IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY IN WIRELESS COMMUNICATIONS AND NETWORKING

Received August 1, 2016, accepted August 11, 2016, date of publication August 31, 2016, date of current version September 16, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2604618

Experimental Study on Key Generation for Physical Layer Security in Wireless Communications

JUNQING ZHANG[1], ROGER WOODS[1], (Senior Member, IEEE), TRUNG Q. DUONG[1], (Senior Member, IEEE), ALAN MARSHALL[2], (Senior Member, IEEE), YUAN DING[1], YI HUANG[2], (Senior Member, IEEE), AND QIAN XU[2]

[1]Institute of Electronics, Communications and Information Technology, Queen's University Belfast, Belfast, BT3 9DT, U.K.
[2]Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, U.K.

Corresponding author: J. Zhang (jzhang20@qub.ac.uk)

This work was supported in part by the Queen's University Belfast University Studentship, Newton Institutional Links under Grant 172719890, in part by the Royal Academy of Engineering Research Fellowship under Grant RF1415/14/22, and in part by the U.S. Ireland R&D Partnership USI033 WiPhyLoc8 grant involving Rice University (USA), University College Dublin (Ireland), and Queen's University Belfast (Northern Ireland).

ABSTRACT This paper presents a thorough experimental study on key generation principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation, through a testbed constructed by using wireless open-access research platform. It is the first comprehensive study through: 1) carrying out a number of experiments in different multipath environments, including an anechoic chamber, a reverberation chamber, and an indoor office environment, which represents little, rich, and moderate multipath, respectively; 2) considering static, object moving, and mobile scenarios in these environments, which represents different levels of channel dynamicity; and 3) studying two most popular channel parameters, i.e., channel state information and received signal strength. Through results collected from over a hundred tests, this paper offers insights to the design of a secure and efficient key generation system. We show that multipath is essential and beneficial to key generation as it increases the channel randomness. We also find that the movement of users/objects can help introduce temporal variation/randomness and help users reach an agreement on the keys. This paper complements existing research by experiments constructed by a new hardware platform.

INDEX TERMS Physical layer security, key generation, wireless communications.

I. INTRODUCTION

Key generation exploiting unpredictable characteristics of wireless channels is information-theoretically secure [1], [2] and has been an active research direction in physical layer security (PLS) [3], [4]. In this technique, two legitimate users, Alice and Bob, measure their common but noisy channel in an alternate manner, through which they can get correlated but not identical observations. Then they will quantize their correlated analog measurements into binary values separately, and their keys are usually not the same. Alice and Bob later reach an agreement on the same key through information reconciliation [5]. Finally, they employ privacy amplification to remove the information revealed during the information reconciliation [6]. Therefore, key generation is able to establish a cryptographic key securely from the noisy observations.

As one of the few implementable PLS techniques, key generation can be constructed in current wireless devices. Many prototypes have been reported involving key extraction from channel state information (CSI) in IEEE 802.11n systems [7], [8], ultra wideband (UWB) systems [9]–[12], and FM/TV systems [13], or from received signal strength (RSS) in IEEE 802.11 systems [14]–[17], IEEE 802.15.4 systems [18]–[23], and Bluetooth systems [24]. The testbeds consist of laptops, smartphones, customized platforms such as universal software radio peripheral (USRP) [25], or any other wireless platform that can provide sufficient channel information.

Key generation requires the channel to satisfy certain conditions with respect to temporal variation, channel reciprocity, and spatial decorrelation. Temporal variation is the

main random source for key generation, which can be introduced by the movement of any users and/or objects in the wireless environment. It is feasible to exploit channel randomness in the frequency domain [7], [8], [18], [22], [26] and spatial domain [27], [28], but the randomness is limited and cannot be updated in a static environment. Experiments have been carried out in the indoor and outdoor environments and have shown that the mobility of users and/or objects is sufficient to introduce randomness [15], [20], [21].

Channel reciprocity indicates that the signals at each end of the same link have identical statistical features, such as channel gains, phase shift, time delay, etc, which is the basis of key generation systems. Although there is ongoing research effort adopting full-duplex hardware [29]–[31], most of the current commercial wireless devices work in half-duplex mode. Key generation usually works in time-division duplexing (TDD) systems and slow fading channels. Therefore, the received signals are generally asymmetric due to the non-simultaneous measurements and independent noise in different hardware devices, whose effects have been studied theoretically in [26] and experimentally in [32]. Non-simultaneous measurements can be compensated by interpolation to emulate the channel being measured at the same time [19], [21] while noise effect can be suppressed by low pass filtering [26], [33].

The conclusion from applying spatial decorrelation means that any eavesdropper located more than half-wavelength away from legitimate users experiences uncorrelated fading. This property is highly influenced by the channel condition [34]. In a rich multipath environment with uniform scattering, according to the Jakes model, when the number of scatters grows to infinity, the correlation function is the Bessel function of zeroth order and the signal decorrelates when $d = 0.4\lambda$ (approximately half-wavelength) [35], which is the theoretic basis of spatial decorrelation. Some experiments have been carried out to verify this property in UWB systems [10]–[12] and IEEE 802.11g systems [36]. In contrast, spatial decorrelation has also been found to not hold in some channel conditions by simulation [37], [38] and experiments [38]–[40]. In this case, key generation cannot be deemed secure and requires special design consideration to combat eavesdropping when eavesdroppers are close to the legitimate users.

In order to design an effective, workable, and secure key generation system, the above three principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation, should be always satisfied. Although there have been a number of theoretical and experimental studies on these principles, to the best of the authors' knowledge, there is no thorough study examining the effects of environment conditions and channel parameters on the key generation. For example, [10], [11], and [36] studied channel reciprocity and spatial decorrelation in indoor environment by keys generated from channel impulse response (CIR) in a UWB system and from RSS in an IEEE 802.11g system, respectively. However, key generation performance greatly depends on the channel conditions, such as the multipath level and dynamicity, which has not been studied comprehensively yet. In addition, the channel parameter used for key generation also has an impact. For example, it has been reported that RSS-based key generation systems are subject to predictable channel attacks [13], [15] while CSI-based systems are robust to such attacks [7], [13].

In this paper, we study key generation principles comprehensively through experiments with different channel conditions. We implement a testbed using a customized FPGA-based wireless platform known as wireless open-access research platform (WARP) [41], which supports IEEE 802.11 orthogonal frequency-division multiplexing (OFDM) physical (PHY) layer and distributed coordination function (DCF) MAC layer protocols. This platform allows us to have full access to the transmission parameters, which are not available in the commercial network interface cards (NICs). A key objective here is to make minimal or even no change to the off-the-shelf wireless protocol, which requires cross-layer design and presents new research challenges. Our contributions are as follows.

- We carry out much more comprehensive experiments than previous research in environments with various multipath and dynamic levels. In particular, we conduct over a hundred tests in an anechoic chamber, a reverberation chamber, and an indoor office environment, which represents little, rich, and moderate multipath, respectively. We consider different dynamic channels, i.e., static, object moving, and mobile scenarios, in these environments. Both CSI and RSS are collected from the testbed and studied with the aim of assessing suitability for key generation when a certain channel conditions satisfy.
- Through the comprehensive experimental results, we are able to offer insights and advices for the design of suitable key generation schemes in different environments and scenarios. We found that in a dynamic environment, (i) the randomness introduced by temporal variation is sufficient for key generation; and (ii) cross-correlation of the channel measurements is high enough to make Alice and Bob reach an agreement, while in a static scenario these properties do not hold and key generation fails. We also conclude that multipath can improve the security performance of key generation. In a multipath environment, spatial decorrelation property holds and eavesdroppers can only get very limited information, while in an environment with little multipath such as an anechoic chamber, eavesdroppers can obtain a highly correlated channel and key generation cannot be deemed secure.
- We complement existing theoretical analysis and practical research by providing results on a new testbed constructed by WARP and much more experiments in different environments.

We have studied temporal variation and channel reciprocity in CSI-based systems through experiments in an indoor office environment [42]. This paper considerably extends and complements our previous work by providing a much more

thorough study through undertaking more detailed experimental work in an anechoic chamber, a reverberation chamber, and an indoor office environment, and performing analysis for both CSI and RSS.

The rest of the paper is organized as follows. Section II introduces CSI, RSS, and related IEEE 802.11 PHY and MAC layer protocols. Section III designs the testbed and presents the test environments and scenarios. Section IV studies the key generation principles. Finally, Section V concludes the paper.

II. PRELIMINARY

In this section, we introduce signal models of CSI and RSS, and the related IEEE 802.11 PHY and MAC layer protocols, which are important background for the entire paper.

A. SIGNAL MODEL

The received signal in time domain can be given as

$$y(t) = h(\tau, t) * x(t - \epsilon) + n(t), \tag{1}$$

where $x(t)$ and $y(t)$ are data input and output, respectively, $h(\tau, t)$ is the CIR, $*$ denotes convolution, ϵ is the time offset in the receiver due to imperfect time synchronization, and $n(t)$ is the hardware noise.

RSS is currently the most popular parameter for key generation as it is available in various wireless standards. RSS is usually reported as the average received signal power, which can be calculated by averaging the received power over a certain samples and written as

$$P(t) = \frac{1}{\Delta T} \int_{t}^{t+\Delta T} |y(t')|^2 dt', \tag{2}$$

where ΔT is the time duration of the samples. For example, one possible method to calculate RSS specified in the Section 8.3.9.2 of the IEEE 802.16 standard [43] is

$$RSS = 10^{-\frac{G_{rf}}{10}} \frac{1.2567 \times 10^4 V_c^2}{(2^{2B})R} \left(\frac{1}{N} \sum_{n=0}^{N-1} |y_{I\ or\ Q}[n]|\right)^2, \tag{3}$$

where B, R and V_c are the ADC precision, input resistance and input clip level, respectively, G_{rf} is the analog gain from antenna connector to ADC input, $y_{I\ or\ Q}[n]$ is the n^{th} sample of the I or Q branch of the signal, and N is the number of samples. The chip CC2520 [44], a popular transceiver for wireless sensor networks (WSNs), calculates RSS by averaging the received power over 8 symbol periods (128 μs), whereas the chip MAX2829 [45], an IEEE 802.11a/b/g transceiver, reports RSS in voltage, although it is mapped from the power. Different interpretations inhibit the theoretical modelling of RSS and present challenges when heterogeneous devices are used [15], [17], [46].

The received signal in frequency domain can be obtained by applying inverse fast Fourier transform (IFFT) to the time domain signal. This is given as

$$\begin{aligned} Y(f, t) &= H(f, t)X(f, t)e^{-j2\pi f\epsilon} + W(f, t) \\ &= \widetilde{H}(f, t)X(f, t) + W(f, t), \end{aligned} \tag{4}$$

where

$$H(f, t) = \int_0^{\tau_{\max}} h(\tau, t)e^{-j2\pi f\tau} d\tau, \tag{5}$$

$$\widetilde{H}(f, t) = H(f, t)e^{-j2\pi f\epsilon}. \tag{6}$$

Here $\tau_{\max}$ is the maximum delay of the CIR. The channel frequency responses (CFRs) can be estimated by

$$\begin{aligned} \widehat{H}(f, t) &= \frac{Y(f, t)}{X(f, t)} \\ &= \widetilde{H}(f, t) + \widehat{w}(f, t). \end{aligned} \tag{7}$$

The CSI mainly includes CIR and CFR, which are related to each other as shown in (5). CIR can be obtained in UWB systems [9]–[12], and their testbeds are usually constructed by oscilloscope, waveform generator, etc. CFR can be estimated in OFDM, which is a popular technique used in IEEE802.11a/g/n. CFR is not publicly available in most of the commercial NICs, but can be obtained in the Intel WiFi Link 5300 NIC [47] or customized hardware platforms, such as WARP or USRP.

A summary of RSS-based and CSI-based key generation systems is given in Table 1.

TABLE 1. Summary of RSS-based and CSI-based key generation systems.

Parameter	Testbed	Representative Work
RSS	IEEE 802.11: Laptop	[14]–[17]
	IEEE 802.15.4: MICAz, TelosB	[18]–[23]
	Bluetooth: Smartphone	[24]
CSI	WiFi Link 5300 NIC-based laptop	[7], [8]
	Customized platforms, USRP and WARP	[13], [32], [42]
	UWB systems constructed by oscilloscope and waveform generator	[9]–[12]

B. IEEE 802.11 PROTOCOL

1) OFDM PHY

The IEEE 802.11a/g/n standards [48] adopt OFDM for signal modulation. The physical layer packet of IEEE 802.11 OFDM consists of a preamble, a SIGNAL field, and a DATA field, as shown in Fig. 1. The preamble is used for automatic gain control (AGC), synchronization and channel estimation, and is equivalent to 4 OFDM symbols in length. The SIGNAL field carries the information of convolutional coding rate R and the mapping scheme for the DATA field, forming a

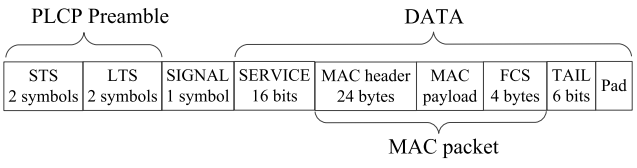


FIGURE 1. Structure of IEEE 802.11 OFDM physical layer packet. Cyclic prefix (CP) is not shown for simplicity. The length of the blocks in the figure is not scaled.

complete OFDM symbol. The number of OFDM symbols of the entire physical layer packet can be calculated as

$$N_{\text{OFDM}} = 4 + 1 + \lceil \frac{8l_{\text{MAC}} + 16 + 6}{N_{subc} N_{bpsc} R} \rceil, \tag{8}$$

where

$$l_{\text{MAC}} = 24 + 4 + l_{\text{payload}} \tag{9}$$

is the number of bytes of the MAC packet, l_{payload} is the number of bytes of the MAC payload, N_{subc} is the number of data subcarriers, 48 in IEEE 802.11 standard, and N_{bpsc} is the number of bits per subcarrier which is determined by the mapping scheme.

In IEEE 802.11 OFDM systems, least square channel estimation is widely used to estimate the channel with the aid of long training symbols (LTSs), which is composed of M (=52) subcarriers. The estimated channel response can be given as

$$\widehat{H}_{uv}(f_m, t) = \widetilde{H}_{uv}(f_m, t) + \widehat{w}_v(f_m, t), \tag{10}$$

where f_m is the m^{th} subcarrier's carrier frequency, u denotes the transmitter (Tx) and v denotes the receiver (Rx).

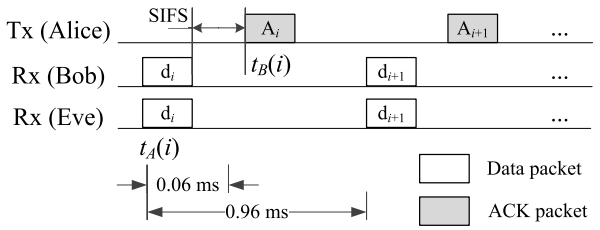


FIGURE 2. Timing between data packets received by the Rx and ACK packets received by Tx. The packet length and time intervals are not scaled.

2) DCF MAC

In IEEE 802.11, the DCF is used to coordinate access to the wireless medium, which is the basis of the standard carrier sense multiple access/collision avoidance (CSMA/CA) access mechanism. In order to ensure reliable reception of the unicast frame, a positive acknowledgement (ACK) frame is transmitted from Rx to Tx after waiting a short interframe space (SIFS) when Rx successfully receives a data packet from Tx, as illustrated in Fig. 2. The time difference between the data packets and the corresponding ACK packets can be calculated by

$$\begin{aligned} \Delta t_{AB} &= t_{\text{data}} + t_{\text{SIFS}} \\ &= N_{\text{OFDM}} \times T_{\text{OFDM}} + t_{\text{SIFS}} \\ &= (5 + \lceil \frac{8l_{\text{MAC}} + 16 + 6}{N^d_{subc} N_{bpsc} R} \rceil) \times \frac{80}{BW} + t_{\text{SIFS}}, \end{aligned} \tag{11}$$

where t_{SIFS} is the time duration of the SIFS and equals to 16 μs in a 20 MHz channel spacing IEEE 802.11 OFDM system, and T_{OFDM} is the time duration for each OFDM symbol which can be calculated as the time for each data symbol ($\frac{1}{BW}$) multiplying total number of data symbols in one OFDM symbol (80 including CP).

When an IEEE 802.11 network is configured as an infrastructure basic service set (BSS), the network is handled by an access point (AP) that broadcasts Beacon frames to all the users, i.e., mobile stations (STAs), in its communication range, typically every 100 ms. The Beacon carries information about the BSS parameters, e.g., timestamp, service set identity (SSID), Beacon interval, etc. STAs can use this information to identify the network and keep synchronized with the AP.

III. TESTBED DESIGN AND TEST ENVIRONMENTS

A. TESTBED AND EXPERIMENTAL DESIGN

The testbed is constructed by using WARP hardware, which is a scalable and extensible programmable wireless platform and allows fast prototype of physical layer algorithms [41]. Due to the limited number of WARP boards, there were eight users in each experiment, with one Alice, one Bob and six eavesdroppers, but this still represents a viable experimental setup. We used the channel measurements of Alice and Bob from one experiment to study temporal variation and channel reciprocity, as presented in Section IV-A and IV-C, respectively. In order to study spatial decorrelation, two placement configurations were used in order to test the effect of the location of eavesdroppers, as shown in Fig. 3. Without loss

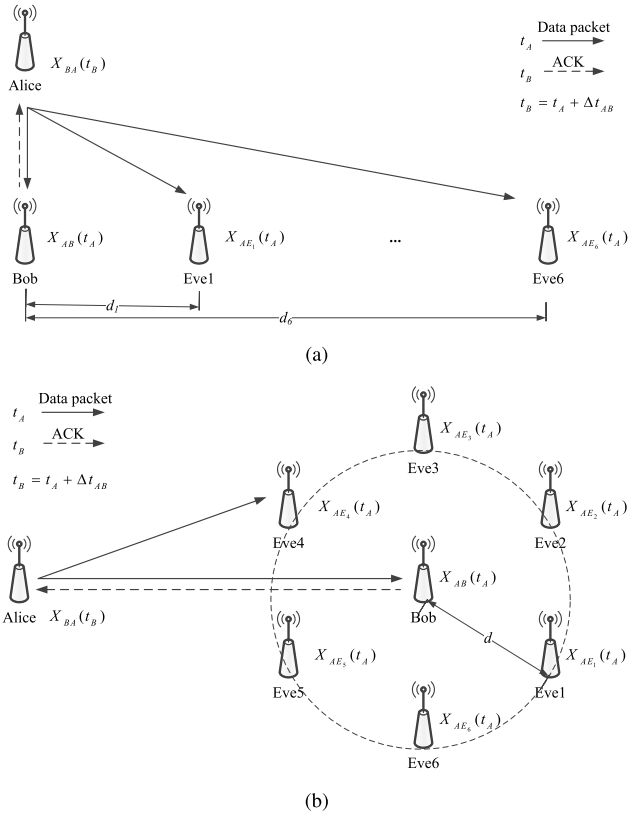


FIGURE 3. User placement. (a) Linear placement. (b) Circular placement.

of generality, eavesdroppers were monitoring Bob. Several experiments were carried out by changing eavesdroppers' distances to Bob and all the results with different distance configurations were put together, as shown in Section IV-D.

An IEEE 802.11 reference design has been developed for WARP v3 hardware, which is a real-time FPGA implementation of the IEEE 802.11 OFDM PHY and DCF MAC. A Python experiment framework has also been developed to (i) control the behavior of the PHY and MAC without interfering with the real-time operation of the wireless interfaces, and (ii) log the transmission parameters, such as timestamp t, received signal power $P_{uv}(t)$, and channel estimation $\widehat{H}_{uv}(f, t)$, etc. The WARP and PC are connected by a 1 Gbps Ethernet switch so that the logged data can be transferred to the PC for further processing. In this paper, the channel measurements $X_{uv}(t)$ consist of $|\widehat{H}_{uv}(f, t_u)|$ and $P_{uv}(t_u)$. The time offset, ϵ, adds rotation to the phase of $\widehat{H}(f, t)$ but does not affect the amplitude. Therefore, the amplitude of frequency response, i.e., $|\widehat{H}(f, t)|$, is used.

All the users were running WARP 802.11 reference design. They operated at a carrier frequency of 2.412 GHz so the wavelength is $\lambda = 12.44$ cm. Alice and Bob were the legitimate users wishing to establish a secure key between them. They were configured as AP and STA, respectively, and formed an infrastructure BSS. Eavesdroppers were not associated to Alice but could overhear and record all the transmissions in the network. They also did not attempt to initiate active attacks such as disrupting the transmissions by jamming, i.e. only passive eavesdropping is considered.

The key advantage of the experimental setup was to make no change to the off-the-shelf wireless standard, so the results can be readily transferred to available commercial wireless systems. Data and ACK packets were used for channel measurement. As shown in Fig. 2, Alice sent data packets to Bob every 0.96 ms,[1] which allowed Bob to get a set of channel measurements $X_{AB}(t_A)$. Bob was associated to Alice, so he transmitted ACK packets to Alice upon successful reception of data packets. The ACK packet is also modulated by OFDM so Alice can get a set of channel measurements $X_{BA}(t_B)$. Although eavesdroppers were not associated to the AP, they were able to receive all the transmissions and record $X_{AE_j}(t_A)$. Bob and eavesdroppers can regularly update their timing through the timestamp received in the Beacon frames, broadcast by Alice every 100 ms. As there is no sender address in the ACK packets, they can only be distinguished by their temporal location compared to the timestamp of the corresponding data packets. Keeping users synchronized is thus essential to pair their channel measurements.

In order to ensure a high cross-correlation between the measurements of Alice and Bob, Δt_{AB} should be kept as small as possible. The minimum length of MAC payload, l_{payload}, required by the WARP 802.11 reference design is 20 bytes, therefore the length of the MAC packets, l_{MAC}, calculated by (9), was configured to be 48 bytes in order to keep the duration of the packet as small as possible. In this paper the WARP boards were running at a rate of 18 Mbps, i.e., $R = 3/4$ and $N_{bpsc} = 2$. In this case, according to (11), $\Delta t_{AB} = 0.06$ ms. This time difference is small enough to ensure the environments experienced by the data packets and the corresponding ACK packets are almost the same. In a slow fading environment, this only contributes a very small displacement. For example, when Alice is moving at a speed of 1 m/s, the distance she moves in this time interval is only 0.006 cm.

[1]The WARP 802.11 reference design requires a transmission resolution of 0.064 ms and $0.96 = 0.064 \times 15$. As a sampling period of 0.96 ms was deemed fast enough to track the signal variation in slow fading channels in this paper, a multiple of 15 was deemed suitable.

B. TEST ENVIRONMENTS AND SCENARIOS

In this paper, we test the key generation performance in different multipath environments. Over a hundred tests were carried out in an anechoic chamber, a reverberation chamber, and an office environment with different scenarios. Anechoic chamber and reverberation chamber represent two extreme environments whose special properties can help provide a better understanding of the key generation applications in various channel conditions.

1) ANECHOIC CHAMBER

Measurements were conducted in an anechoic chamber located in the ECIT research center, Queen's University Belfast to study the key generation principles in a free space environment where there is little multipath but always with a strong and dominant line-of-sight (LoS) path. A setup photo with eavesdroppers placed linearly is shown in Fig. 4(a).

2) REVERBERATION CHAMBER

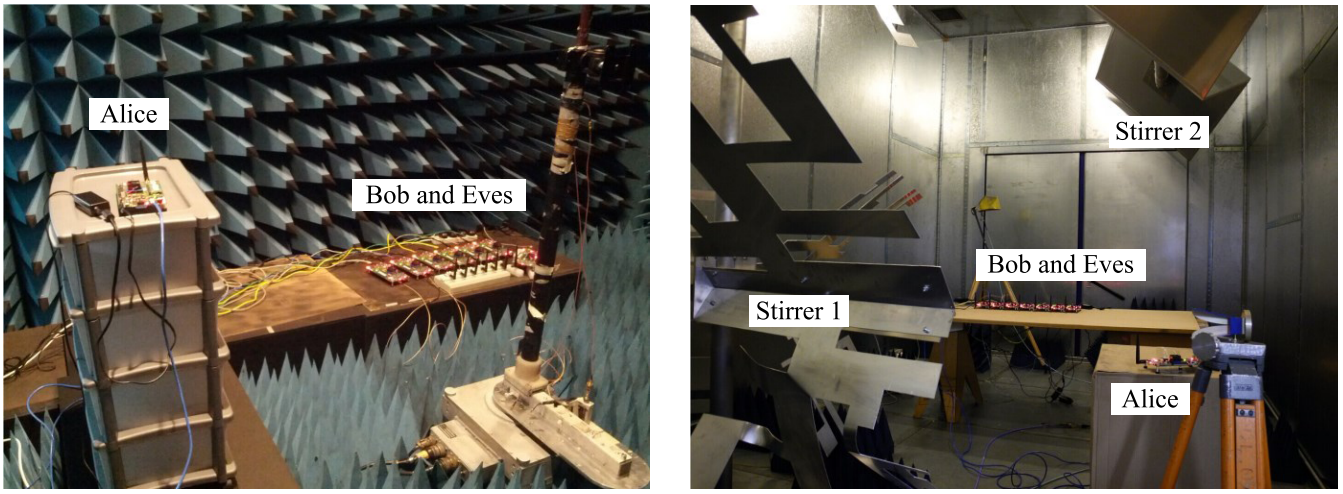
Experiments were done in a reverberation chamber located in the University of Liverpool where a rich multipath environment was created. A setup photo with eavesdroppers placed linearly is shown in Fig.4(b).

3) OFFICE ENVIRONMENT

The experiments were also carried out in an office environment in the ECIT research center, Queen's University Belfast, which is a typical indoor environment with cupboards, chairs, desks, etc.

We considered different scenarios to study the key generation performance under various levels of channel dynamicity. We tested three scenarios for the experiments in the anechoic chamber and office environment.

- *Static*: All the users were stationary with no movement in the room.
- *Object Moving*: All the users were stationary with an object, a person, moving at the speed of about 1 m/s in the room.
- *Mobile*: Bob and eavesdroppers were stationary while Alice was put on a trolley and moved by a person at the speed of about 1 m/s.



(a) (b)

FIGURE 4. Experiment setup. (a) Photograph of experiment setup in the anechoic chamber located in the ECIT research center, Queen's University Belfast. (b) Photograph of experiment setup in the reverberation chamber located in the University of Liverpool.

In the reverberation room, we rotated two stirrers continuously at 5 degrees per second in order to create a dynamic environment.

IV. STUDY OF KEY GENERATION PRINCIPLES

In these experiments, the key generation principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation, were studied. We also evaluated the randomness of the key sequence quantized from the measurements. Unless otherwise specified, measurements were taken for 60 s, which is much larger than the coherence time of the channel (in the order of 10 ms) and long enough to represent the channel variation.

The channel measurements, i.e., CSI and RSS, were then quantized into binary values using single-bit cumulative distribution function (CDF)-based quantizer [19], which is given in Algorithm 1.

Algorithm 1 CDF-Based Quantization Algorithm

INPUT: $X_{uv}(t)$ % Analog channel measurement
OUTPUT: K_{uv}^X % Quantized key bits

$F(x) = \Pr(X_{uv}(t) < x)$
$\eta_0 = -\infty$
$\eta_1 = F^{-1}(0.5)$
$\eta_2 = \infty$
for $j \leftarrow 1$ *to* N **do**
  if $X_{uv}(t_j) < \eta_1$ **then**
    $K_{uv}^X(j) = 0$
  else
    $K_{uv}^X(j) = 1$
  end if
end for

Temporal variation can be quantified by the temporal autocorrelation function (ACF). In a *wide sense stationary* (WSS) random process, the ACF is irrelevant of the observation time t but only determined by the time difference Δt, which is defined as

$$R_{X_{uv}}(\Delta t) = \frac{E\{(X_{uv}(t) - \mu_{X_{uv}})(X_{uv}(t+\Delta t) - \mu_{X_{uv}})\}}{E\{|X_{uv}(t) - \mu_{X_{uv}}|^2\}}, \tag{12}$$

where $E\{\cdot\}$ denotes the expectation calculation and $\mu_{X_{uv}}$ is the mean value of $X_{uv}(t)$.

Signal similarity is quantified using the Pearson correlation coefficient, expressed as

$$\rho_{uv,u'v'}^X = \frac{E\{X_{uv}X_{u'v'}\} - E\{X_{uv}\}E\{X_{u'v'}\}}{\sigma_{X_{uv}}\sigma_{X_{u'v'}}}, \tag{13}$$

where $\sigma_{X_{uv}}$ is the standard deviation of $X_{uv}(t)$. The correlation coefficient is used in the analysis of channel reciprocity and spatial decorrelation.

Since the channel measurements of users are not identical due to non-simultaneous measurements and noise, there are key mismatches between users after quantization. The key disagreement rate (KDR) can be defined as

$$KDR_{uv,u'v'}^X = \frac{\sum_{j=1}^{N_k} |K_{uv}^X(j) - K_{u'v'}^X(j)|}{N_k}, \tag{14}$$

where K_{uv}^X and $K_{u'v'}^X$ are the keys quantized from $X_{uv}(t)$ and $X_{u'v'}(t)$, respectively, and N_k is the length of keys. KDR is an essential parameter for key generation and determined by the cross-correlation and quantization scheme [36]. Therefore, KDR is also used to evaluate channel reciprocity and spatial decorrelation.

A. TEMPORAL VARIATION

Temporal variation is commonly adopted as random sources for key generation since it can be readily introduced by the

movement of the users and/or objects in the wireless environments. A wireless channel can be modelled as a *wide sense stationary uncorrelated scattering* (WSSUS) random process in a rich scattering multipath environment [49]. Under this assumption, it has been analyzed through simulation in [26] that OFDM subcarrier's channel response $\widehat{H}_{uv}(f_m, t)$ is a WSS random process.

In this section, temporal ACFs of CSI and RSS were calculated from the experimental results in the anechoic chamber, the reverberation chamber, and the office environment. $R_{\widehat{H}_{uv}}(f_m, \Delta t)$ and $R_{P_{uv}}(\Delta t)$ were calculated using (12) by substituting $X_{uv}(t)$ with $|\widehat{H}_{uv}(f_m, t)|$ and $P_{uv}(t)$, respectively. The experimental results in the anechoic chamber are plotted in Fig. 5 for static, object moving, and mobile scenarios. For CSI, only $R_{\widehat{H}_{BA}}(f_1, \Delta t)$ was selected as an example for brevity, as other subcarriers' ACFs were quite similar.

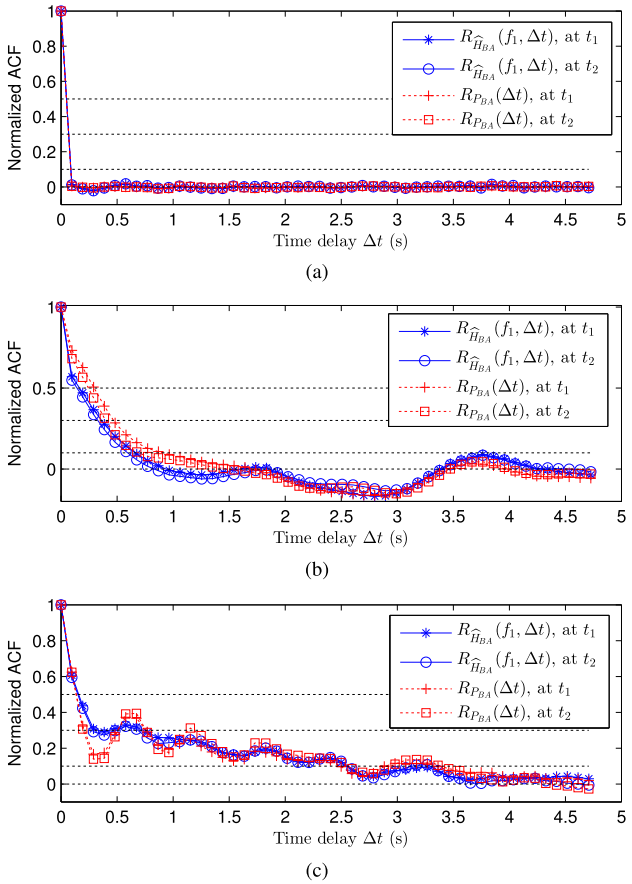


FIGURE 5. Normalized temporal ACF, $R_{\widehat{H}_{BA}}(f_1, \Delta t)$ and $R_{P_{BA}}(\Delta t)$, in the anechoic chamber. $t_2 = t_1 + 10$ s. (a) Static scenario. (b) Object moving scenario. (c) Mobile scenario.

As there is no interference from other wireless networks inside the anechoic chamber, the channel remains the same in the static scenario. Therefore, the variation of the received signal is only due to the hardware noise, which is temporally uncorrelated, as shown in Fig. 5(a). This seems beneficial for key generation as the samples are temporally independent, however, it is challenging for the users to agree on the same key as discussed in Section IV-C. In the object moving and mobile scenarios, as shown in Fig. 5(b) and Fig. 5(c), respectively, the samples are correlated in the time domain and $R_{\widehat{H}_{BA}}(f_1, \Delta t)$ and $R_{P_{BA}}(\Delta t)$ only depends on Δt but is irrelevant to the observation time t, indicating both $|\widehat{H}_{BA}(f_1, t)|$ and $P_{BA}(t)$ are WSS random processes.

The curves of $R_{\widehat{H}_{uv}}(f_m, \Delta t)$ and $R_{P_{uv}}(\Delta t)$ are quite similar, although we did observe from experiments that $|\widehat{H}_{uv}(f_m, t)|$ usually decorrelates a little faster than $P_{uv}(t)$, with an example shown in Fig. 6. In addition, $R_{X_{uv}}(\Delta t)$ in different scenarios varied because it is affected by both the environment and channel variation introduced by movement of users/objects.

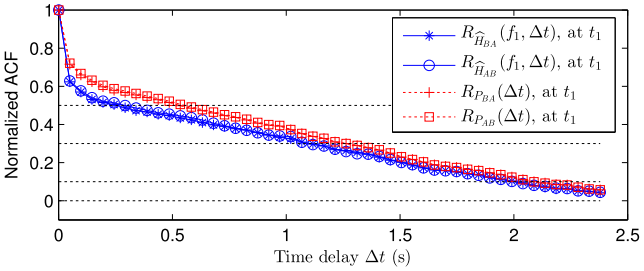


FIGURE 6. Normalized temporal ACF, $R_{X_{BA}}(\Delta t)$ and $R_{X_{AB}}(\Delta t)$, at t_1 in the office environment with mobile scenario.

The experimental results in the reverberation chamber and the office environment also indicate that in a dynamic environment, i.e., mobile and object moving scenarios in office environment and stirrer moving scenario in the reverberation chamber, $|\widehat{H}_{uv}(f_m, t)|$ and $P_{uv}(t)$ are also WSS random processes. Their ACF curves are similar to Fig. 5(b) and Fig. 5(c), and not plotted for brevity. As a WSS random process, when the time intervals between the samples are fixed, they will have the same correlation between each other. As a consequence, in a dynamic channel with users/objects moving at a constant speed, it is feasible to use a fixed rate to probe the channel, simplifying the channel probing design of the key generation.

B. RANDOMNESS

Temporal variation is the main random source for key generation. An experiment was run with the same setting as the mobile scenario in the office environment but lasted 300 s in order to collect more data for randomness evaluation. The channel was originally sampled at a rate of 0.96 ms, at which there exists redundancy between adjacent data samples. Therefore, the measurements were resampled by a period of T_p and then quantized to binary values using the single-bit CDF-based quantization scheme introduced in Algorithm 1. The optimal probing rate T_p can be found by evaluating the randomness of the key sequence. The normalized ACFs are shown in Fig. 6, from which the correlation coefficient $R_{\widehat{H}_{AB}}(f_1, T_p)$ and $R_{P_{AB}}(T_p)$ can be read. It may be observed that $R_{X_{BA}}(\Delta t)$ and $R_{X_{AB}}(\Delta t)$ overlap each other.

The randomness of the key sequence was evaluated by the National Institute of Standards and Technology (NIST)

random test suite [50], which has been widely used in key generation applications [7], [8], [14], [15], [20], [21], [24], [26]. There are 15 tests in total, each evaluating a specific randomness feature, e.g., frequency test focuses on the proportion of ones and zeros, and DFT test detects the periodic feature of the sequence, etc. Each test returns a P-value, which is compared to a significance value, α, with typical value in the range of [0.001, 0.01]. When the P-value $> \alpha$, the sequence is accepted as random. We chose α as 0.01, the same as other work [7], [8], [14], [15], [20], [21], [24], [26]. We ran 8 tests, over half of the test suite, which still satisfies the requirements of NIST. Some of the tests require extremely long sequences which were not applied in this paper. For example, random excursions variant test recommends the input sequence longer than 10^6, which is currently not available in our experiments.

TABLE 2. Randomness test results of key sequences quantized from CSI, $|\widehat{H}_{AB}(f_1, t)|$. The gray cells fail the randomness test.

Corr coeff $X\%$	56.9%	44.2%	32.5%	20.2%	14.1%	10.2%
T_p (s)	0.1	0.5	1	1.5	1.8	2
Sequence length	2998	598	298	198	166	148
Frequency	1	1	1	0.887	0.877	1
Block frequency	0	0.859	0.869	0.596	0.48	0.596
Runs	0	0	0.005	0.156	0.536	0.324
Longest run of 1s	0	0.052	0.575	0.361	0.1	0.568
DFT	0.183	0.252	0.41	0.493	0.915	0.821
Serial	0	0	0.153	0.458	0.714	0.76
	0	0.589	0.145	0.278	0.468	0.862
Appro. entropy	0	0	0.038	0.291	0.732	0.614
Cum. sums (fwd)	0.027	0.503	0.855	0.767	0.898	0.969
Cum. sums (rev)	0.027	0.503	0.855	0.634	0.766	0.969

TABLE 3. Randomness test results of key sequences quantized from RSS, $P_{AB}(t)$. The gray cells fail the randomness test.

Corr coeff $X\%$	65.8%	51.1%	38%	23.1%	16.4%	12.2%
T_p (s)	0.1	0.5	1	1.5	1.8	2
Sequence length	2998	598	298	198	166	148
Frequency	0.001	0.086	0.203	0.887	0.088	0.411
Block frequency	0	0.31	0.495	0.377	0.289	0.724
Runs	0	0.005	0.001	0.004	0.942	0.271
Longest run of 1s	0	0.002	0.038	0.402	0.121	0.361
DFT	0.397	0.694	0.193	0.493	0.413	0.597
Serial	0	0	0.28	0.212	0.502	0.444
	0	0.858	0.98	0.82	0.362	0.716
Appro. entropy	0	0	0.012	0.011	0.231	0.32
Cum. sums (fwd)	0.001	0.144	0.264	0.634	0.148	0.718
Cum. sums (rev)	0	0.082	0.365	0.51	0.175	0.568

The randomness test results of keys quantized from $|\widehat{H}_{AB}(f_1, t)|$ and $P_{AB}(t)$ are shown in Table 2 and Table 3, respectively, where the gray cells fail the randomness test, i.e., P-value $< \alpha$. As may be observed from the tables, when the correlation between the two adjacent measurements is high, the key sequence fails several tests. Temporal ACF describes how fast the signal decorrelates against time and thus can be used to determine the optimal probing interval. Too short a probing interval between two adjacent measurements will result in sample redundancy and impact the randomness of the key sequence, while too large an interval will lead to a low key generation rate (KGR) and limit its practical application. In this example, the system cannot generate a random key sequence from $|\widehat{H}_{AB}(f_1, t)|$ until the correlation coefficient between adjacent samples is below 20.2% and the probing rate T_p reaches greater than 1.5 s, which is the optimal probing rate.

C. CHANNEL RECIPROCITY

The channel fading at each end of the link is reciprocal. However, the signals measured by each user are asymmetric due to the non-simultaneous measurements and the uncorrelated hardware noise. The similarity between the received signals of Alice and Bob can be quantified by the cross-correlation relationship defined in (13) and KDR defined in (14) by substituting $X_{AB}(t_A)$ and $X_{BA}(t_B)$.

The cross-correlation coefficients and KDR of the experiments in the anechoic chamber, reverberation chamber, and office environment are depicted in Fig. 7(a), Fig. 7(b), and Fig. 7(c), respectively. As shown in Fig. 7(a) and Fig. 7(c), when the channel is static, the independent hardware noise is the only contributor to the signal variation, therefore the cross-correlation coefficients are almost zero. The corresponding KDRs in the static channel are around 0.5, which are no better than a random guess. This makes key generation un-operational as the legitimate users are not able to reach an agreement.

As shown in Fig. 7(a) and Fig. 7(c), in the mobile scenarios, the correlation coefficients are high, and all the KDRs are acceptable and could be later corrected by information reconciliation techniques. For example, BCH code can correct up to 25% key disagreement [26]. In the object moving scenario in the anechoic chamber and office environment, the correlation is not as high as in the mobile scenario. This is because when one user is moving, the channel is changing more significantly than the object moving scenario where only some paths are affected. However, as may be observed from Fig. 7(c), when there are two objects moving in the office environment, the correlation is as high as that of the mobile scenario, which means the increased movement helps improve the correlation. This can also be observed from the results of the reverberation chamber, where there is rich multipath.

In all the examples, $\rho^{P}_{AB,BA}$ is higher than the corresponding $\rho^{\widehat{H}_m}_{AB,BA}$. As shown in (2), RSS is calculated by averaging over one packet, therefore, some of the noise effects have been canceled out. In addition, the channel estimation $\widehat{H}_{uv}(f_m, t)$ is subject to synchronization errors such as frequency and timing offset.

D. SPATIAL DECORRELATION

Spatial decorrelation is essential to the security of key generation systems. KDR is usually used to quantify the disagreement between Alice and Bob. However, it can also be extended to quantify the disagreement between legitimate users and eavesdroppers. The cross-correlation coefficient and KDR can be calculated using (13) and (14), respectively, by substituting $X_{AB}(t_A)$ and $X_{AE_j}(t_A)$. The average correlation

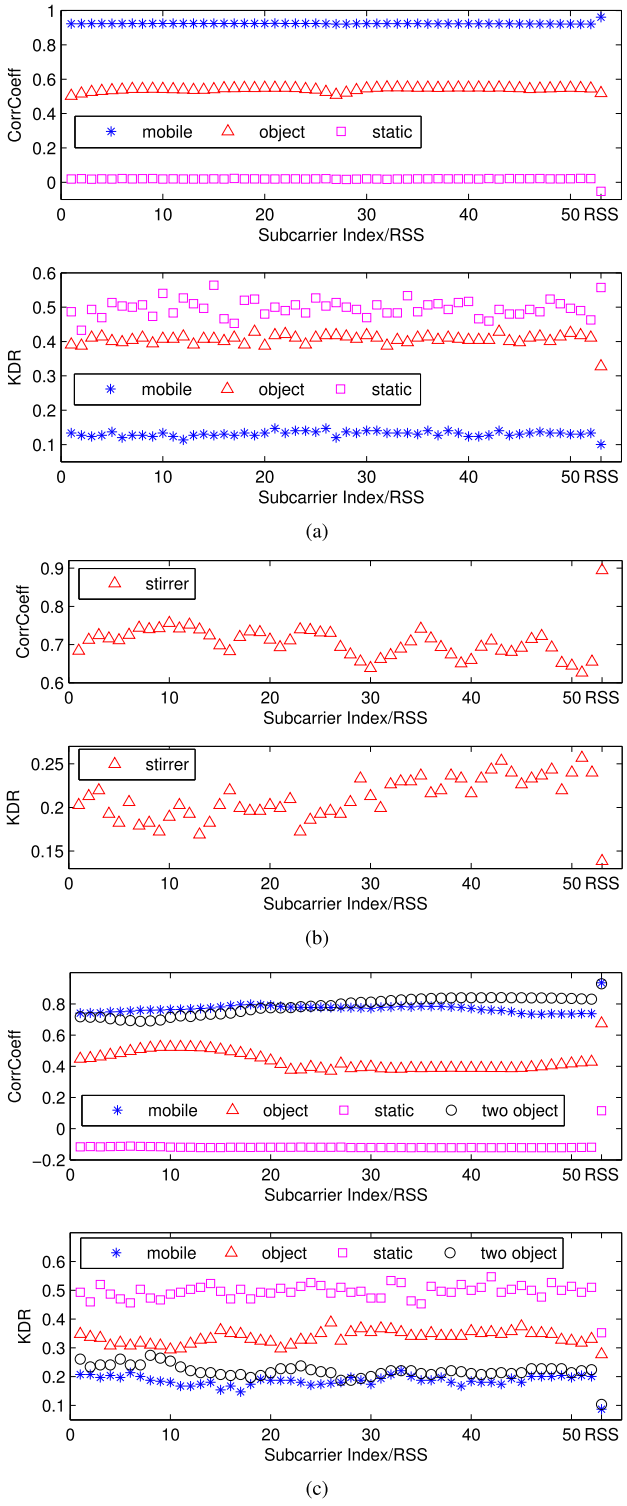


FIGURE 7. Cross-correlation coefficients, $\rho^{X}_{AB,BA}$, and KDRs, $KDR^{X}_{AB,BA}$, of CSI and RSS with static, object (stirrer) moving, and mobile scenarios in different environments. (a) Anechoic chamber. (b) Reverberation chamber. (c) Office environment.

coefficient of channel estimation can be given as

$$\bar{\rho}^{\widehat{H}}_{uv,u'v'} = \frac{1}{M}\sum_{i=0}^{M-1} \rho^{\widehat{H}_m}_{uv,u'v'}. \tag{15}$$

The average KDR of channel estimation can be written as

$$\overline{KDR}^{\widehat{H}}_{uv,u'v'} = \frac{1}{M}\sum_{i=0}^{M-1} KDR^{\widehat{H}_m}_{uv,u'v'}. \tag{16}$$

In this section, we use $\bar{\rho}^{P}_{uv,u'v'}$ and $\overline{KDR}^{P}_{uv,u'v'}$ to represent $\rho^{P}_{uv,u'v'}$ and $KDR^{P}_{uv,u'v'}$, respectively. Then we could use $\bar{\rho}^{X}_{uv,u'v'}$ and $\overline{KDR}^{X}_{uv,u'v'}$ for the simplicity of notation.

1) EAVESDROPPERS IN LINEAR PLACEMENT

Multiple experiments were carried out with different distance configurations but the same setup shown in Fig. 3(a). The results of CSI and RSS are shown in Fig. 8 and Fig. 9, respectively. The points with distances smaller than 0 are the average correlation coefficients, $\bar{\rho}^{X}_{AB,BA}$, and average KDRs, $\overline{KDR}^{X}_{AB,BA}$, between Alice and Bob, which are shown for comparison.

As can be observed from Fig. 8 and Fig. 9, the shapes of the curves in the same environments obtained by CSI and RSS are quite similar while the absolute values are slightly different.

As shown in Fig. 8(a) and Fig. 9(a), for the mobile scenario in the anechoic chamber, when the eavesdroppers were in the proximity of Bob, their correlation coefficients, $\bar{\rho}^{X}_{AB,AE_j}$, fluctuate greatly. This effect is more severe in an environment with strong LoS, as the same phenomenon is not observed in the reverberation chamber and office environment. In the mobile scenario of experiments in the anechoic chamber, even when eavesdroppers are separated far enough from Bob, e.g., 40 cm (about 3λ) in this section, $\bar{\rho}^{X}_{AB,AE_j}$ reaches a high level and remains almost constant. In an environment with little multipath such as anechoic chamber, the signal variation is mainly due to the change of the LoS. Therefore, these nodes experience similar signal variations and high cross-correlation. In the object moving scenario, some $\bar{\rho}^{X}_{AB,AE_j}$ are even higher than $\bar{\rho}^{X}_{AB,BA}$ when eavesdroppers are close to Bob. The system cannot be deemed secure in these dynamic scenarios as the $\overline{KDR}^{X}_{AB,AE_j}$ are very close to or even smaller than $\overline{KDR}^{X}_{AB,BA}$. In the static scenario, all the users, including legitimate users, cannot reach an agreement on the same key sequence.

The results from reverberation chamber are shown in Fig. 8(b) and Fig. 9(b). There is very rich multipath in the reverberation chamber, therefore, no matter how close eavesdroppers are located from the legitimate user, their signal paths are very diverse. Thus, eavesdroppers' signals have little correlation with Bob's. $\overline{KDR}^{X}_{AB,AE_j}$ are always around 0.5, which indicates that eavesdroppers almost have no information of the keys quantized by the legitimate users.

The experimental results from the office environment are between the above two extreme cases, as shown in Fig. 8(c) and Fig. 9(c). The multipath helps decrease the spatial correlation between the users and $\overline{KDR}^{X}_{AB,BA}$ is much smaller than $\overline{KDR}^{X}_{AB,AE_j}$. This is very beneficial for the security of key generation as it indicates that eavesdroppers cannot get any

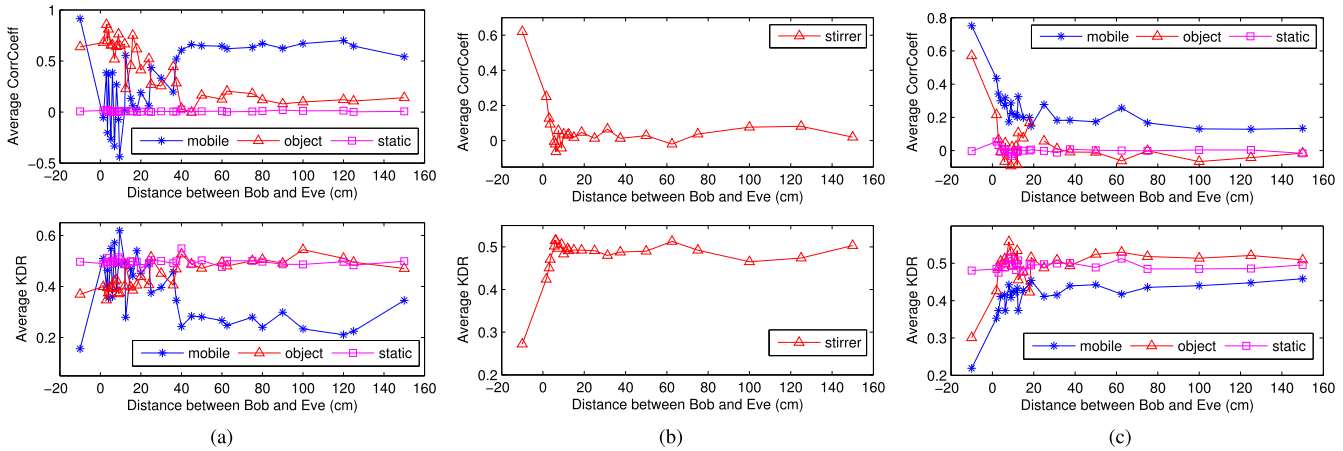


FIGURE 8. Average correlation coefficients, $\bar{\rho}^{\widehat{H}}_{AB,AE_j}$, and average KDRs, $\overline{KDR}^{\widehat{H}}_{AB,AE_j}$, with static, object (stirrer) moving, and mobile scenarios in different environments. Eavesdroppers are in linear placement. $\lambda = 12.44$ cm. The points with distances smaller than 0 are the average correlation coefficients, $\bar{\rho}^{\widehat{H}}_{AB,BA}$, and average KDRs, $\overline{KDR}^{\widehat{H}}_{AB,BA}$, between Alice and Bob, which are shown for comparison. (a) Anechoic chamber. (b) Reverberation chamber. (c) Office environment.

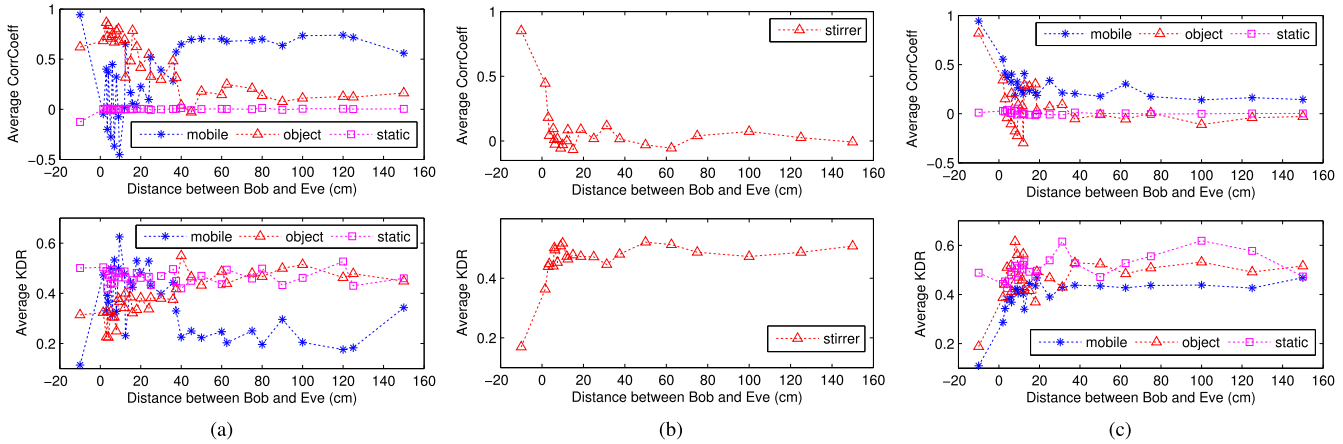


FIGURE 9. Average correlation coefficients, $\bar{\rho}^{P}_{AB,AE_j}$, and average KDRs, $\overline{KDR}^{P}_{AB,AE_j}$, with static, object (stirrer) moving, and mobile scenarios in different environments. Eavesdroppers are in linear placement. $\lambda = 12.44$ cm. The points with distances smaller than 0 are the average correlation coefficients, $\bar{\rho}^{P}_{AB,BA}$, and average KDRs, $\overline{KDR}^{P}_{AB,BA}$, between Alice and Bob, which are shown for comparison. (a) Anechoic chamber. (b) Reverberation chamber. (c) Office environment.

useful information about the key generated by the legitimate users. The results of the mobile scenario validate the analysis in [36], where the authors studied spatial decorrelation by collecting RSS via laptops in an indoor environment.

It is worth noting that in the reverberation chamber and office environment, even when the eavesdroppers are very close to the legitimate users, their received signals are quite different. However, in a strong LoS environment such as an anechoic chamber, even when the eavesdroppers are several wavelengths away (3λ in this example), they can still observe a high correlated signal from the legitimate users. Therefore, special attention is required to thwart eavesdropping in environments with strong LoS. Multipath is usually considered to be detrimental to wireless systems as it increases the complexity of the equalizer, however, it is beneficial in key generation application due to the uncertainty introduced.

2) EAVESDROPPERS IN CIRCULAR PLACEMENT

Further experiments were carried out by putting six eavesdroppers around Bob in a circle as shown in Fig. 3(b).[2] The experiments were done in the reverberation chamber with stirrer moving scenario and in the office environment with mobile and object moving scenarios.[3] Eve4 and Eve5 were located between Alice and Bob while Eve1 and Eve2 were behind Bob. However, as can be observed from Fig. 10

[2]Only five eavesdroppers were used when the distance $d = 7$ cm due to the space limit.

[3]Experiments with circular placement of eavesdroppers were not carried out in the anechoic chamber due to installment issues.

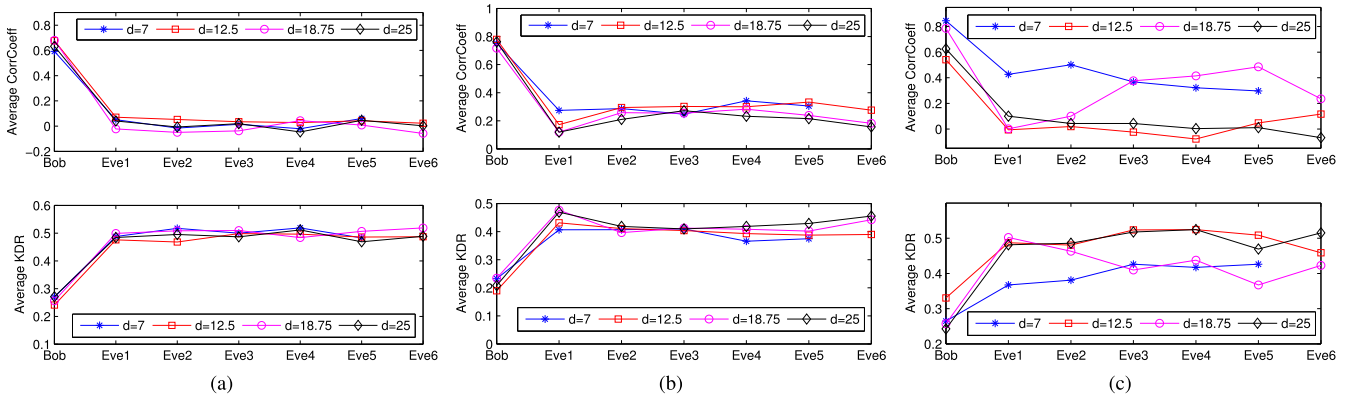


FIGURE 10. Average correlation coefficients, $\bar{\rho}^{\hat{H}}_{AB,BA}$ and $\bar{\rho}^{\hat{H}}_{AB,AE_j}$, and average KDRs, $\overline{KDR}^{\hat{H}}_{AB,BA}$ and $\overline{KDR}^{\hat{H}}_{AB,AE_j}$, with stirrer moving scenario in the reverberation chamber, and object moving and mobile scenarios in the office environment. Eavesdroppers are in circular placement. $\lambda = 12.44$ cm. (a) Stirrer moving, reverberation chamber. (b) Mobile, office environment. (c) Object moving, office environment.

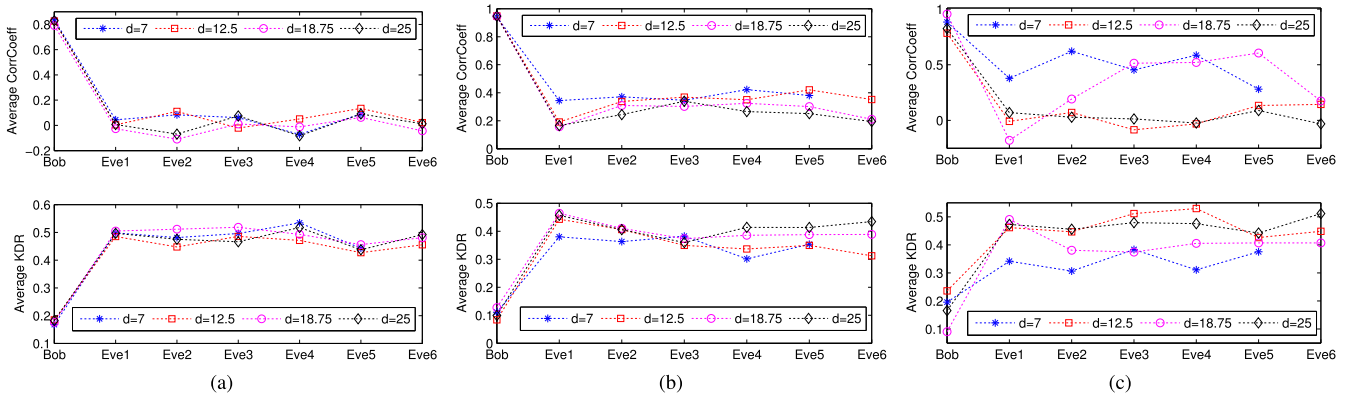


FIGURE 11. Average correlation coefficients, $\bar{\rho}^{P}_{AB,BA}$ and $\bar{\rho}^{P}_{AB,AE_j}$, and average KDRs, $\overline{KDR}^{P}_{BA}$ and $\overline{KDR}^{P}_{AB,AE_j}$, with stirrer moving scenario in reverberation chamber, and object moving and mobile scenarios in the office environment. Eavesdroppers are in circular placement. $\lambda = 12.44$ cm. (a) Stirrer moving, reverberation chamber. (b) Mobile, office environment. (c) Object moving, office environment.

and Fig. 11, there seems no relationship between $\bar{\rho}^{X}_{AB,AE_j}$ and the location of eavesdroppers, because in a multipath environment, the signal is coming from all directions due to the reflection, scattering, and refraction, etc. This property is quite beneficial for key generation, as even if eavesdroppers are located between the legitimate users, they still cannot get a better correlation.

V. CONCLUSION

This paper comprehensively studied key generation principles, i.e., temporal variation, channel reciprocity, and spatial decorrelation, by using CSI and RSS collected from experiments. The testbed was implemented using WARP reference design, which supports IEEE 802.11 OFDM PHY and DCF MAC. This enabled us to measure the channel using data and ACK packets without any change to the off-the-shelf wireless protocol. Over a hundred experiments have been carried out in an anechoic chamber, a reverberation chamber, and an office environment with static, object moving, and mobile scenarios. The key generation principles were studied by the experimental results. Both CSI and RSS were proved to be applicable for key generation.

Through the comprehensive experimental results, we offer insights and guideline for the key generation system design. When the channel is sufficiently dynamic, temporal variation is an ideal random source and the legitimate users are able to agree on the same key. However, in a static channel, the cross-correlation between the channel measurements of two users is too small and the key mismatch cannot be corrected. In a multipath environment, the spatial decorrelation is satisfied and the security of the key generation system is guaranteed. In an environment with little multipath such as an anechoic chamber, eavesdroppers could observe a highly correlated signal to the legitimate users, which results in potential information leakage and requires special attention.

ACKNOWLEDGMENT

This paper was presented in part at the IEEE Global Communications Conference Workshop on Trusted Communications with Physical Layer Security, San Diego, California, USA, December, 2015.

REFERENCES

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

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] 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.

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

[5] C. Huth, R. Guillaume, T. Strohm, P. Duplys, I. A. Samuel, and T. Güneysu, "Information reconciliation schemes in physical-layer security: A survey," *Comput. Netw.*, to be published.

[6] C. H. Bennett, G. Brassard, and C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[7] 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.

[8] 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.

[9] 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.

[10] M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dresden, Germany, Jun. 2009, pp. 1–5.

[11] S. T.-B. Hamida, J.-B. Pierrot, and C. Castelluccia, "Empirical analysis of UWB channel characteristics for secret key generation in indoor environments," in *Proc. 21st IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Instanbul, Turkey, Sep. 2010, pp. 1984–1989.

[12] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," in *Proc. IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Paris, France, Sep. 2014, pp. 80–85.

[13] 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.

[14] 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.

[15] 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.

[16] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, Sep. 2013.

[17] R. Guillaume, F. Winzer, A. Czylwik, C. T. Zenger, and C. Paar, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC Fall)*, Boston, MA, USA, Sep. 2015, pp. 1–5.

[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] 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.

[20] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.

[21] 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.

[22] 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.

[23] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1796–1806, Aug. 2016.

[24] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using Bluetooth wireless signal strength measurements," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2014, pp. 293–301.

[25] *Ettus Research*, accessed on Sep. 1, 2016. [Online]. Available: http://www.ettus.com

[26] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[27] 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.

[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] H. Vogt and A. Sezgin, "Full-duplex vs. half-duplex secret-key generation," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Rome, Italy, Nov. 2015, pp. 1–6.

[30] H. Vogt, K. Ramm, and A. Sezgin, "Practical secret-key generation by full-duplex nodes with residual self-interference," in *Proc. 20th Int. ITG Workshop Smart Antennas*, Munich, Germany, Mar. 2016, pp. 1–5.

[31] A. Sadeghi, M. Zorzi, and F. Lahouti. (2016). "Analysis of key generation rate from wireless channel in in-band full-duplex communications." [Online]. Available: http://arxiv.org/abs/1605.09715

[32] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. 17th IEEE Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Edinburgh, U.K., Jul. 2016, pp. 1–5.

[33] 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, Egypt, Oct. 2007, pp. 401–410.

[34] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[35] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[36] C. T. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. Workshop Wireless Commun. Secur. Phys. Layer*, Coimbra, Portugal, Jul. 2015, pp. 1–6.

[37] X. He, H. Dai, Y. Huang, D. Wang, W. Shen, and P. Ning, "The security of link signature: A view from channel models," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 103–108.

[38] X. He, H. Dai, W. Shen, P. Ning, and R. Dutta, "Toward proper guard zones for link signature," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2104–2117, Mar. 2016.

[39] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. 4th Eur. Workshop Syst. Secur.*, Salzburg, Austria, Apr. 2011, pp. 8:1–8:6.

[40] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 200–204.

[41] *WARP Project*, accessed on Sep. 1, 2016. [Online]. Available: http://warpproject.org

[42] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM subcarrier's channel response," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[43] *IEEE Standard for Air Interface for Broadband Wireless Access Systems*, IEEE Standard 802.16, 2012.

[44] *CC2520 2.4 GHz IEEE 802.15.4/ZIGBEE RF Transceiver*, accessed on Sep. 1, 2016. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2520.pdf
[45] *MAX2828/MX2829 Single-/Dual-Band 802.11 a/b/g World-Band Transceiver ICs*, accessed on Sep. 1, 2016. [Online]. Available: http://datasheets.maximintegrated.com/en/ds/MAX2828-MAX2829.pdf
[46] J. Bardwell. *You Believe You Understand What You Think I Said... The Truth About 802.11 Signal and Noise Metrics*, accessed on Sep. 1, 2016. [Online]. Available: http://www.n-cg.net/ncgpdf/WiFi_SignalValues.pdf
[47] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 1, p. 53, Jan. 2011.
[48] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Standard 802.11, 2012.
[49] P. A. Bello, "Characterization of randomly time-variant linear channels," *IEEE Trans. Commun. Syst.*, vol. 11, no. 4, pp. 360–393, Dec. 1963.
[50] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22 Revision 1a, Apr. 2010.

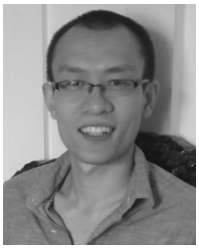
JUNQING ZHANG received the B.Eng. and M.Eng. degrees in electrical engineering from Tianjin University, China, in 2009 and 2012, respectively, and the Ph.D. degree in electronics and electrical engineering from Queen's University Belfast, U.K., in 2016. He is currently a Post-Doctoral Research Fellow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

ROGER WOODS (M'95–SM'01) received the B.Sc. degree (Hons.) 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. He has founded 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 four patents. He has authored over 200 papers. He is a member of the IEEE Signal Processing and Industrial Electronics Societies. He serves on the Advisory Board for the IEEE SPS Technical Committee on the Design and Implementation of Signal Processing Systems. He serves 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 for the 2014 Asilomar IEEE Conference on Signals, Systems, and Computers. He serves on the program committees of a number of the 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. He has authored or co-authored over 200 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, mm-waves communications, and localization for radios and networks.

Dr. Duong received the best paper award at the IEEE Vehicular Technology Conference 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, the *IET Communications*, the Wiley *Transactions on Emerging Telecommunications Technologies*, and the *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, the *IET Communications*, the IEEE Wireless Communications Magazine, the IEEE Communications Magazine, the *EURASIP Journal on Wireless Communications and Networking*, the *EURASIP Journal on Advances Signal Processing*.

ALAN MARSHALL (M'88–SM'00) has spent over 24 years in the telecommunications and defense Industries. He has been a Visiting Professor in 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 founded a successful spin-out company Traffic Observation & Management (TOM) 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 of the section B: *Computer and Communications Networks and Systems* for the Computer Journal of the British Computer Society, a member of Editorial Board of the *Journal of Networks*, and serves on the program committees of a number of the IEEE conferences.



YUAN DING received the bachelor's degree from Beihang University (BUAA), Beijing, China, in 2004, the master's degree from Tsinghua University, Beijing, in 2007, and the Ph.D. degree from Queen's University Belfast, Belfast, U.K., in 2014, all in electronic engineering.

He was a RF Engineer with Motorola Research and Development Centre, Beijing, from 2007 to 2009. He joined Freescale Semiconductor Inc., Beijing, from 2009 to 2011, as a RF Field Application Engineer, responsible for high power base-station amplifier design. He is currently a Research Fellow with the ECIT Institute, Queen's University of Belfast. His research interests are in antenna array, physical layer security, and 5G related areas.

Dr. Ding was a recipient of the IET Best Student Paper Award at LAPC 2013 and a recipient of the Young Scientists Awards in General Assembly and Scientific Symposium, 2014 XXXIst URSI.

YI HUANG (S'91–M'96–SM'06) received the B.Sc. degree in physics from Wuhan University, China, the M.Sc. (Eng.) degree in microwave engineering from NRIET, Nanjing, China, and the D.Phil. degree in communications from the University of Oxford, Oxford, U.K., in 1994.

He has been conducting research in wireless communications, applied electromagnetics, radar and antennas for the past 25 years. His experience includes three years spent with NRIET, China, as a Radar Engineer and various periods with the Universities of Birmingham, Oxford, and Essex, U.K., as a member of Research Staff. He was a Research Fellow with British Telecom Labs in 1994, and then joined the Department of Electrical Engineering and Electronics, University of Liverpool, U.K., as a Faculty member in 1995, where he is currently a Full Professor in wireless engineering, the Head of High Frequency Engineering Research Group, the M.Sc. Programme Director and the Deputy Head of the Department. He has authored over 200 refereed papers in leading international journals and conference proceedings. He is the Principal Author of the popular book *Antennas:from Theory to Practice* (Wiley, 2008). He has received many research grants from research councils, government agencies, charity, EU, and industry, and acted as a Consultant to various companies, and served on a number of national and international technical committees. He has been an Editor, an Associate Editor, or a Guest Editor of four of international journals. He has been a Keynote/Invited Speaker and an Organiser of many conferences and workshops such as the IEEE iWAT 2010, the WiCom 2006, 2010, and the LAPC2012. He is the Editor-in-Chief of *Wireless Engineering and Technology*, a U.K. National Republic of European COST-IC1102, an Executive Committee Member of the IET Electromagnetics PN, and a fellow of IET, U.K.

QIAN XU received the B.Eng. and M.Eng. degrees from the Department of Electronics and Information, Northwestern Polytechnical University, Xi'an, China, in 2007 and 2010, respectively, and the Ph.D. degree in electrical engineering from the University of Liverpool, U.K., in 2016.

He was a RF Engineer, Nanjing, China, in 2011, and an Application Engineer with CST, Shanghai, China, in 2012. His research interests include statistical electromagnetics, computational electromagnetics, reverberation chamber and anechoic chamber.