Optimal Resource Allocation in Joint Secret Key Generation and Data Transfer Schemes

Miroslav Mitev
School of CSEE
University of Essex
Colchester, UK
Email: mm17217@essex.ac.uk

Arsenia Chorti
ETIS, Université Paris Seine,
Université Cergy-Pontoise, ENSEA, CNRS
Cergy-Pontoise, France
Email: arsenia.chorti@ensea.fr

Martin Reed
School of CSEE
University of Essex
Colchester, UK
Email: mjreed@essex.ac.uk

***Abstract*—Due to computational complexity and latency constraints in the nodes of many IoT systems, alternatives to public key encryption are sought for session key generation schemes. In this work we investigate novel cross-layer security protocols in which session keys are generated at the physical layer using standard techniques of secret key generation (SKG) from shared randomness. In this framework, we study the optimal power allocation in block-fading additive white Gaussian noise (BF-AWGN) channels, with short-term power constraints, when a subset of the subcarriers are used for SKG and the rest for data transmission. Fixing the amount of data that can be transmitted with a single key, allows us to first identify the optimal subset of subcarriers that should be devoted to SKG and the respective power allocation policy which, depending on the available overall power, might not be unique. Subsequently, a further step is taken in our analysis to account for the impact of the proposed power allocation with long-term power-constraints.**

***Index Terms*—Shared randomness, secret key generation, resource allocation, physical layer security, wireless communications.**

I. Introduction

A major concern in the deployment of IoT and ad-hoc networks is related to security. Many standard cryptographic schemes, particularly those in the realm of public key encryption (PKE), are computationally intensive and can rapidly drain the battery of power constrained devices [1], [2]. To address such issues the national institute of standards and technology (NIST) has recently published its report on approved lightweight cryptographic primitives; these include many standard symmetric key block ciphers such as the advanced encryption standard (AES) and many newer lightweight ones, e.g., CLEFIA, but exclude the well known PKE schemes such as the Rivest-Shamir-Adleman (RSA) or the Diffie-Helman and the El Gamal variant. The reason for the latter decision is the fact that they are not quantum resistant with key lengths manageable by constrained IoT nodes [3]. Therefore, lightweight quantum resistant alternatives to PKE for key generation and distribution are needed.

A promising avenue in this direction, which is currently being considered for beyond fifth generation (B5G) systems, is offered by physical layer security (PLS). Of particular interest in PLS technologies are techniques for secret key generation (SKG) from shared randomness that have been shown to provide a viable alternative for quantum resistant, lightweight, key generation and distribution [4]. The task of SKG from correlated observations was first studied in [5] and [6]. A straightforward SKG approach can be built by exploiting the reciprocity of the wireless fading coefficients between two terminals during the channel coherence time [7].

Building on this premise, we focus on the possibility of developing cross-layer security schemes in which session keys are generated at the physical layer and subsequently passed to upper layers to be used in NIST approved protocols such as the authentication header (AH) and the encapsulating security payloads (ESP) of the IPSec, in essence modifying the Internet key exchange (IKE) protocol to accept keys from PHY. On this basis, we posit that it is possible to identify the minimum SKG rate necessary to encrypt the transmitted data. Our contribution is to propose simultaneously performing SKG and data transfer utilising standard cryptographic algorithms that use the keys generated using the SKG. Furthermore we contribute an analysis of this method that determines optimum power allocation and channel allocation. The motivation behind this approach is latency reduction; data could be immediately transmitted whenever they become available, which can be critical in latency sensitive applications such as haptic communication systems.

In our system model, we assume that a block fading additive Gaussian noise (BF-AWGN) channel is used with multiple orthogonal subcarriers, a subset of which is used for SKG and the rest for data transfer. We then identify the optimal subcarrier allocation along with the optimal power allocation under a short-term power constraint. We show that the strongest subcarriers - in terms of SNR - should be used for data transfer and the weakest for SKG. Furthermore, the standard waterfilling algorithm is to be used for data transfer. On the other hand, the power allocation for the SKG subcarriers might not be unique, depending on the overall available power. Although the proposed policy is optimal in the short-term, if it is applied repeatedly (*i.e* applied over the long-term) the use of order statistics shows that a loss in the achievable rate can be induced because of the reduction in channel variability. Our findings are demonstrated with numerical results, while in future work the proposed scheme will be compared in terms of rates and latency with other schemes in which SKG and data transfer are separated.

II. Authenticated Encryption Protocols Using SKG

The standard SKG procedure typically encompasses three phases [5]:

1) Advantage distillation: The legitimate nodes exchange probe signals to obtain estimates of their reciprocal channel state information (CSI) and pass them through a suitable quantizer [8]. Commonly, the received signal strength (RSS) has been used as the CSI parameter for generating the shared key, while in [9] the phase has been used.

2) Information reconciliation: Discrepancies in the quantizer local outputs, due to imperfect channel estimation are reconciled through public discussion using a suitable coding technique. For example any Slepian-Wolf coder such as standard forward error correction (FEC) codes could be used (e.g., LDPC, BCH, etc.) [7], [9].

3) Privacy amplification: Applying universal hash functions to the reconciled information ensures that the generated keys are uniformly distributed and completely unpredictable by an adversary. Privacy amplification ensures that the generated keys have maximum entropy (i.e., are uniformly distributed). More importantly, it ensures that even if an adversary has access to (even a large) part of the decoder output, the final secret key can be unpredictable.

To develop robust protocols that can withstand tampering attacks, standard symmetric key block ciphers and message authentication (MAC) schemes can be used in conjunction with SKG. As a sketch of such a protocol, let us assume a system with three parties: Alice and Bob, who wish to exchange messages with confidentiality and integrity, and Eve, that can act as a passive and active attacker. Alice wishes to transmit over a wireless multipath channel a secret message `m` to Bob. The following algorithms are employed: the SKG scheme, a symmetric encryption algorithm denoted by `Es` with corresponding decryption `Ds` and a MAC denoted by `Sign` with a corresponding verification algorithm `Ver`.

The SKG procedure is launched between Alice and Bob; at the output of her Slepian Wolf decoder Alice obtains a secret key `K` and a corresponding coset. She breaks her key into two parts `K={Ke, Ki}` and uses the first part of the key to encrypt the message as the ciphertext `cipher=Es(Ke, m)`. Subsequently, using the second part of the key she signs the ciphertext using the signing algorithm `t=Sign(Ki, cipher)` and transmits to Bob the extended ciphertext $\mathtt{C} = [\mathtt{coset}||\mathtt{cipher}||\mathtt{t}]$.

Bob checks the integrity of the received ciphertext as follows: from `C` he extracts `coset, cipher` and `t`. From `coset` and his own observation he evaluates `K={Ke, Ki}`. Subsequently, Bob evaluates `v=Ver(Ki, cipher, t); v` is either equal to $\perp$ if the integrity test failed or `cipher` if the integrity test was successful. The integrity test will fail if any part of `C` was modified; for example, if `coset` was modified during the transmission then Bob would have evaluated a wrong key `K` and the integrity test would have failed. If the integrity test is successful then Bob decrypts `m=Ds(Ke, cipher)`. In the following, we will focus on multicarrier systems in which keys are generated at the physical layer and used in authentication/encryption protocols at upper layers as described above.

III. System Model

In our PHY system model we assume Alice and Bob exchange data over a Rayleigh BF-AWGN channel with N orthogonal blocks (e.g., in the frequency domain), which, for simplicity, will be referred to as subcarriers. Without loss of generality the variance of the AWGN in all links is assumed to be unity. We further assume that CSI estimation on all subcarriers has been performed and that both Alice and Bob have precise CSI estimates (the case of imperfect CSI estimation is left as future work).

We note in passing that irrespective of whether SKG or data transfer is performed, Alice and Bob need to exchange pilot signals to obtain estimates of their reciprocal CSI (full CSI needs to be available at Tx and Rx). These CSI estimates can be subsequently used to either conduct the secret key generation or be used to optimally allocate the available power to maximize the data transfer rate using a waterfilling algorithm. In further detail, after CSI estimation, if SKG is to be performed on a specific subcarrier, then it is necessary for Alice (or Bob) to further transmit side information required for "information reconciliation", e.g., the coset of the Slepian-Wolf decoder output if block codes are used[1]. If on the other hand, a given subcarrier is chosen for data transfer, then the estimated CSI will be used to optimize the power allocation.

Bearing this in mind, in this study we assume an initial SKG only phase is used to generate the first keys to be used for the encryption of the first set of data. In subsequent blocks however, we assume that both data transfer and SKG are performed in parallel; under this assumption, we will identify the optimal allocation of subcarriers and power in order to maximize the data transfer rate under a security and a short-term power constraint. The security constraint will take the form of a minimum key rate to data rate ratio as will be discussed in the following.

As a result of the previous discussion, the overall set of orthogonal subcarriers comprises two subsets; a subset $\mathcal{D}$ that is used for data transmission with cardinality $|\mathcal{D}| = D$ and a subset $\bar{\mathcal{D}}$ with cardinality $|\bar{\mathcal{D}}| = N - D$ used for SKG only. Over $\mathcal{D}$ the legitimate users exchange messages using Gaussian codebooks so that their achievable data transfer rate, with channel gain g_i on the i-th subcarrier and allocated power p_i, is given by [10]:

$$C_{data} = \frac{1}{D} \sum_{i \in \mathcal{D}} \log_2(1 + g_i p_i). \tag{1}$$

The channel gains, g_i for the sake of notation, are ordered as below:

$$g_1 \geq g_2 \geq \cdots \geq g_N. \tag{2}$$

[1]The final step of privacy amplification, in which a common key is extracted at both Alice and Bob is performed locally without any further information exchange.

On the subset $\bar{\mathcal{D}}$, Alice and Bob establish a secret key by exchanging constant probe signals as in [7], [11] with power level $p_j, j \in \bar{\mathcal{D}}$. We denote $Z_{A,j}, Z_{B,j}$ to be zero-mean, circularly-symmetric complex AWGN random variables:

$$Z_{A,j}, Z_{B,j} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}). \tag{3}$$

Throughout our work, a rich Rayleigh multipath environment is assumed, such that the fading coefficients rapidly decorrelate over short distances. The fading coefficients denoted by $H_j, j = 1, \ldots, N$ are assumed to be independent and identically distributed (i.i.d) zero-mean circularly-symmetric complex Gaussian random variables:

$$H_j \sim \mathcal{CN}(\mathbf{0}, \sigma_H^2 \mathbf{I}), \tag{4}$$

where σ_H^2 is the fading variance. Given the above, Alice's and Bob's observations on the j-th SKG subcarrier can then be expressed as:

$$X_{A,j} = \sqrt{p_j} H_j + Z_{A,j}, \text{ for } j \in \bar{\mathcal{D}}, \tag{5}$$

$$X_{B,j} = \sqrt{p_j} H_j + Z_{B,j}, \text{ for } j \in \bar{\mathcal{D}}. \tag{6}$$

Using this model, the SKG rate on the j-th subcarrier is [7]:

$$R(p_j) = \log_2 \left(1 + \frac{p_j \sigma^2}{2 + \frac{1}{p_j \sigma^2}} \right), \tag{7}$$

where $\sigma^2 = 4\sigma_H^4$ and the SKG rate using the RSS is given by:

$$C_{key} = \frac{1}{|N - D|} \sum_{j \in \bar{\mathcal{D}}} \log_2 \left(1 + \frac{p_j \sigma^2}{2 + \frac{1}{p_j \sigma^2}} \right). \tag{8}$$

Finally, in our system model a short-term power constraint is assumed:

$$\sum_{i=1}^{N} p_i \leq NP, \; p_i \geq 0, \; \forall i \in \{1, \ldots, N\}. \tag{9}$$

IV. Optimal Power and Subcarrier Allocation with Short-Term Power Constraints

The achievable sum rates for data transfer, denoted by C_D and SKG, denoted by C_K, are given by

$$C_D = DC_{data}, \tag{10}$$

$$C_K = (N - D) C_{key}. \tag{11}$$

Depending on the exact choices of the cryptographic suites to be employed, it is possible to reuse the same key for the encryption of multiple blocks of data, e.g., as in the cipher block chaining (CBC) mode with a randomized initialization vector. In practise, a single key of length 256 bits is used to encrypt up to gigabytes of data. As a result, we will assume that for a particular protocol it is possible to identify the ratio of key to data bits, which in the following we will denote by β. Specifically, in the system model presented in Section III, we assume that the following security constraint should be met:

$$C_K = \beta C_D, \;\; 0 < \beta \leq 1. \tag{12}$$

Depending on the application, the necessary minimum value of β can be identified. We will find the optimal trade-off between data transmission and SKG in terms of subcarrier allocation and power allocation, under the short-term power constraint (9). To this end, we formulate the following optimization problem:

$$\max_{p_i, i \in \mathcal{D}} \sum_{i \in \mathcal{D}} \log_2(1 + g_i p_i), \;\; \text{s.t. (9) and (12).} \tag{13}$$

To solve the problem, the following two Lemmas are stated.

Lemma 1: In order to maximize C_D the strongest D subcarriers – in terms of SNR – are used for data transmission and the rest, $N - D$, for SKG.

Proof: Let us assume that $\mathcal{D}^*$ is the subset of subcarriers indices which maximizes C_D and $\mathcal{D}_{ord} = \{1, 2, \ldots, D\}$ the subset of the first D ordered subcarrier indices. Then, after fixing a subcarrier power level $p_d > 0$, $\forall \; d \in \mathcal{D}^*$ with $d \notin \mathcal{D}_{ord}$ it follows that a better index exists, i.e., $\exists \; d' \in \mathcal{D}_{ord}$ with $d' \notin \mathcal{D}^*$, s.t.,

$$\log_2(1 + g_d p_d) < \log_2(1 + g_{d'} p_d). \tag{14}$$

As a consequence of Bellman's principle [12] the optimal sum rate in (13) has to consist of optimal subcarrier rates, (14) contradicts this fact and hence, $\mathcal{D}^* = \mathcal{D}_{ord} = \{1, 2, \ldots, D\}$. ■

Consequently, in the following we can use the fact that

$$\mathcal{D}^* = \{1, 2, \ldots, D\}. \tag{15}$$

Next we turn our attention on how the available power for SKG should be used. Let us assume that the overall power expended for SKG can be expressed as

$$P_s = (N - D) p_s, \tag{16}$$

where p_s denotes the average SKG power and P_s the overall SKG power. Given (16), and by taking the first and the second derivative of $R(p_s)$, it is straightforward to see it is a monotonic function in p_s and it is convex if $p_s < \frac{1}{\sqrt{2}\sigma^2}$ and concave if $p_s > \frac{1}{\sqrt{2}\sigma^2}$.

Lemma 2: If $p_s > \frac{1}{\sqrt{2}\sigma^2}$ the set $\bar{\mathcal{D}}$ comprises the weakest $N - D$ subcarriers – in terms of SNR – and the power allocation is equal on all of them, so that:

$$C_K = (N - D) \log_2 \left(1 + \frac{p_s \sigma^2}{2 + \frac{1}{p_s \sigma^2}} \right). \tag{17}$$

Consequently the overall power allocation vector takes the form:

$$\mathbf{p} = \{p_1, p_2, \ldots, p_D, p_s, p_s, \ldots, p_s\}, \tag{18}$$

where the number of elements equal to p_s is $N - D$.

If $p_s < \frac{1}{\sqrt{2}\sigma^2}$ the set $\bar{\mathcal{D}}$ consists of a single subcarrier on which the full power available for SKG is allocated, so that:

$$C_K = \log_2 \left(1 + \frac{P_s \sigma^2}{2 + \frac{1}{P_s \sigma^2}} \right). \tag{19}$$

Proof: We note that when multiple subcarriers are to be used the power should be equally distributed to them. To prove

this we use the definition of a concave function and apply Jensen's inequality [13], [14]:

$$R\left(\sum_{i=1}^{K}\delta_i x_i\right) > \sum_{i=1}^{K}\delta_i R(x_i). \tag{20}$$

Substituting $\delta_i = 1/K$ and $x_i = P_s/b_i$ with $\sum_{i=1}^{K}\delta_i = 1$, we have that:

$$R\left(\sum_{i=1}^{K}\frac{P_s}{Kb_i}\right) > \sum_{i=1}^{K}\frac{1}{K}R\left(\frac{P_s}{b_i}\right) \Leftrightarrow$$
$$KR\left(\frac{1}{K}\sum_{i=1}^{K}\frac{P_s}{b_i}\right) > \sum_{i=1}^{K}R\left(\frac{P_s}{b_i}\right) \tag{21}$$

From the RHS of (21) we can see the power allocation on each subcarrier is P_s/b_i, so we can add the following power constraint $\sum_{i=1}^{K}P_s/b_i \leq P_s$. Due to the fact, R is monotonically increasing function with p_j, we have:

$$KR\left(\frac{P_s}{K}\right) \geq KR\left(\frac{1}{K}\sum_{i=1}^{K}\frac{P_s}{b_i}\right) \Leftrightarrow$$
$$KR\left(\frac{P_s}{K}\right) > \sum_{i=1}^{K}R\left(\frac{P_s}{b_i}\right). \tag{22}$$

Equation (22) proves that in order to maximize the sum rate R the legitimate users have to distribute their power equally when multiple subcarriers are used.

Next we show that all the subcarriers have to be used. Recalling the definition of a concave function for a single δ on the interval $[0, b]$ we have that:

$$R((1-\delta)0 + \delta b) > (1-\delta)R(0) + \delta R(b), \tag{23}$$

with $\delta = a/b$ for $f(0) > 0,$ and $0 < a < b$, we have:

$$R\left(\left(1-\frac{a}{b}\right)0 + \frac{a}{b}b\right) > \left(1-\frac{a}{b}\right)R(0) + \frac{a}{b}R(b) \Leftrightarrow$$
$$R(a) > R(0)\frac{b-a}{b} + \frac{a}{b}R(b) \geq \frac{a}{b}R(b) \Leftrightarrow$$
$$\frac{R(a)}{a} > \frac{R(b)}{b}. \tag{24}$$

Setting $a = x/v$ and $b = x/u$ gives:

$$uf\left(\frac{x}{u}\right) < vf\left(\frac{x}{v}\right) \tag{25}$$

for $0 < u < v$ and $x > 0$. Given that when $p_s > \frac{1}{\sqrt{2\sigma^2}}$, i.e., when $R(p_s)$ is concave, we have that:

$$R\left((N-D)p_s\right) < 2R\left(\frac{N-D}{2}p_s\right) < \dots$$
$$\dots < (N-D-1)R\left(\frac{N-D}{N-D-1}p_s\right) < (N-D)R(p_s), \tag{26}$$

which shows that all available subcarriers have to be used.

On the other hand when $p_s < \frac{1}{\sqrt{2\sigma^2}}$, i.e., $R(p_s)$ is convex and by the definition of a convex function we have that:

$$R((1-\delta)0 + \delta b) < (1-\delta)R(0) + \delta R(b), \tag{27}$$

which results in:

$$R\left((N-D)p_s\right) > 2R\left(\frac{N-D}{2}p_s\right) > \dots$$
$$\dots > (N-D-1)R\left(\frac{N-D}{N-D-1}p_s\right) > (N-D)R(p_s), \tag{28}$$

which shows that in this case it is optimal to use a single subcarrier for SKG. Lemma 2 follows. ■

As a result of Lemma 2, we explore the following two cases, Case 1 for R concave and Case 2 for R convex.

A. Case 1: $p_s > \frac{1}{\sqrt{2\sigma^2}}$

Theorem 1: When $p_s > \frac{1}{\sqrt{2\sigma^2}}$ the optimal power allocation for data transmission and SKG on each subcarrier are:

$$p_i^* = \left[\frac{1-\beta\mu}{\lambda\ln(2)} - \frac{1}{g_i}\right]^+, i = 1, \dots, D \tag{29}$$

$$p_s^* = \left[\frac{Q \pm \sqrt{Q^2 - F^2}}{\frac{4\sigma^2}{\sqrt{8}}F}\right]^+, \tag{30}$$

where:

$$[x]^+ \triangleq \max(x, 0), \tag{31}$$
$$Q = 2\sigma^4\mu N - 2\sigma^4\mu D - 3\sigma^2\lambda\ln(2), \tag{32}$$
$$F = \sqrt{8}\lambda\sigma^2\ln(2). \tag{33}$$

For the feasibility of (29) and (30) we have:

$$\mu < \frac{1}{\beta}, \tag{34}$$
$$\mu \geq \frac{\lambda\ln(2)(3+\sqrt{8})}{2\sigma^2(N-D)}, \tag{35}$$
$$\lambda > 0. \tag{36}$$

Proof: If $p_s > \frac{1}{\sqrt{2\sigma^2}}$ the optimization problem can be re-written as:

$$\max_{p_i}\sum_{i=1}^{D}\log_2(1+g_i p_i) \tag{37}$$

s.t. (9) and

$$\beta\left(\sum_{i=1}^{D}\log_2(1+g_i p_i)\right) = (N-D)\log_2\left(1 + \frac{p_s\sigma^2}{2+\frac{1}{p_s\sigma^2}}\right). \tag{38}$$

As the Karush-Kuhn-Tucker (KKT) conditions are satisfied, to obtain the optimal power allocation we formulate the Lagrangian, which after a few algebraic manipulations takes the form:

$$\mathcal{L}_p = \left(\sum_{i=1}^{D}\log_2(1+g_i p_i)\right)(1-\mu\beta) - \lambda\left(\sum_{i=1}^{N}p_i + NP\right)$$
$$+ \mu\left((N-D)\log_2\left(1 + \frac{\sigma^2 p_s}{2+\frac{1}{\sigma^2 p_s}}\right)\right), \tag{39}$$

where λ and μ are the dual Lagrange multipliers, that correspond to (9) and (38), respectively. The problem (37) has

concave objective and constraint functions, and as a result the optimal power allocation is given in (29) and (30) is the unique solution. ■

B. Case 2: $p_s < \frac{1}{\sqrt{2}\sigma^2}$

***Theorem** 2:* When $p_s < \frac{1}{\sqrt{2}\sigma^2}$ a single random subcarrier with index $j > D$ can be used for SKG and without loss of generality we can set $j = D+1$. The optimal power allocation for data transmission and SKG is then expressed as:

$$p_i^* = \left[\frac{1-\beta\mu}{\lambda \ln(2)} - \frac{1}{g_i}\right]^+, i = 1, \ldots, D, \tag{40}$$

$$P_s^* = \left[\frac{Q' \pm \sqrt{Q'^2 - F'^2}}{\frac{4\sigma^2}{\sqrt{8}}F'}\right]^+, \tag{41}$$

where:

$$Q' = 2\mu\sigma^4 - 3\sigma^2\lambda\ln(2) \tag{42}$$

$$F' = \sqrt{8}\lambda\sigma^2\ln(2). \tag{43}$$

For the feasibility of (40) and (41) we have:

$$\mu < \frac{1}{\beta}, \tag{44}$$

$$\mu \geq \frac{\lambda\ln(2)(3+\sqrt{8})}{2\sigma^2}, \tag{45}$$

$$\lambda > 0. \tag{46}$$

Proof: If $p_s < \frac{1}{\sqrt{2}\sigma^2}$ then (12) takes the form:

$$\beta\left(\sum_{i=1}^{D}\log_2(1+g_i p_i)\right) = \log_2\left(1 + \frac{P_s\sigma^2}{2+\frac{1}{P_s\sigma^2}}\right). \tag{47}$$

By using the KKT conditions it is straightforward to see that the optimal power allocation for each subcarrier is presented in (40) and (41). ■

By applying (10) and using the modified water-filling solution of the maximization problem given in (13) the achievable data rates can be simulated (See Fig. 1 and Fig. 2). In Fig. 1 we can clearly see the dependence of the achievable sum rate on β and D. While varying β the achievable C_D changes and due to its concavity we can always identify the unique maximum achieved for the optimal D and power allocation. For small values of β we can see that the fewer SKG subcarriers that are used the greater sum rate we achieve. When β increases the optimal subcarrier allocation changes, and a larger number of subcarriers are needed to meet the security constraint.

As expected, in Case 2, varying β directly affects the achievable sum rate. In agreement with intuition, from Fig. 2 we see that the smaller the β, the greater rate we achieve.

V. Long-term Issues with the Short-term Policy

Having a short-term power constraint allows us to optimally allocate the subcarriers and the available power assuming that the Rayleigh channel fading coefficients are i.i.d. random variables as in (4). However, the optimal short-term solution suggests that the weakest subcarriers should be used for SKG. If this policy is applied in the long-term, it is obvious that it will have an impact on the actual statistical properties and the distribution of the coefficients used for SKG. This effect is investigated in the present section.

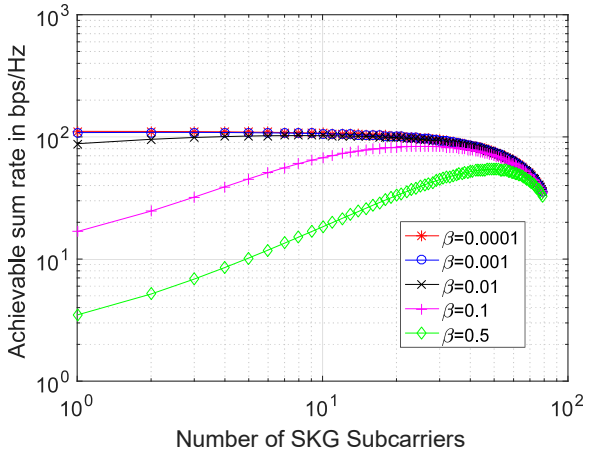

Fig. 1. Case1: Achievable sum rate C_D averaged over 10,000 simulations for different values of β, defined in (12), number of subcarriers used for data transmission and for SKG. Parameters: $(p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1, N = 100$.

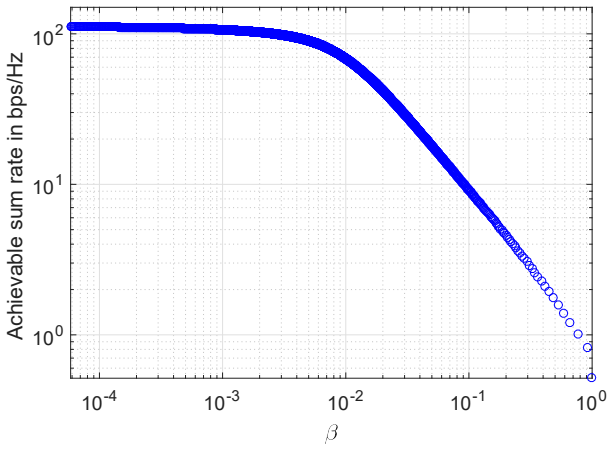

Fig. 2. Case2: Achievable sum rate C_D averaged over 10,000 simulations for different values of β, defined in (12). Parameters: $N = 100, D = 99, (p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1$.

The fading coefficients are assumed to be zero-mean circularly-symmetric complex Gaussian random variables as in (4). We have seen that the weakest $N-D$ subcarriers should be used for SKG, where D depends on the system parameters as well as the exact fading realizations. The distribution of the channel gains of the SKG subcarriers for $l = \{D+1, \ldots, N\}$ can then be expressed as [15]:

$$p(g_l) = \frac{N!}{\sigma^2(N-l)!(l-1)!}\left(1-e^{-\frac{g_l}{\sigma^2}}\right)^{N-l}\left(e^{-\frac{g_l}{\sigma^2}}\right)^{l} \tag{48}$$

where σ^2 is the variance of channel gains.

As a result, the impact of choosing the weakest $N-D$

subcarriers for SKG in the long-term will impact the variance of each of them, which is now given by:

$$\sigma_i^2 = \sigma^2 \sum_{q=i}^{N} \frac{1}{q^2}, \quad i \in \{D+1, \ldots, N\}. \tag{49}$$

As an example, the variance of the weakest of N subcarriers is scaled with a factor N^{-2}. In Fig. 3 and 4 we compare the rates that are achievable for Case 1 and 2, respectively, in the short-term and in the long-term with the proposed short-term policy. We see that for small values of β the incurred penalty for both cases is small. However, when β increases a higher reduction of the sum rates is observed.

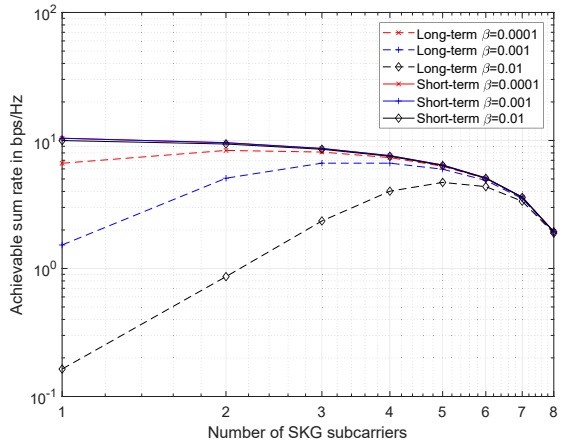

Fig. 3. Case1: Achievable sum rate C_D for different values of β, defined in (12), number of subcarriers used for data transmission and for SKG. Parameters: $(p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1, N = 10$.

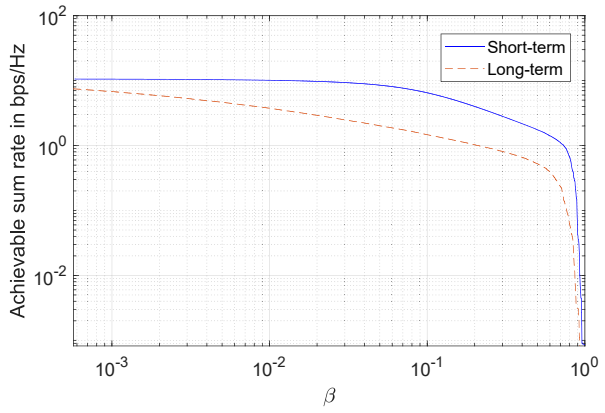

Fig. 4. Case2: Achievable sum rate C_D for different values of β, defined in (12). Parameters: $N = 10, D = 9, (p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1$.

VI. Conclusion

In this work we investigated the possibility of jointly performing data transfer and SKG in a Rayleigh BF-AWGN environment. We studied the maximization of the data transfer rate under two constraints: a constraint on the SKG rate vs the data rate, and, a short-term overall power constraint. Our analysis demonstrated that in this scenario the strongest subcarriers – from an SNR point of view – should be allocated to data transfer and the weakest to SKG. Accordingly, the optimal power allocation for the data transfer has been shown to be expressed in the waterfilling form while the power allocation for the SKG subcarriers depends on the overall available power and might not be unique. Furthermore, we investigated the impact of utilizing the optimal short-term policy in the long-term. The use of order statistics revealed that systematically choosing the weakest subcarriers for SKG can result, in the worst case, in a scaling inversely proportional to the square of N, the number of subcarriers, for the SKG variance. However, for small values of N and β the incurred penalty is small. In future work we will compare this approach with other possible allocation policies.

References

[1] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," in *Proc. IEEE*, vol. 103, no. 10, Oct 2015.

[2] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," in *Proc. IEEE*, vol. 103, no. 10, Oct 2015.

[3] K. McKay, L. Bassham, M. Turan, and N. Mouha, "Report on lightweight cryptography," *NIST Interagency/Internal Report (NISTIR) - 8114*, Mar 2017.

[4] A. Chorti, "A study of injection and jamming attacks in wireless secret sharing systems," in *Proc. Workshop on Communication Security (WCS), EUROCRYPT*, Mar 2017.

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

[6] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[7] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul 2006.

[8] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE Int. Conf. Computer Commun. (INFOCOM)*, 2011.

[9] C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Florence, Italy, 2015.

[10] G. Caire, G. Taricco, and E. Biglieri, "Optimum power control over fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1468–1489, July 1999.

[11] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, Nov 2017.

[12] R. Bellman and R. Kalaba, *Dynamic Programming and Modem Control Theory*. NY: Academic Press, 1966.

[13] O. Hölder, "Ueber einen mittelwertsatz," *Gttinger Nachr.*, pp. 38–47, 1889.

[14] J. Jensen, "Sur les fonctions convexes et les inégualités entre les valeurs moyennes," *Acta Math.*, pp. 175–193, 1906.

[15] H. Yang and M. Alouini, *Order Statistics in Wireless Communications*. NY: Cambridge University Press, 2011.