AN EFFECTIVE KEY GENERATION SYSTEM USING IMPROVED CHANNEL RECIPROCITY

Junqing Zhang[⋆] *Roger Woods*[⋆] *Alan Marshall*[†] *Trung Q. Duong*[⋆]

[⋆] ECIT, Queen's University Belfast
Belfast, BT3 9DT, UK
Email: {jzhang20, r.woods, trung.q.duong}@qub.ac.uk
[†]Department of Electrical Engineering and Electronics, University of Liverpool
Liverpool, L69 3GJ, UK
Email: Alan.Marshall@liverpool.ac.uk

ABSTRACT

In physical layer security systems there is a clear need to exploit the radio link characteristics to automatically generate an encryption key between two end points. The success of the key generation depends on the channel reciprocity, which is impacted by the non-simultaneous measurements and the white nature of the noise. In this paper, an OFDM subcarriers' channel responses based key generation system with enhanced channel reciprocity is proposed. By theoretically modelling the OFDM subcarriers' channel responses, the channel reciprocity is modelled and analyzed. A low pass filter is accordingly designed to improve the channel reciprocity by suppressing the noise. This feature is essential in low SNR environments in order to reduce the risk of the failure of the information reconciliation phase during key generation. The simulation results show that the low pass filter improves the channel reciprocity, decreases the key disagreement, and effectively increases the success of the key generation.

Index Terms— Physical layer security, key generation, channel reciprocity, low pass filter, key disagreement

1. INTRODUCTION

Key generation from the randomness of the wireless channel has attracted increasing research interest, as it is a promising alternative to the public key cryptography for establishing a secret key between two legitimate users, Alice and Bob [1]. This technique is based on the channel reciprocity, which means if the users probe each other at the same time, they will produce the same measurement. However, due to the half duplex nature of the most commercial radio transceivers, Alice and Bob cannot probe simultaneously, thus in a noisy and dynamic changing environment, the channel reciprocity is impacted by the noise and asynchronous timing of the measurements. This results in the disagreement of the keys that are generated at each side, which can be quantified by the key disagreement rate (KDR) defined as the ratio between the number of the mismatch bits and the number of total key bits.

Researchers have aimed to improve the channel reciprocity by filtering or interpolation. Azimi-Sadjahi *et al.* [2] filtered the received signal with a narrow low pass filter to reduce the noise. Ali *et al.* [3] employed a Savitzky-Golay filter in order to follow the underlying slow-moving features of the received signal strength (RSS) traces. Zhu *et al.* [4] used a weighted sliding window smoothing to eliminate the issue of noise. Patwari *et al.* [5] and Liu *et al.* [6] implemented a cubic Farrow filter for interpolation to address the non-simultaneous measurement problem, respectively.

While these efforts have improved the channel reciprocity between Alice and Bob, they all extract the key from RSS. There is no analytical modelling of the relationship between the RSS and the noise. Thus the design of the low pass filter is mainly empirical which is less effective to suppress the high frequency components of the noise. In this paper, a physical layer key generation system based on IEEE 802.11 OFDM is proposed for indoor environments. The system extracts keys from OFDM subcarriers' channel responses. The feasibility of this overall approach has already been discussed in [7]. In this paper, by theoretically modelling the OFDM subcarriers' channel responses, the mathematical model of the channel reciprocity is obtained and a low pass filter is accordingly designed to reduce the effects of noise. Our contributions are summarized as follows:

- The mathematical modelling and analysis of the channel reciprocity based on the theoretical model and frequency domain analysis of the OFDM subcarriers' channel responses.
- Design of an effective low pass filter based on the theoretical model of the channel reciprocity to target to eliminate the effects of noise, improve the channel reciprocity and ultimately reduce the KDR between legitimate users.

2. SYSTEM MODEL

2.1. Channel Model

The wireless multipath channel can be modelled by a linear time-varying system with a complex channel impulse response $h(\tau, t)$, which can be written as

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

where L is the number of channel taps, $h(\tau_l, t)$ and τ_l are the complex attenuation and the delay of the l-th tap at time t, $\tau_l = lT$, respectively and T is the system's hardware sampling period, $\delta(\cdot)$ is the Dirac delta function. According to the central limit theorem, in a rich scattering multipath environment $h(\tau_l, t)$ can be approximated by zero-mean complex Gaussian random variables [8], i.e., $h(\tau_l, t) \sim C\mathcal{N}(0, \sigma_h^2(l))$.

In an OFDM system, channel frequency response $H(f, t)$ and channel impulse response $h(\tau, t)$ are an FFT pair. $H(f, t)$ can be obtained by applying IFFT operation to $h(\tau, t)$

$$\begin{aligned} H(f_m, t) &= \sum_{l=0}^{L-1} h(\tau_l, t)\text{exp}(-j2\pi f_m \tau_l) \\ &= \sum_{l=0}^{L-1} h(\tau_l, t)\text{exp}(-j2\pi ml/M), \end{aligned} \tag{2}$$

where $f_m = m\Delta f$, m is the subcarrier index, $-\frac{M}{2} + 1 \leq m \leq \frac{M}{2}$ and Δf is the frequency difference between two adjacent subcarriers, $\Delta f = \frac{1}{MT}$.

As each channel tap $h(\tau_l, t)$ is a time-variable modelled as a complex Gaussian process and $H(f_m, t)$ is a linear combination of $h(\tau_l, t)$, $H(f_m, t)$ is also a complex Gaussian random process, which is applicable for key generation.

2.2. Wide Sense Stationary (WSS) Model

A rich scattering multipath channel can be modelled as wide sense stationary uncorrelated scattering (WSSUS) random process [9]. The autocorrelation function (ACF) of $h(\tau, t)$ under this assumption is given by

$$r_h(\tau, \Delta t) = E\left[h(\tau, t)^* h(\tau, t + \Delta t)\right]. \tag{3}$$

The mean value of m-th subcarrier's channel response $H(f_m, t)$ is 0 and its ACF can be calculated by

$$\begin{aligned} &r_H(f_m, t, t + \Delta t) = E\left[H(f_m, t)^* H(f_m, t + \Delta t)\right] \\ &= \sum_{l=0}^{L-1}\sum_{i=0}^{L-1} E\left[h(\tau_l, t)^* h(\tau_i, t + \Delta t)\right]\text{exp}(j2\pi m(l - i)/M) \\ &= \sum_{l=0}^{L-1} E\left[h(\tau_l, t)^* h(\tau_l, t + \Delta t)\right]. \end{aligned} \tag{4}$$

The mean value of $H(f_m, t)$ is a constant and its ACF only depends on the time delay, thus the channel response $H(f_m, t)$ is a WSS random process.

2.3. Power Spectral Density (PSD) Model

In the indoor environment, the fading characteristics is different from the mobile case, and thus a Bell-shaped Doppler power spectrum is used, which is defined in [10] and given by

$$S(f) = \frac{\sqrt{A}/(\pi f_d)}{1 + A(\frac{f}{f_d})^2}, \tag{5}$$

where A is a constant, e.g., in IEEE 802.11 channel, $A = 9$ and f_d is the Doppler spread, whose maximum values $f_{d,max}$ were found to be approximately 6 Hz at a center frequency of 5.25 GHz and approximately 3 Hz at a center frequency of 2.4 GHz by experiments in indoor environment [10].

When all the channel taps are modelled by the Bell-shaped Doppler power spectrum, the normalized ACF of the l-th tap can be written as:

$$R_h(\tau_l, \Delta t) = \frac{r_h(\tau_l, \Delta t)}{r_h(\tau_l, 0)} = R_h(\Delta t). \tag{6}$$

The normalized ACF of the m-th subcarrier's channel response can be written as

$$\begin{aligned} R_H(f_m, \Delta t) &= \frac{r_H(f_m, \Delta t)}{r_H(f_m, 0)} \\ &= \frac{\sum_{l=0}^{L-1} E[h(\tau_l, t)^* h(\tau_l, t + \Delta t)]}{\sum_{l=0}^{L-1} E[|h(\tau_l, t)|^2]} \\ &= \frac{\sum_{l=0}^{L-1} R_h(\Delta t) E[|h(\tau_l, t)|^2]}{\sum_{l=0}^{L-1} E[|h(\tau_l, t)|^2]} \\ &= R_h(\Delta t). \end{aligned} \tag{7}$$

Thus, the subcarrier's channel response $H(f_m, t)$ has the same ACF as the channel taps and is independent of the subcarrier index m, which can be given by

$$R_H(\Delta t) = R_h(\Delta t). \tag{8}$$

Therefore, the PSD of all the subcarriers' channel responses is the same as the channel taps', i.e., Bell-shaped Doppler power spectrum given in (5). Thus the main energy of subcarriers' channel responses is in the range $[-f_d, f_d]$.

3. CHANNEL RECIPROCITY ANALYSIS AND FILTER DESIGN

3.1. Channel Reciprocity Analysis

In least square (LS) estimation of OFDM channels, the estimated subcarriers' channel responses can be given as

$$\widehat{H}(f_m, t) = H(f_m, t) + w(f_m, t), \tag{9}$$

where $w(f_m, t)$ is modelled as additive Gaussian white noise.

Due to the half duplex mode of the hardware, Alice and Bob cannot probe simultaneously. The estimated subcarriers' channel response of Alice and Bob can be written as

$$\widehat{H}_A(f_m, t_A(i)) = H(f_m, t_A(i)) + w(f_m, t_A(i)), \quad (10)$$

$$\widehat{H}_B(f_m, t_B(i)) = H(f_m, t_B(i)) + w(f_m, t_B(i)), \quad (11)$$

where $t_A(i)$ and $t_B(i)$ denote the probing time of Alice and Bob, respectively. As $|t_A(i) - t_B(i)|$ is deliberately kept very small, $H(f_m, t_A(i))$ and $H(f_m, t_B(i))$ are highly correlated. However, due to the white nature of the noise, $w(f_m, t_A(i))$ and $w(f_m, t_B(i))$ are not correlated, no matter how close in time they are, which contributes to the discrepancy between Alice's and Bob's channel estimation and impacts the channel reciprocity.

3.2. Filter Design

As discussed in Section 2.3, the main energy of $H(f_m, t)$ is in the range of $[-f_d, f_d]$, thus a low pass filter can be effectively designed to eliminate the high frequency components of the channel estimation, which helps to improve the correlation between Alice's and Bob's channel estimation.

Unlike other work, a more effective finite impulse response low pass filter with specific parameters is designed to target to remove the noise effect. The cut off frequency f_c is selected as $2f_d$ to eliminate most of the high frequency components of the noise while keeping the useful signal unaffected. The order of the filter is 20 and a Kaiser window with length 21 and $\beta = 3$ is also implemented.

The estimation of the Doppler spread is difficult, thus cut off frequency f_c is fixed as $2f_{d,max}$. As $f_{d,max}$ is very small, keeping f_c fixed will not affect greatly the performance.

4. SIMULATION RESULTS

4.1. Simulation Model

A transceiver model is implemented in Matlab based on the IEEE 802.11 OFDM protocol. The channel is modelled as a time-variant multipath fading channel [11]. All the channel taps are modelled as independent complex Gaussian random variables whose average power follows an exponential power delay profile and a Bell-shaped Doppler power spectrum with $f_d = 6$ Hz. The theoretical 50% coherence time is 56 ms [7].

The system is sampled with sampling frequency f_s, the sampled sequence is then passed to a low pass filter to eliminate the high frequency components. The total equivalent sampled time is 500 s. In order to get a random key sequence, the time interval between two consecutive samples, whose amplitude is to be quantized to generate the keys, should be larger than the coherence time [7]. Thus, the filtered sequence is re-sampled with sampling period $T_s = 200$ ms, which is much larger than the coherence time.

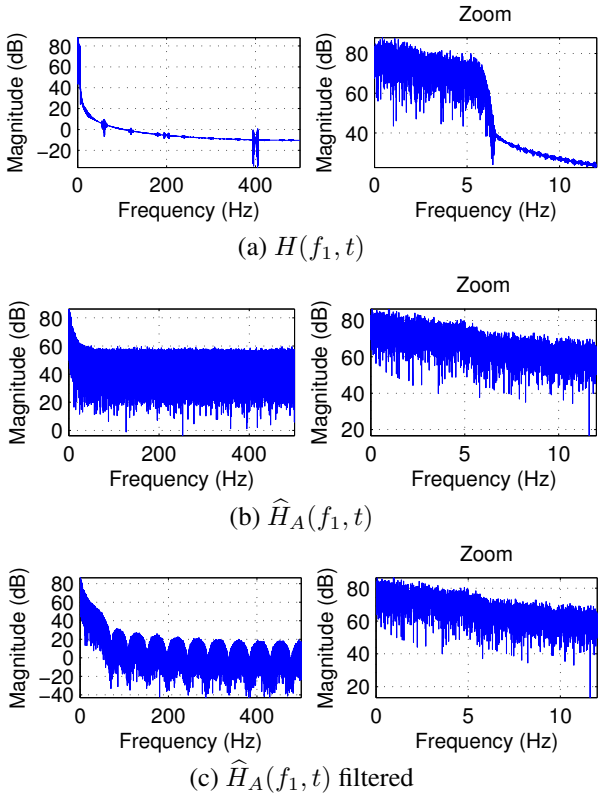

Fig. 1. Frequency domain analysis (magnitude)

4.2. Frequency Domain Analysis

The frequency domain analysis is performed with a sampling frequency f_s = 1000 Hz and total sampling points 500000. The 1st subcarrier's channel response is chosen as an example. As may be observed from Fig. 1(a), the main energy of $H(f_1, t)$ is in the range of $[0, 6]$ Hz, which matches the simulation setting $f_d = 6$ Hz. However, there are lots of high frequency components in the channel estimation due to the noise effect as shown in Fig. 1(b). The implemented low pass filter has a significant effect on suppressing the high frequency components while leaving the low frequency components unaffected, which can be observed from Fig. 1(c).

4.3. Key Disagreement Analysis

The amplitude of OFDM subcarriers' channel responses are quantized into key bits by cumulative distribution function based quantization scheme [7] and the KDR is calculated. The system is filtered by the low pass filter with $f_s = 1000$ Hz, 100 Hz and 50 Hz, respectively. Different SNR environments are tested. The performance and a comparison with the unfiltered system are shown in Fig. 2 and Fig. 3.

As may be observed from the figures, the KDR is reduced in all cases. When SNR = 5 dB, the KDR is averagely improved by $71.06\%, 38.72\%, 18.76\%$ for $f_s = 1000$Hz, 100Hz

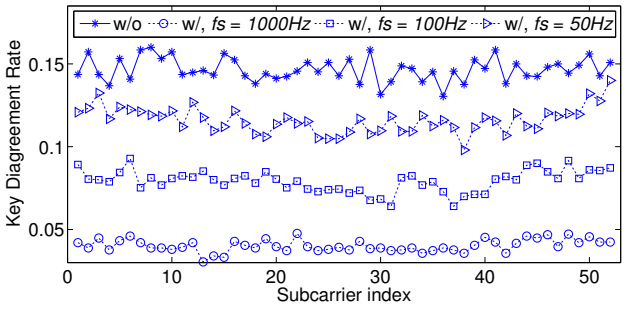

Fig. 2. KDR without and with low pass filter, SNR = 10 dB

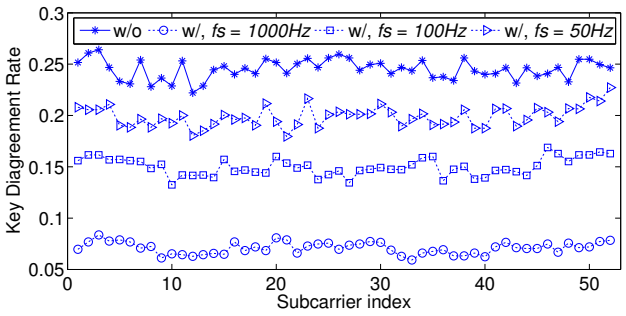

Fig. 3. KDR without and with low pass filter, SNR = 5 dB

and 50Hz respectively. With a relatively higher sampling frequency compared to the cut off frequency of the filter, a significant improvement can be achieved.

5. DISCUSSION

5.1. Necessity Analysis

As can be observed from Fig. 2 and Fig. 3, even with the help of the low pass filter, there is still key disagreement due to the fact that the low frequency components of the noise cannot be removed by the low pass filter. Thus, information reconciliation is still required in order to make Alice and Bob agree on the same key. However, the correction capacity of information reconciliation is limited. For example, Dodis *et al.* [12] designed secure sketch with BCH code implemented to correct the disagreement and the maximum correcting capacity rate of a BCH code $[n, k, t]$ can be written as

$$\eta = \frac{t_{max}}{n} = \frac{2^{m-2} - 1}{2^m - 1}, \tag{12}$$

which approaches 0.25 when m becomes large. As shown in Fig. 3, when SNR = 5 dB, the raw KDR is around 0.25; thus the system has a high possibility of failing the information reconciliation. Therefore, the implementation of a low pass filter to decrease the KDR is necessary, especially in low SNR environments, as it can reduce the risk of the failure of the information reconciliation, thus avoiding a restart of all the key generation process with the resulting energy consumption.

5.2. Feasibility Analysis

The improvement of the channel reciprocity is at a cost of more energy and memory, however, it is affordable in mobile devices. For example, current 3G cellular devices regularly monitor the channel at 1500 Hz for closed loop power control. Therefore, sampling at a rate of 1000 Hz is well within their capability. What is more, the cost for filter is low, especially for one with small number of filter orders. Finally, as the key only needs to be refreshed when required, compared to the energy consumption of the data communication, the consumption by key generation is relatively small.

5.3. Interpolation

In our work, interpolation is not implemented as the packet duration is short. For example, in a 20 MHz channel spacing IEEE 802.11 OFDM system, a packet with a maximum rate and minimum length results in an over-the-air time of only 34 μs. The turnaround time between the Tx mode and Rx mode is also very small. For example, it only takes 1 μs for a MAX2829 transceiver to change from Rx to Tx and 1.2 μs from Tx to Rx. The minimum 50% coherence time in an indoor environment is 56 ms, which is much larger. Thus $H(f_m, t_A(i))$ and $H(f_m, t_B(i))$ will be highly correlated and is not the main issue contributing to the key disagreement.

6. CONCLUSION

A theoretical modelling and analysis on the channel reciprocity has been carried out in this paper. The key is extracted from the randomness of the OFDM subcarriers' channel responses, and the procedure is theoretically modelled. In key generation systems, the asynchronous nature of the channel probing and the white nature of the channel noise are the major issues that impact the channel reciprocity and increase the KDR. Based on the channel reciprocity model, an effective low pass filter is accordingly designed to eliminate the noise, improve the channel reciprocity and ultimately reduce the KDR. Through the simulation results of the frequency domain analysis and KDR, it is concluded that the channel reciprocity improvement is necessary especially in low SNR environment to reduce the risk of failing the information reconciliation and improve the success of the key generation.

7. ACKNOWLEDGEMENT

The authors gratefully acknowledge support from the Queen's University Belfast scholarship and US-Ireland R&D Partnership USI033 'WiPhyLoc8' grant involving Rice University (USA), University College Dublin (Ireland) and Queen's University Belfast (Northern Ireland).

8. REFERENCES

[1] Kui Ren, Hai Su, and Qian Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun. Mag.*, vol. 18, no. 4, pp. 6–12, 2011.

[2] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, and Bulent Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. 14th ACM Conf. on Computer and Communications Security (CCS)*, Alexandria, USA, Oct. 2007, pp. 401–410.

[3] Syed Taha Ali, Vijay Sivaraman, and Diethelm Ostry, "Zero reconciliation secret key generation for body-worn health monitoring devices," in *Proc. 5th ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WiSec)*, New York, USA, Apr. 2012, pp. 39–50.

[4] Xiaojun Zhu, Fengyuan Xu, Edmund Novak, Chiu C Tan, Qun Li, and Guihai Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proc. 32nd IEEE Int. Conf. on Computer Communications (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 2283–2291.

[5] Neal Patwari, Jessica Croft, Suman Jana, and Sneha Kumar 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, 2010.

[6] Hongbo Liu, Jie Yang, Yan Wang, and Yingying Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. 31st IEEE Int. Conf. on Computer Communications (INFOCOM)*, Orlando, Florida, USA, Mar. 2012, pp. 927–935.

[7] Junqing Zhang, Alan Marshall, Roger Woods, and Trung Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *Proc. IEEE GLOBECOM Workshop on Trusted Communications with Physical Layer Security (TCPLS)*, Austin, USA, Dec. 2014, pp. 1406–1411.

[8] Yanpei Liu, Stark C Draper, and Akbar M Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[9] Philip Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. on Communications Systems*, vol. 11, no. 4, pp. 360–393, 1963.

[10] Vinko Erceg *et al.*, "TGn channel models," Tech. Rep. 03/940r4, IEEE TGn 802.11, May 2004.

[11] Cyril-Daniel Iskander, "A matlab-based object-oriented approach to multipath fading channel simulation," White Paper 18869, Mathworks, Natick, MA, Feb. 2008.

[12] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, 2008.