



**QUEEN'S
UNIVERSITY
BELFAST**

Secure Key Generation from OFDM Subcarriers' Channel Response

Zhang, J., Marshall, A., Woods, R., & Duong, T. Q. (2014). *Secure Key Generation from OFDM Subcarriers' Channel Response*. Paper presented at IEEE Global Communications Conference (GLOBECOM'14), Austin, United States. <http://globecom2014.ieee-globecom.org/IEEE%20GLOBECOM%202014%20Advance%20Program%2011.13.14.pdf>

Document Version:

Early version, also known as pre-print

Queen's University Belfast - Research Portal:

[Link to publication record in Queen's University Belfast Research Portal](#)

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Secure Key Generation From OFDM Subcarriers' Channel Response

Junqing Zhang*, Alan Marshall[†], Roger Woods*, 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—The ability to exchange keys between users is vital in any wireless based security system, so a key generation technique exploits the randomness of the wireless channel is a promising alternative to existing key distribution techniques, e.g., public key cryptography. In this paper a secure key generation scheme based on the subcarriers' channel responses over time in OFDM systems is proposed. We first implement a time-variant multipath channel with its channel impulse response modelled as a wide sense stationary (WSS) uncorrelated scattering random process and demonstrate that each subcarrier's channel response is also a WSS random process. We then define the $X\%$ coherence time as the time required to produce an $X\%$ correlation coefficient in the autocorrelation function (ACF) of each channel tap, and find that when all the channel taps have the same Doppler power spectrum, each subcarrier's channel response has the same ACF as the channel taps. The subcarrier's channel response is therefore sampled every $X\%$ coherence time and quantized into key bits. We test all the key sequences' randomness using National Institute of Standards and Technology (NIST) statistical test suite and the results indicate that the commonly used sampling interval as 50% coherence time cannot guarantee the randomness of the key sequence.

I. INTRODUCTION

Key generation from the randomness of the wireless channel is currently receiving intensive attention in the research community because it can offer information theoretical security rather than computational security [1]. Traditionally, the distribution of the keys between different users is performed by public key cryptography, which depends on the computational hardness and requires a key management infrastructure. However it is a major challenge for wireless sensor networks and ad hoc networks to accomplish this task as sensor nodes have limited computational budget and the distribution infrastructure in ad hoc networks cannot always be guaranteed.

The notion of generating keys from their common wireless channel to ensure privacy is a promising approach to establish private communication between legitimate users, Alice and Bob. In operation, Alice first sends a probing signal to Bob who will measure some physical modality through the received signal, e.g., received signal strength (RSS), phase, channel state information (CSI) etc. Bob then immediately sends a probing signal back to Alice who will also measure the same physical modality as Bob. The concept is then to generate

keys from the highly correlated measurements at each side. For indoor environment, the channel changes slowly so its coherence time is quite large (of the order of 10 ms) in comparison to the transmission time, therefore the channel can be regarded as static during Alice and Bob's measurements. Thus, Alice and Bob can produce almost identical measurements. Then, by waiting another coherence time to do the next probing, they can obtain another measurement that is uncorrelated with the previous. This is repeated until enough measurements are obtained to be quantized into key bits. Assuming that an eavesdropper, Eve, is more than a half wavelength away from both Alice and Bob, then due to the spatial decorrelation, the channel between Eve and Alice/Bob is completely different from the channel between Alice and Bob, so Eve cannot produce the same measurement results as Alice or Bob. Thus Alice and Bob can establish a secret key between each other that is unknown to Eve.

Theoretically, every physical modality related to the channel randomness can be used for key generation, however RSS is the most popular parameter. Most practical work is implemented in IEEE 802.11 systems [2]–[4] or IEEE 802.15.4 systems [5]–[7] because RSS information is available in their commercial network interface cards (NICs) or transceivers. However RSS can only provide averaged channel information, so we can only get one uncorrelated RSS from one measurement within the coherence time. This results in a low key generation rate (KGR) which limits its application in cryptography. For example, the KGR from RSS reported in [2] is only 1.3 bit/sec while advanced encryption standard (AES) requires a key length at least 128 bits, which takes approximately 2 minutes to generate a full key. Although there exists an extended effort to improve the KGR by leveraging MIMO [4] or multi-bit quantization [7], it cannot change the fact that RSS is an averaged parameter and loses a lot of useful channel information.

Some simulation work has been undertaken to generate the key from the phase [8]–[10]. Specifically, Wang *et al.* [9] proposed a phase based key generation scheme which can measure multiple randomized phase information within a single coherence time interval. Whilst their system does not suffer from the low KGR problem, the accurate estimation of

44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84

85 the phase information limits its practical application in key
86 generation.

87 Alternatively, CSI, including channel impulse response
88 (CIR) and channel frequency response (CFR) is a powerful
89 tool and presents a promising application for key genera-
90 tion [11], [12]. CSI is fine-grained channel information so it
91 does not suffer from the same information loss, which leads
92 to a higher achievable KGR than RSS based schemes [11].
93 However, in the case of CIR based schemes [11], those channel
94 taps with small magnitude are highly subject to noise, which
95 results in a high key mismatch between Alice and Bob. Liu
96 *et al.* [12] present a CFR based key generation scheme using
97 the Intel 5300 WiFi card and reports a KGR of 60 bits/packet
98 while the KGR of RSS based schemes with the same setting
99 is only 2 bits/packet. However their work lacks theoretical
100 modelling of the system or the channel.

101 Previous work generating key from RSS or CSI claim that
102 in order to guarantee the randomness of the key sequence,
103 the measurement sampling interval should be larger than one
104 coherence time [13], which is defined as the time over which
105 the time correlation function is above 0.5 [14]. However,
106 coherence time estimation is difficult in indoor environment
107 as the Doppler spread is usually introduced by the moving of
108 scattering objects rather than the transmitters or the receivers.
109 It has been observed that whenever the experiments are
110 actually performed, the authors usually just pick a time interval
111 that is large enough so that their key sequence can pass the
112 randomness test [12]. Thus, there is no evidence that sampling
113 interval as coherence time will actually produce secure random
114 keys.

115 In this paper, an approach for generating the key bits
116 securely from OFDM subcarriers' channel responses is pro-
117 posed. We implement a time-variant multipath channel model
118 and IEEE 802.11 OFDM transceiver, and then generate keys
119 from the subcarriers' channel responses. Our work differs
120 from the previous work, e.g. [12], in that we quantize the
121 key from the channel response of each individual subcarrier
122 over time rather than across all of them. This allows us to
123 theoretically model a subcarrier's channel response as a wide
124 sense stationary (WSS) random process and then analyze the
125 relationship between the randomness of the key and the corre-
126 lation coefficient of the measurements. Our main contributions
127 are summarized as follows:

- 128 • We implement a time-variant multipath fading channel
129 with its CIR as modelled a *wide sense stationary uncorre-*
130 *lated scattering* (WSSUS) random process and show that
131 each subcarrier's channel response is also a WSS random
132 process. Thus, while each subcarrier's channel response
133 is sampled by the same time interval, the measurements
134 will have the same correlation relationship between each
135 other. We further explore this concept to show that when
136 all the channel taps are modelled by the same Doppler
137 power spectrum, the subcarriers' channel responses will
138 have the same autocorrelation function (ACF) as the
139 channel taps.
- 140 • We explore the relationship between the correlation co-

efficient of different sampled measurements and the ran- 141
domness of the key sequence generated from these mea- 142
surements. We extend the idea of the coherence time by 143
defining $X\%$ coherence time which is the time required 144
to make an $X\%$ correlation coefficient of the ACF of each 145
channel tap. We show that the commonly acknowledged 146
 50% coherence time between different samples does not 147
guarantee the randomness of the quantized key bits. 148

149 The rest of the paper is organized as follows. Section II
150 models both the channel taps and subcarriers' channel re-
151 sponses of the time-variant multipath channel as WSS ran-
152 dom processes. Section III defines the $X\%$ coherence time.
153 Section IV outlines the simulation model and presents the
154 performance of the model while Section V proposes the
155 subcarrier's channel response based key generation scheme
156 and the randomness test results of the key sequence. Section VI
157 concludes the paper.

158 II. SYSTEM MODEL

159 A. Channel model

160 The wireless multipath channel can be modelled as a
161 linear time-varying system with a complex low-pass equiv-
162 alent response $h(\tau, t)$ [15]. If there are L discrete multipath
163 components, the output of the channel consists of the sum of
164 L delayed and attenuated versions of the input. Thus we have

$$165 y(t) = \sum_{l=0}^{L-1} h(\tau_l, t)x(t - \tau_l), \quad (1)$$

166 where $h(\tau_l, t)$ and τ_l are the complex attenuation and the delay
167 of the l -th multipath at time t , $\tau_l = lT_s$ and T_s is the system's
168 sampling period.

169 The CIR $h(\tau, t)$ is written as

$$170 h(\tau, t) = \sum_{l=0}^{L-1} h(\tau_l, t)\delta(\tau - \tau_l). \quad (2)$$

171 According to the central limit theorem, $h(\tau_l, t)$ can be approx-
172 imated as zero-mean complex Gaussian random variables, so
173 $h(\tau_l, t) \sim \mathcal{CN}(0, \sigma_h^2(l))$.

174 In an OFDM system with B MHz channel spacing and M
175 evenly spaced subcarriers, the frequency of each subcarrier is
176 shown as

$$177 f_m = m\Delta f, \quad (3)$$

178 where m is the subcarrier index, $-\frac{M}{2} + 1 \leq m \leq \frac{M}{2}$ and Δf
179 is the frequency difference between two adjacent subcarriers,
180 $\Delta f = \frac{B}{M}$. For example, in an IEEE 802.11 OFDM system
181 [16] with 20 MHz channel spacing, there are 64 subcarriers in
182 total (only 52 subcarriers are used to transmit data, the others
183 are used as guard bands), thus $M = 64$, $B = 20$ MHz and
184 $\Delta f = \frac{B}{M} = 312.5$ kHz.

185 In an OFDM system, CFR $H(f, t)$ and CIR $h(\tau, t)$ are an
186 FFT pair. We obtain $H(f, t)$ by applying IFFT operation to
187

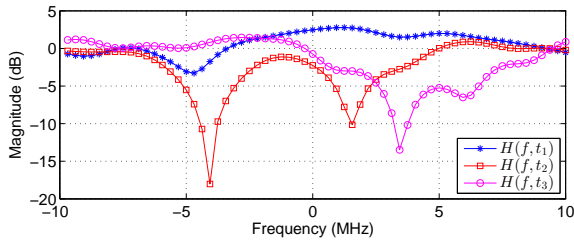


Fig. 1. Channel frequency response at different time

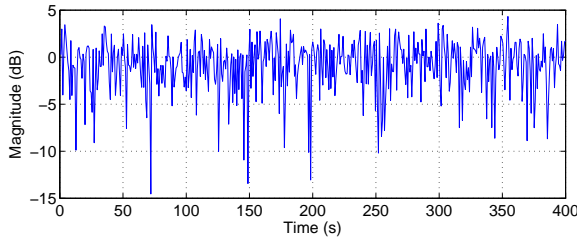


Fig. 2. $H(f_1, t)$, time variation of the 1-st subcarrier's channel response

184 $h(\tau, t)$

$$\begin{aligned} H(f_m, t) &= \sum_{l=0}^{L-1} h(\tau_l, t) \exp(-j2\pi f_m \tau_l / M) \\ &= \sum_{l=0}^{L-1} h(\tau_l, t) \exp(-j2\pi m \Delta l T_s / M). \end{aligned} \quad (4)$$

185 Because $h(\tau, t)$ varies with time, $H(f_m, t)$ is also time-
186 variant. A frequency selective fading channel's frequency
187 response at different time is shown in Fig. 1 and the 1-st
188 subcarrier's channel response over time $H(f_1, t)$ is shown in
189 Fig. 2. As each channel tap $h(\tau_l, t)$ is modeled as a complex
190 Gaussian process and $H(f_m, t)$ is a linear combination of
191 $h(\tau_l, t)$, $H(f_m, t)$ is also a complex Gaussian random process,
192 which can be used for key generation.

193 B. WSS model

194 1) *WSSUS modelling of the multipath channel*: The mod-
195 elling of a rich scattering multipath channel as WSSUS was
196 first proposed by Bello [17]. The time-varying nature of the
197 channel is modelled mathematically by treating $h(\tau, t)$ as a
198 WSS random process in t with an ACF [15]

$$R_h(\tau_i, \tau_j, \Delta t) = E [h(\tau_i, t) h^*(\tau_j, t + \Delta t)]. \quad (5)$$

199 In most multipath channels, the attenuation and phase shift
200 associated with different delays (i.e., paths) are assumed to be
201 uncorrelated. This *uncorrelated scattering* (US) assumptions
202 leads to

$$R_h(\tau_i, \tau_j, \Delta t) = R_h(\tau_i, \Delta t) \delta(\tau_i - \tau_j), \quad (6)$$

203 where $\delta(\cdot)$ is a Dirac delta function.

204 Equation (6) embodies both the WSS and US assumptions.
205 It is often referred to as the WSSUS model for fading. This

ACF is denoted by $R_h(\tau, \Delta t)$ and is given by 206

$$R_h(\tau, \Delta t) = E [h(\tau, t) h^*(\tau, t + \Delta t)]. \quad (7)$$

2) *WSS modelling of the subcarriers' channel responses*: 207

The channel response of m -th subcarrier is given in equation 208

(4). The mean value and ACF can be calculated as 209

$$\begin{aligned} E [H(f_m, t)] &= \sum_{l=0}^{L-1} E [h(\tau_l, t)] \exp(-j2\pi f_m \tau_l / M) \\ &= 0, \end{aligned} \quad (8)$$

and 210

$$\begin{aligned} R_H(f_m, t_1, t_2) &= E [H(f_m, t_1) H^*(f_m, t_2)] \\ &= \sum_{l=0}^{L-1} \sum_{i=0}^{L-1} E [h(\tau_l, t_1) h^*(\tau_i, t_2)] \exp(j2\pi f_m T_s (l - i) / M). \end{aligned} \quad (9)$$

As $h(\tau, t)$ is modelled as WSSUS, equation (9) can be 211
simplified to 212

$$R_H(f_m, \Delta t) = \sum_{l=0}^{L-1} E [h(\tau_l, t) h^*(\tau_l, t + \Delta t)]. \quad (10)$$

The mean value of $H(f_m, t)$ is a constant and its ACF only 213
depends on the time delay, thus channel response $H(f_m, t)$ is 214
a WSS random process. So when we sample $H(f_m, t)$ by the 215
same time interval, all the adjacent sampled points will have 216
the same correlation coefficient between each other. 217

218 III. COHERENCE TIME AND CORRELATION

219 Coherence time is a statistical measure of the time duration
220 over which the CIR is essentially invariant and quantifies the
221 similarity of the channel response [14]. It can be quantified
222 through channel's correlation relationship at different times
223 and usually is defined as the time over which the correlation
224 function is above 50%.

225 In a multipath channel, each channel tap can have a different
226 Doppler power spectrum. The power spectral density (PSD)
227 and the ACF of the fading process form an FFT pair. The
228 normalized ACF of the l -th tap can be given as:

$$R_h(\tau_l, \Delta t) = \frac{E [h(\tau_l, t) h^*(\tau_l, t + \Delta t)]}{E [|h(\tau_l, t)|^2]}. \quad (11)$$

229 The $X\%$ coherence time [18] is defined as that value of
230 $T_{c, X\%}(\tau_l)$ such that the correlation coefficient is $X\%$, i.e.,

$$R_h(\tau_l, T_{c, X\%}(\tau_l)) = \frac{X}{100}. \quad (12)$$

231 In some Doppler power spectrum models, e.g., Jakes model,
232 the ACF is not a monotonic function, so there will be several
233 Δt for some correlation coefficients. We use the first Δt which
234 sets the correlation coefficient $X\%$ as $T_{c, X\%}(\tau_l)$.

235 When all the channel taps are modelled as the same Doppler
236 power spectrum, then all the channel taps have the same ACF,
237 so we can get:

$$R_h(\tau_l, \Delta t) = R_h(\Delta t), \quad l = 0, 1, \dots, L - 1, \quad (13)$$

$$T_{c, X\%}(\tau_l) = T_{c, X\%}, \quad l = 0, 1, \dots, L - 1. \quad (14)$$

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

$$\begin{aligned}
 R_H(f_m, \Delta t) &= \frac{E[H(f_m, t)^* H(f_m, t + \Delta t)]}{E[|H(f_m, t)|^2]} \\
 &= \frac{\sum_{l=0}^{L-1} E[h(\tau_l, t)^* h(\tau_l, t + \Delta t)]}{\sum_{l=0}^{L-1} E[|h(\tau_l, t)|^2]} \\
 &= \frac{\sum_{l=0}^{L-1} E[R_h(\tau_l, \Delta t) |h(\tau_l, t)|^2]}{\sum_{l=0}^{L-1} E[|h(\tau_l, t)|^2]} \\
 &= \frac{R_h(\Delta t) \sum_{l=0}^{L-1} E[|h(\tau_l, t)|^2]}{\sum_{l=0}^{L-1} E[|h(\tau_l, t)|^2]} \\
 &= R_h(\Delta t). \tag{15}
 \end{aligned}$$

240 Thus the subcarrier's channel response has the same ACF as
 241 the channel taps and is independent of subcarrier index m . All
 242 the subcarriers' channel responses have the same ACF as

$$R_H(\Delta t) = R_h(\Delta t). \tag{16}$$

243 If we extend the concept of coherence time to the subcarrier's
 244 channel response, then when all the channel taps have the
 245 same Doppler power spectrum, all the subcarriers' channel
 246 responses have the same coherence time as the channel taps.

247 IV. SIMULATION MODEL IMPLEMENTATION AND 248 PERFORMANCE ANALYSIS

249 A. Simulation model

250 A transceiver model is implemented in Matlab based on
 251 IEEE 802.11 OFDM [16]. The channel is modelled as a
 252 time-variant multipath fading channel [19]. All the channel
 253 taps are modelled as independent complex Gaussian random
 254 variables whose average power follows the exponential power
 255 delay profile and a Bell-shaped Doppler power spectrum [20].
 256 The normalized Bell-shaped Doppler power spectrum can be
 257 expressed (in linear values, not dB values) as

$$S(f) = \frac{\sqrt{A}/(\pi f_d)}{1 + A(\frac{f}{f_d})^2}, \tag{17}$$

258 where A is a constant, in IEEE 802.11 channel, $A = 9$ and
 259 f_d is the Doppler spread, whose values were found to be
 260 up to approximately 6 Hz at 5.25 GHz center frequency and
 261 up to approximately 3 Hz at 2.4 GHz center frequency by
 262 experiments in indoor environment [20].

263 The ACF of the Bell-shaped Doppler spectrum is given as

$$R(\Delta t) = \exp\left(-\frac{2\pi f_d}{\sqrt{A}} \Delta t\right). \tag{18}$$

264 So the 50% coherence time can be calculated as

$$T_{c,50\%} = \frac{\sqrt{A}}{2\pi f_d} \ln 2. \tag{19}$$

265 The Doppler spread f_d is 6 Hz in the simulation. We use
 266 20 MHz channel spacing and 20 MHz sampling frequency for
 267 the IEEE 802.11 OFDM model. Every 0.8 ms Alice sends a
 268 probing signal to Bob who will record the CFR. Then Bob
 269 sends a probing signal to Alice who will record the CFR as

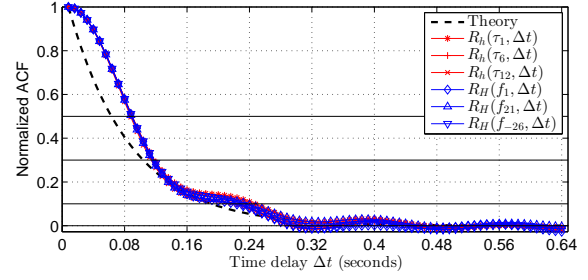


Fig. 3. ACF of selected channel taps and subcarriers, the Theory curve is calculated by (18)

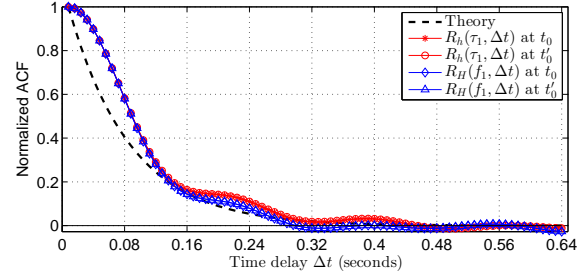


Fig. 4. WSS illustration, the Theory curve is calculated by (18)

270 well. We run the simulation for equivalently 400 s so there are
 271 500,000 measurements in total. The theoretical 50% coherence
 272 time calculated by (19) is 56 ms so the total simulation time
 273 is long enough to represent the channel variation.

274 B. ACF and WSS property of the simulation model

275 We calculate several channel taps and subcarriers' ACF and
 276 the results are shown in Fig. 3. All the channel taps have
 277 almost the same ACF, showing a high consistence of the
 278 simulation model. All the subcarriers have almost the same
 279 ACF as the channel taps because all the taps are modelled
 280 as the same Doppler power spectrum, which is also shown
 281 analytically in (15).

282 The WSS property of the simulation model is evaluated
 283 by comparing two ACFs observed at different times. In the
 284 example shown in Fig. 4, $t'_0 = t_0 + 10$ s, the ACF of
 285 channel taps and subcarriers does not vary with the observation
 286 time. The WSS property of the channel guarantees that the
 287 correlation relationship between different sampling data only
 288 depends on their sampling time difference. Thus we can make
 289 sure that all the adjacent data sampled by the same time
 290 interval will have the same correlation relationship between
 291 each other.

292 V. FREQUENCY RESPONSE BASED KEY GENERATION

293 A. Quantization

294 Quantization is the method to convert the measurements
 295 into key bits. Different schemes differ in the quantization
 296 level and threshold. Cumulative distribution function (CDF)
 297 based quantization is frequently used in key generation [7],
 298 [12]. The threshold is chosen according to the cdf of the
 299

TABLE I
RANDOMNESS TEST RESULTS OF $H(f_1, t)$ SAMPLED BY DIFFERENT $X\%$ COHERENCE TIME

Correlation coefficient $X\%$	50%	40%	30%	20%	15%	12%	10%	9%	7%
$T_{c,X\%}$ (s)	0.0832	0.096	0.1104	0.1328	0.1552	0.1992	0.2232	0.2312	0.2456
Sequence length	4760	4166	3622	3012	2576	2008	1792	1730	1628
Frequency	0.7942	0.8042	0.7904	0.9129	0.9372	0.8583	0.7768	0.7364	0.8043
Block frequency	0.0734	0.0142	0.5148	0.2217	0.3898	0.6528	0.9615	0.8183	0.8906
Runs	0	0	0	0	0.0014	0.7894	0.6379	0.1119	0.7275
Longest run of ones	0	0	0.0073	0.0061	0.1237	0.8042	0.5978	0.2257	0.7489
DFT	0.0034	0.1229	0.3254	0.0262	0.9136	0.5123	0.0564	0.6994	0.3281
Serial	0	0	0	0.0311	0.3526	0.6656	0.0584	0.9481	0.256
	0	0.6715	0.1282	0.3259	0.8062	0.9309	0.32	0.9778	0.4512
Approximate entropy	0	0	0	0.0024	0.0484	0.2643	0.0296	0.2217	0.0131
Cumulative Sums(fwd)	0.9387	0.7382	0.802	0.9029	0.8424	0.8117	0.7024	0.8618	0.7297
Cumulative Sums(fwd)	0.7237	0.5147	0.9108	0.9662	0.9049	0.6458	0.9386	0.8994	0.5073

measurements, which can be made to guarantee the proportion of 0s and 1s are equally the same, a very important feature for a random sequence. In addition, it is very flexible as it can be used as either single-bit or multi-bit quantization. In our system, single-bit cdf based quantization is adopted to quantize Alice and Bob's m -th subcarrier's channel response $H(f_m, t)$ into key bits, which is detailed in Algorithm 1; K is the quantization level.

Algorithm 1 CDF based quantization algorithm

- 1: $F(x) = P(H(f_m, t) < x)$
- 2: $\eta_k = F^{-1}(\frac{k}{2^K}), k = 1, 2, \dots, 2^K - 1$
- 3: $\eta_0 = -\infty$
- 4: $\eta_{2^K} = \infty$
- 5: Construct Gray code b_k and assign them to different intervals $[\eta_{k-1}, \eta_k]$
- 6: $key(n, K) = b_k$, if $\eta_{k-1} \leq H(f_m, t_n) < \eta_k$

B. Information reconciliation and privacy amplification

There can be mismatch between the key generated in Alice and Bob due to the noise, hardware difference etc. Information reconciliation is used to correct the key discrepancy, either using error correcting codes or some interactive information reconciliation protocols [3]. In our scheme, secure sketch [21] is employed to make Alice and Bob agree on the same key.

Some information is publicly transmitted between Alice and Bob in the information reconciliation stage, which can also be heard by Eve. So privacy amplification using universal hash function is employed to remove the revealed information.

C. Randomness test

We use a statistical test suite provided by National Institute of Standards and Technology (NIST) [22] to evaluate the randomness of the key bit generated from the subcarrier's channel response, which is commonly employed in key generation [2], [3], [10], [12], [23].

There are 15 tests in total. The null hypothesis under test is that the sequence being tested is random. All the tests return a P -value which summarizes the strength of the evidence against the null hypothesis. When the P -value is larger than the chosen

significance level (α), the sequence is accepted as random. Typically, α is chosen in the range [0.001, 0.01]. In this paper, α is chosen as 0.01. Some tests require an extremely long sequence, e.g., several tests recommend the input sequence length larger than 10^6 , which is currently not available in the simulation, thus we run 8 tests, half of all the 15 tests, which still satisfies NIST's requirements [22].

We calculate each subcarrier's $X\%$ coherence time, $T_{c,X\%}$, through its ACF, and then sample the $H(f_m, t)$ every $T_{c,X\%}$ time over the entire 400 s simulation time. We generate a relatively long sequence in order to draw a more reliable conclusion on the randomness of the key sequence. We test all the sampled sequences with NIST's statistical test suite and compare their results; an example is shown in Table I. All the cells highlighted in grey are those failing the test (P -value < 0.01).

The poor performance on the "runs" test concurs with intuition. A run is an uninterrupted sequence of identical bits and the focus of the "runs" test is the total number of runs in the sequence. When the sample time is small, the channel is highly correlated, as the subcarrier's channel response has a high possibility that the next sample's amplitude has the same sign; thus it is quantized into the same bits whenever single-bit quantization is used, which results in less runs.

In previous work, any two channels that are separated by the coherence time is considered as uncorrelated [14] and usually 50% coherence time is used. However, it may be observed from the randomness test results, that it actually requires a correlation coefficient smaller than 50% between different samples in order to make the quantized key bits pass the NIST statistical randomness test.

D. Discussion

We have proposed a key generation scheme based on a particular subcarrier's frequency response over time. Channel frequency response is a good representation of the channel. We can simultaneously extract the key from several subcarriers' channel responses. Each generated key sequence can be concatenated to form a longer sequence or used independently for different applications. Key generation based on subcarrier's channel response has several advantages. Compared with RSS

299
300
301
302
303
304
305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328
329
330
331
332
333
334

335
336
337
338
339
340
341
342
343

344
345
346
347
348
349
350
351

352
353
354
355
356
357
358

359

360

361

362

363

364

365

366

367

based key generation, there are more than one subcarrier's channel response available for extraction, which offers a potential to achieve much higher KGR. Compared with phase based key generation, channel estimation in OFDM system is quite mature and so the subcarrier's channel response is easier to obtain than phase information, and with a higher accuracy. Thus compared to RSS and phase based schemes, subcarriers' channel responses based key generation is more applicable to practical application in cryptography.

VI. CONCLUSION

In this paper, we propose a key generation scheme that extracts keys from the subcarriers' channel responses. To the best of the authors' knowledge, this is the first paper that tests the randomness of the key sequences generated from measurements sampled by different $X\%$ coherence time. Current research that uses RSS and CSI for key generation proposes using a figure of 50% coherence time as the time to sample the channel. However, we find that using 50% coherence time cannot guarantee the randomness of the key sequence. We have modelled both the channel taps and subcarriers' channel response as WSS random processes and find they have the same ACF when all the channel taps have the same Doppler power spectrum. We sample a particular subcarrier's channel response $H(f_m, t)$ by $X\%$ coherence time and quantize the sampled measurements into key bits, whose randomness is tested by NIST's randomness statistical test suite. Coherence time estimation of an indoor environment, and implementation of our scheme based on WARP system will be the focus of our future work.

REFERENCES

- [1] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Commun. Mag.*, vol. 18, no. 4, pp. 6–12, 2011.
- [2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telemetry: extracting a secret key from an unauthenticated wireless channel," in *Proc. of the 14th Annual International Conference on Mobile Computing and Networking*, San Francisco, USA, Sep. 2008, pp. 128–139.
- [3] 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. of the 15th Annual International Conference on Mobile Computing and Networking*, Beijing, China, Sep. 2009, pp. 321–332.
- [4] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. of the 29th IEEE International Conference on Computer Communications (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–9.
- [5] 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, 2013.
- [6] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. of the 31st IEEE International Conference on Computer Communications (INFOCOM)*, Orlando, Florida USA, Mar. 2012, pp. 927–935.
- [7] 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, 2010.
- [8] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207–212, 1996.
- [9] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. of the 30th IEEE International Conference on Computer Communications (INFOCOM)*, Shanghai, China, Apr. 2011, pp. 1422–1430.
- [10] 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, 2012.
- [11] Y. Liu, S. C. Draper, and A. 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.
- [12] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. of the 32nd IEEE International Conference on Computer Communications (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 3048–3056.
- [13] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, 2010.
- [14] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice Hall, 2001.
- [15] M. C. Jeruchim, P. Balaban, and K. S. Shanmugan, *Simulation of Communication Systems: Modeling, Methodology and Techniques*, 2nd ed. Kluwer Academic/Plenum Publishers, 2000.
- [16] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 2012.
- [17] P. Bello, "Characterization of randomly time-variant linear channels," *IEEE Transactions on Communications Systems*, vol. 11, no. 4, pp. 360–393, 1963.
- [18] H. Jung, T. Kwon, K. Cho, and Y. Choi, "REACT: Rate adaptation using coherence time in 802.11 WLANs," *Computer Communications*, vol. 34, no. 11, pp. 1316–1327, 2011.
- [19] C.-D. Iskander, "A matlab-based object-oriented approach to multipath fading channel simulation," Mathworks, Natick, MA, White Paper 18869, Feb. 2008.
- [20] V. Erceg *et al.*, "TGn channel models," IEEE TGn 802.11, Tech. Rep. 03/940r4, May 2004.
- [21] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. 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.
- [22] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, Tech. Rep. Special Publication 800-22 Revision 1a, Apr. 2010.
- [23] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, 2013.