is low as it has a small order. In addition, current 3G cellular devices regularly monitor the channel at 1500 Hz for closed loop power control. As may be observed from Fig. 6, a sampling frequency of 200 Hz already produces a good improvement on the correlation relationship. Hence, the sampling overhead is well within the capability of mobile devices. Therefore, the implementation of the LPF is worthwhile to improve the cross-correlation of the measurements, while introducing only a small overhead and cost.

V. PERFORMANCE EVALUATION

The channel responses of OFDM subcarriers are sampled at a frequency f_s. The sampled data $\widehat{H}_q[k]$ is then passed to the LPF in order to improve the cross-correlation relationship. The filter data is later re-sampled by a probing rate T_p to reduce the redundancy. In our system, a single-bit cumulative distribution function (CDF)-based quantization [16] is adopted to convert $\widehat{H}_q[k]$ into binary values K_k. These binary sequences may be used separately as keys to different cryptographic applications. Alternatively, we can concatenate multiple binary sequences together to form a longer sequence, i.e., $K = [K_1||...||K_k||...||K_{N_s}]$, where $||$ denotes concatenation and N_s is the number of uncorrelated subcarriers, which will be analyzed in detail in Section V-A2. Information reconciliation technique, such as secure sketch [46], is used to correct the key disagreement between the users, and privacy amplification

TABLE III

RANDOMNESS TEST RESULTS OF KEY SEQUENCES QUANTIZED FROM $\widehat{H}_q[k]$. THE PROBING RATES T_p ARE SET AS DIFFERENT $X\%$ COHERENCE TIME $T_c(X\%)$

Corr coeff $X\%$	50%	30%	15%	12%	10%	9%
$T_c(X\%)$(s)	0.067	0.097	0.136	0.154	0.2	0.226
Sequence length	7462	5154	3676	3246	2500	2212
Frequency	0.61	0.956	0.767	0.861	0.968	0.799
Block frequency	0	0.001	0.242	0.185	0.408	0.021
Runs	0	0	0	0.001	0.02	0.046
Longest run of 1s	0	0	0.014	0.824	0.85	0.668
DFT	0	0.005	0.283	0.729	0.054	0.654
Serial	0	0	0.21	0.104	0.211	0.495
	0	0.257	0.943	0.88	0.107	0.667
Appro. entropy	0	0	0	0.012	0.282	0.472
Cum. sums (fwd)	0.521	0.652	0.565	0.854	0.967	0.252
Cum. sums (rev)	0.316	0.704	0.837	0.743	0.981	0.404

is finally employed to remove the information revealed to eavesdroppers during the information reconciliation.

In this section, we evaluated the performance of our key generation system in terms of randomness, KGR, and KDR.

A. Randomness Test

1) Single Random Source: A statistical randomness test suite provided by National Institute of Standards and Technology (NIST) [47] is adopted to test the randomness of the key sequence generated from the channel responses of OFDM subcarriers, which is widely used in the key generation systems [12], [13], [20], [22]. Table III shows the results of the randomness test of keys quantized from a single subcarrier. Each test returns a *P-value* which is compared with a threshold (0.01 in this paper). The cells highlighted in gray fail the random test, i.e., *P-value* < 0.01.

As may be observed from the Table III, using the commonly acknowledged 50% coherence time $T_c(50\%)$ as the probing rate cannot generate random sequences at all. In these results, the probing rate needs to be increased to $T_c(10\%)$ in order for the system to be able to extract a random key sequence. This is the optimal probing rate.

Temporal correlation can also be tackled by using decorrelation algorithms [16], [25]. The decorrelation algorithms themselves do not introduce more entropy but only aggregate the energy. In addition, the algorithms' complexities increase with the data block length [48], which may not be applicable to limited computational capacity devices. A rule of thumb for the optimal probing rate is thus attractive as it does not require any other additional signal processing.

2) Multiple Random Source: In a multipath channel with L independent channel taps, theoretically there should be up to L independent subcarriers. However, the average power of the taps is not evenly distributed. For example, it follows an exponential-decay profile in the indoor environment and the power will be mostly concentrated in the first few taps, as shown in Table IV.

Only the taps with short delays are the main contributors to the randomness. Therefore, the number of uncorrelated subcarriers for key generation N_s will also be smaller than L.

TABLE IV

POWER DISTRIBUTION OF CIR UNDER EXPONENTIAL-DECAY POWER DELAY PROFILE. THE TOTAL POWER $\sum_{l=0}^{L-1}\sigma_{h_l}^2$ IS NORMALIZED TO 1

L	$\sigma_{h_1}^2$	$\sum_{l=0}^{1}\sigma_{h_l}^2$	$\sum_{l=0}^{2}\sigma_{h_l}^2$	$\sum_{l=0}^{3}\sigma_{h_l}^2$
6	86.47%	98.17%	99.75%	99.96%
11	63.21%	86.46%	95.01%	98.16%
21	39.35%	63.21%	77.69%	86.47%

In this section, we selected N_s subcarriers satisfying

$$-0.5 < R_{\widehat{H}}(f_k, f_i, 0) < 0.5, \tag{39}$$

quantized them separately and finally concatenated these binary values to form a new sequence. As may be observed from Fig. 1, subcarriers have slightly different $T_c(X\%)$. In order to focus on the frequency correlation between two binary sequences K_k and K_i, we use a relatively large probing rate, 0.5 s, so there will be little temporal correlation within K_k.

NIST randomness test is applied to the new sequence and the results are shown in Table V. We also did the same process to the theoretical channel response $H_q[k]$ for comparison. For all the multipath environments, $N_s < L$, which matches our intuitive analysis that the first N_s channel taps are the dominant contributor to the randomness. In addition, when there is richer scattering in the environment, i.e., more channel taps, there are more random sources for extraction, which is due to that the channel is more frequency-selective.

B. KGR

Channel parameter (CSI, RSS, etc) and probing rate are the key factors for the KGR. In this paper, due to the employment of the fine-grained channel responses of OFDM subcarriers and determination of optimal probing rate, our system can achieve a much higher KGR than existing single-dimensional parameter-based key generation systems.

The KGR of single-dimensional parameter-based key generation systems, e.g., RSS-based systems, can be written as

$$KGR' = \frac{1}{T_p}. \tag{40}$$

Single-dimensional parameter-based key generation systems lose lots of useful information of the channel. For example, RSS only has amplitude information.

Our scheme can achieve a higher KGR than single-dimensional parameter-based schemes. Firstly, we can extract keys from the real and imaginary parts of the channel estimation simultaneously, a general feature of key generation from fine-grained CSI [25], [49], which can double the KGR compared to the single-dimensional parameter-based systems. Secondly, we extract randomness from both the time and frequency domains. In particular, in a frequency-selective fading channel, there are up to N_s frequencies applicable for key generation in our scheme, which will significantly improve

TABLE V
RANDOMNESS TEST RESULTS OF KEY SEQUENCES CONCATENATED FROM MULTIPLE SUBCARRIERS

L	6				11				21			
Data	$H_q[k]$		$\widehat{H}_q[k]$		$H_q[k]$		$\widehat{H}_q[k]$		$H_q[k]$		$\widehat{H}_q[k]$	
N_s	1	2	3	4	3	4	4	5	8	9	9	10
Sequence length	1000	2000	3000	4000	3000	4000	4000	5000	8000	9000	9000	10000
Frequency	0.899	0.928	1	0.635	0.97	0.949	0.949	0.909	0.84	0.899	0.966	0.984
Block frequency	0.958	0.604	0.393	0.245	0.477	0.941	0.939	0.478	0.987	0.942	0.282	0.417
Runs	0.164	0.152	0.77	0.129	0.798	0.429	0.974	0.887	0.035	0.016	0.849	0.968
Longest run of 1s	0.66	0.164	0.522	0.712	0.953	0.688	0.824	0.962	0.286	0.024	0.518	0.651
DFT	0.384	0	0.093	0	0.019	0	0.146	0	0.01	0	0.033	0
Serial	0.423 0.332	0.101 0.041	0.928 0.841	0.663 0.754	0.237 0.454	0.771 0.8	0.199 0.1	0.336 0.328	0.324 0.623	0.528 0.137	0.594 0.636	0.769 0.664
Appro. entropy	0.33	0.254	0.988	0.228	0.305	0.809	0.692	0.398	0.044	0.511	0.367	0.591
Cum sum (fwd)	0.989	0.956	0.948	0.736	0.744	0.965	0.989	0.954	0.997	0.999	0.979	0.986
Cum sum (rev)	0.999	0.902	0.948	0.876	0.778	0.986	0.989	0.881	0.999	0.987	0.963	0.981

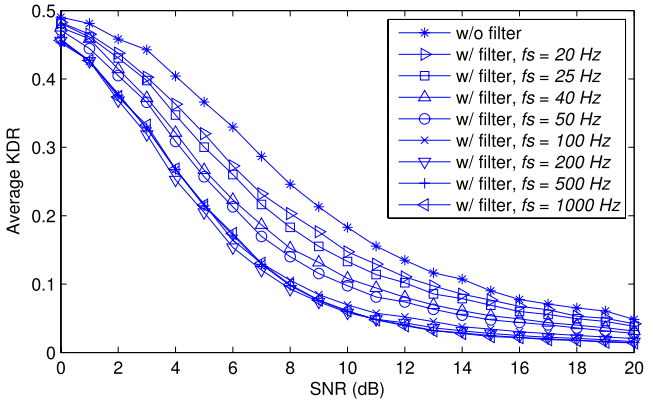

Fig. 7. The average KDR in different SNR environments under an LPF with different sampling frequency.

the KGR. Therefore, the KGR of our system can be given as

$$KGR = \sum_{i=1}^{N_s} \frac{2}{T_p(i)}, \tag{41}$$

where $T_p(i)$ is i^{th} subcarrier's optimal probing rate.

C. KDR

As can be observed from Fig. 7, even with the help of the LPF, there is still disagreement between Alice and Bob. This is because the noise effect can only be suppressed, but not completely eliminated. Therefore, information reconciliation is necessary to make Alice and Bob agree on the same key. However, all the information reconciliation techniques are upper bounded by the correction capacity. Taking the secure sketch [46] as an example, the $[n, k, t]$ BCH code can be implemented to correct the disagreement with a maximum correction capacity rate of

$$\eta = \frac{t_{max}}{n} = \frac{2^{m-2} - 1}{2^m - 1}, \tag{42}$$

which approaches 0.25 when m becomes large. The KDR should be smaller than the correction capacity η in order to guarantee all the disagreement to be corrected by information reconciliation. There is a lower bound of SNR for the key generation working successfully, which equals 8 dB when there is no LPF, or 4 dB when the correlation is improved by the LPF with sampling frequency $f_s = 100$ Hz or higher, as shown in Fig. 7. This extends the working SNR range by 4 dB. Even in high SNR environments, the introduction of LPF is still beneficial. A reduction in the KDR decreases the burden of the information reconciliation, and can ease its design. In addition, a lower KDR requires fewer rounds of information reconciliation and less information is revealed to eavesdroppers. Therefore, the correlation improvement by LPF can make the key generation system much more efficient.

VI. CONCLUSION AND FUTURE WORK

An efficient key generation system that exploits the randomness from OFDM subcarrier's channel responses is proposed. The efficiency is achieved by using an optimal probing rate, randomness extraction from multiple subcarriers, and improved cross-correlation of the measurements.

The appropriateness of OFDM subcarrier's channel responses as a random source for key generation is verified through theoretical modelling and analysis. The time and frequency autocorrelation relationship of the OFDM subcarrier's channel responses is modelled theoretically and it helps determine the optimal probing rate and the number of subcarriers that can be used for key extraction. Cross-correlation of the channel measurements is modelled and noise is found to have a more detrimental effect than non-simultaneous measurements in a slow fading channel. An LPF is subsequently proposed to suppress the high frequency components of noise, improve the cross-correlation coefficient and reduce the KDR, which extends the SNR working range of the system. We evaluated our system in terms of randomness, KGR and KDR, and showed that OFDM subcarrier's channel responses are valid for key generation. In a real environment, the channel may change dynamically due to uncontrolled movement of users/objects, which results in variable statistical channel features, such as varying Doppler spread and coherence bandwidth. Optimal probing rate and uncorrelated subcarriers selection are determined by Doppler spread and coherence bandwidth, respectively. Our future work will be to design an adaptive key generation system exploiting randomness from time and frequency domains, which adjusts the probing parameters according to the channel condition.

REFERENCES

[1] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.

[2] H. Yang, Y. Zhang, Y. Zhou, X. Fu, H. Liu, and A. V. Vasilakos, "Provably secure three-party authenticated key agreement protocol using smart cards," *Comput. Netw.*, vol. 58, pp. 29–38, Jan. 2014.

[3] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1299–1314, Jun. 2015.

[4] Y. Zou, X. Wang, and L. Hanzo. (2015). "A survey on wireless security: Technical challenges, recent advances and future trends." [Online]. Available: http://arxiv.org/abs/1505.07919

[5] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.

[6] Z. Zhang, X. Wang, K. Long, A. V. Vasilakos, and L. Hanzo, "Large-scale MIMO-based wireless backhaul in 5G networks," *IEEE Wireless Commun.*, vol. 22, no. 5, pp. 58–66, Oct. 2015.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[8] T. Wang, Y. Liu, and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Netw.*, vol. 21, no. 6, pp. 1835–1846, Aug. 2015.

[9] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016.

[10] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[11] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec. 2014.

[12] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, Sep. 2008, pp. 128–139.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Beijing, China, Sep. 2009, pp. 321–332.

[14] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. 29th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[15] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. 31st IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, USA, Mar. 2012, pp. 927–935.

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

[17] L. Yao, S. T. Ali, V. Sivaraman, and D. Ostry, "Decorrelating secret bit extraction via channel hopping in body area networks," in *Proc. 23rd IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sydney, NSW, Australia, Sep. 2012, pp. 1454–1459.

[18] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, Sep. 2013.

[19] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1422–1430.

[20] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[21] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, Alexandria, VA, USA, Oct. 2007, pp. 401–410.

[22] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.

[23] W. Xi *et al.*, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proc. 22nd IEEE Int. Symp. Quality Service (IWQoS)*, Hong Kong, May 2014, pp. 350–359.

[24] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[25] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[26] B. T. Quist and M. A. Jensen, "Maximizing the secret key rate for informed radios under different channel conditions," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5146–5153, Oct. 2013.

[27] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, Atlanta, GA, USA, Dec. 2013, pp. 1245–1250.

[28] B. T. Quist and M. A. Jensen, "Maximization of the channel-based key establishment rate in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5565–5573, Oct. 2015.

[29] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[30] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst., Appl., Services (MobiSys)*, Washington, DC, USA, Jul. 2011, pp. 211–224.

[31] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2283–2291.

[32] *WiPhyLoc8 Project*, accessed Apr. 19, 2016. [Online]. Available: http://wiphyloc8.org/

[33] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, Austin, TX, USA, Dec. 2014, pp. 1302–1307.

[34] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "An effective key generation system using improved channel reciprocity," in *Proc. 40th IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, Apr. 2015, pp. 1727–1731.

[35] P. A. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. Commun. Syst.*, vol. 11, no. 4, pp. 360–393, Dec. 1963.

[36] J. W. Wallace, M. A. Jensen, A. L. Swindlehurst, and B. D. Jeffs, "Experimental characterization of the MIMO wireless channel: Data acquisition and analysis," *IEEE Trans. Wireless Commun.*, vol. 2, no. 2, pp. 335–343, Mar. 2003.

[37] A. F. Molisch *et al.*, *IEEE 802.15.4a Channel Model-Final Report*, IEEE Standard 802.15-04/662r0, 2004.

[38] H. Minn, V. K. Bhargava, and K. B. Letaief, "A robust timing and frequency synchronization for OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 2, no. 4, pp. 822–839, Jul. 2003.

[39] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. New York, NY, USA: Wiley, 2010.

[40] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11, 2012.

[41] C. Iskander, "A MATLAB-based object-oriented approach to multipath fading channel simulation," MathWorks, Natick, MA, USA, White Paper 18869, Feb. 2008.

[42] V. Erceg *et al.*, *TGn Channel Models*, IEEE Standard 802.11-03/940r4, May 2004.

[43] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 902–915, Jul. 1998.

[44] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2001.

[45] H. Jung, T. Kwon, K. Cho, and Y. Choi, "REACT: Rate adaptation using coherence time in 802.11 WLANs," *Comput. Commun.*, vol. 34, no. 11, pp. 1316–1327, Jul. 2011.

[46] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[47] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-22, Apr. 2010.
[48] S. Gopinath, R. Guillaume, P. Duplys, and A. Czylwik, "Reciprocity enhancement and decorrelation schemes for PHY-based key generation," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. Phys. Layer Secur. (TCPLS)*, Austin, TX, USA, Dec. 2014, pp. 1367–1372.
[49] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag. (EuCAP)*, Berlin, Germany, Mar. 2009, pp. 1499–1503.

Junqing Zhang received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China, in 2009 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from Queen's University Belfast, U.K., in 2016. He is currently a Post-Doctoral Research Fellow with Queen's University Belfast. His research interests include physical layer security, cryptography, and OFDM.

Alan Marshall (M'88–SM'00) has spent over 24 years with the telecommunications and defense industries. He has been a Visiting Professor of Network Security with the University of Nice/CNRS, France, and an Adjunct Professor for Research with Sunway University Malaysia. He is currently the Chair in Communications Networks with the University of Liverpool, where he is also the Director of the Advanced Networks Group. He has formed a successful spin-out company, Traffic Observation & Management Ltd., specializing in intrusion detection and prevention for wireless networks. He has authored over 200 scientific papers and holds a number of joint patents in the areas of communications and network security. His research interests include network architectures and protocols, mobile and wireless networks, network security, high-speed packet switching, quality of service and experience architectures, and distributed haptics. He is a fellow of The Institution of Engineering and Technology. He is a Section Editor (section B: Computer and Communications Networks and Systems) of the *Computer Journal* of the British Computer Society, a member of the Editorial Board of the *Journal of Networks*, and also on the program committees of a number of the IEEE conferences.

Roger Woods (M'95–SM'01) received the B.Sc. (Hons.) degree in electrical and electronic engineering and the Ph.D. degree from Queen's University Belfast, in 1985 and 1990, respectively. He is currently a Full Professor with Queen's University Belfast, and has created and leads the Programmable Systems Laboratory. He has co-founded a spin-off company, Analytics Engines Ltd., which looks to exploit a lot of the programmable systems research. His research interests are in heterogeneous programmable systems and system level design tools for data, signal and image processing, and telecommunications. He holds 4 patents and has authored over 170 papers. He is a member of the IEEE Signal Processing and Industrial Electronics Societies and is on the Advisory Board of the IEEE SPS Technical Committee on the Design and Implementation of Signal Processing Systems. He is on the Editorial Board for the *ACM Transactions on Reconfigurable Technology and Systems*, the *Journal of VLSI Signal Processing Systems*, and the *IET Proceedings on Computer and Digital Techniques*. He acted as the General Chair of the 2014 Asilomar IEEE Conference on Signals, Systems, and Computers, and is on the program committees of a number of IEEE conferences.

Trung Q. Duong (S'05–M'12–SM'13) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden, in 2012. Since 2013, he has been with Queen's University Belfast, U.K., as a Lecturer (Assistant Professor). He has authored or co-authored 170 technical papers published in scientific journals and presented at international conferences. His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, millimeter-waves communications, and localization for radios and networks.

Dr. Duong received the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, and the IEEE International Conference on Communications in 2014. He is currently a recipient of the Royal Academy of Engineering Research Fellowship. He currently serves as an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, *IET Communications*, *Transactions on Emerging Telecommunications Technologies* (Wiley), and *Electronics Letters*. He has also served as the Guest Editor of the special issue on some major journals, including the IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, *IET Communications*, the *IEEE Wireless Communications Magazine*, the *IEEE Communications Magazine*, the *EURASIP Journal on Wireless Communications and Networking*, and the *EURASIP Journal on Advances Signal Processing*.