Hindawi Publishing Corporation
International Journal of Antennas and Propagation
Volume 2015, Article ID 106360, 13 pages
http://dx.doi.org/10.1155/2015/106360

Research Article

Analysis of Secret Key Randomness Exploiting the Radio Channel Variability

Taghrid Mazloum and Alain Sibille

LTCI, Télécom ParisTech, CNRS, 46 rue Barrault, 75013 Paris, France

Correspondence should be addressed to Taghrid Mazloum; taghrid.mazloum@telecom-paristech.fr

Received 27 May 2015; Accepted 3 September 2015

Academic Editor: Larbi Talbi

A few years ago, physical layer based techniques have started to be considered as a way to improve security in wireless communications. A well known problem is the management of ciphering keys, both regarding the generation and distribution of these keys. A way to alleviate such difficulties is to use a common source of randomness for the legitimate terminals, not accessible to an eavesdropper. This is the case of the fading propagation channel, when exact or approximate reciprocity applies. Although this principle has been known for long, not so many works have evaluated the effect of radio channel properties in practical environments on the degree of randomness of the generated keys. To this end, we here investigate indoor radio channel measurements in different environments and settings at either 2.4625 GHz or 5.4 GHz band, of particular interest for WIFI related standards. Key bits are extracted by quantizing the complex channel coefficients and their randomness is evaluated using the NIST test suite. We then look at the impact of the carrier frequency, the channel variability in the space, time, and frequency degrees of freedom used to construct a long secret key, in relation to the nature of the radio environment such as the LOS/NLOS character.

1. Introduction

Traditionally, a set of cryptographic based mechanisms and protocols provides communication security through data encryption. In symmetric encryption methods, the main drawback is the key management, which includes key generation and distribution, since the same secret key is used for data encryption and data decryption [1]. While this issue is alleviated by asymmetric techniques using a pair of public and private keys [1], their high computational cost stresses the need for new security techniques, especially for wireless communications and emerging Internet of Things in which the energy consumption is of major importance.

The robustness of these widespread classical cryptography mechanisms relies on computational constraint on the attacker. However, with the continuous progress of high power computing, unconditionally secured systems are more and more required [2]. In this respect, information-theoretic based security assumes unlimited computing power for the illegal user and claims that only the gathered information may help the eavesdropper to break the data privacy [2, 3]. In this framework, a special approach to physical layer security (PhySec) field [2] intends to achieve wireless communications and data protection by exploiting the inherent properties of the wireless propagation channel such as the multipath fading, interference, and noise.

One of the main PhySec techniques is secret key generation (SKG) [4, 5], which facilitates key management as opposed to conventional cryptosystems. Secret key distribution is mainly avoided since each legitimate terminal (typically referred to as Alice and Bob) is assumed to generate the same secret key from the radio propagation channel, considered as a common source of randomness [4, 5]. Indeed, when channel reciprocity applies, typically when Alice and Bob use the same frequency at the same time instant, they share the same wireless channel. Randomness is ensured through multipath fading, which results in decorrelation properties in the spatial, temporal, and frequency domains. Consequently, an eavesdropper (Eve) is probably not able to efficiently exploit her own measured channel in order to crack the key (Figure 1).

A robust shared key is characterized by its length and its randomness. In fact, channel estimation noise is a main factor limiting the number of shared bits extracted from a single

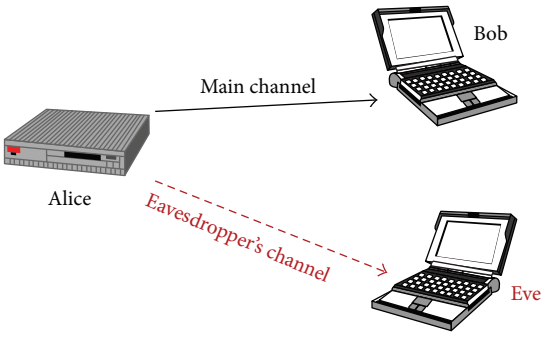

Figure 1: Wireless link between legitimate terminals in the presence of an eavesdropper.

channel observation (see [6–11] for an information-theoretic framework). Therefore, researchers attempt to access more randomness by exploiting various channel degrees of freedom such as the spatial diversity existing in multiple antenna systems [6], the frequency diversity in orthogonal frequency division multiplexing (OFDM) systems [12], and the time diversity in ultrawideband (UWB) channels [8, 9].

In addition to key length constraint, the random character of the key is essential in making eavesdropping extremely difficult, which requires a small correlation between the channel samples seen by Alice/Bob and by Eve. Jana et al. [13] assessed security performance by investigating real measured channels in both indoor and outdoor conditions. The measurements using 802.11-based laptops exhibited the weakness of SKG behavior in nearly static environments, where the entropy of extracted key bits is very low. Security in such environments may be enhanced by creating channel fluctuations using beamforming technique [14, 15]. However, when either terminals or scattering objects are moving, is the randomness of the key sufficiently guaranteed? Furthermore, how may the security performance be improved in static environments?

The statistical National Institute of Standards and Technology (NIST) test suite [16] is usually used to assess the effectiveness of extracting randomness from the wireless channel [13, 17–21]. Furthermore, it is more effective to test the ability of the whole source of randomness to provide really random bit strings [20] rather than testing a unique key realization. It is noteworthy that this randomness evaluation occurs directly after the quantization phase and is improved by privacy amplification [22] in the last step of SKG.

According to this brief analysis of the literature, it turns out that most papers evaluate theoretically and practically SKG techniques by emphasizing either key reliability between legitimate users or key vulnerability with respect to Eve. The randomness of keys as a function of their source (i.e., the characteristics of the radio channel) has not been extensively considered. In this context, the main contributions of the present paper are as follows:

(1) Investigate real indoor measured channels in different environments and settings, considering varying separation distances between users on the one hand and LOS/NLOS propagation conditions on the other hand.

(2) Analyze the quality of the generated keys from the randomness point of view, using the NIST test suite, in relation to the channel properties (coherence bandwidth, carrier frequency, and LOS/NLOS).

(3) Compare the key quality for suitably long keys, when the key bits are derived from either space, time, frequency, or jointly space-frequency degrees of freedom. This is especially relevant when targeting WIFI for the implementation of SKG.

The paper is organized as follows. Section 2 presents the measurement campaign carried out in different conditions. Section 3 describes the quantization algorithm used to transform the channel complex coefficients into a stream of key bits. The key randomness is then tested through NIST test suite introduced in Section 4. Section 5 explains how to construct a sufficient long secret key by exploiting the channel variability in the spatial (or time) and frequency domain. Results invoking the relation between the key randomness and the real channel features are discussed in Section 6. Finally, the conclusion is drawn in Section 7.

2. Measuring Systems and Scenarios

Measurements have been performed in the premises of Télécom ParisTech (TPT), which is a century-old engineering education building with highly heterogeneous internal structuring due to many refurbishing events over the years. The measurements were conducted on a school holiday in order to ensure the absence of detectable human movement in the area. A 4-port vector network analyzer (VNA, Agilent ENA E5071C) has been used to record channel coefficients over 4 GHz of bandwidth (2–6 GHz) with 2.5 MHz as frequency step. This step, which translates into a maximum channel response delay of 400 ns, is enough to avoid aliasing, given the instrument noise floor and the typical delay spread of multipaths in the concerned environments. Table 1 presents the VNA setup parameters. One port of the VNA has been devoted to Alice, as transmitter, whereas the three remaining ports have been devoted to Bob, as receivers. Each port was equipped with an identical UWB bicone antenna with 2 dBi gain, specifically designed for the frequency stability of the radiation pattern [23]. The VNA has been calibrated with a "full 4-port" method including the (highly phase stable) cables, resulting as output at each frequency in the full 4×4 matrix of the complex channel coefficients including all antennas.

The measurements have been carried out in classrooms and in an auditorium, in order to have indoor scenarios of sufficiently different characteristics, including identical or different heights for the terminals; LOS or NLOS propagation condition; and also different room sizes. Figure 2 shows the floor plans of both classrooms and auditorium where the environment is mainly constituted of concrete, plywood, and partition walls. In the classroom scenario, the terminals have been placed at the same height (1.3 m from the ground),

Table 1: VNA setup parameters.

Start frequency	2 GHz
Stop frequency	6 GHz
Frequency points	1601
IF bandwidth	5 KHz
Transmitted power	10 dBm
Dynamic range	96 dB
Typical noise floor	−86 dBm

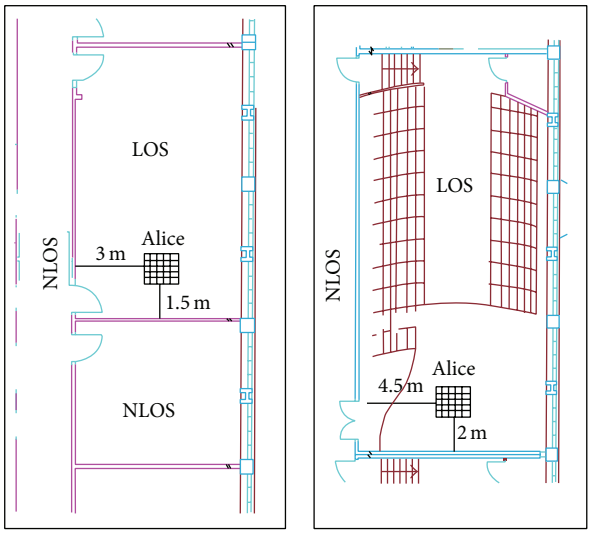

Figure 2: TPT measurement floor plans: classrooms (a) and auditorium (b).

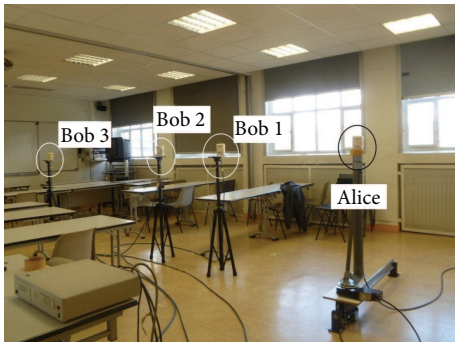

Figure 3: A sketch of measurement run in TPT classrooms scenario.

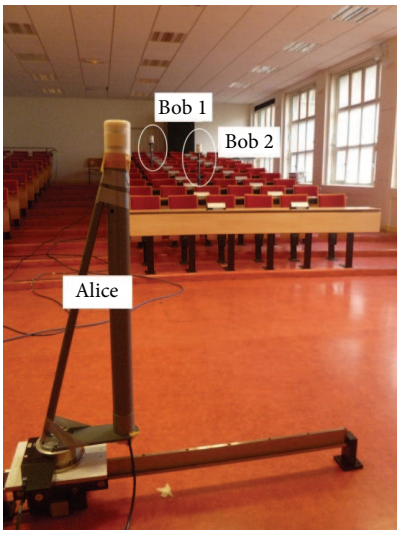

Figure 4: A sketch of measurement run in TPT auditorium scenario.

whereas in the auditorium they have been placed at different heights as seen in Figures 3 and 4. The location of Alice was fixed for each of the two environments whereas the remaining three antennas have been moved across the area in a set of irregular locations, mostly within the room but also in the adjacent corridor or in an adjacent room. More clearly, the antennas representing Bob have 51 different positions in the classrooms scenario and 42 positions in the auditorium scenario, where only 25 total positions are in NLOS condition with respect to Alice. The NLOS scenario encompasses either room-to-room or room-to-corridor propagation conditions, as shown in Figure 2.

In each measurement run, the three receivers representing Bob are steady while the transmitter representing Alice is spatially scanned over a square grid of 11 × 11 points (30 cm side and 3 cm step) confined to a small area so as to capture fast fading. More clearly, since the grid step is about half a wavelength at 5 GHz, we can expect to achieve close to statistically independent channel coefficients owing to spatial fading. The total 4 GHz bandwidth enables us to investigate in this paper the security performance of wideband (WB) channels centered at either 2.4625 GHz or 5.4 GHz (typical of the WIFI band) with, for example, a bandwidth of either 20, 40, 80, or even 160 MHz, according to the series of WIFI (IEEE 802.11) standards.

3. Channel Quantization

In a Time Division Duplex (TDD) system, such as for IEEE 802.11, Alice and Bob successively estimate their channel state information (CSI) by successively sending each other a known probe signal, using the same frequency band. Owing to the electromagnetic reciprocity law, the CSIs at both Alice and Bob are very similar. Therefore, assuming they use a common quantization algorithm, they are able to jointly translate their continuous CSI into a shared string of cryptographic key bits which may be used by the upper-layer protocols in order to strengthen security.

However, some mismatches between Alice-Bob keys may occur, especially for ordinary commercial wireless devices in the case of TDD and additive noise or channel estimation inaccuracies. Fortunately, such key mismatches may be diminished by an efficient quantization algorithm, employing suitable censoring schemes. While some algorithms increase Alice-Bob's key agreement by dropping down samples falling

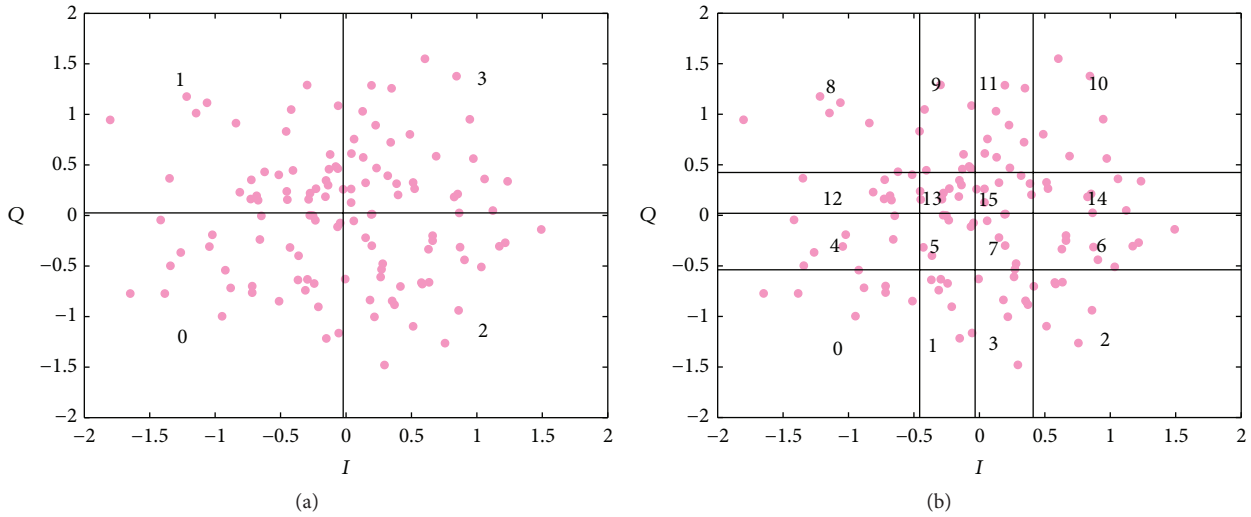

FIGURE 5: Correspondence between symbols and QR: (a) $M = 4$, (b) $M = 16$.

into a predefined guardband region [6, 24], the time required to construct a long secret key increases, which reduces the effectiveness of such algorithms. Alternatively, a more efficient protocol adapts the quantization scheme to the channel observation [6, 21], for example, the channel quantization alternating (CQA) algorithm using two alternative maps [6]. Since key mismatches may still occur, a reconciliation step [3], using, for example, LDPC codes, is required to obtain exactly the same shared key bits between Alice and Bob. This part of the whole SKG mechanism is not considered in the present work, since it is not expected to specifically impact the SKG performance in relation to the radio channel characteristics.

Although the most common channel metric used in SKG is the received signal strength [13, 14, 18, 24] because this parameter is widely accessible in most radio receivers, it only partially exploits the channel information and the entropy of the generated keys is not very high. Alternatively, the channel phase information has been investigated and found to generate more random and secure stream of bits, such as in [25, 26]. Another candidate for SKG is the channel impulse response (CIR) of UWB channels, whose ability to support SKG techniques has been proved experimentally [8, 27, 28]. Nevertheless, we can efficiently establish sufficient long and random key bits by exploiting more channel information at once, which is achieved by making use of the joint real and imaginary parts of channel coefficients (complex CSI) [6].

In the present work, we chose this option and based the SKG mechanism on the CQA algorithm [6]. At each time instant, Alice chooses and sends Bob publicly an adaptive map index, for which the current channel observation is less sensitive to mismatches between Alice and Bob keys, without revealing any relevant information to Eve. To that aim, the quantization regions (QRs) of Alice's map are computed by quantifying the cumulative distribution functions (CDFs) of each of the aggregated real and imaginary parts of CSI into $\sqrt{M}$ statistically equal quantization intervals, resulting in M QRs. Then, each alternative map of Bob results from the shifting of quantization thresholds with the same probability in a different direction (please refer to [6] for further insights).

Figures 5(a) and 5(b) depict a particular channel realization in the complex I-Q plane and show Alice's map by presenting the correspondence between symbols and QRs, both for $M = 4$ and $M = 16$. The interest of increasing M is to establish a certain length of key with less required channel samples. However, as seen in [29], this yields an increase in the bit disagreement between legitimate users keys, which complicates in turn the key reconciliation step. Hence, increasing M requires an improvement in the signal-to-noise ratio (SNR) in order to alleviate the key reliability issue [29].

In [6], the effectiveness of the CQA algorithm for complex Gaussian channels is analyzed first in terms of bit disagreement between keys extracted by Alice, Bob, and Eve and secondly in terms of randomness, without testing, but by relating it to the independence between the real and imaginary parts of Gaussian channels. In a previous preliminary work [29], we have studied the reliability and the confidentiality of the wireless data transmission by computing the disagreement between keys bits, employing CQA on the channels whose measurements are explained in Section 2. The keys have been extracted from spatially variant channels at 5.4 GHz and the results have been discussed in terms of the impact of narrow band or WB channels on key randomness based security. In [11], the lack of spatial stationarity between Bob and Eve is addressed in terms of both theoretical bounds and keys bits disagreement. In [30], a novel security mechanism combining SKG and "tag signals" has been proposed, without deep analysis on key randomness quality. Here, we focus on a global understanding of the key randomness and security performance, according to the various features of the radio channel. Further, we do not consider the presence of Eve, which has been already considered in [10, 11, 29, 30].

Table 2: NIST tests limitations.

Monobit frequency	$N \geq 100$
Block frequency	$N \geq 100$
Runs	$N \geq 100$
Serial	$m < \lfloor \log_2 N \rfloor - 2$
Approximate entropy	$m < \lfloor \log_2 N \rfloor - 5$

4. NIST Test Suite for Key Randomness Evaluation

The fact that key bits are not statistically independent reduces the key quality since in an information-theoretic framework Eve may exploit any useful information to collapse the key space. In this context, the source of randomness, in addition to the admitted quantization algorithm, is the most critical aspect that mainly affects the key robustness behavior. Hence, we aim to assess the security performance in terms of randomness, which can be achieved using the NIST test suite [16]. We notice that these tests are not able to prove the perfect randomness of a key. However, each test shows whether the key bits follow a certain expected behavior owing to key generation process [20]. There are 16 statistical tests in total, but we are not able to apply all these tests owing to limitations on the requirement of each tested key length. Table 2 shows length limitations for some tests applied in this paper where m is the length in bits of the bit strings used in each test and N is the key length in bits. The remaining tests require very long keys and do not apply to the physical layer based wireless security scheme we here target.

Some tests try to show whether the sequence of bits has the statistical properties of a random sequence. Consistently, the "monobit frequency" and the "block frequency" tests investigate these randomness criteria on, respectively, the entire key bits and in subblocks. For example, if we consider the following sequence of N bits,

$$\underbrace{00\cdots00}_{N/4}\,\underbrace{10\cdots10}_{N/4}\,\underbrace{11\cdots11}_{N/4}\,\underbrace{01\cdots01}_{N/4}, \tag{1}$$

we notice that it passes the monobit frequency test since 0 and 1 are equiprobable bits in the whole sequence whereas it is not the case in subblocks where too many bits equal either to 0 or to 1 may be present, leading to failure of the block frequency test. Another test, that is, the "runs" test, checks whether the frequency of runs, that is, uninterrupted strings of identical bits either 0 or 1, is as expected for a random sequence. In other words, it determines whether the transition between bits 0 and 1 is too fast or too slow. Accordingly, the sequence in the above example is considered random since the number of runs is very close to that expected for a random sequence (i.e., $N/2$ runs). However, the sequence

$$\underbrace{00\cdots00}_{N/3}\,\underbrace{11\cdots11}_{N/3}\,\underbrace{00\cdots00}_{N/3} \tag{2}$$

is not random since only 3 runs are computed.

Both the "approximate entropy" (ApEnt) test and the "serial" test focus on the frequency of occurrences of all possible overlapping 2^m strings of m-bit length each, across the entire key bits. Their purpose is to compare the frequency of overlapping strings of several consecutive lengths against the expected result for a random sequence. For that, the ApEnt test uses two consecutive lengths (m and $m+1$) while the serial test uses three consecutive lengths (m, $m-1$, and $m-2$). Moreover, the serial test differs from the ApEnt test by the fact that longer bit strings can be used in the former for the same key length, as shown in Table 2. According to both the ApEnt test with $m = 1$ and the serial test with $m = 2$, the first sequence example is supposed to be random since strings of 2 bits are almost equiprobable whereas the second key example fails these two tests. Furthermore, if we consider strings of higher lengths, the first sequence may fail the tests. More information about these statistical tests can be found in [16].

For a single key, each randomness test indicates whether the key is accordingly random or not. Furthermore, in order to relate the quality of the randomness to the features of the radio channel, a set of generated keys is tested by each randomness test, which returns a percentage of sequences passing the test. Then, we computed the "mean pass rate" by averaging the percentages of sequences passing each NIST test and thus over all the applied statistical tests, which provides a global assessment of the randomness for each specific scenario. In the computation of the mean pass rate, we exclude the monobit frequency test for reasons explained in Section 6.

5. Channel Variability in SKG

In practice, a long secret key results from the concatenation of symbols derived from several estimated channel samples. Hence, channel variability is a crucial requirement to establish long random secret key bits. The quality of the key in part depends on the statistical independence between key bits, which to some extent can be reduced to the lack of correlation between channel samples. Such independence stems from sufficiently separated samples, in whatever domain sampling might be, which involves the physical propagation mechanisms and characteristics of the radio environment. In this part, we investigate the impact of the space, time, frequency, and joint space-frequency degrees of freedom on the SKG performance.

5.1. Space versus Time Variability. Space variability stems from several differing positions for a single antenna or (although coupling and other effects can disturb this simple picture) from several antennas (multiantenna channel). Time variability can simply result from one given antenna being moved over differing positions, in which case it is generally equivalent to spatial variability. This is valid in, so far as the velocity is small enough, that when multiplied by the CIR delay spread, the result is much smaller than the wavelength (in other words, the channel can be assumed to be static over the CIR duration). Time variability can also come from movement of scatterers (such as vehicles in outdoor scenarios or pedestrians in indoor scenarios [31]) in

Table 3: Frequency channel characteristics for each BW.

BW (MHz)	Number of subcarriers	Number of data subcarriers	Subcarrier separation (MHz)
20	64	52	0.3125
40	128	108	0.3125
80	256	243	0.3125
160	512	468	0.3125

the surroundings of the transmitter and the receiver. This type of time variability is not equivalent to spatial variability.

In TPT measurements, spatial variability is provided by the movement of Alice over the 11×11 square grid as explained in Section 2, which is equivalent to the first type of time variability. These 121 antenna positions allow testing the SKG performance provided by spatial degrees of freedom, where Alice's antenna can take random positions over the grid, providing as many N_S complex channel coefficients in order to construct $(N = N_S \log_2 M)$-bit key at a given frequency. Hence, we randomly choose to construct 60 sets of random Alice positions for each Bob's position and each available frequency in the 20 MHz bandwidth. A statistical distribution can then be computed over Bob's positions, over the frequencies in the 20 MHz bandwidth, and over the 60 random sets of Alice positions.

5.2. Frequency Variability. In real world applications, a spatial degree of freedom may not always be available (e.g., in single antennas links with very stable channels). In such a case, SKG is not applicable unless we find another source of channel variability, hence the need to exploit the frequency variability existing in WB channels.

In order to investigate SKG performance in frequency variant channels, the data has been processed consistently with the 802.11a/g/n/ac standard, that is, in order to obtain complex channel coefficients at the required number of subcarriers for each bandwidth BW as shown in Table 3. For that purpose, the measurements were frequency interpolated. Moreover, for the same WIFI standard consistency, we discarded the channel coefficients at frequencies responsible for transmitting pilot bits and we kept only those at data transmitting frequencies. Table 3 shows some frequency channel characteristics for each bandwidth and according to the same standard.

Given these parameters, not all the subcarriers need to be used to generate keys of enough bit length; then comes the question of how to choose the subcarriers. Intuitively, more correlation is likely to occur when the frequency difference between two channel coefficients is reduced. Unless the ratio between the number of available and the number of required subcarriers is an integer, there is no unique and obvious way to choose the subcarriers used in the SKG process. Hence, Alice chooses randomly a set of N_f frequency subcarriers, from which $(N = N_f \log_2 M)$-bit key is extracted, and she sends publicly this set to Bob. Although this information is transmitted also to Eve, it is not very relevant since it does not indicate any information about the key. Finally, a set of secret keys is obtained over Bob's positions, over the 121 positions of Alice, and over the random sets of subcarriers (arbitrarily taken to be 10 sets).

5.3. Joint Space-Frequency Variability. Intuitively, with smaller coherence bandwidth, the SKG will be able to more efficiently exploit frequency variability. Unfortunately, the coherence bandwidth changes from an environment to another and is out of control. SKG performance should be achieved also in environments where the coherence bandwidth is small, which is a difficulty when no sufficient spatial variability is provided. As a way of mitigation, we here consider the possibility to exploit jointly the space and frequency degrees of freedom, so as to relax the requirements on each of both individually. A potential use case is that of MIMO systems (such as IEEE 802.11n/ac), providing spatial variability, together with OFDM technology providing frequency variability.

Based on the features of the TPT campaign, spatial variability is provided by considering either every two consecutive Alice positions on each row of the grid or each four-square consecutive Alice position on every two consecutive rows of the grid, as an array antenna resulting, respectively, in either 110 sets of 2-array antennas or in 100 sets of 4-square array antennas. More clearly, the vector

$$V = \left[X_1^1, \ldots, X_1^{N_{\text{ant}}} \cdots X_i^1, \ldots, X_i^{N_{\text{ant}}} \cdots X_{N_f}^1, \ldots, X_{N_f}^{N_{\text{ant}}}\right] \quad (3)$$

is used to construct a single key of length $N = N_{\text{ant}} N_f \log_2 M$, where N_{ant} is the number of array antennas. $X_i^1, \ldots, X_i^{N_{\text{ant}}}$ together form N_{ant}-array antennas at the ith chosen frequency. Finally, a set of keys is obtained over Bob's positions, over the sets of N_{ant}-array antennas, and over the 10 sets of randomly chosen subcarriers.

6. Results

In the following, we use a fixed key length ($N = 128$) in the key randomness quality evaluation, with the exception of the pure spatial variability case where a comparison between different key lengths is carried out. For each channel variability type, a statistical distribution over the extracted keys is formed, as explained in Section 5, in order to compute a mean pass rate using the NIST tests. Table 4 shows the number of tested keys for each type of channel variability.

Whatever the source of channel variability used to generate the key, our results show that all the keys pass the monobit frequency test. This is due to the statistically equal quantization intervals on each I and Q, used to transform channel coefficients into discrete sequences of bits through CQA. Consequently, all the strings (of length $\log_2 \sqrt{M}$) have the same probability to occur and, equivalently, the probability to have either bit 0 or bit 1 is 1/2. Accordingly, we exclude the monobit frequency test when we compute the mean pass rate.

Table 4: Size of key set versus the variability type.

Variability	Number of keys		
	LOS	NLOS	Total
Space	36720	13500	50220
Frequency	82280	30250	112530
Joint space-frequency			
$N_{ant} = 2$	74800	27500	102300
$N_{ant} = 4$	68000	25000	93000

For $N = 128$ and according to Table 2, we chose $m = 1$ for the ApEnt test and both $m = 3$ and $m = 4$ for the serial test. CQA results in equiprobable nonoverlapping strings of length 2 bits for $M = 16$, while it is not the case for $M = 4$. Consequently, on the one hand, the percentage of sequences passing the ApEnt test is very high for $M = 16$ whatever the channel variability type while that of the serial test is smaller especially for frequency variability with BW = 20 MHz (starting from a percentage of 0.3533). On the other hand, for $M = 4$, the passing of the ApEnt test depends mainly on the correlation between I and Q of the channel coefficients. It also depends on the correlation of the used subsequent channel coefficients. Therefore, the worst case is considered for LOS case exploiting frequency variability with BW = 40 MHz and thus with a percentage of 0.7273. Moreover, small mean pass rates for $M = 4$ stem from the approximately complete fail of serial tests.

6.1. Spatial Variability

6.1.1. Key Length Effect. Figure 6 represents the mean rate of key sequences passing the chosen selection of NIST tests and for both $N = 128$ and $N = 242$. The spatial channel variability is used here to construct the key of N bits with $M = 4$. $N_S = 64$ and $N_S = 121$ channel samples are needed to, respectively, construct a 128-bit key and 242-bit key. Whatever the used frequency, it is shown that shorter keys better profit from the channel randomness. While maintaining the same M, we need more channel samples in order to construct a longer secret key and consequently the probability to have more correlated samples increases, yielding bits with more correlations.

6.1.2. Carrier Frequency Effect. Figure 7 shows the mean pass rate for $N = 128$, for both 5.4 GHz and 2.4625 GHz bands, and with respect to LOS/NLOS cases. The impact of carrier frequency is not really meaningful in Figures 6 and 7 since the mean pass rates are very high, that is, nearly 1, in good part owing to the random positions taken by Alice over the grid. Nonetheless, this impact may be shown for the worst-case scenario corresponding to consecutive Alice positions over the regular grid, and thereby the 5.4 GHz band offers more random keys than 2.4625 GHz band. Indeed, the distance between two adjacent Alice positions on the grid corresponds almost to $\lambda/2$ at 5.4 GHz and to $\lambda/4$ at 2.4625 GHz, while $\lambda/2$ typically corresponds to the coherence distance over which channels are statistically well decorrelated in omnidirectional scenarios, resulting in extracted bits with a good level of independence.

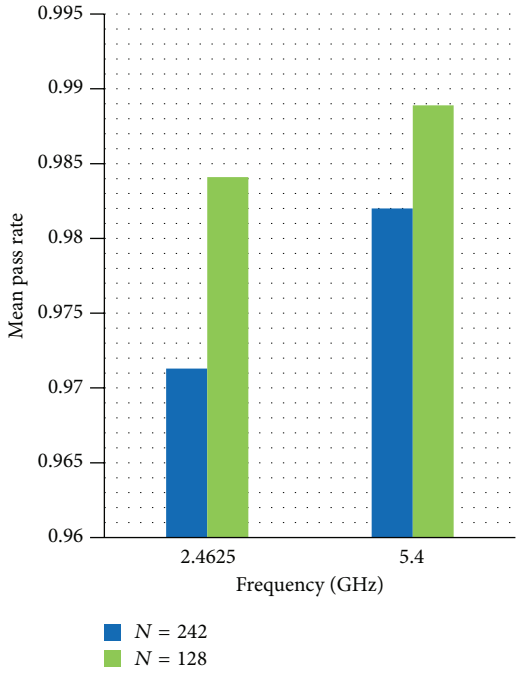

Figure 6: Mean pass rate exploiting spatial variability for both $N = 128$ and $N = 242$.

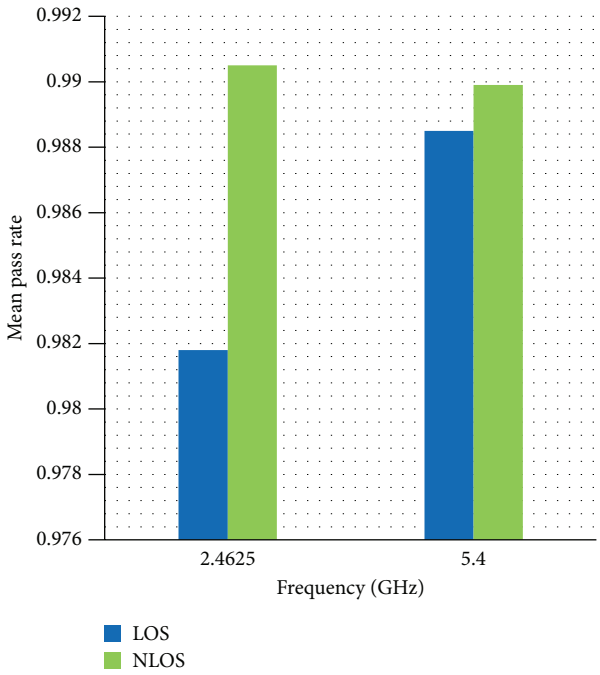

Figure 7: Mean pass rate exploiting spatial variability with respect to LOS/NLOS and for $N = 128$.

6.1.3. LOS/NLOS Effect. The key randomness is enhanced in NLOS propagation conditions, as shown in Figure 7, due to

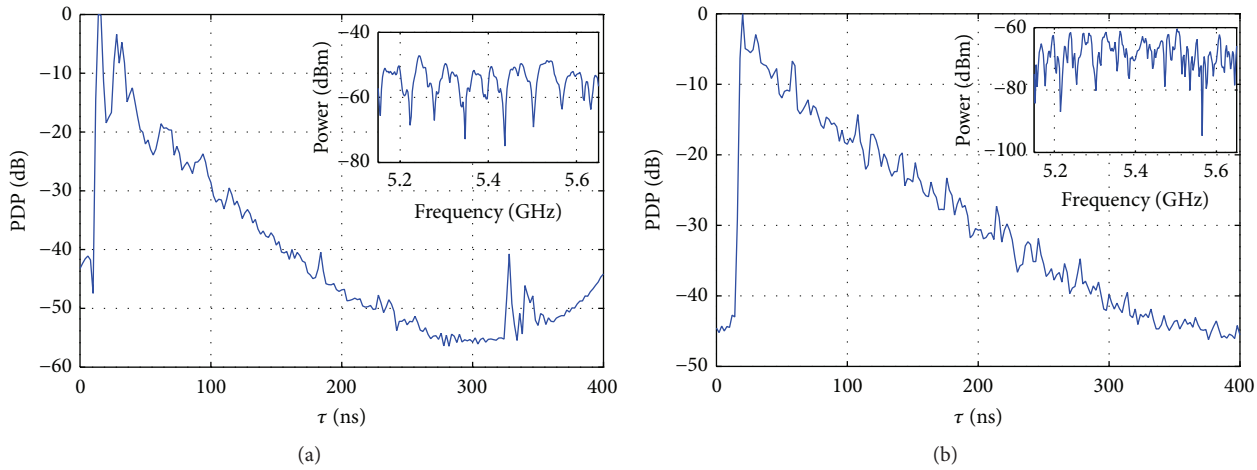

Figure 8: Examples of PDPs and channel transfer functions: (a) LOS, (b) NLOS.

the lack of a dominant path yielding then more fluctuation of the channel transfer function than in LOS cases.

Briefly speaking, it is noteworthy that in all cases the mean pass rate is very high, indicating that the spatial degree of freedom is suitable for random key generation. As discussed above, spatial variability can be translated into time variability through a random movement of Alice in space, providing adequate key randomness. As an extra advantage, such a time variant scheme would make it difficult for Eve to track accurately Alice's positions, reducing her ability to gather deterministic information about the channel characteristics and to guess the sequence of bits.

6.2. Frequency Variability. A quantitative measure of the key randomness behavior with respect to the frequency variability domain can be found from the analysis of the root mean square (RMS) delay spread τ_{rms} and consequently of the coherence bandwidth which typically varies inversely to the RMS delay spread. For each position of Alice over the square grid, CIR is computed by taking inverse Fourier transforms of the frequency responses recorded over 500 MHz bandwidth centered on either 2.4625 GHz or 5.4 GHz band and filtered with a Hamming window. The power delay profile (PDP) $P(\tau)$ is then the average of the 121 squared CIRs computed over the grid. Therefore,

$$P(\tau) = E\left\{\left|h(\vec{\mathbf{r}}, \tau)\right|^2\right\}, \tag{4}$$

where $h(\vec{\mathbf{r}}, \tau)$ and τ are, respectively, the space-varying complex CIR and the path delay. $E\{\cdot\}$ denotes the expectation over the space domain $\vec{\mathbf{r}}$. Subsequently, τ_{rms} is calculated as follows:

$$\tau_{\text{rms}} = \sqrt{\frac{\int_0^{\tau_{\max}} (\tau - \overline{\tau})^2 P(\tau)\, d\tau}{\int_0^{\tau_{\max}} P(\tau)\, d\tau}}, \tag{5}$$

where $\tau_{\max}$ and $\overline{\tau}$ are, respectively, the maximum excess delay and the mean delay. The latter is defined as follows:

$$\overline{\tau} = \frac{\int_0^{\tau_{\max}} \tau P(\tau)\, d\tau}{\int_0^{\tau_{\max}} P(\tau)\, d\tau}. \tag{6}$$

Only multipath components with amplitude within 20 dB from the peak of each PDP are included in the computation of τ_{rms} and $\overline{\tau}$. Figure 8 shows two examples of normalized measured PDPs and their corresponding frequency responses for both LOS and NLOS cases. It is clear that the NLOS PDP is rich in multipath components and thereby exhibits higher delay spread than the LOS one having a few dominant peaks at short delays. Figure 9 plots the variation of τ_{rms} as a function of the distance, both for LOS and NLOS cases.

We assess key randomness exploiting frequency variability while maintaining the same key length; that is, $N = 128$ bits. To this end, we determine the number of subcarriers N_f used for SKG according to M; that is, $N_f = 64$ for $M = 4$ and $N_f = 32$ for $M = 16$. Figure 10 shows the variation of the mean pass rate as a function of the distance between Alice and Bob at 5.4 GHz band, for different bandwidths and for both LOS and NLOS conditions. We note that 128 key bits cannot be extracted by exploiting the frequency variability in BW = 20 MHz when $M = 4$. Figure 11 considers the impact of the carrier frequency on the key randomness behavior for BW = 40 MHz and $M = 16$.

6.2.1. Both LOS/NLOS and Distance Effect. Figure 10 shows that the higher the separation distance between Alice and Bob, the higher the mean pass rate, especially for LOS channels or for small values of M. Moreover, NLOS channels provide statistically more random secure key bits as seen in Figures 10 and 11. The same behaviors are noticed in Figure 9 with respect to the delay spread. Hence, the improvement of the mean pass rate is explained by an increase of τ_{rms} indicating a reduction in the coherence bandwidth, which yields less channel correlations for close frequency responses. Furthermore, the advantage of NLOS channels over the LOS

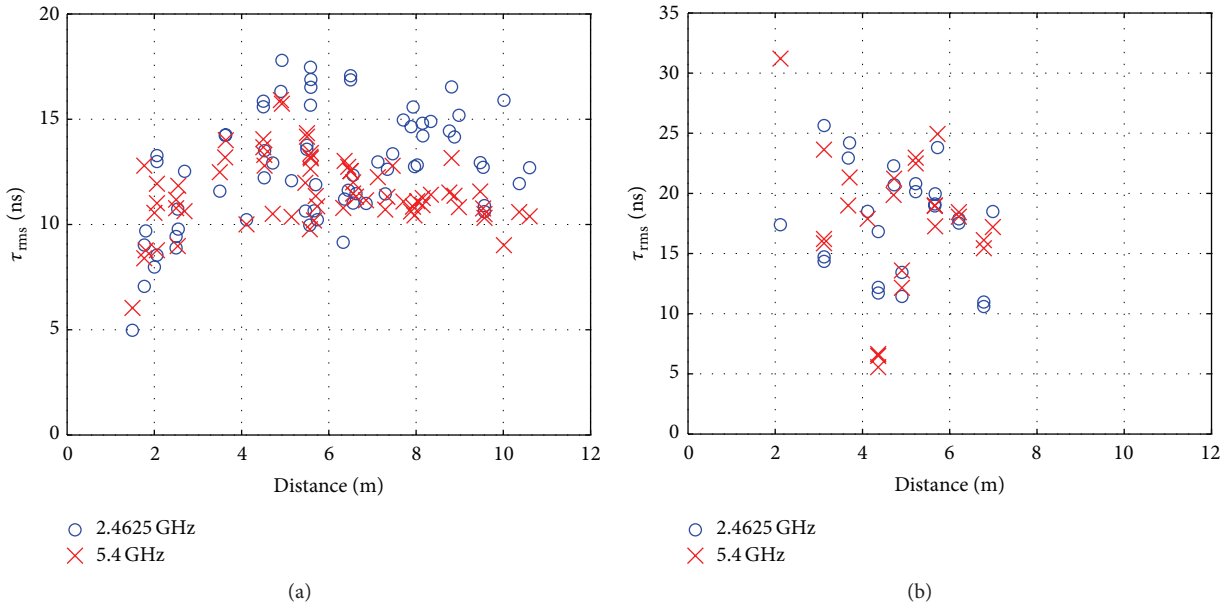

FIGURE 9: Variation of the RMS delay spread τ_{rms} with the distance: (a) LOS, (b) NLOS.

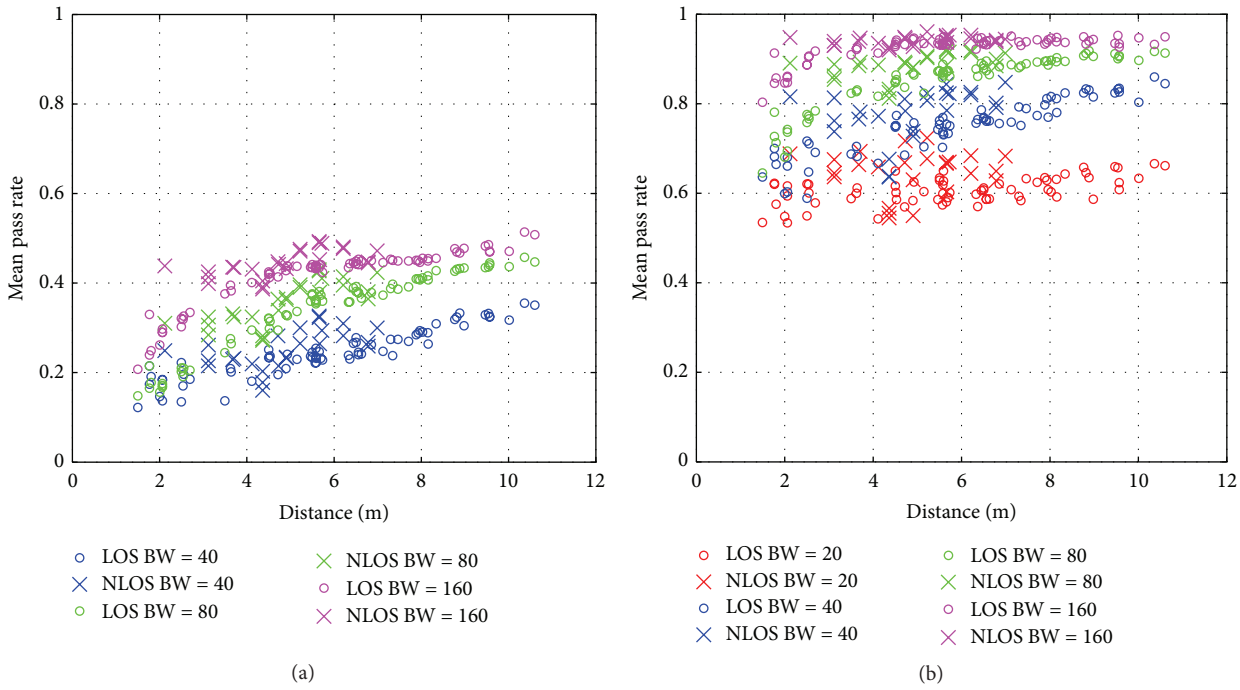

FIGURE 10: Mean pass rate as a function of the distance for 5.4 GHz and for frequency variability: (a) $M = 4$, (b) $M = 16$.

ones in providing random keys comes from the multipaths richness of the former: the lack of proper Rayleigh fading reduces the channel variability in the frequency domain and creates insufficient randomness for a satisfactory success to NIST tests. Nonetheless, τ_{rms} takes relatively small values ranging from 5 ns to 30 ns due to the open and little cluttered environment of TPT investigated locations. These values are consistent with typical ones for indoor environments; see, for example, [32]. An improvement in mean pass rate is thus expected for richer scattering environments.

6.2.2. Bandwidth Effect. Larger available bandwidths yield larger separation of the subcarriers used for SKG and consequently smaller correlations. This results in improved key randomness, as seen in Figure 10. Figures 12 and 13 illustrate

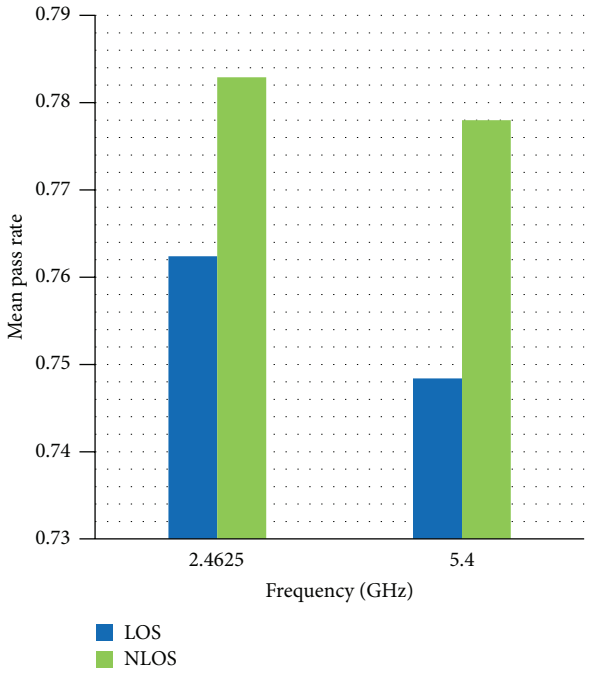

FIGURE 11: Mean pass rate exploiting frequency variability for BW = 40 MHz and $M = 16$.

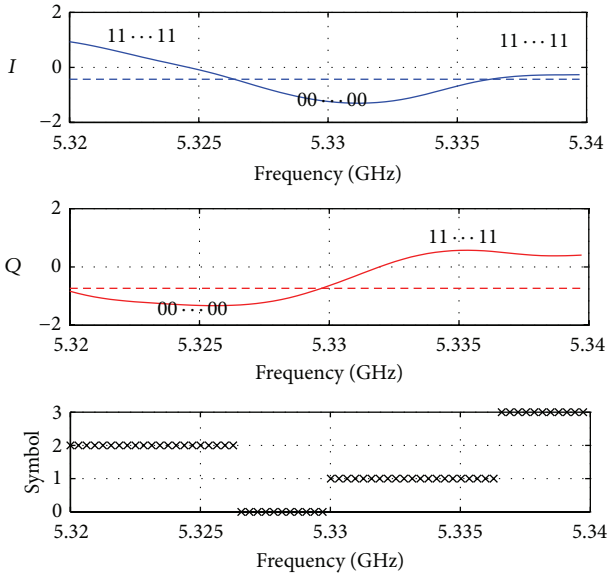

FIGURE 12: Example illustrating SKG from very close channel responses, for $M = 4$.

two examples of key generation from, respectively, very close and very far spaced channel responses, for $M = 4$. It is clear that more randomness is provided by the case where the channel coefficients are very far spaced where the SKG profits from the whole bandwidth while the efficient bandwidth is reduced in the other case yielding a key with poor randomness.

6.2.3. Carrier Frequency Effect. As seen in Figure 11, the carrier frequency affects the key randomness behavior just

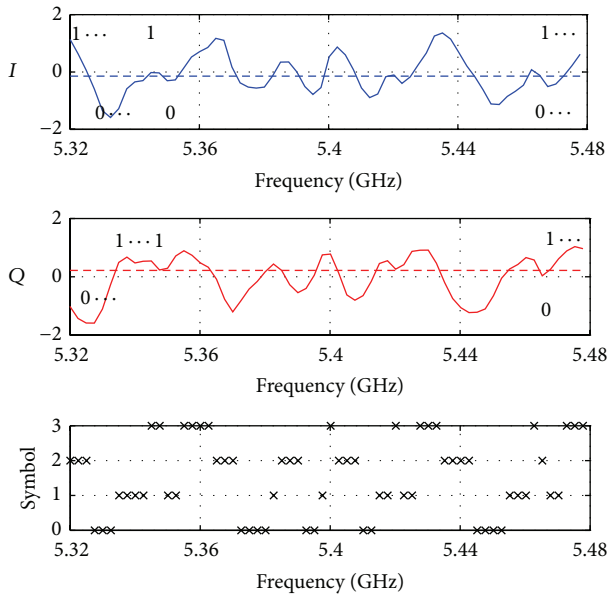

FIGURE 13: Example illustrating SKG from far spaced channel responses, for $M = 4$.

for LOS channels where higher mean pass rates are seen for the smallest carrier frequency (i.e., 2.4625 GHz). This is explained by the decrease in the coherence bandwidth or equivalently by the increase in the RMS delay spread, when the frequency gets lower, as shown in Figure 9(a). Furthermore, as displayed in Figure 9(b), τ_{rms} does not change with the frequency for NLOS channels. The behavior of τ_{rms} with the carrier frequency is consistent with results obtained in [33, 34]. However, the difference in mean pass rates is weak, implying that there is no strong preference between the low and high WIFI band from this point of view. Still, the fact that the low band is limited to 20 MHz bandwidth while the high band reaches 160 MHz provides a clear advantage for SKG, given the above results.

6.3. Joint Space-Frequency Variability. Figure 14 compares the mean pass rate for the three types of channel variability in the 5.4 GHz band for both $M = 4$ and $M = 16$. The full space variability provides the most robust keys and thereby the most suitable source for SKG. However, such a scheme either would require the terminal mobility over all the scanned positions before generating a key or would need those many antennas in a stable scenario. Therefore, we now assess the security provided by joint space-frequency variability, for both $N_{\text{ant}} = 2$ and $N_{\text{ant}} = 4$, which relaxes such requirements. Indeed, this scheme provides more random keys, especially with $N_{\text{ant}} = 4$, than the pure frequency domain variability, which stems from the larger average difference between frequency channels and the resulting reduced correlations between channel coefficients. Simply stated, for fully decorrelated antenna signals, the increase in N_{ant} reduces the bandwidth requirements. This is a very encouraging result for the effectiveness of SKG toward physical layer security. Since many wireless devices

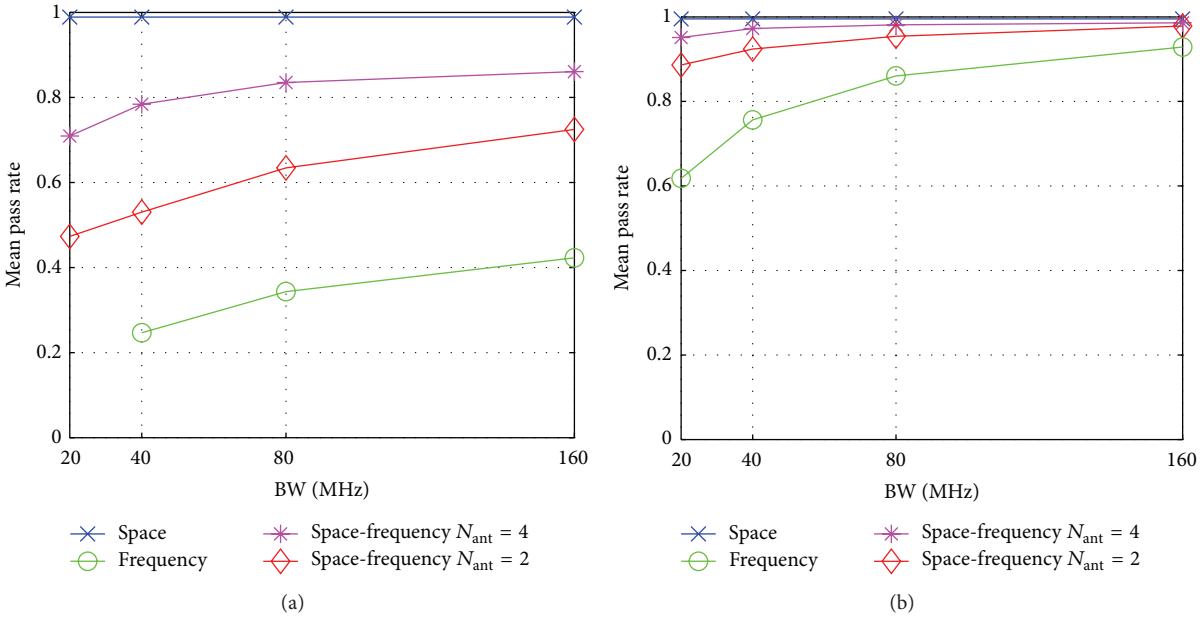

FIGURE 14: Comparison of key randomness in different channel variability at 5.4 GHz: (a) $M = 4$, (b) $M = 16$.

(for 3G, 4G, WIFI, etc.) tend to be multiantenna systems, such a solution will certainly be more and more feasible in the short term future. We also stress the importance of increasing M, which well improves the key randomness despite the requirement of a high SNR.

7. Conclusion

In this paper, we presented a study of SKG and of key randomness by exploiting different degrees of freedom in the channel characteristics, based on space, frequency, and joint space-frequency variability. The random character of the key has been evaluated using the statistical NIST tests and the analysis has been targeted to relate this randomness to major channel features such as LOS/NLOS propagation and the nature of the radio environment. To this end, a set of indoor radio channel measurements have been carried out and the data coefficients have been processed using the CQA algorithm in order to construct secure keys of suitable length.

The results showed that the spatial variability, in particular in small area confined to spatial fading, is very efficient in ensuring random keys for the shared secret key. However, since the spatial variability is a difficult requirement to occur in real daily life, it is better to exploit another channel variability which could be the frequency variability. In this work, we have specifically focused on 802.11a/g/n/ac standards, which impose limitations on the bandwidth and on the set of usable subcarriers. Under this constraint, we showed that the frequency variability by itself may not be enough to support high randomness SKG, especially when the coherence bandwidth is large for short distances in environments with little scattering/reverberation. An alternative approach is to exploit jointly the spatial and frequency degrees of freedom, which relaxes the constraints on the frequency variability of the channel or, said differently, on the nature of the radio environment.

We noticed that randomness is improved for NLOS scenario cases but also that the presence of a strong or significant LOS component reduces the variability, especially in the frequency domain, and makes the extracted keys less random. While we have used in this work omnidirectional antennas, it can be expected that directional antennas will further impact the level of security brought about by SKG, although this will very much depend on the type of antennas used by Alice/Bob/Eve and will need further investigations. Finally, we stress the importance of applying a multibit extraction algorithm when the SNR and channel estimation errors allow, since this effectively improves key randomness.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work has been supported by the PHYLAWS project (EU FP7-ICT 317562 [35]). The authors are grateful to Francesco Mani for his contribution to the measurements in TPT premises.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 3rd edition, 2003.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[6] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010.

[7] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proceedings of the IEEE International Symposium on Information Theory*, pp. 2593–2597, IEEE, Seattle, Wash, USA, June 2006.

[8] M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. A. B. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in *Proceedings of the 6th Annual Communication Networks and Services Research Conference (CNSR '08)*, pp. 88–95, Halifax, Canada, May 2008.

[9] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.

[10] T. Mazloum, F. Mani, and A. Sibille, "A disc of scatterers based radio channel model for secure key generation," in *Proceedings of the 8th European Conference on Antennas and Propagation (EuCAP '14)*, pp. 1290–1294, IEEE, The Hague, The Netherlands, April 2014.

[11] T. Mazloum and A. Sibille, "Performance of secret key generation in non stationary channels," in *Proceedings of the 9th European Conference on Antennas and Propagation (EuCAP '15)*, Lisbon, Portugal, April 2015.

[12] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th Annual ACM International Conference on Mobile Computing and Networking (MobiCom '09)*, pp. 321–332, Beijing, China, September 2009.

[14] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[15] T. Ohira, "Secret key generation exploiting antenna beam steering and wave propagation reciprocity," in *Proceedings of the European Microwave Conference*, pp. 9–12, Paris, France, October 2005.

[16] W. Burr, D. Dodson, and W. Polk, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Information Technology Laboratory, NIST Information Technology Laboratory, Gaithersburg, Md, USA, 2010.

[17] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th Annual International Conference on Mobile Computing and Networking (MobiCom '08)*, pp. 128–139, San Francisco, Calif, USA, September 2008.

[18] G. R. Tsouri and J. Wilczewski, "Reliable symmetric key generation for body area networks using wireless physical layer security in the presence of an on-body eavesdropper," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL '11)*, pp. 1–6, ACM, Barcelona, Spain, October 2011.

[19] S. Y. Baek and J. Park, "A study on wireless secret key randomness in multiuser networks," in *Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC '13)*, pp. 1048–1052, Jeju, South Korea, October 2013.

[20] I. Tunaru, B. Denis, and B. Uguen, "Random patterns of secret keys from sampled IR-UWB channel responses," in *Proceedings of the IEEE International Conference on Ultra-WideBand (ICUWB '14)*, pp. 74–79, Paris, France, September 2014.

[21] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN '10)*, pp. 70–81, Stockholm, Sweden, April 2010.

[22] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part III: privacy amplification," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 839–851, 2003.

[23] H. Ghannoum, S. Bories, C. Roblin, and A. Sibille, "Biconical antennas for intrinsic characterization of the UWB channel," in *Proceedings of the IEEE International Workshop on Antenna Technology: Small Antennas and Novel Metamaterials (IWAT '05)*, pp. 101–104, March 2005.

[24] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proceedings of the IEEE INFOCOM*, 9, p. 1, San Diego, Calif, USA, March 2010.

[25] A. Sayeed and A. Perrig, "Secure wireless communications: secret keys through multipath," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '08)*, pp. 3013–3016, Las Vegas, Nev, USA, April 2008.

[26] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proceedings of the IEEE INFOCOM*, pp. 1422–1430, Shanghai, China, April 2011.

[27] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[28] M. G. Madiseh, S. He, M. McGuire, S. Neville, and S. Dong, "Verification of secret key generation from UWB channel observations," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–5, IEEE, Dresden, Germany, June 2009.

[29] T. Mazloum, F. Mani, and A. Sibille, "Analysis of secret key robustness in indoor radio channel measurements," in *Proceedings of the IEEE 81st Vehicular Technology Conference (VTC Spring '15)*, pp. 1–5, Glasgow, Scotland, May 2015.

[30] R. Moliere, F. Delaveau, C. L. K. Ngassa, C. Lemenager, T. Mazloum, and A. Sibille, "Tag signals for early authentication and secret key generation in wireless public networks," in *Proceedings of the European Conference on Networks and Communications (EuCNC '15)*, pp. 108–112, Paris, France, June 2015.

[31] P. Barsocchi, S. Chessa, I. Martinovic, and G. Oligeri, "A cyber-physical approach to secret key generation in smart environments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 4, no. 1, pp. 1–16, 2013.

[32] D. Tholl and H. Hashemi, "Statistical modeling and simulation of the RMS delay spread of indoor radio propagation channels," *IEEE Transactions on Vehicular Technology*, vol. 43, no. 1, pp. 110–120, 1994.

[33] T. Jamsa, V. Hovinen, A. Karjalainen, and J. Iinatti, "Frequency dependency of delay spread and path loss in indoor ultra-wideband channels," in *Proceedings of the Institution of Engineering and Technology Seminar on Technologies and Applications in Ultra Wideband Systems*, pp. 254–258, London, UK, April 2006.

[34] S. Geng and P. Vainikainen, "Frequency and bandwidth dependency of UWB propagation channels," in *Proceedings of the IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '06)*, pp. 1–5, IEEE, Helsinki, Finland, September 2006.

[35] http://www.phylaws-ict.org/.