Estimation of the Secret Key Rate in Wideband Wireless Physical-Layer-Security

Marco Zoli, Miroslav Mitev, André N. Barreto and Gerhard Fettweis
Barkhausen Institut gGmbH
Dresden, Germany

***Abstract*—In this work we investigate the problem of secret key generation (SKG) between two communicating wireless devices, according to the physical-layer security paradigm. We propose a general framework for any communication channel or waveform. In details, we study a filterbank-based method, which allows the generation of secret security keys from a wideband radio channel, independently from the baseband modem implementation. We believe that channel awareness is of utmost importance to understand the applicability of SKG methods, i.e., knowing their secret bit-rate under different channel scenarios. For that purpose, we investigate the SKG performance by means of Monte Carlo simulations that collect radio channel statistics and obtain the SKG performance through mutual information numerical estimation.**

I. Introduction

As wireless communications become pervasive elements of our life, ensuring their reliability and security is becoming ever more crucial. Cryptography is fundamental to adequately achieve privacy, confidentiality, integrity and authentication in digital communications. The current security framework of connected systems relies on cryptographic protocols applied at the upper network layers. However, these cryptographic tools may not satisfy the needs of future heterogeneous Internet-of-things (IoT) paradigm. In fact, encryption and key distribution protocols might not easily scale with the number of devices, satisfy strict latency requirements, or, furthermore, respect a low energy consumption [1]. Moreover, quantum computing promises to undermine asymmetric cryptography schemes [2], which are the fundamental part of modern security mechanisms. Over the last decades a branch of information theory, called physical-layer security (PLS) has evolved opening opportunities for lightweight quantum-proof security protocols. The goal of PLS is to increase the security of communication links by exploiting the properties of the physical layer (PHY), i.e., noise, interference, propagation and circuits. Promising PLS schemes include: radio-frequency (RF) fingerprinting, physical unclonable functions (PUFs) and wiretap codes. For a comprehensive survey on the topic, we refer the reader to [3]. It is worth noting that this promising technique has been so far confined to theoretical work or laboratory experiments, and not yet employed in real-life communications systems, such as 3GPP-5G and WiFi [4]. Considering the upcoming challenges of future generation networks, such as 6G, it is clear that an holistic security paradigm should support strong security protocols, but also scalability and flexibility to reduce energy consumption or latency. Thus, PLS methods are likely to be an important complement to the existing encryption infrastructure [5].

In this work we focus on the PLS-based secret key generation (SKG) approach. SKG aims at solving the key exchange problem between two communicating devices by exploiting the reciprocity of radio channels as a common source of randomness. The key extracted from the radio channel can be used in a symmetric cipher, such as the advanced encryption standard (AES), to achieve confidentiality. In fact, SKG can be in principle performed on-demand, reusing communications data, and saving so time and energy. It is still necessary to bridge the gap between theoretical PLS results and real-life implementations, working towards the realization of lightweight security schemes [4], [6]. Several methods were proposed in the literature to implement SKG by mapping PHY observable quantities into binary keys, such as RSSI-based methods [7], or, OFDM-based methods [8], by observing channel-state-information (CSI). An overview of the literature on SKG can be found in [1].

In practise, there are difficulties for SKG. For once, the PLS system architecture: the interaction of all the parts must be understood by a joint communication and security perspective. For instance, many approaches assume that we can obtain CSI from the communication baseband processor (named hereby modem) to generate the keys. This CSI information is usually not available from external interfaces, or, when it is, may not be trustworthy. With this in mind, the authors proposed in [4] the concept of a PLS-Box: a dedicated PHY container where to implement the PLS functions. In particular, by tapping the received signal directly from the RF front-end (without relying on the modem) some information about the radio channel can be derived and used in the key exchange. This can be done by means of a ”filterbank” [4] processing, in which parallel filters decompose the received signal over the communication bandwidth, providing as output an observation of the channel [9]. The channel frequency-selective property is in fact exploited to generate a random bit sequence. By doing so, it is not necessary to replicate all the modem functions like synchronization and channel estimation and, also, SKG can work with any PHY waveform (as long as its transmitted power spectral density is known), without the requirement of a matched receiver, e.g., as in the OFDM methods. Another big challenge is that SKG performance depends heavily on the actual channel statistics, both in time and in space. Differently from conventional method, the

PLS paradigm is based on stochastic processes (such as the radio channel), but must be anyway capable to provide stable security solutions in most real-life situations. or example, the presence of direct line-of-sight plays a crucial role, limiting the randomness of the channel and, consequently, the size of the generated secret key [4]. Therefore, PLS requires a "channel awareness" in order to control its reliability. This means that we must know when SKG can generate a given number of secret bits or not, because of the radio channel. The final SKG rate depends on many implementation aspects, such as the employed quantization method, reconciliation protocol and privacy amplification technique [1]. However, the theoretical SKG rate represents the maximum number of secret bits to extract and use. After observing (or estimating) the reciprocal channel, two communicating devices can only keep the amount of valuable information bits at disposal at PHY layer. According to the concept of data processing inequality [10], any further processing can only indeed reduce the amount of information (i.e., entropy) that we want to convey onto the SKG key. This motivates the goal of this work, i.e. the estimation of the maximum SKG rate in terms of mutual information. Then, we show how the SKG performance depend on channel parameters such as the delay spread, as well as on implementation parameters, such as the number of the filters.

The rest of the paper is organized as follows: Section II reviews the basic concepts of the SKG process and introduces our channel model. Section III presents our simulation set-up and Section IV the corresponding numerical evaluation for the proposed scheme. Finally Section V concludes this paper.

II. Secret Key Generation in Wideband Channels

A. Secret Key Generation

We analyze two wireless devices, namely Alice and Bob, who want to communicate confidentially. To protect their communication, Alice and Bob use a symmetric cipher for encryption and decryption of their messages. However, to properly operate the cipher at both ends, a shared secret key must be generated and exchanged. Generating and sharing this symmetric key is the key exchange problem between Alice and Bob that we want to solve.

We propose a solution utilizing the concept of PLS-based SKG using the radio channel reciprocity. First, we assume that Alice and Bob are already authenticated. At PHY, we assume that Alice and Bob communicate using a wideband waveform with known power spectral density (PSD), or that both transmitters have the same PSD. Also, it is assumed that they operate in time-division duplex (TDD) on the same frequency bandwidth. The waveform transmitted by Alice is received by Bob with distortion, according to the channel impulse response (CIR) caused by multipath propagation. Assuming that the channel is static between two TDD slots and ignoring hardware impairments, the channel between Alice and Bob can be considered to be reciprocal. Thus, the same CIR can be observed on the reverse direction, when Bob transmits a waveform to Alice. As the location of all the reflections and scatterers in the environment is unknown, the CIR can be considered to be random. Furthermore, it uniquely characterizes the link between Alice and Bob: they can use the propagation channel as a common entropy source, from which a secret channel "signature" can be extracted. The presence of multipath is an advantage for the purpose of PLS, as it increases the source entropy, protecting Alice and Bob from external attackers. Because of the spatial decorrelation [11] observed in wireless propagation channels, an eavesdropper Eve has small chances to experience the same propagation effects when she is located in a different position away from Bob and/or Alice [1].

The theoretical secret key rate is the maximum number of bits that can be secretly generated. Given the noisy channel observation vectors $\mathbf{C}^A$, $\mathbf{C}^B$, $\mathbf{C}^E$ at Alice, Bob and Eve, respectively, Maurer [12] has derived lower and upper bounds for the secret key rate $R\left(\mathbf{C}^A;\mathbf{C}^B|\mathbf{C}^E\right)$. In this paper we assume that the observations of Eve are independent from the observations at Alice and Bob. In this case these bounds become:

$$R(\mathbf{C}^A,\mathbf{C}^B|\mathbf{C}^E) = I\left(\mathbf{C}^A,\mathbf{C}^B\right) \tag{1}$$

where I is the mutual information to be estimated.

B. Channel model

Differently from conventional cryptographic key exchange methods, such as Diffie-Hellman, SKG methods depend on the temporal and spatial properties of the radio channel, which are usually unknown and may change over time. In this work, we consider the equivalent baseband radio channel in time domain, with a time-invariant CIR modelled as follows:

$$s(t) = \sum_{i}^{N_p} a_i \delta(t-\tau_i) \tag{2}$$

where N_p is the number of multipath components, $\delta(t)$ is the Dirac impulse function, and a_i, τ_i are the complex amplitude and the propagation delay of the i-th path. This CIR characterizes completely the radio channel between Alice and Bob. Depending on the environment, a_i and τ_i shape the multipath, defining the energy dispersion over time. Equation (2) can be transformed into frequency domain as follows:

$$S(f) = \sum_{i}^{N_p} a_i e^{-j(2\pi f \tau_i)} \tag{3}$$

$S(f)$ is our starting point in the SKG evaluation, since everything is based on channel reciprocity. It represent the channel-transfer-function and is composed by a sum of complex exponential, including the parameters a_i and τ_i, for each path. Calling $\varphi_i = 2\pi f \tau_i$, its composition is illustrated in Figure 1 for a generic frequency f. The constructive or destructive sum of the complex vectors in (3) determine the frequency selectivity in the communication bandwidth. In case of $N_p \to \infty$, thanks to the central limit theorem, we know that $|S(f)|$ follow a Rayleigh distribution, and $|S(f)|^2$ a χ-squared distribution.

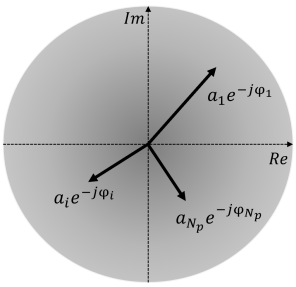

Figure 1. Illustration of $S(f)$ in terms of sum of complex exponentials, for a generic f frequency. This represents the entropy source for SKG.

C. Signal model

We assume that Alice and Bob exchange information using wideband waveforms $x^A(t)$ and $x^B(t)$. Based on that, the received signals at Alice and Bob, respectively, can be expressed as

$$y^A(t) = s(t) * x^B(t) + n^A(t) \tag{4}$$

$$y^B(t) = s(t + \Delta t) * x^A(t + \Delta t) + n^B(t + \Delta t) \tag{5}$$

where n^A and n^B denote the independent additive white Gaussian noise (AWGN) terms observed at Alice and Bob, respectively and $*$ the convolution operator. The delay Δt accounts for the fact that in a TDD system Alice and Bob observe the channel at different time instants. We consider the radio channel to be time-invariant, by neglecting its evolution over time, i.e., $s(t) = s(t + \Delta t)$. Assuming a high signal-to-noise ratio (SNR) regime, and translating the above equations into the frequency domain we obtain simply:

$$Y^A(f) \approx S(f) \cdot X(f) \approx Y^B(f) \tag{6}$$

where $Y^A(f), Y^B(f)$ and $X(f)$ corresponds to the Fourier transform of $y^A(t), y^B(t)$ and $x(t)$, respectively. It is clear that the reciprocity of the channel is reflected in the received signals of Alice and Bob, without the need to perform a direct estimation of the channel.

Given this, we want to answer the following question:
How many information bits can be generated by Alice and Bob observing the radio channel for SKG?

To answer we must estimate the mutual information between Alice and Bob as common shared entropy, as described in (1). Generally, the entropy pool available for SKG depends on the statistical nature of multipath, which itself depends on the physical and environmental scenario of the wireless link. This includes the antennas, the objects in the surroundings, the carrier wavelength and the RF processing chains. Here in our simplified model, the complexity of the radio channel is modelled only by the channel amplitudes a_i and delays τ_i for all paths with index i, as given in (3). In the following, to answer we provide a numerical evaluation of the mutual information using a Monte Carlo simulation. We calculate the number of secret bits that can be generated at a single channel realization. The analysis can be easily extended to obtain the number of bits generated per unit of time by considering the coherence time of the channel [4]. Note that the other required steps in the SKG protocol, as outlined in [1], [4], fall out of the scope of the work.

III. Simulation set-up

The equivalent baseband radio channel is given by a tapped-delay-line (TDL) model provided in 3GPP TR 38.901 v16 Section Sec.7.7.2 [13]. In particular, the channel TDL-A has been used in the simulations. The advantages of this choice are twofold: the TDL model is fast to simulate, and has a flexible delay spread (DS) parameter. The channel is non-line-of-sight, with independent Rayleigh fading at each path, and no Doppler is considered. The number of paths N_p is fixed to 23, with no specific clustering. Large-scale fading phenomena such as path-loss or shadowing are not taken into consideration in this work. Antennas are assumed ideally isotropic. An example of realization of this channel model, is given by Figure 2, where a power-delay-profile is illustrated as $10\log_{10}(|s(t)|^2)$ recalling (2).

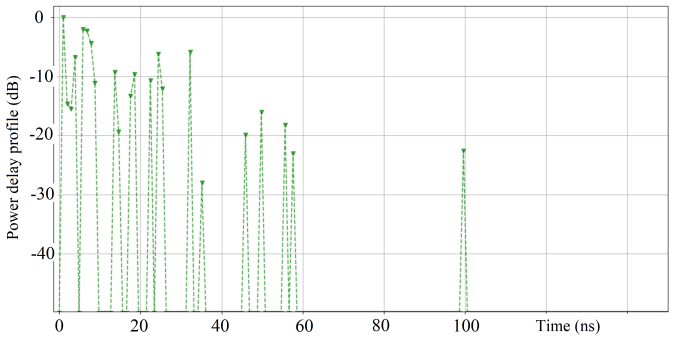

Figure 2. Power-delay-profile of the TDL-A channel model with a delay spread of 10 ns. The power on the vertical axis is normalized in relation to the strongest path to 0dB.

In our simulation, the communication waveform (i.e, $x(t)$) is an unmodulated chirp with constant envelope. This choice allows Alice and Bob to probe the channel with a known PSD over the defined bandwidth, equal to 500 MHz. The bandwidth enables a time-domain CIR resolution of 2 ns.

For each Monte-Carlo iteration, the realization of a received signal (i.e, $y(t)$) is obtained by convolving the transmitted chirp waveform with a CIR realization of the baseband radio TDL-A, plus additive white thermal noise. The SNR computed on the signals samples has been set to 10dB. Finally, the Monte-Carlo simulation iterates over 5×10^5 channel and noise realizations.

A. Channel signature

For each Monte-Carlo round, we process the received signals performing a PSD estimation using Welch's method to obtain the channel information over frequency. Considering Figure 3, the blue curve is an example of the transmitted chirp PSD, and the green curve is an example of the received PSD by Alice. Recalling (6), the received PSD is in fact proportional

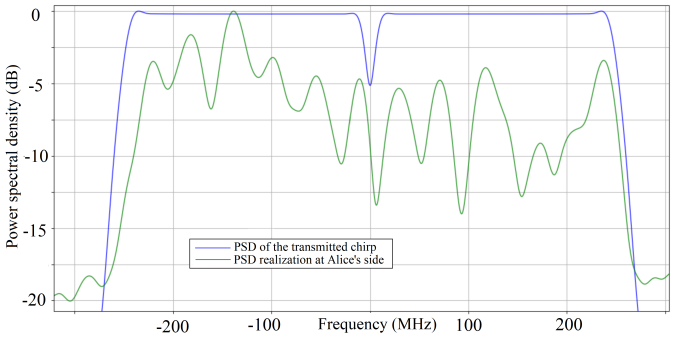

Figure 3. Comparison between the PSD of the transmitted chirp and an example of Alice's received PSD, containing the channel signature. The power on the vertical axis is normalized to 0 dB.

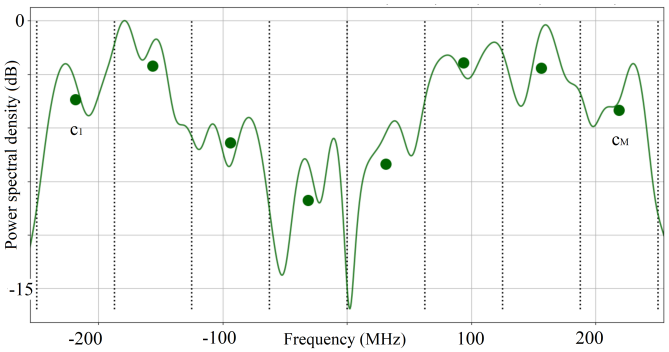

Figure 4. A realization of Alice's channel observation with $M = 8$ filters. The power on the vertical axis is normalized to 0 dB.

to $10\log_{10}(|Y(f)|^2)$, and it contains the channel signature, i.e. $10\log_{10}(|S(f)|^2)$. This means that the power fluctuations in the green curve over the bandwidth represent the frequency selectivity of the TDL-A model, i.e., the valuable entropy source for SKG.

In line with our SKG purpose, two considerations are here anticipated:

- the dynamic range of fades determines the range of values for the PSD. This will be the support of the distribution of the channel observation points (i.e., (1) $\mathbf{C}^A$ and $\mathbf{C}^B$);
- the PSD values along the frequency are correlated to each other [9]. The correlation among different frequency components is dependent on the power delay profile of the channel in (2).

B. Channel observation

According to the proposed framework in [4], we proceed our analysis by explaining how Alice and Bob obtain channel observations starting from the signals in (4). We assume that Alice and Bob do not obtain the full PSD, but only a discretized version of it. This flexible way of processing includes the case of OFDM, with a number of spaced sub-carriers, but also the proposed method based on parallel filters. To account for that, we equivalently implement the filtering by ideally dividing the PSD into M sub-bands over the bandwidth. Figure 4 shows an example of this with $M = 8$. The vertical dotted lines represent the boundaries of the filters, whereas the green dots represent the corresponding filtering output in terms of power in dB. The green dots are the observations points, indicated with $\mathbf{C}^A$ and $\mathbf{C}^B$, for Alice and Bob. They are computed by simply averaging the PSD values falling into each sub-band from 1 to M. In the end, these points represent the channel signature samples to be quantized into SKG bits. As explained in [4], the same processing can be achieved with actual finite-impulse-response filters in analog or digital design.

Within our Monte Carlo simulation, the realizations of these filters outputs compose the necessary statistics for estimating the mutual information between Alice and Bob. The j-th element c_j^A in $\mathbf{C^A}$ of Alice's set, is modelled as a random variable, correlated to the others over the bandwidth, but also coupled to the Bob's corresponding variable c_j^B, thanks to channel reciprocity. Only AWGN alters the perfect reciprocity between the two sets of channel observation in this work.

C. Mutual Information estimation

Finally, we estimate the mutual information (I) between Alice and Bob filters outputs, expressed in the following terms (H means Shannon entropy):

$$I = \int_{D_\mathbf{C}} \int_{D_\mathbf{C}} p_J(\mathbf{C}^A, \mathbf{C}^B) \log_2 \left(\frac{p_J(\mathbf{C}^A, \mathbf{C}^B)}{p(\mathbf{C}^A) p(\mathbf{C}^B)} \right) d\mathbf{C}^A d\mathbf{C}^B \tag{7}$$

where $p_J(\cdot)$ denotes the joint Alice-Bob probability density function (PDF), $p(\cdot)$ denotes the marginal PDF, and $D_\mathbf{C}$ is the M-dimensional domain of the random vectors $\mathbf{C}^A$ and $\mathbf{C}^B$. In detail we have:

$$I(\mathbf{C}^A, \mathbf{C}^B) = H(\mathbf{C}^A) + H(\mathbf{C}^B) - H_J(\mathbf{C}^A, \mathbf{C}^B) \tag{8}$$

$$H(\mathbf{C}^A) = H(c_1^A, \ldots, c_M^A) \tag{9}$$

$$H(\mathbf{C}^B) = H(c_1^B, \ldots, c_M^B) \tag{10}$$

$$H_J(\mathbf{C}^A, \mathbf{C}^B) = H(c_1^A, \ldots, c_M^A; c_1^B, \ldots, c_M^B) \tag{11}$$

The optimal conditions to have maximum entropy would achieved with independent filters outputs, with an ideal fading range down to $-\infty$ dB. In our simulation, we noticed that the minimum fading point is around -25 dB, because of the channel frequency selectivity and the SNR$= 10$ dB. Different results can be obtained with different channel models or bandwidth. In practise, as rule of thumb, we compute here an upper bound of the possible marginal entropy. We assume to have an excursion of 25 dB for each filter observation point, a resolution of 0.1 dB in power, and that each filter output is uniformly distributed in $[-25, 0]$ dB. Finally:

$$H_{max}(M) = \sum_j^M H(c_j) = M \cdot \log_2(250) = M \cdot 7.97 \tag{12}$$

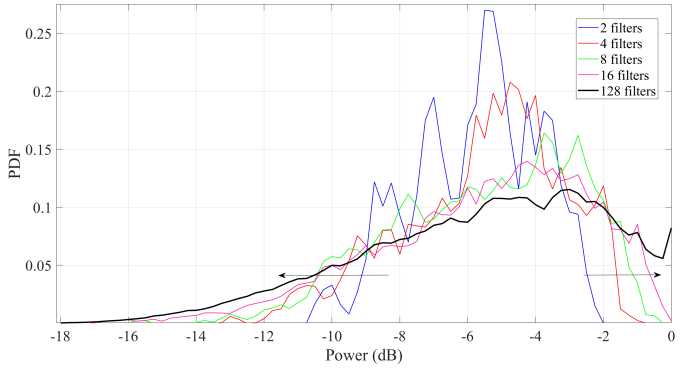

Figure 5. The probability density functions of the observed filters outputs. The delay spread of the TDL channel is 10 ns.

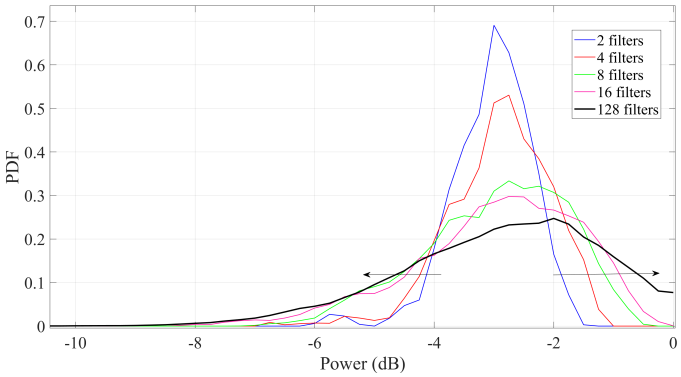

Figure 6. The probability density functions of the observed filters outputs. The delay spread of the TDL channel is 300 ns.

so an upper bound of approximately 8 bit (1 Byte) per filter with ideal channel conditions for SKG. Being Alice and Bob in high SNR regime, we know that $H(\mathbf{C}^A) \approx H(\mathbf{C}^B)$:

$$I(\mathbf{C}^A, \mathbf{C}^B) \leq H_{max}(M) \tag{13}$$

Unfortunately, this value is only indicative, and is not reachable in reality. Filters outputs are correlated and their non-uniform distributions significantly diminish the available entropy, as shown in the following.

In the end, obtaining a closed-form solution for (7) for any arbitrary channel power delay profile can be a daunting task, because of the distributions of multipath parameters α and τ in (3). In this work we use the NPEET library (https://github.com/gregversteeg/NPEET), which implements Kraskov estimators [14], to solve (7). This library allows the estimation of the mutual information directly from the continuous-value filters outputs (i.e., $\mathbf{C}$), without the estimation of their joint PDFs and without any assumptions on their distribution or correlation.

IV. Results

A. Monte Carlo results

Table I presents the NPEET estimation of mutual information for $M = 2, 4, 8$ filters, over 4 different radio channel DS: 10, 30, 100, and 300 ns. This choice includes most of the modern radio link scenarios with a short, medium and long DS [9]. Because of computational constraints, i.e., due to the M dimensions of observation points, we show results only up to 8 filters. This limit is due to the problem known as curse of dimensionality [15], which increases non-linearly the convergence time with the number of filters, and is still an open research topic.

Table I
Mutual Information Results

	Delay Spread [ns]			
	10	30	100	300
2 filters, mutual info [bit]:	7.1	6.5	5.8	4.6
4 filters, mutual info [bit]:	13.7	12.7	11.3	9.0
8 filters, mutual info [bit]:	19.2	16.8	15.6	14.1

Although these preliminary results are not enough to support general conclusions for SKG (for example with 128 bits of key size), we can outline some interesting trends:

1) increasing the number of filters results in more bits of mutual information;
2) increasing the delay spread results in less bits of mutual information.

To explain these numerical results, we analyzed the marginal PDF of the filters outputs for several values of M, with DS equal to 10 and 300 ns. This is shown in Figures 5 and 6, respectively. We also performed a fitting of the PDFs to characterize the distributions found in the simulations. Selecting the case with 128 filters (black curves in figures),

we found that the best fit is given by the Weibull distribution, with λ as scale parameter and k as shape parameter. In detail, when choosing a DS equal to 10 ns, the parameters of the distribution are $\lambda = 1.66$ and $k = 6.67$, whereas in case of DS equal to 300 ns, the parameters become $\lambda = 1.75$ and $k = 3.43$. Considering a generic filter output, its marginal PDF is then approximately:

$$p(c, k, \lambda) = \frac{k}{\lambda}\left(\frac{-c}{\lambda}\right)^{k-1} e^{-(-c/\lambda)^k}, \ \forall -c \geq 0 \qquad (14)$$

where c represent the power value observed at the filter's output in dB, as illustrated in Figure 4.

B. Mutual information vs number of filters

With reference to Figures 5 and 6, it is observed that the increase in the number of filters M, i.e., from 2 to 128, results in greater spread of the PDF and therefore, indirectly increases the overall entropy. This confirms the results found in the Table I. Even though this result seems a natural conclusion, the mutual information cannot grow indefinitely, hence, we expect that the achievable mutual information versus M will saturate: there must be an optimal choice for the value of M, where Alice and Bob obtain most of the available entropy in common. Moreover, we need to keep in mind that the degree of intra-correlation over the bandwidth is in fact limiting the achievable mutual information, as compared to an ideal scenario, where all filters outputs are independent. In other words, a large number of filters M can help to harvest more entropy, but increases the risk to generate correlated bits in the SKG key, after quantization. This would reduces the effective randomness of the secret key and its security strength.

C. Mutual information vs delay spread

In our simulations, experiencing a higher DS directly impacts the filter outputs, resulting into smaller fades depth. Comparing Figures 5 and 6, a clear difference is observed between the distribution tails at the left side of the figures. Figure 5 can reach -18 dB, whereas Figure 6 approximately -10 dB. This limits the variance of the filters' outputs, hence, reducing the entropy for SKG (independently from their distribution). This can be explained by the fact that increasing the DS, results into higher number of resolvable paths (the bandwidth is always equal to 500MHz). This directly impacts the distribution of the filter's output as the overall power is the sum of the powers of these resolvable paths. In fact, for a high number of paths this distribution can be approximated by a gamma or chi-squared distribution, whose degrees of freedom increase with the number of resolvable paths [16], and becomes less random. By having a restricted support of the distributions in the observed points, the attainable entropy in common is therefore smaller than what is available in the channel signature.

V. Conclusions

In this work we have shown a new investigation approach to assess the SKG rate in wideband channels. The proposed general framework uses numerical mutual information estimators to assess the achievable SKG rate between Alice and Bob over 500 MHz of communication bandwidth. We have implemented a Monte Carlo simulation to collect realistic statistics of the radio channel. Our results show values of mutual information ranging from 5 to 20 bits, using 2 to 8 filters, respectively. Further research is necessary to expand this preliminary work to a larger number of filters and to take care of the correlation of their outputs. As a future work we plan to investigate more channels models, e.g., Ricean, and also introduce the adversary Eve in our model.

Acknowledgment

This work is financed by the Saxon State government out of the State budget approved by the Saxon State Parliament.

References

[1] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[2] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, Sep. 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8490169/

[3] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[4] M. Zoli, A. N. Barreto, S. Köpsell, P. Sen, and G. Fettweis, "Physical-Layer-Security Box: a concept for time-frequency channel-reciprocity key generation," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, no. 1, p. 114, Dec. 2020. [Online]. Available: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-020-01712-6

[5] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, and I. Oppermann, "6G white paper: Research challenges for trust, security and privacy [white paper]," *6G Research Visions, University of Oulu*, 2020.

[6] W. Trappe, "The challenges facing physical layer security," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 16–20, Jun. 2015. [Online]. Available: http://ieeexplore.ieee.org/document/7120011/

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. 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*, 2008, pp. 128–139.

[8] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 3048–3056.

[9] M. Zoli, A. Barreto, and G. Fettweis, "Investigating the eavesdropper attack in physical layer security wireless key generation: a simulation case study," in *IEEE Vehicular Technology Conference (VTC-Spring)*, no. April, Helsinki, Finland, 2021.

[10] T. Cover, *Elements of information theory*, J. W. . Sons, Ed., 2012.

[11] S. Salous, *Radio Propagation and Channel Modelling*, J. W. . Sons, Ed., 2013.

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

[13] 3GPP, "Release 16, TR 38.901, Study on channel model for frequencies from 0.5 to 100 GHz," accessed 2019. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications

[14] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical Review E*, vol. 69, no. 6, p. 066138, Jun. 2004. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevE.69.066138

[15] N. Kouiroukidis and G. Evangelidis, "The effects of dimensionality curse in high dimensional kNN search," in *2011 15th Panhellenic Conference on Informatics*, 2011, pp. 41–45.

[16] U. Karabulut, A. Awada, I. Viering, A. N. Barreto, and G. P. Fettweis, "Low complexity channel model for mobility investigations in 5g networks," in *IEEE Wireless Comm. and Networking Conf. (WCNC)*, no. May, Seoul, Korea, 2020.