This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Effect of Radio Channel and Antennas on Physical-Layer-Security Key Exchange

ALESSANDRO SANTORSOLA[1], MARCO ZOLI[2], ANDRÉ N. BARRETO[2] (SENIOR MEMBER, IEEE), VINCENZO PETRUZZELLI[1], AND GIOVANNA CALÒ[1] (MEMBER, IEEE)

[1]Department of Electrical and Information Engineering, Polytechnic University of Bari, Bari, Italy (e-mail: giovanna.calo@poliba.it - alessandro.santorsola@outlook.it)
[2]Barkhausen Institut, Dresden, Germany (e-mail: marco.zoli@barkhauseninstitut.org)

Corresponding author: Giovanna Calò (e-mail: giovanna.calo@poliba.it).

ABSTRACT The wireless channel is inherently an open medium which exposes wireless communication users to the risk of interception. The vulnerabilities of the wireless channel have led to the search for innovative and efficient security solutions at different levels of the network protocol. In particular, the physical layer level allows for implementing some security functions, such as key generation and exchange, by exploiting the intrinsic randomness of the wireless communication channel. In this paper, we analyze the effect of wireless channel and of antenna characteristics on physical layer security (PLS) key generation. The aim is to put in evidence the relation between physical quantities, such as radio channel characteristics or antenna directivity, with higher level secrecy performance indicators, such as the key mismatch between the different communication nodes and the key randomness. For this purpose, we developed a comprehensive numerical model, which implements all the different steps, from signal generation and wireless propagation modeling to key generation through spectral quantization. The reported results show that the multipath richness of the radio channel, as in outdoor urban scenarios, improves the PLS secrecy performances with respect to simpler propagation scenarios. Moreover, we show that the use of more directive antennas in the legitimate communication link improves secrecy. An opposite effect is achieved when the directivity of the eavesdropper antenna is increased, thus improving its ability to perform passive attacks.

INDEX TERMS Antennas and propagation, Computational electromagnetics, Electromagnetic propagation, Key generation, Physical-Layer Security, Radio channel.

I. INTRODUCTION

WIRELESS communication networks provide today important digital infrastructures for our society with seamless connectivity and reliable services. Thanks to their flexibility, wireless mobile systems are becoming more and more pervasive, especially for emerging applications such as Internet of things (IoT), smart homes/buildings/cities, Industry 4.0, vehicle-to-vehicle communication, as well as e-Health. Given the "open" nature of the wireless communications, it is clear today more than ever the need for efficient solutions for communications security and privacy. These solutions should guarantee reliable information exchange between an information source (i.e. Alice) and a legitimate receiver (i.e. Bob) and, at the same time, authentication, confidentiality and integrity with respect to any other malicious node (i.e. Eve).

A well-assessed way to secure communication between two nodes is encryption/decryption, which relies on mathematical complexity. However, conventional key exchange protocols, such as the Diffie-Hellman (D-H) one, can require significant computation effort. The effort needed can become even higher to contrast the ever-increasing computing resources of the attacker. In fact, as a countermeasure, the key can be lengthened to increase security at the expenses of a larger computation overhead [1], [2]. In many applications, the computation overhead constraint is stringent since many new technologies rely on low-cost and low-energy devices that cannot afford the computational complexity of conventional protocols. Some examples of these applications are Internet of Things (IoT), sensor networks, cognitive radio networks,

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

and vehicular networks [1], [3], [4], [5]. In this kind of scenarios, the physical-layer key-generation schemes are considered very promising since they do not require expensive computations.

Physical layer security (PLS) has been studied to provide an innovative form of security for wireless networks. Unlike classical cryptography, key-based PLS techniques relay on the inherent randomness of the wireless channel to generate encryption keys without requiring expensive computation [1]. This approach differs also from key-less PLS techniques, which for example exploit beam forming or artificial noise injection to degrade the signal in directions different from the one of intended communication [6] and that do not use the physical layer for key generation.

In fact, a critical step in the majority of security systems is the establishment of authenticated keys, which is, for instance a central requirement for IoT security.

The PLS encryption schemes can be regarded as a cross-layer solution that combines the secret key generation and exchange at the physical layer and the encryption/decryption at the application layer [1]. Moreover, in PLS encryption, the key exchange is performed between the two legitimate nodes without the need of involving third parties for generation and certification of public keys. This makes the process lighter and faster. The keys are also updated autonomously by the legitimate nodes, thus easing the implementation of security protocols. This feature is particularly advisable for IoT applications.

Thanks to the radio channel properties of spatial decorrelation and reciprocity, the same radio channel realization can be observed by two legitimate communicating devices, but not exactly by the malicious eavesdroppers [1]. The unpredictability of the radio channel can be regarded as a promising feature for security, which can be exploited for addressing, in particular, the well-known problem of key exchange.

PLS-based key exchange was also shown to be advantageous in terms of energy consumption with respect to conventional cryptography methods. For example, in [7] the authors show that the energy consumption of the RSSI (Received Signal Strength Indicator) scheme proposed is only 2.4 % of ECDH (Elliptic Curve Diffie-Hellman), to parity of hardware configuration.

Recently, many experimental works have demonstrated the PLS key generation with different radio technologies [8]. Most of them are based on the temporal fading of the radio channel, using the RSSI [9], [10], [11] However, in this context the radio channel must be observed for a long time [12] and the communicating devices must move with significant speed [13]. Also, an RSSI-based approach is vulnerable to proximity and predictable-channel attacks [9], [14]. An alternative strategy proposed in the literature is based on the wideband characteristics of the radio channel, i.e., on the resolvable temporal dispersion, or, equivalently, on the frequency selectivity. As described in [15], in fact, with Orthogonal Frequency Division Multiplexing (OFDM) waveforms it is possible to sound the channel with pilot subcarriers over different frequencies and to extract a security key from the channel state information. This can be performed even with static devices, and it reuses some pieces of the communication information. In this way, longer security keys can be generated in a shorter time, as compared to RSSI-based PLS methods.

In [16] and [17], the authors have proposed a strategy for time-frequency key-generation, based on filter-bank processing, which allows key generation by sampling and quantization of the received signal spectrum. This method is particularly suited for broadband communications, where the channel multipath affects the received spectrum and this feature can be used for the generation of keys. The advantages of the proposed filter-bank approach, with respect to RSSI-based one, are related to the possibility of performing key generation also in static environments and from a generic baseband received signal, such as OFDM, pulse-based ultra-wide band (UWB) or chirp modulation, etc., provided that enough bandwidth is available to resolve the multipath.

Although widely researched, many aspects of PLS key generation are still to be investigated in depth and, in particular, the relationship between physical quantities, such as radio channel characteristics and antenna directivity, with higher level parameters such as the secrecy performance indicators of the PLS generated keys.

For this purpose, this paper proposes a multilevel analysis based on a comprehensive numerical model that simulates the Tx/Rx chain, from signal generation to key extraction through quantization of the received spectra. The model considers, for the secret key generation, the electromagnetic wave propagation in complex scenarios. In the literature, different approaches have been considered for the evaluation of PLS security channel modeling [18], [19]. Among the different approaches, in this paper, we have chosen to model the channel using QuaDRiGa (QUAsi Deterministic RadIo channel GenerAtor) [20], [21], which implements a geometry-based stochastic approach taking into account all relevant propagation effects.

In this paper, we considerably extend the results presented in [16] and [17], where the filter-bank technique was firstly proposed. The main contributions of this paper can be summarized as it follows:

1) Investigation of the effect of the radio channel on the secrecy performance indicators. For this purpose, we analyze two different simulation scenarios: 1) an ideal Line-of-Sight (LoS) two-ray propagation model, and 2) a realistic propagation scenario, i.e., 3GPP 38.901 UMa LoS. These scenarios are representative of very small and big amount of multipath richness.
2) Evaluation of the key mismatch rate between the two legitimate nodes, i.e. Alice and Bob, and between a legitimate node and the eavesdropper (i.e. Eve) in connection with the variation of the signal-to-noise ratio (SNR) and of Eve position. For this purpose, Eve

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

position is varied either along the x axis or with respect to a circle centered at Alice position.

3) Evaluation of the key mismatch rate in connection with the variation of the antenna directivity either at Bob or at Eve terminals.
4) Analysis of the quality of the generated keys from the randomness point of view, using the NIST test suite, in relation to the channel properties, the SNR, and the antenna directivity. For this purpose, the keys generated by the filter-bank processing are analyzed against a set of NIST tests. Moreover, the proportion of sequences passing each of the selected tests is evaluated over 100 Monte Carlo realizations.
5) Demonstration, through the comprehensive numerical analysis, which relates the SNR, the channel, and antenna characteristics to the key mismatch and the key randomness, that a rich multipath environment is fundamental to ensure a good level of confidentiality. We show that the antenna characteristics can change the key generation performances in terms of key mismatch and randomness.

The rest of the paper is organized as follows: in Section II, the numerical model is described evidencing the different simulation steps necessary to perform key generation. Section V reports the simulation results for two different propagation scenarios, i.e., a two-ray propagation model and a realistic urban outdoor scenario, which are characterized by different levels of multipath contribution and randomness. The reported simulation results are obtained for different positions of the eavesdropper with respect to the legitimate communication nodes. Section VI discusses the effect of the variation of the antenna directivity on the secrecy performances of the generated keys. The variations of the beamwidth of either the legitimate node or the eavesdropper are considered. Finally, in Section VII the conclusions are reported.

II. PLS KEY GENERATION

A. KEY EXCHANGE PROBLEM

We assume a wireless scenario consisting of three communication entities (e.g., nodes), namely Alice, Bob and Eve. Alice and Bob are assumed to be authenticated legitimate nodes who want to communicate securely. In the meanwhile, Eve, a third undesired node of the network, plays the role of the passive eavesdropper, i.e., intercepting the legitimate communication. To achieve confidentiality, Alice and Bob rely on the use of a cipher, e.g. advanced encryption standard (AES), to encrypt their communication. We know that Alice's and Bob's security relies on their private encryption/decryption key, and not on the cipher algorithm itself, according to Kerckhoffs's principle. Therefore, to adequately perform encryption and decryption, Alice and Bob must have at disposal a proper symmetric secret key to operate the cipher. The key represents a secret element that must be generated and shared between Alice and Bob before communication, and must be kept safe from Eve. This is the key exchange problem. Conventional cryptography solves this problem of Alice-Bob-Eve key exchange using methods based on the difficulty of solving mathematical problems, such as prime number factorization or discrete logarithms, which have been adopted in most of modern security protocol. It is worth stressing that conventional cryptography is independent from the medium or the context of communications, being in fact usually implemented in dedicated software libraries.

B. RADIO CHANNEL PROPERTIES

In this work we investigate an alternative solution to the key exchange problem within the PLS field named channel-reciprocity-key-generation (CRKG). This PLS method is based on the radio channel itself, i.e. the communication medium between Alice and Bob. In principle, three characteristics of the radio channel enable CRKG [22]:

1) Channel multipath: in realistic outdoor conditions Alice, Bob and Eve are surrounded by buildings, cars, vegetation and other obstacles, or indoors by furniture and walls. The wireless environment composed by scattering objects determines a multipath propagation among the wireless nodes. Reflections, refractions and diffractions onto the scattering objects spread the transmitted signal in space. Even though this unavoidable dispersion is traditionally seen as detrimental for communications, it turns out to be beneficial for PLS purposes. In fact, the random disposition of scattering objects around the nodes is hardly predictable, influencing in a "chaotic" way the physical layer (PHY) communication performance. This multipath represents the original source of entropy at PHY for PLS;
2) Channel reciprocity: the influence of multipath is symmetric at both sides of communication: Alice-to-Bob and Bob-to-Alice. The reciprocity of the wireless communication allows Alice and Bob to observe the same effect of the radio channel between them. It is worth mentioning that, although the channel is always symmetric, the channel impulse response is only symmetric in time division duplex (TDD) [23]. This creates the conditions not only to extract a random key from the radio channel, but at the same time to share it;
3) Spatial decorrelation: the radio channel properties change over space and time. This is true for Alice and Bob, but also for Eve, which is supposed to be located in a different position from the legitimate nodes. This means that Alice and Bob experience a unique radio channel which can be exploited for the purpose of CRKG. One of the consequences of the multipath is the channel spatial decorrelation, which protects Alice and Bob from Eve. This means that Eve can experience the same Alice-Bob channel, only if she is superimposed to Bob (or Alice), i.e., in the same position, and with the same PHY settings. Otherwise, the farther she goes from Bob (or Alice), the less coherent (i.e., less correlated) her multipath becomes with respect to the legitimate channel. In terms of PLS, this represents a

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

sort of spatial "security zone" for Alice and Bob against Eve.

Thanks to the three channel properties, the CRKG method allows Alice and Bob to generate a secret key directly from processing the PHY communication signals, without third-party assistance. Thus, the PLS key exchange is performed in a peer-to-peer way by reusing the available wireless PHY resources. This represents the main PLS advantage with respect to conventional cryptographic methods, and, because of this, CRKG might significantly reduce energy or time required for key exchange before encryption or decryption [16].

C. KEY GENERATION

According to the methodology proposed in [16], the key generation (channel-reciprocity-key-generation CRKG) is performed here directly on the baseband received signals in a simple manner with a single-threshold filtering process. The complex baseband received signals for the three communication nodes (i.e Alice, Bob, and Eve) with known bandwidth B can be described as:

$$\begin{cases} y_a(t) = h_{ab}(t) * x_b(t) + n_a(t) \\ y_b(t) = h_{ba}(t) * x_a(t) + n_b(t) \\ y_e(t) = h_{ea}(t) * x_a(t) + n_e(t) \end{cases} . \tag{1}$$

where $y_a(t)$, $y_b(t)$, and $y_e(t)$ are the received signals by Alice, Bob, and Eve, respectively, $x_a(t)$ and $x_b(t)$ are the signals transmitted by Alice and Bob, and $n_a(t)$, $n_b(t)$, and $n_e(t)$ are the additive white Gaussian noise (AWGN) terms. The operator "*" denotes the convolution between signals. The channel impulse response between Alice and Bob is assumed reciprocal, i. e. $h_{ab}(t) = h_{ba}(t)$, whereas the one pertaining to Eve, $h_{ae}(t)$, is in general different from $h_{ab}(t)$, thanks to the radio channel spatial properties. The wideband received signal $y_i(t)$, (with i=a, b, or e in case of Alice, Bob or Eve), is decomposed through M filters, each with impulse response $g_m(t)$, with m varying from m=1 to m=M. The output of each filter can be evaluated, for each value of i and m as:

$$y_{i,m}(t) = y_i(t) * g_m(t) \tag{2}$$

The power at the output of each filter is calculated by integrating and averaging the filter output $y_{i,m}(t)$ over a certain interval T (e.g., a frame or preamble duration of the PHY signal) or, equivalently, by integrating the Fourier transformed signals:

$$P_{i,m} = \int_{f_1}^{f_2} |Y_{i,m}(f)|^2 \, df \tag{3}$$

where $Y_{i,m}(f)$ is the Fourier transformed spectrum of the received signal $y_{i,m}(t)$, and f_1 and f_2 are the lower and upper frequency edges of the m-th sub-band. The power at the output of each filter $P_{i,m}$ is directly compared against a threshold ϵ_i computed as the median value of the spectrum of the received signal $y_i(t)$. The m-th bit of the key is extracted as it follows:

$$K_{i,m} = \begin{cases} 1, & if \quad P_{i,m} > \epsilon_i \\ 0, & if \quad P_{i,m} < \epsilon_i \end{cases} . \tag{4}$$

Fig. 1 shows a schematic example of key generation. The nominal bandwidth is subdivided into sub-bands (equivalently to filters). The sub-bands are delimited by vertical dash-dotted lines in the figure. Each sub-band has an associated power level, named sub-band level, evaluated as the average received power in the sub-bands and illustrated by the green solid lines. The binary quantization threshold is given by the median value of the whole power spectrum, in the nominal bandwidth, as depicted by the horizontal red line. When a green sub-band level is lower (or higher) than the red threshold, a zero (or one) value is generated in the sub-band. In total, in the-case-of-study simulations reported, the final raw key generated contains 128 bits.

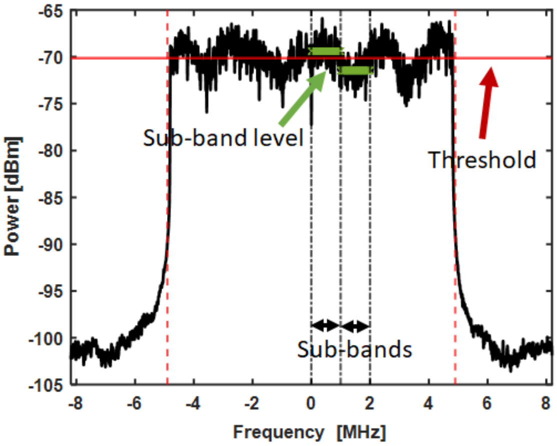

FIGURE 1. Working principle of the single-threshold key extraction in the frequency domain. The red horizontal line represents the quantization threshold, the vertical dash-dotted lines delimit two exemplary sub-bands, where the green lines denote the sub-bands average power levels.

D. CRKG PROTOCOL

Figure 2 schematizes how the CRKG protocol works with the following main steps:

1) Channel probing: when Alice and Bob exchange PHY frames, they also probe the radio channel in a given time window and with a given waveform bandwidth [16]. The meaning of probing is that a given transmitted frame is distorted according to the multipath and therefore, it carries the channel signature in itself at the receiver side. We assume that Alice and Bob exchange several frames over the channel and store the baseband sampled data. In the meanwhile, Eve is passively collecting all the frames in the air. The duration and the accuracy of the channel probing phase depends on the PHY specifications. Probing reciprocity and duration are crucial aspects of the CRKG protocol;

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

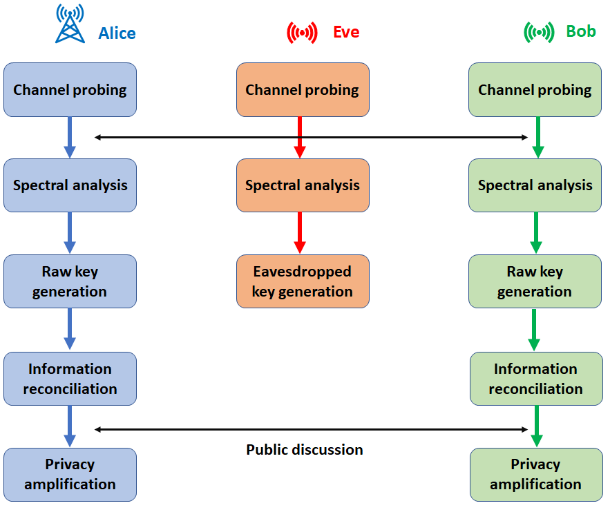

FIGURE 2. Schematic representation of key generation steps

2) Signal processing: by analyzing the wideband power spectra of the collected PHY data, Alice and Bob can observe the frequency selectivity of the multipath, i.e., the channel signature to map onto the security key. This phase of the CRKG protocol can be implemented in different ways: for example by exploiting different waveforms such as OFDM [11] and wideband signals [24] or by exploiting the channel diversity in multiple input multiple output (MIMO) settings [25]. The spectral analysis is necessary for the proposed filter-bank method [16], [17] analyzed in this paper. Further details are provided in the following sections. We assume the CRKG protocol to be public, so Eve is also post-processing the overheard communication data for CRKG, as well as Alice and Bob;
3) key generation: the key generation is the core process of CRKG. The goal is to turn the spectral components of the PHY data (and so the channel signature) into a binary sequence, called raw key, in the following. Alice and Bob generate a pair of keys, by quantizing the analyzed spectrum. Further details are provided in the following sections. In parallel, Eve can generate two keys from the eavesdropped data;
4) Information reconciliation: the keys generated out of the probed radio channel might differ for some erroneous bits, due to noise (or interference) in the received signals. The mismatching of the raw keys limits the reciprocity between Alice and Bob. Therefore, an additional correcting phase called information reconciliation is required. Through a public discussion Alice and Bob exchange the reconciliation data, while trying to minimize the information leakage to Eve. Many reconciliation methods are available, mostly based on Forward-Error-Correction (FEC) [8]. For example, FEC schemes, such as Bose-Chaudhuri-Hocquenghem (BCH) codes or Secure-Sketch [26] can uniform the quantized keys correcting up to 20 % of the bits [27], [28]. Reconciliation is a delicate stage, because the whole security scheme could collapse, if Alice and Bob do not match the generated keys. There are also Eve's threats during the reconciliation phase, but are out of the scope of this work;
5) Privacy amplification: finally, Alice and Bob can additionally leverage on hash-function (i.e., one-way function) [22]. This phase acts as a "lock", preventing an attacker to guess the reconciliated key.

In this work, we focus on the first three steps the CRKG protocol, which are directly dependent on the PHY characteristics, such as radio channel and antenna radiation properties.

E. PLS ASSUMPTIONS

In this work, we have taken into account the following assumptions for the simulations:

- there is no mobility in the channel, and no Doppler effect;
- the power spectral characteristics of Alice-to-Bob frame is equal to Bob-to-Alice's one, to assure reciprocity in the key generation;
- the PHY includes OFDM as modulation waveform, in TDD mode, with only additive white Gaussian noise (AWGN) and no interference;
- the hardware impairments given by synchronization, quantization and RF chains [16] are neglected.

III. SIMULATIONS DESCRIPTION

A. LTE WAVEFORM

Given the statistical nature of the secret key generation process, we set up a Monte Carlo [29] simulation framework in MATLAB, including modern radio channel models and noise realizations. The key generation essentially works on several received baseband OFDM frames collected during the Monte Carlo iterations. Note that, the PHY communication performance is out of the scope of the work. The OFDM waveform specifications are given in Table 1.

TABLE 1. 3GPP OFDM Waveforms Specifications [30]

Nominal Channel Bandwidth [MHz]	10
Frame Duration [ms]	10
Over Sampling Factor	1.536
Sampling Frequency [MHz]	15.3
FFT Size / Total Sub-Carriers	1024
Sub-Carrier Spacing [kHz]	15
Sub-Carriers per Sub-Channel	12
Useful Symbol Time [μs]	66.6667

B. CHANNEL MODEL

The channel model is implemented through QuaDRiGa, as aforementioned. The QuaDRiGa model is based on statistical distributions of small- and large-scale fading parameters extracted from channel measurements. It allows for simulating different scenarios and carrier frequencies, by taking into account all relevant propagation effects [20], [21]. In particular,

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

in this work QuaDrIGa has been used for two reasons: 1) to take into account the impact of realistic antennas, and 2) to generate realistic channel impulse response for outdoor urban scenarios.

C. MONTE CARLO STEPS

For each round of the Monte Carlo simulation, the following steps have been performed for Alice, Bob and Eve:

- selecting QuaDrIGa antennas (Alice, Bob and Eve) and channel scenario to be simulated, as detailed in the following;
- generating the channel impulse responses (CIR);
- performing the convolution between the transmitted OFDM frame with the QuaDrIGa CIR;
- adding thermal noise on the baseband received frame samples, proportionally to an arbitrary Signal-to-Noise Ratio (SNR);
- input the received frames to the CRKG algorithm to generate keys.

The optimal number of Monte Carlo realizations was determined by a convergence analysis, compromising between computational resources and statistical significance. In total, the following simulation results refer to 100 Monte Carlo realizations.

D. SIMULATION SCENARIOS

We considered two different simulation scenarios: 1) an ideal Line-of-Sight (LoS) two-ray propagation model with fixed ground permittivity (i.e. metallic reflector); 2) a realistic propagation scenario, i.e., 3GPP 38.901 UMa LoS scenario, which models the wireless channel for typical macro Base Stations (BS), deployed above rooftop in densely populated urban areas. In the following, they are labelled as "2-ray" and "3GPP", respectively. They are representative of very small and big amount of multipath richness. The 3GPP scenario includes 12 random scattering clusters, with 20 sub-paths each.

As depicted in Fig. 3, we assume that Alice acts as an LTE evolved NodeB (eNB), whereas Bob and Eve act as User Equipment (UE). Those are role in our simulations. The transmitted power is equal to 20 dBm in uplink and downlink. Alice antenna is placed at 25 m height from the ground, whereas the height of Bob and Eve antennas from the ground was arbitrarily chosen equal to 2.5 m. The height of the eNB was chosen according to the specifications of the Quadriga 3GPP scenario.

In the following, we report simulation results for the two reference propagation scenarios, with different Eve positions: As shown in Figs. 3 (a) and (b), Eve's position is either varied along the x axis or with respect to a circle centered at Alice's position. In all the considered simulations, Alice's antenna is placed at $(x_A = 0, y_A = 0)\ m$, whereas Bob's position is fixed at $(x_B = 150, y_B = 0)\ m$. Moreover, Alice's antenna is an array of five half-wavelength dipoles with maximum radiation along the x axis and maximum gain $G_A = 10.24$ dBi. Unless differently stated in the following, Bob and Eve are by default equipped with half-wavelength dipole antennas with maximum gain $G_B = G_E = 2.15$ dBi.

Alice radiation pattern in the horizontal plane is also reported in Fig. 3, superimposed to the device positions in the simulation area. The 5-dipole Alice antenna array is a Uniform-Linear-Antenna (ULA) with half-wavelength spaced dipoles. It was chosen as a reference antenna, thanks to the predictability of its radiation characteristics. In fact, the presence of well-known main and side-lobes helps to put in evidence the dependence of the secrecy performances on the antenna radiation diagram.

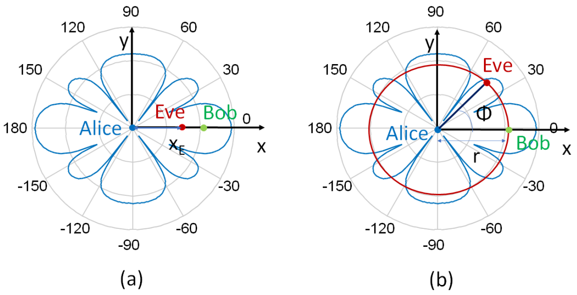

FIGURE 3. Schematic of Eve position variation: (a) along the x axis, and (b) along a circle of radius r centered at Alice position.

IV. CRKG PERFORMANCE

In order to quantify the effect of the different propagation scenarios and of the antenna characteristics on the key generation, two reference performance indicators have been chosen: the key mismatch rate and the key randomness. The key mismatch between Alice's and Bob's raw key bits is calculated as the Hamming distance in percentage with respect to the key size (i.e., 128 bit). The key randomness is evaluated according to the National Institute of Standards and Technology (NIST). In particular, we will focus in the following on the performance evaluation of the generated raw keys, leaving out results on reconciliation and amplification for future works.

A. KEY RANDOMNESS

Regarding the key randomness, we will report in the following the results of some of the NIST tests, which are part of a complete test suite for testing random number generators [31]. In particular, we will consider the following tests:

1) Runs test: it evaluates the total number of runs in the generated raw key, where a run is an uninterrupted sequence of identical bits.
2) Longest run of ones in a block: it determines whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence;
3) Frequency (Monobit) test: it evaluates the proportion of zeroes and ones for the entire sequence. The number of ones and zeros in a truly random sequence is expected to be approximately the same.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

4) Cumulative sums (forward/reverse): it computes the partial sums of successively larger subsequences of bits, starting from the beginning (forward) or from the end (reverse) of the bit sequence. This test evaluates whether there are too many zeroes or ones at the early stages or at the late stages of a bit sequence.

According to [31], a p-value is associated to each test and it is compared to a significance level α. The randomness tests for a given bit sequence are considered successful (i.e., the key can be considered as random) if the associated p-value is greater than the significance level α (the threshold was chosen to be $\alpha = 1\ \%$.)

The four selected tests give an indication of various randomness features of the generated keys and they are applicable to relatively short bit sequences. For each round of the Monte Carlo simulation, corresponding to different noise and channel realizations, a 128-bit key is generated and tested for randomness as described above.

Indeed, not all the generated bit sequences will pass the randomness tests, therefore, it is necessary to define a metric that somehow quantifies the ability of generating random sequences through the single-threshold filter method. For this purpose, according to the procedure described in [31], we have evaluated the proportion of sequences passing each of the selected tests, over the 100 Monte Carlo realizations. A confidence interval is defined as:

$$(1-\alpha) \pm 3\sqrt{(\frac{\alpha(1-\alpha)}{m})} \tag{5}$$

where α is the test significance level and m is the number of realizations. If the proportion of sequences passing a test falls outside of the confidence interval, then there is evidence that the CRKG method is not fully able to generate random sequences, according to the selected test.

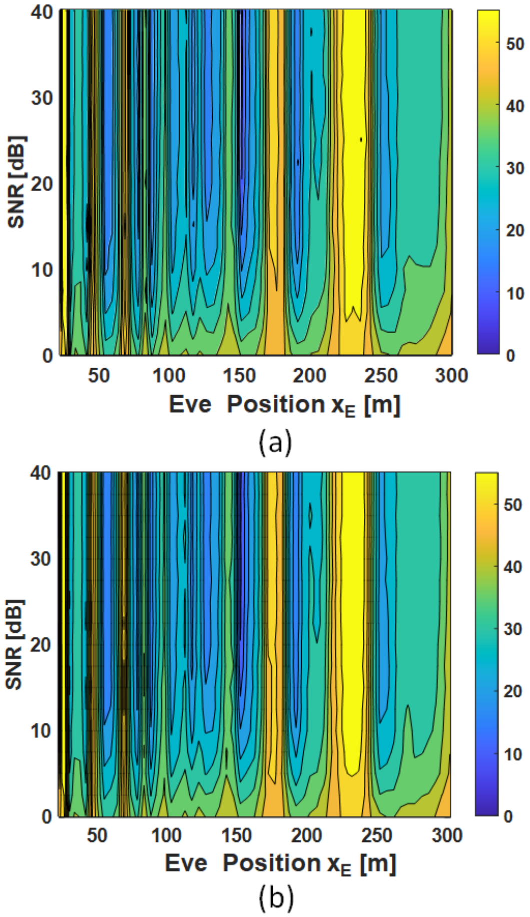

FIGURE 4. Key mismatch rate [%] calculated by comparing the raw keys generated (a) by Alice and Eve (Alice-vs-Eve), and (b) by Bob and Eve (Bob-vs-Eve), as a function of Eve position x_E and of the SNR [dB], in the case of the 2-ray scenario. Bob position is $x_B = 150\ m$ and $y_B = 0\ m$.

V. RESULTS

A. VARIATION OF EVE POSITION ALONG THE X AXIS

1) Two-ray scenario

With a reference to the schematic representation in Fig. 4 (a), we first consider a static variation of Eve's position along the x_E axis. For each position of Eve, the random keys are generated from the received spectra at the three nodes, according to the procedure described in Section II. Fig. 4 shows the Monte Carlo average key mismatch rate, calculated by comparing the raw keys generated (a) by Alice and Eve (Alice-vs-Eve), and (b) by Bob and Eve (Bob-vs-Eve). This percentage is function of Eve's position x_E, from 0 to 300 m, and of the SNR, from 0 to 40 dB, in the 2-ray scenario. We remind that Bob is located 150 m away from Alice.

The results reported in Fig. 4 show very similar behaviors for the Alice-vs-Eve (Fig.4 (a)) and for the Bob-vs-Eve (Fig. 4 (b)). In an environment with little multipath such as the 2-ray scenario, the signal variation is mainly due to the change of the LoS contribution and to the constructive/destructive interference with the ground reflected ray. No other reflections or obstacles are considered and the received signal spectrum mainly depends on the distance between the nodes, to parity of other parameters such as antenna height, antenna radiation diagrams, etc.. Therefore, there are positions where Eve's received spectrum exhibits the same characteristics as Alice's (or Bob's) one and Eve experiences similar signal variations as the legitimate nodes and high cross correlation. Since only two rays are considered in the 2-ray channel model (i.e. the LoS and the ground-reflected one), the randomness of the channel is low, and so its entropy. This allows an efficient key reconstruction by Eve. As shown in Figs. 4, the key mismatch is strongly dependent on Eve's position along the x axis, following the constructive/destructive interference pattern typical of two-ray propagation. The maps exhibit, in fact, different regions of low key mismatch (denoted by the blue color), where an efficient attack by Eve is likely to occur, given our simulation setup. Moreover, these low key-mismatch regions alternate with high key mismatch regions (yellow regions) where the attack is not favorable and Eve would face 50 % probability to guess a given bit of Alice's key (i.e. it is equivalent to the case where Eve flips a coin).

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

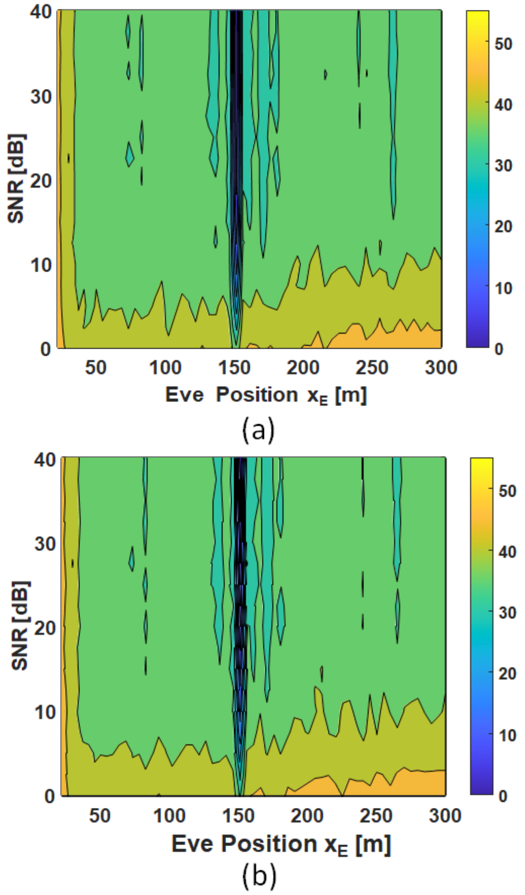

FIGURE 5. Key mismatch rate [%] calculated by comparing the raw keys generated by (a) Alice and Eve (Alice-vs-Eve), and (b) Bob and Eve (Bob-vs-Eve), as a function of Eve position x_E and of the SNR [dB] in the case of the 3GPP scenario. Bob position is $x_B = 150\ m$ and $y_B = 0\ m$.

2) 3GPP scenario

Fig. 5 shows the same key mismatch rate as before, but in the 3GPP scenario. It is calculated by comparing the raw keys generated (a) by Alice and Eve (Alice-vs-Eve), and (b) by Bob and Eve (Bob-vs-Eve), as a function of Eve's position x_E and of the SNR. Except for the propagation scenario, all the other simulation parameters are the same as in the previous case.

As we can see from Fig. 5, most of the plot corresponds to a value of the key mismatch around 37 % (green region), for most of the SNR values considered. This means that Eve can guess 63 % of the key, slightly more than the optimal 50 %. The key mismatches obtained here are comparable with other works in literature, e.g., [11], [32], although different PLS key generation setups hinder a direct comparison.

Given the multi-path richness of the 3GPP propagation scenario, Eve's received spectrum is, in general, different from Alice's and Bob's one. The received signal at the different nodes is affected by constructive and destructive interference of multiple rays, depending on the node positions and on the scattering from obstacles. When Eve is located in a different position with respect to Bob, the signal paths contributing to Eve received spectrum are very diverse with respect to Bob's ones. The multi-path therefore increases the spatial de-correlation between the different receivers (e.g. Bob and Eve). This occurrence has the effects of 1) reducing Eve's ability of reconstructing the key, and 2) making Alice-vs-Eve and Bob-vs-Eve key mismatches generally independent from Eve's position.

A different situation occurs in the nearby of Bob's position (i.e. $x_B = 150\ m$ and $y_B = 0\ m$) (for each SNR), where the key mismatch tends to zero (blue color). Of course here, Eve experiences the same channel conditions as Bob, and therefore, she is able to sniff successfully the secret key, on average.

The results reported in Figs. 4 and 5 are coherent with the analysis proposed in [11] on the results of experimental studies on RSSI- and CSI-based key generation methods. Comparing the different scenarios, the results in [11], although not directly comparable, confirm our conclusion that a rich multipath environment, like the outdoor 3GPP studied in this paper, is fundamental to ensure a good level of confidentiality.

It is worth pointing out that in each of the analyzed cases, as expected, the Alice-vs-Eve and Bob-vs-Eve key mismatch maps were almost equal. Therefore, for the sake of brevity, in the following we will just report the results for the Alice-vs-Eve key mismatch. In practical scenarios, there might be significant differences between Eve's keys generated in sniffing the uplink or downlink, because of PHY specifications, but this is beyond the scope of the paper.

3) Legitimate node secrecy performance

Considering the legitimate communication link between Alice and Bob, it is now useful to evaluate the key mismatch Alice-vs-Bob, and the randomness of the generated raw keys. The latter has been achieved through the evaluation of the proportion of sequences (i.e. proportion of generated keys) passing the different NIST tests. These two secrecy performance indicators are only linked to the characteristics of the channel between Alice and Bob, and are independent from Eve's position.

Figure 6 (a) shows the key mismatch rate between Alice and Bob raw keys (Alice-vs-Bob) calculated for the 2-ray (blue curves) and for the 3GPP (red curves) scenarios.

As we can see from Fig. 6 (a), the Alice-vs-Bob key mismatch is slightly lower for the 3GPP scenario. This means that the higher multi-path contributions in the 3GPP scenario help to increase the correlation between the legitimate node signals and to improve the key reconstruction. In particular, the key mismatch is below 20 % for SNR values above 7 dB and 5 dB, in the case of the 2-ray and the 3GPP scenarios, respectively, and it tends to zero for higher SNR values. As also illustrated in [17], the key mismatch has a natural decreasing trend versus the SNR in dB. This can be explained considering that, the channel fading at each legitimate node of the link is reciprocal. However, the signal spectra received by Alice and Bob can be asymmetric owing

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

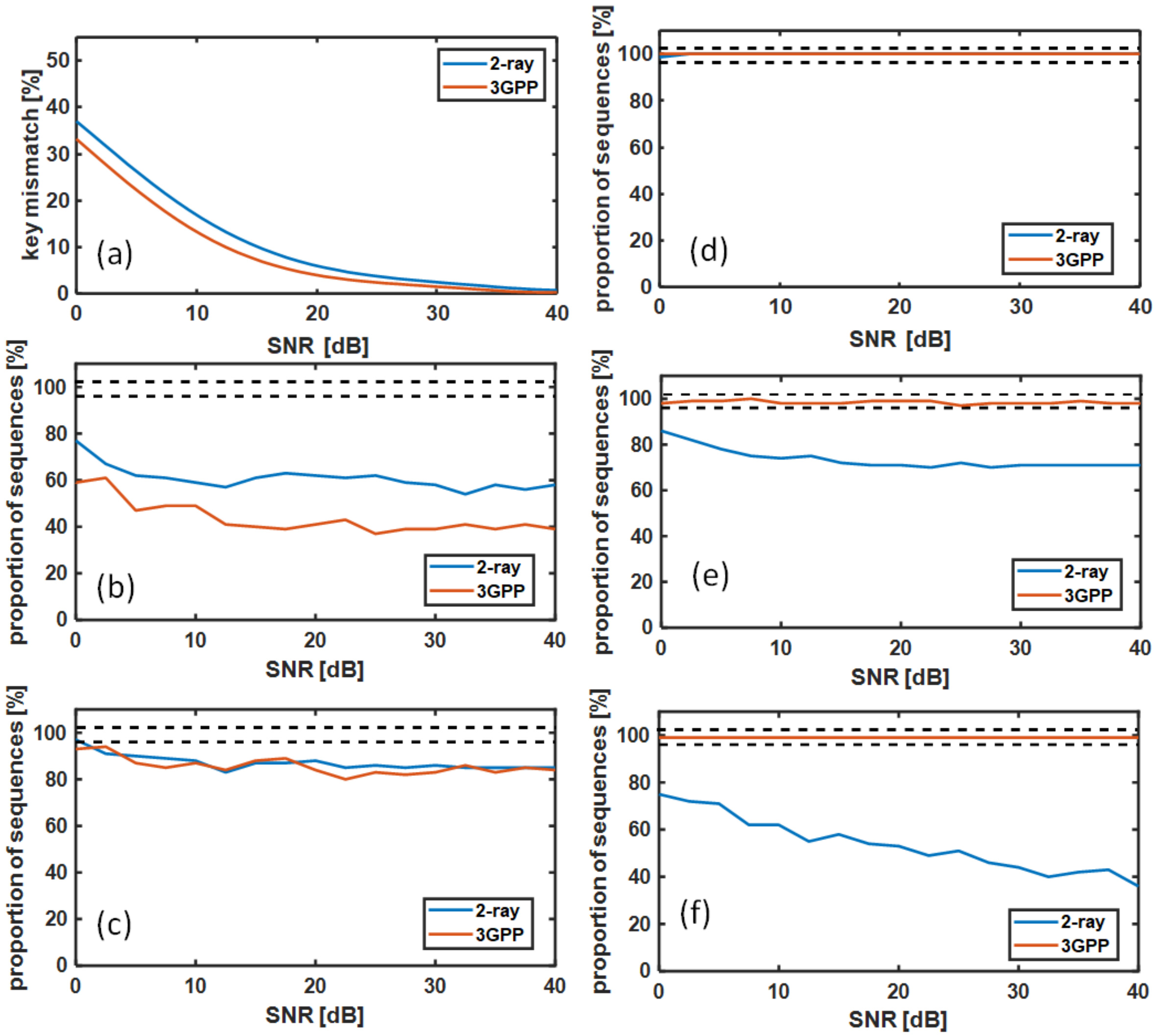

FIGURE 6. (a) key mismatch rate [%] between Alice and Bob raw keys (Alice-vs-Bob) calculated for the 2-ray (blue curves) and for the 3GPP (red curves) scenarios. (b-f) proportion of sequences [%] passing (b) the runs test, (c) the longest-run-of-ones test, (d) the frequency test, (e) the cumulative sum (forward) test, and (f) cumulative sum (reverse) test. The proportion of sequences passing a test is calculated, as a function of the SNR, over the 100 realization of the Monte Carlo simulations, for Alice raw key in the 2-ray (blue curves) and in the 3GPP (red curves) scenarios. The confidence interval, given by eq. 5 is delimited by the black dashed lines.

to the uncorrelated noise processes (e.g. associated to the hardware at the two nodes). For lower SNR values, the key generation is mostly influenced by noise fluctuations rather than by multi-path contributions. Therefore, when noise is the dominant phenomenon, the key mismatch is higher and the legitimate nodes do not fully reconstruct the key. The behavior of the key mismatch rate as a function of the SNR (Fig. 6 (a)) is in line with that obtained in [32] and [33] with different PLS key-generation methods.

Provided that the performances are comparable with other different PLS-based key generation methods, the advantages of our filter-bank approach can be summarized as it follows: 1) it is virtually applicable to a generic baseband signal, 2) it is not only limited to a particular modulation scheme such as OFDM, but it can be used also for other modulation schemes, e.g. pulse-based ultra-wide band (UWB) or chirp modulation, and 3) it is suitable also for static environments.

Considering the key randomness, Figs. 6 (b)-(f) show the proportion of sequences [%] passing (b) the runs test, (c) the longest-run-of-ones test, (d) the frequency test, (e) the cumulative sum (forward) test, and (f) cumulative sum (reverse) test. The confidence interval, defined by eq. 5, is delimited by the black dashed lines. The proportion of sequences passing a test is calculated, as a function of the SNR, over the 100 realization of the Monte Carlo simulations, for Alice's raw key in the 2-ray (blue curves) and in the 3GPP (red curves) scenarios.

As we can see from Fig. 6 (b), the curves representing the proportion of sequences passing the runs test are outside the confidence interval for both scenarios (with a slightly better performance for the 2-ray scenario). Therefore, for what concerns the runs test, the CRKG based on the single-

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

threshold filtering is not fully able to generate random keys. For example, considering the curve pertaining to the 2-ray scenario (blue curve), 60 % to 80 % of the generated keys pass the runs test. This means that 20 % to 40 % of the generated raw keys tend to have sequences of correlated bits, thus deviating from the optimal secret key. In details, this is caused by the correlation between filter outputs on the observed channel signature. This effect is present among the adjacent sub-bands filters within the communication bandwidth, because of the nature of channel frequency selectivity. Then it is directly reflected in the quantized bit sequences. Other more advanced secret key generation methods might lead to different results [16].

Similar behavior of Fig. 6 (b) is found also for the longest-run-of-ones test shown in Fig. 6 (c). Moreover, Figs. 6 (d)-(e) show that, as regards the 2-ray scenario, the proportion of sequences passing a test are within the confidence interval only in the case of the frequency test (Fig. 6 (d)), where its blue curve is superimposed by the red one. Conversely, in the case of the 3GPP scenario (red color), the proportion of sequences passing the frequency test (Fig. 6 (d)), and both the forward and reverse cumulative sum tests (Fig. 6 (e) and (f)) are always within the confidence interval.

Considering the results in Figs. 6, we can state that not all the randomness features evaluated by the selected NIST tests are sensitive to the scenario. In the examined cases, the multipath richness of the 3GPP scenario significantly improves the test outcome only in the cases of the cumulative sum reverse/forward test (Figs. 6 (e) and (f))), which evaluate whether there are too many zeroes or ones at the early stages or at the late stages of a bit sequence. Moreover, the correlation between filter outputs in the single-threshold key generation method tends to give sequences of correlated bits, as indicated in Figs.6 (b) and (c).

B. VARIATION OF EVE'S ANGULAR POSITION

Recalling Fig. 3 (b), we consider the variation of Eve's static position along a circle centered at Alice's node ($x_A = 0$ m and $y_A = 0$ m). In the following results calculated for the two reference scenarios, i.e., 2-ray and 3GPP, the radius of the circle is equal to $r = 150$ m, which corresponds to Bob's distance from Alice. All the settings are identical to the previous analysis.

1) Two-ray scenario

Fig. 7 shows the key mismatch rate calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve) as a function of Eve's angular position Φ and of the SNR in the case of the 2-ray scenario.

Considering the radiation pattern of Alice's antenna array shown in Fig. 3, it can be noticed that the positions of the maxima and of the minima in Fig. 7 follow the positions of the maxima and minima in the radiation pattern, i.e. main and side lobes and radiation nulls. This behavior is coherent with the simplicity of the 2-ray channel model, where only the LoS and the ground-reflected rays are considered. In the 2-ray scenario, for a fixed distance r between Alice and Eve (as in the analyzed case) the multipath contribution to the received signal is the same. Therefore, the variations of the received spectra are mainly dominated by the signal level (i.e. by the antenna radiation pattern), whereas the low multi-path contribution gives high cross correlation, thus making Eve able to reconstruct the key. As we can see from Fig. 7, the Alice-vs-Eve key mismatch varies with the angle Φ between low (i.e. less than 10 %, color blue) and high values (up to 50 %, color yellow).

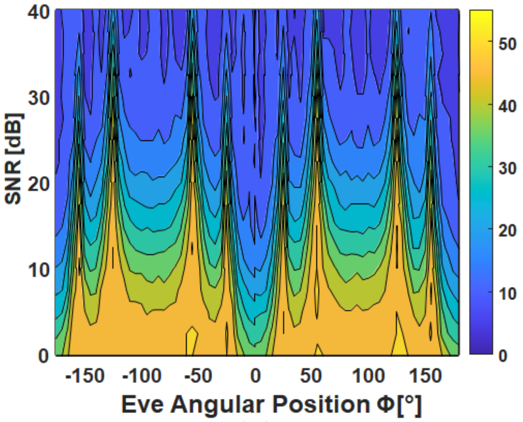

FIGURE 7. Key mismatch rate [%] calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve) as a function of Eve angular position Φ and of the signal to noise ratio SNR [dB], in the case of the 2-ray scenario. Bob position is $x_B = 150$ m and $y_B = 0$ m and Eve static position varies along a circle with radius $r = 150$ m. The key mismatch for the raw keys generated by Bob and Eve (Bob-vs-Eve) has the same behavior.

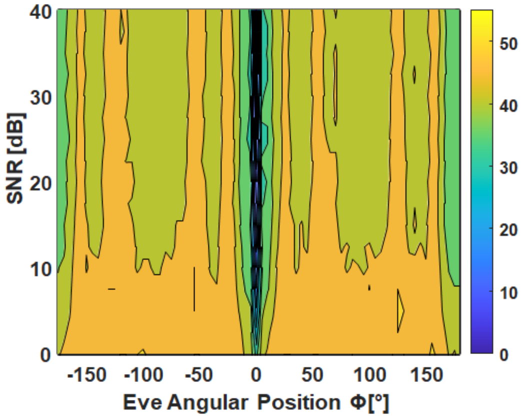

FIGURE 8. Key mismatch rate [%] calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve) as a function of Eve angular position Φ and of the signal to noise ratio SNR [dB], in the case of the 3GPP scenario. Bob position is $x_B = 150$ m and $y_B = 0$ m and Eve static position varies along a circle with radius $r = 150$ m. The key mismatch for the raw keys generated by Bob and Eve (Bob-vs-Eve) has the same behavior.

2) 3GPP scenario

Figure 8 shows the key mismatch rate calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve), as a function of Eve angular position Φ and of the SNR in the case of the realistic 3GPP scenario.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

It can be noticed that, in the realistic scenario, the oscillations of the Alice-vs-Eve (and Bob-vs-Eve) key mismatch are flattened. As discussed before, the multi-path richness increases the spatial decorrelation, so that Eve's received spectrum is different from that of the legitimate nodes. This reduces Eve's ability of reconstructing the key, almost irrespective from her position. The key mismatch rate is always above 37 % for all the SNR values, reaching 50 % for SNR<10 dB. Again, up to 63 % of the key can be guessed by Eve, on average. This guarantees an acceptable level of secrecy for the raw keys. As expected, for all the SNR values, a degenerate point occurs when Eve is in correspondence of Bob's position (i.e. $\Phi = 0°$). The key mismatch tends to zero (dark blue color) and Eve, therefore, is able to fully reconstruct the secret key.

Again, the advantages given by the rich multipath scenario in terms of PLS security are clear.

The Alice-vs-Bob key mismatch and the proportions of sequences passing a test are the same as in Fig. 8, since they do not depend on Eve position, and are not shown hereby.

VI. EFFECT OF ANTENNA BEAMWIDTH ON KEY GENERATION

In the previous section we highlighted the effect of the propagation scenario on the secrecy performances expressed in terms of key mismatch and key randomness. Here, we want to put in evidence the effect of the antenna characteristics on the key generation. In particular, we focus on the realistic 3GPP scenario, which is more interesting in terms of secrecy performances. In particular, we consider the variation of the beamwidth of the legitimate node (i.e. Bob) and of the eavesdropper (i.e. Eve). For the sake of comparison, Alice's antenna (i.e. the 5-dipole array) and all the other simulation parameters are kept unchanged with respect to the previously analyzed results.

A. VARIATION OF BOB'S BEAMWIDTH

We first consider the effect of the variation of Bob's 3-dB beamwidth in the azimuth direction (defined according to [21] in the case of a custom antenna type). In this case, the variation of the azimuth beamwidth corresponds to a 3-dB beam aperture $\Delta\Phi_B$ in the xy plane of Bob's radiation diagram. In order to compare the different results, the direction of maximum radiation of Bob antenna has been oriented toward Alice for all the simulations.

For each value of $\Delta\Phi_B$, we consider the variation of Eve's static position along a circle centered at Alice ($x_A = 0\ m$ and $y_A = 0\ m$), according to the schematic representation in Fig. 4 (b). The radius of the circle is equal to $r = 150\ m$, which corresponds to Bob distance from Alice.

Fig. 9 shows the key mismatch rate calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve) as a function of Eve's angular position Φ for an arbitrarily chosen value of SNR equal to 10 dB, and for different values of Bob's antenna beamwidth $\Delta\Phi_B$. In particular, when Bob's antenna has $\Delta\Phi_B = 360°$, the results are very similar to the half-wavelength dipole case analyzed before.

From Fig. 9, we can see that the influence of $\Delta\Phi_B$ variation on the Alice-vs-Eve key mismatch is moderate. Nonetheless, the key mismatch slightly increases for narrower beam widths, thus making Eve's attack slightly less effective especially near Bob's position, i.e. $x_B = 150\ m$ and $y_B = 0\ m$. Actually, when Bob's antenna beam-width is varied, a further element of asymmetry is introduced between the nodes (i.e. Bob and Eve have different antennas). Having different radiation diagrams, Eve and Bob weight differently the multi-path contributions.This slightly increases the decorrelation between Eve and Bob and, consequently, the key mismatch.

Considering the legitimate communication link between Alice and Bob, for the different values of Bob's beamwidth $\Delta\Phi_B$, we evaluated the Alice-vs-Bob key mismatch and the randomness of the generated key, as well as in Fig. 6.

In fact, Fig. 10 shows (a) the key mismatch rate between Alice and Bob raw keys (Alice-vs-Bob) and (b)-(f) the proportion of sequences [%] passing (b) the runs test, (c) the longest-run-of-ones test, (d) the frequency test, (e) the cumulative sum (forward) test, and (f) cumulative sum (reverse) test. The proportion of sequences passing a test are calculated, as a function of the SNR, over the 100 realization of the Monte Carlo simulations, for different values of Bob beamwidth $\Delta\Phi_B$.

As we can see from Fig. 10 (a), the Alice-vs-Bob key mismatch is lower for larger beamwidth, thus guaranteeing a better key exchange between the legitimate nodes. This can be explained considering that, reducing the beamwidth (i.e. increasing the antenna directivity), tends to privilege the LoS path contribution and to weigh less the secondary paths due to reflections by obstacles. Therefore, more directive antennas tend to filter out the multipath contributions, which are

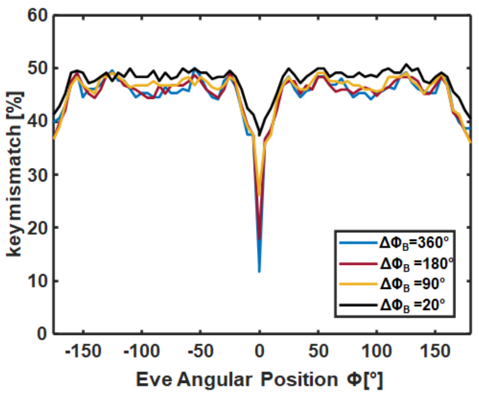

FIGURE 9. key mismatch rate [%] calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve), as a function of Eve angular position Φ for a fixed value of SNR=10 dB and for different values of Bob antenna beam-width $\Delta\Phi_B$, in the case of the 3GPP scenario. Bob position is $x_B = 150\ m$ and $y_B = 0\ m$ and Eve static position varies along a circle with radius $r = 150\ m$.The key mismatch for the raw keys generated by Bob and Eve (Bob-vs-Eve) has the same behavior.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

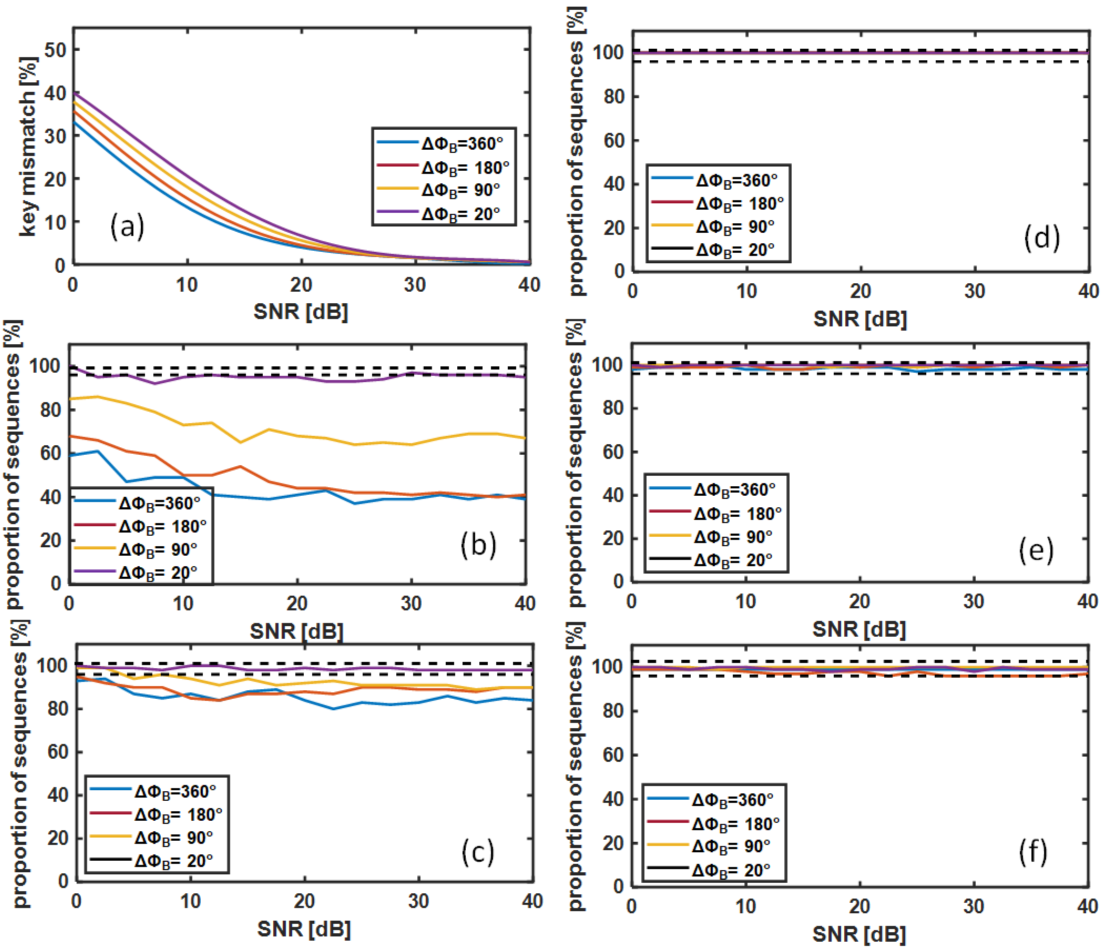

FIGURE 10. (a) Key mismatch rate [%] between Alice and Bob raw keys (Alice-vs-Bob) calculated for the 3GPP scenario as a function of the SNR [dB] and for different values of Bob antenna beamwidth $\Delta\Phi_B$. (b-f) proportion of sequences [%] passing (b) the runs test, (c) the longest-run-of-ones test, (d) the frequency test, (e) the cumulative sum (forward) test, and (f) cumulative sum (reverse) test. The proportion of sequences passing a test is calculated, as a function of the SNR, over the 100 realization of the Monte Carlo simulations for Alice raw key in the 3GPP scenario.

conversely better appreciated by a less directive one (e.g. the dipole). As evidenced before, higher multi-path contributions are beneficial to increase the correlation between the legitimate node signals and to improve the key reconstruction. The multipath gives oscillation in the received spectra that are significantly larger than those induced by noise fluctuations. These oscillations can be regarded as a signature of the channel and, given the channel reciprocity, Alice and Bob can better reconstruct the key. When Bob has a more directive antenna, oscillations in the spectra due to multipath are generally more flattened and the noise contributions become more significant in the key generation. This reduces the signal correlation thus slightly increasing the key mismatch rate.

As regards the randomness, considering the frequency and the cumulative sum tests (Fig. 10 (d) - (f)), the outcome of the tests does not significantly change with Bob's beamwidth $\Delta\Phi_B$ and the proportion of sequences falls always within the confidence interval. Conversely, as Fig. 10 (b) and (c) show, the $\Delta\Phi_B$ beamwidth variation influences more significantly the outcome of the runs and of the longest-run-of-one tests. In particular, the proportion of sequences passing these two tests increases for decreasing values of $\Delta\Phi_B$, thus corresponding to an improved randomness of the raw keys.

To qualitatively explain these results, we report in Figs. 11 the quantization power levels of the 128 sub-bands. They are indicated with empty circles in Fig. 11 (a) and (b) and they are two exemplary Monte Carlo realizations, both with SNR equal to 10 dB. Two different cases are considered: (a) $\Delta\Phi_B = 180°$ and (b) $\Delta\Phi_B = 20°$. The red line denotes the single quantization threshold. Figs. 11 (c) and (d) provide a graphical representation of the related generated bits (one bit for each filter), with a piecewise plot between 0 and 1. In a nutshell, more excursions between 0 and 1 are present for narrower beamwidth (Fig. 6 (c)). This tends to improve the randomness features of the generated key.

Comparing Figs. 11 (a) and (b), we can see different effects due to Bob's antenna: the power levels oscillations (indicated by the circles) are more evident when Bob's antenna is less directive (i.e., (a)). Given the used key generation method as described in Section III, many identical bits are more likely to be generated consecutively in the corresponding key sequence (Fig. 11 (c)), because they all are above or below

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

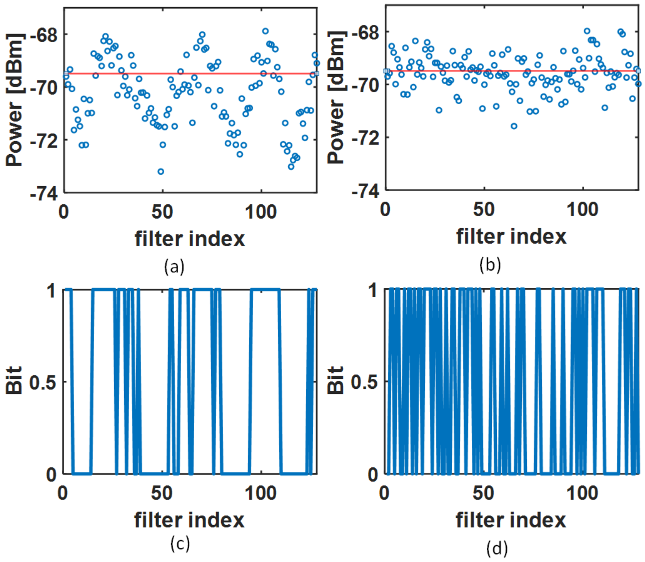

FIGURE 11. Average power value (circles) in the 128 sub-filters, each corresponding to a generated bit, for one of the Monte Carlo realization with SNR=10 dB in the case of (a) $\Delta\Phi_B = 180^\circ$ and (b) $\Delta\Phi_B = 20^\circ$. The red line denotes the threshold. (c) and (d) graphical representation of the corresponding generated bits in the case of (c) $\Delta\Phi_B = 180^\circ$ and (d) $\Delta\Phi_B = 20^\circ$.

the red threshold. Conversely, the more directive antenna (i.e., Fig. 6 (b)) flattens the oscillations deviation around the threshold, increasing the 0/1 or 1/0 excursions in Fig. (d).

In summary, with more directive antennas at Bob's side, the dynamic range of the filter levels becomes smaller, but more threshold crossing might occur. This is helpful for the key randomness, but, at the same time, it increases the probability of mismatch in the key quantization. This also explains Fig. 10 (a), where more errors are, in fact present, when Bob is equipped with a narrower beamwidth antenna (violet curve where $\Delta\Phi_B = 20^\circ$).

B. VARIATION OF EVE'S BEAMWIDTH

In order to verify if Eve's attack can become more effective by increasing her antenna directivity, we now consider the effect of the variation of Eve's 3-dB beamwidth on the secrecy performance indicators. For this purpose, we have fixed two different values of Bob's beamwidth, i.e. $\Delta\Phi_B = 360^\circ$ and $\Delta\Phi_B = 20^\circ$, which are representative of low and high directivity values. For each of the two values of $\Delta\Phi_B$, Eve's beamwidth $\Delta\Phi_E$ is varied in the azimuth direction. Also in this case, the directions of maximum radiation of Eve and Bob antennas are oriented towards Alice for all the simulations.

Figure 12 shows the key mismatch calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve) as a function of Eve's angular position Φ for an arbitrarily chosen value of SNR equal to 10 dB and for different values of Eve antenna beamwidth $\Delta\Phi_E$. Bob beamwidth is equal to (a) $\Delta\Phi_B = 360^\circ$, and (b) $\Delta\Phi_B = 20^\circ$.

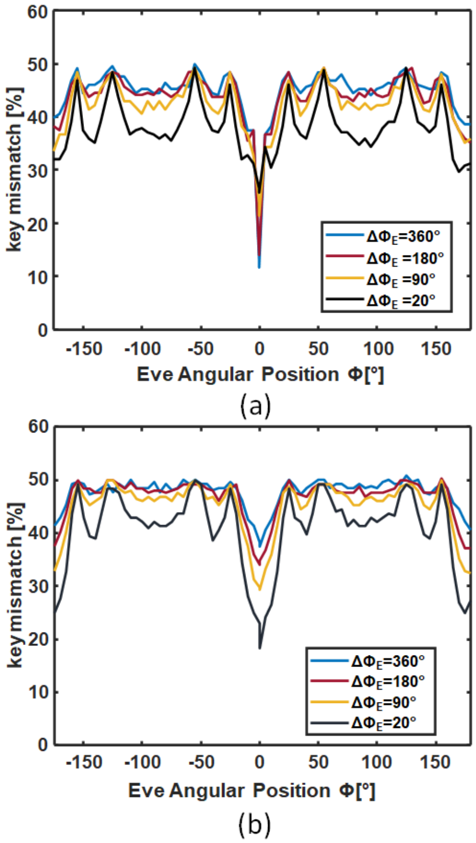

FIGURE 12. key mismatch rate [%] calculated by comparing the raw keys generated by Alice and Eve (Alice-vs-Eve), as a function of Eve angular position Φ for a fixed value of SNR=10 dB for (a) Bob beam-width $\Delta\Phi_B = 360^\circ$ and (b) Bob beam-width $\Delta\Phi_B = 20^\circ$ in the case of the 3GPP scenario. The different curves correspond to different values of Eve antenna beam-width $\Delta\Phi_E$. Bob position is $x_B = 150\ m$ and $y_B = 0\ m$ and Eve static position varies along a circle with radius $r = 150\ m$.The key mismatch for the raw keys generated by Bob and Eve (Bob-vs-Eve) has the same behavior.

From Figs. 12 (a) and (b), we can infer that, for both values of Bob's beamwidth, the increase of Eve's directivity reduces the Alice-vs-Eve key mismatch, thus slightly improving Eve's ability to reconstruct the key. Moreover, as before, Eve's attack tends to be more effective in correspondence of the sidelobes of Alice's antenna radiation diagram. These sidelobes are represented in the black curve by all the valleys among the peaks. This effect disappears by decreasing Eve's directivity (from black curve to blue curve), where the curve becomes flatter. Nonetheless, for the same value of Eve's beamwidth $\Delta\Phi_E$, the Alice-vs-Eve key mismatch increases when Bob's antenna is more directive (Fig. 12 (b)). As before, the worst case occurs when Eve is in the same position as Bob ($\Phi = 0^\circ$), since they experience almost the same propagation channel. The mismatch goes down in this point reaching 10 % and 20 % values, respectively, in Figs. 12 (a) and (b). This means in practice that Eve can guess 90 % or 80 % of Alice-Bob's key successfully, on average.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

VII. CONCLUSION

In this paper, we analyzed the problem of key exchange in wireless communications exploring the Physical-Layer-Security paradigm of channel-reciprocity-key-generation (CRKG). Thanks to a Monte Carlo simulation framework developed in Matlab, the performance of key generation between the legitimate nodes (i.e. Alice and Bob) and the eavesdropper (i.e. Eve) were evaluated in terms of bit mismatch rate and in terms of key randomness.

In details, we focused our investigation on the impact of the radio channel and of the antenna characteristics on the secrecy performance of PLS generated keys. Two reference propagation scenarios, namely 2-ray and 3GPP, and different antenna half-power-beamwidths were tested against the variation of the eavesdropper Eve position.

The results show that:

- a rich multipath environment, like the outdoor 3GPP studied in this work, is fundamental to ensure a good level of confidentiality. In fact, in the 3GPP scenario, almost irrespective of Eve position, the Alice-vs-Eve key mismatch remains above 37 % for all the considered values of SNR. This means that in Line-of-Sight, or LoS-dominant Ricean channels, the CRKG protocol might not meet its theoretical expectations. New PLS solutions for Line-of-Sight are still to be explored;
- achieving optimal random keys (i.e., passing all NIST tests) is not a trivial task, with simple processing and quantization methods like the ones implemented in this study. This is shown in Figs. 6 and 10;
- when Eve is near to Bob (in the order of meters) the CRKG is not secure at all. In practice, Eve's position information might be unknown, since she is only passively overhearing the communications. This might be the case in many real-life situations, such as local transports or crowded events, for example. This stresses the importance of the localization information for future works;
- the antenna pattern of the communicating devices has a significant impact on the key generation performance, such as mismatch rate, as illustrated in Figs. 7, 8, 9 and 12. The footprint of the antenna radiation patter is, in fact, mirrored approximately in the mismatch rate map with yellow and blue colors;
- the use of directive antennas (or equivalently beamforming), can significantly change the PLS performance of Alice and Bob key matching and their isolation against Eve, with respect to the case of omni-directional antennas. This was explained by Fig. 11, confirming once more the importance of taking into account the radiating antenna elements in the PLS modelling, and not only the radio channel.
- we need to work towards a CRKG optimization, trying to achieve a sort of awareness of the PHY conditions for PLS key exchange: for example, estimating the available entropy in the channel and setting a proportional target of maximum security level; or, for example, estimating the SNR and the reciprocity, predicting if the keys reconciliation will fail or not. This can help to build a proactive PLS protocol, rather than reactive or best-effort.

REFERENCES

[1] Li Sun and Qinghe Du. A review of physical layer security techniques for internet of things: Challenges and solutions. Entropy, 20(10):730, 2018.

[2] Rushan Lin, Li Xu, He Fang, and Chuan Huang. Efficient physical layer key generation technique in wireless communications. EURASIP Journal on Wireless Communications and Networking, 2020(1):1–15, 2020.

[3] Soheyb Ribouh, Kelvin Phan, Arnav Vaibhav Malawade, Yassin Elhillali, Atika Rivenq, and Mohammad Abdullah Al Faruque. Channel state information-based cryptographic key generation for intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 2020.

[4] Kemedi Moara-Nkwe, Qi Shi, Gyu Myoung Lee, and Mahmoud Hashem Eiza. A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. IEEE Access, 6:11374–11387, 2018.

[5] Yulong Zou, Jia Zhu, Liuqing Yang, Ying-Chang Liang, and Yu-Dong Yao. Securing physical-layer communications for cognitive radio networks. IEEE Communications Magazine, 53(9):48–54, 2015.

[6] Abraham Sanenga, Galefang Allycan Mapunda, Tshepiso Merapelo Ludo Jacob, Leatile Marata, Bokamoso Basutli, and Joseph Monamati Chuma. An overview of key technologies in physical layer security. Entropy, 22(11):1261, 2020.

[7] Christian T. Zenger, Mario Pietersz, Jan Zimmer, Jan-Felix Posielek, Thorben Lenze, and Christof Paar. Authenticated key establishment for low-resource devices exploiting correlated random channels. Computer Networks, 109:105–123, 2016. Special issue on Recent Advances in Physical-Layer Security.

[8] Jehad M Hamamreh, Haji M Furqan, and Huseyin Arslan. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2):1773–1828, 2018.

[9] Sriram Nandha Premnath, Suman Jana, Jessica Croft, Prarthana Lakshmane Gowda, Mike Clark, Sneha Kumar Kasera, Neal Patwari, and Srikanth V Krishnamurthy. Secret key extraction from wireless signal strength in real environments. IEEE Transactions on mobile Computing, 12(5):917–930, 2012.

[10] Junqing Zhang, Alan Marshall, and Lajos Hanzo. Channel-envelope differencing eliminates secret key correlation: Lora-based key generation in low power wide area networks. IEEE Transactions on Vehicular Technology, 67(12):12462–12466, 2018.

[11] J. Zhang, R. Woods, T.Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu. Experimental study on key generation for physical layer security in wireless communications. IEEE Access, 4:4464–4477, 2016.

[12] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In Proceedings of the 14th ACM international conference on Mobile computing and networking, pages 128–139, 2008.

[13] Jiang Wan, Anthony Bahadir Lopez, and Mohammad Abdullah Al Faruque. Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security. In 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), pages 1–10. IEEE, 2016.

[14] Miroslav Mitev, Arsenia Chorti, Martin Reed, and Leila Musavian. Authenticated secret key generation in delay-constrained wireless systems. EURASIP Journal on Wireless Communications and Networking, 122(1), 2020.

[15] Hongbo Liu, Yang Wang, Jie Yang, and Yingying Chen. Fast and practical secret key extraction by exploiting channel response. In 2013 Proceedings IEEE INFOCOM, pages 3048–3056. IEEE, 2013.

[16] Marco Zoli, André Noll Barreto, Stefan Köpsell, Padmanava Sen, and Gerhard Fettweis. Physical-layer-security box: a concept for time-frequency channel-reciprocity key generation. EURASIP Journal on Wireless Communications and Networking, 2020:1–24, 2020.

[17] Marco Zoli, André Barreto, and Gerhard Fettweis. Investigating the eavesdropper attack in physical layer security wireless key generation: a simulation case study. In accepted for publication at IEEE Vehicular Technology Conference (VTC-Spring), number April, Helsinki, Finland, 2021.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3131616, IEEE Access

[18] Michel Daoud Yacoub. The $\alpha - \eta - \kappa - \mu$ fading model. IEEE Transactions on Antennas and Propagation, 64(8):3597–3610, 2016.

[19] Aashish Mathur, Yun Ai, Manav R. Bhatnagar, Michael Cheffena, and Tomoaki Ohtsuki. On physical layer security of $\alpha - \eta - \kappa - \mu$ fading channels. IEEE Communications Letters, 22(10):2168–2171, 2018.

[20] Stephan Jaeckel, Leszek Raschkowski, Kai Börner, and Lars Thiele. Quadriga: A 3-d multi-cell channel model with time evolution for enabling virtual field trials. IEEE Transactions on Antennas and Propagation, 62(6):3242–3256, 2014.

[21] S Jaechel, L Raschakowski, K Borner, and L Thiele. Quadriga—quasi deterministic radio channel generator. User Manual and Documentation, 2019.

[22] Junqing Zhang, Guyue Li, Alan Marshall, Aiqun Hu, and Lajos Hanzo. A new frontier for iot security emerging from three decades of key generation relying on wireless channels. IEEE Access, 8:138406–138446, 2020.

[23] Guyue Li, Aiqun Hu, Chen Sun, and Junqing Zhang. Constructing Reciprocal Channel Coefficients for Secret Key Generation in FDD Systems. IEEE Communications Letters, 22(12):2487–2490, 2018.

[24] S. Tmar-Ben Hamida, J.-B. Pierrot, B. Denis, C. Castelluccia, and B. Uguen. On the Security of UWB Secret Key Generation Methods against Deterministic Channel Prediction Attacks. In 2012 IEEE Vehicular Technology Conference (VTC Fall), pages 1–5. IEEE, September 2012.

[25] Miroslav Mitev, Arsenia Chorti, E. Veronica Belmega, and H. Vincent Poor. Protecting physical layer secret key generation from active attacks. Entropy, 23(8), 2021.

[26] Christopher Huth, René Guillaume, Thomas Strohm, Paul Duplys, Irin Ann Samuel, and Tim Güneysu. Information reconciliation schemes in physical-layer security: A survey. Computer Networks, 109:84–104, November 2016.

[27] James Massey. Step-by-step decoding of the bose-chaudhuri-hocquenghem codes. IEEE Transactions on Information Theory, 11(4):580–585, 1965.

[28] Yagiz Sutcu, Qiming Li, and Nasir Memon. Protecting biometric templates with sketch: Theory and practice. IEEE Transactions on Information Forensics and Security, 2(3):503–512, 2007.

[29] Nicholas Metropolis and Stanislaw Ulam. The monte carlo method. Journal of the American statistical association, 44(247):335–341, 1949.

[30] Vishwanath Ramamurthi and Wei-Peng Chen. Mobility based mimo link adaptation in lte-advanced cellular networks. pages 235–241, 11 2010.

[31] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, NIST Special Publication, 2001.

[32] Nasser Aldaghri and Hessam Mahdavifar. Physical Layer Secret Key Generation in Static Environments. IEEE Transactions on Information Forensics and Security, 15:2692–2705, 2020.

[33] Junqing Zhang, Alan Marshall, Roger Woods, and Trung Q Duong. Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers. IEEE Transactions on Communications, 64(6):2578–2588, 2016.

ALESSANDRO SANTORSOLA received the Bachelor Degree in Computer Engineering and the Master Degree in Telecommunication Engineering (Cyber Security) from the Polytechnic University of Bari, Bari, Italy, in 2018 and 2021, respectively. His main research interests are wireless and network security, IoT & IIoT, numerical simulations,physical layer security and ML/AI algorithms for security.

MARCO ZOLI received the Ph.D.degree on Radio Channel Characterization for Future Wireless Networks and Applications, from University of Bologna, Italy, in 2018. He joined the Barkhausen Institut, Dresden, Germany, in 2019, as Research Associate, working on Physical Layer Security. His main research interests are antennas, telecommunications, wireless technologies, security and privacy, numerical simulations and open science.

ANDRÉ NOLL BARRETO (Senior Member, IEEE) received the M.Sc. degree in electrical engineering from Catholic University (PUC-Rio), Rio de Janeiro, Brazil, in 1996, and the Ph.D. degree in electrical engineering from Technische Universität Dresden, Germany, in 2001. He held several positions with academia and industry in Switzerland (IBM Research) and Brazil (Claro, Nokia Technology Institute/INDT, Universidade de Brasília, and Ektrum). He joined the Barkhausen Institut, Dresden, Germany, in 2018. He is currently researching wireless communications for the reliable, resilient, and secure Internet of Things. He was the Chair of the Centro-Norte Brasil Section of the IEEE in 2013 and 2014, and the General Co-Chair of the Brazilian Telecommunications Symposium in 2012.

VINCENZO PETRUZZELLI graduated in Electrical Engineering at the University of Bari in 1986. He is currently engaged as Associate Professor in Electromagnetic Fields at the Department of Electrical and Electronic Engineering, Polytechnic University of Bari. He is a Member of Electronic Engineer doctorate Courses. He acts as Reviewer of European and National Projects. He was member of the Management Committee of the MP0805 COST action ”Novel Gain Materials and Devices Based on III-V-N Compounds”. Over the years he has dealt with various research topics: integrated plasmonic nanoantennas for wireless on-chip optical communications; innovative optical devices for the optical Interconnects on chip; periodic structures for laser cavities based on the optical self-collimation property of mesoscopic structures; plasmonic periodic nanostructures for the realization of plasmonic sensors. He has coauthored over 330 publications, 132 of which published on international journals and 155 presented at international conferences.

GIOVANNA CALÒ (M’03) received the Master Degree in Electronic Engineering and the Ph.D. degree in Electromagnetism from the Polytechnic University of Bari, Bari, Italy, in 2002 and 2006, respectively. She joined the Department of Electrical and Electronic Engineering, Polytechnic University of Bari, in 2002, where she is currently Associate Professor of Electromagnetism. Her main research interests are computational electromagnetics, on-chip optical interconnections, integrated plasmonic nanoantennas for wireless on-chip optical communications, photonic crystals, plasmonic nanostructures and components.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/