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

Miroslav Mitev, Arsenia Chorti, Martin Reed

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

Miroslav Mitev
School of Comp. Science and Electr. Eng.
University of Essex
Colchester, UK
mm17217@essex.ac.uk

Arsenia Chorti
ENSEA, UMR 8051, CNRS
Université Cergy-Pointoise
Cergy-Pontoise, France
arsenia.chorti@ensea.fr

Martin Reed
School of Comp. Science and Electr. Eng.
University of Essex
Colchester, UK
mjreed@essex.ac.uk

***Abstract*—Due to computational complexity and latency constraints in the nodes of many IoT systems, alternatives are sought for session key generation schemes that rely on public key encryption. 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 is 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 in the long-term.**

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 is offered by physical layer security (PLS) that has gained significant attention in recent years in the information theory and communications communities. 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 [9].

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. In this study we investigate the possibility of simultaneously performing SKG and data transfer. 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 system.

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 and that 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. However, although the proposed policy is optimal in the short-term, if it is repeatedly used it is demonstrated with the use of order statistics that a loss in the achievable rate will be induced because of the reduction in channel variability. Our finding are demonstrated with numerical results, while in n 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 SKG standard procedure typically encompasses three phases [5]:

1) Advantage distillation: The legitimate nodes exchange probe signals to obtain estimates of their reciprocal CSI and pass them through a suitable quantizer [7]. Commonly, the received signal strength (RSS) has been used as the CSI parameter for generating the shared key, while in [8] the CSI phase has been used.

2) Information reconciliation: Discrepancies in the quantizer local outputs due to imperfect channel estimation are reconciled through public discussion using Slepian Wolf decoders. Numerous practical information reconciliation approaches using standard forward error correction (FEC) codes (e.g., LDPC, BCH, etc.) have been proposed [8], [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 in 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 $\texttt{C} = [\texttt{coset}||\texttt{cipher}||\texttt{t}]$.

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 was 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 A.E. 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 experienced in all links is assumed to be unity. We further assume that CSI estimation on all subcarriers has been performed and the 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 conclude 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 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, both data transfer and SKG is to 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 [11]:

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

Without loss of generality the channel gains g_i are assumed to be ordered, i.e.,

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

On the subset $\bar{\mathcal{D}}$, Alice and Bob establish a secret key by exchanging constant probe signals as in [9], [10] with

[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.

power level $p_j, j \in \bar{\mathcal{D}}$. We denote $Z_{A,j}, Z_{B,j}$ to be circularly-symmetric complex Gaussian 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 H 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:

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

where σ^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:

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

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

Under this assumption, the SKG rate on the j-th subcarrier is [9]:

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

and the SKG rate 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 simply 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 randomized initialization vector (IV). 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. Assume that overall power expendited 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 this 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 $\bar{\mathcal{D}}$ consist 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 applying 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:

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

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

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

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

$$KR\left(\frac{P_s}{K}\right) > \sum_{i=1}^{K}R\left(\frac{P_s}{b_i}\right). \tag{23}$$

Equation (23) 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:

$$R((1-\delta)0 + \delta b) > (1-\delta)R(0) + \delta R(b), \tag{24}$$

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

$$R\left(\left(1-\frac{a}{b}\right)0 + \frac{a}{b}b\right) > \left(1-\frac{a}{b}\right)R(0) + \frac{a}{b}R(b) \Leftrightarrow \tag{25}$$

$$R(a) > R(0)\frac{b-a}{b} + \frac{a}{b}R(b) \geq \frac{a}{b}R(b) \Leftrightarrow \tag{26}$$

$$\frac{R(a)}{a} > \frac{R(b)}{b}. \tag{27}$$

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

$$uf\left(\frac{x}{u}\right) < vf\left(\frac{x}{v}\right) \tag{28}$$

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:

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

$$\dots < (N-D-1)R\left(\frac{N-D}{N-D-1}p_s\right) < (N-D)R(p_s), \tag{29}$$

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:

$$R((1-\delta)0 + \delta b) < (1-\delta)R(0) + \delta R(b), \tag{30}$$

which results in:

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

$$\dots > (N-D-1)R\left(\frac{N-D}{N-D-1}p_s\right) > (N-D)R(p_s), \tag{31}$$

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:*

$$p_i^* = \left[\frac{1-\beta\mu}{\lambda\ln(2)} - \frac{1}{g_i}\right]^+, i = 1, \dots, D \tag{32}$$

$$p_s^* = \left[\frac{Q \pm \sqrt{Q^2 - F^2}}{\frac{4\sigma^2}{\sqrt{8}}F}\right]^+, \tag{33}$$

where:

$$[x]^+ \triangleq \max(x, 0), \tag{34}$$

$$Q = 2\sigma^4\mu N - 2\sigma^4\mu D - 3\sigma^2\lambda\ln(2), \tag{35}$$

$$F = \sqrt{8}\lambda\sigma^2\ln(2). \tag{36}$$

For the feasibility of (32) and (33) we have:

$$\mu < \frac{1}{\beta}, \tag{37}$$

$$\mu \geq \frac{\lambda\ln(2)(3+\sqrt{8})}{2\sigma^2(N-D)}, \tag{38}$$

$$\lambda > 0. \tag{39}$$

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

$$\max_{p_i}\sum_{i=1}^{D}\log_2(1+g_i p_i) \tag{40}$$

s.t. (9) and

$$\beta\left(\sum_{i=1}^{D}\log_2(1+g_i p_i)\right) = (N-D)\log_2\left(1 + \frac{p_s\sigma^2}{2+\frac{1}{p_s\sigma^2}}\right). \tag{41}$$

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:

$$\mathcal{L}_p = \left(\sum_{i=1}^{D}\log_2(1+g_i p_i)\right)(1-\mu\beta) - \lambda\left(\sum_{i=1}^{N}p_i + NP\right)$$
$$+ \mu\left((N-D)\log_2\left(1 + \frac{\sigma^2 p_s}{2+\frac{1}{\sigma^2 p_s}}\right)\right), \tag{42}$$

where λ and μ are the dual Lagrange multipliers, that correspond to (9) and (41), respectively. The problem (40) has concave objective and constraint functions,and as a result the optimal power allocation for each subcarrier is given in (32) and (33) 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 $j = N$. The optimal power allocation for data transmission and SKG is then expressed as:*

$$p_i^* = \left[\frac{1-\beta\mu}{\lambda\ln(2)} - \frac{1}{g_i}\right]^+, i = 1, \ldots, D, \tag{43}$$

$$P_s^* = \left[\frac{Q' \pm \sqrt{Q'^2 - F'^2}}{\frac{4\sigma^2}{\sqrt{8}}F'}\right]^+, \tag{44}$$

where:

$$Q' = 2\mu\sigma^4 - 3\sigma^2\lambda\ln(2) \tag{45}$$

$$F' = \sqrt{8}\lambda\sigma^2\ln(2). \tag{46}$$

For the feasibility of (43) and (44) we have:

$$\mu < \frac{1}{\beta}, \tag{47}$$

$$\mu \geq \frac{\lambda\ln(2)(3+\sqrt{8})}{2\sigma^2}, \tag{48}$$

$$\lambda > 0. \tag{49}$$

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

$$\beta\left(\sum_{i=1}^{D}\log_2(1+g_i p_i)\right) = \log_2\left(1+\frac{P_s\sigma^2}{2+\frac{1}{P_s\sigma^2}}\right). \tag{50}$$

By using the KKT conditions it is straightforward to see that the optimal power allocation for each subcarrier is presented in (43) and (44). ■

Simulation results for the the achievable data sum rates are presented in 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 less SKG subcarriers are used the greater sum rate we achieve. When β becomes greater the optimal subcarrier allocation changes, and a larger number of subcarriers is necessary 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.

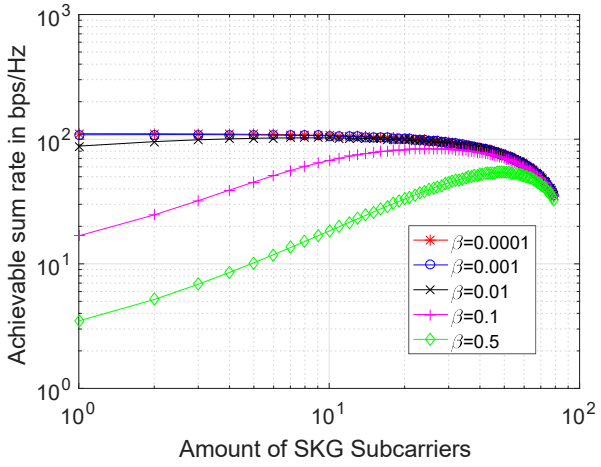

Fig. 1: Case1: Achievable sum rate C_D averaged over $10,000$ simulations for different values of β, defined in (12), number of subcarriers used for data transmission and for SKG. Parameters: $(p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1, N = 100$.

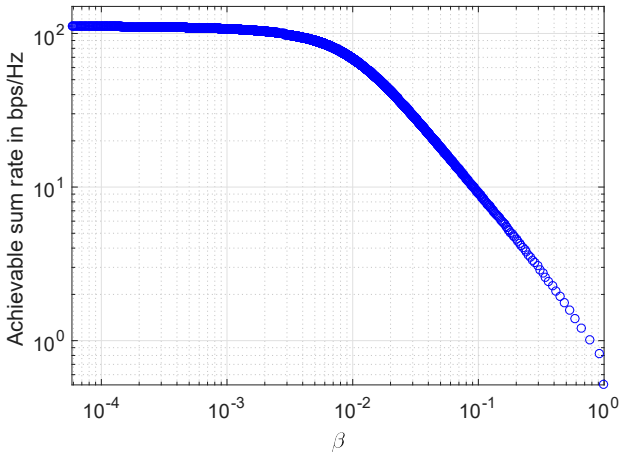

Fig. 2: Case2: Achievable sum rate C_D averaged over $10,000$ simulations for different values of β, defined in (12). Parameters: $N = 100, D = 99, (p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1$.

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.

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. To simplify the following analysis, we assume that all of the SKG subcarriers are i.i.d. and that their distribution corresponds to the distribution of the weakest out of N ordered random

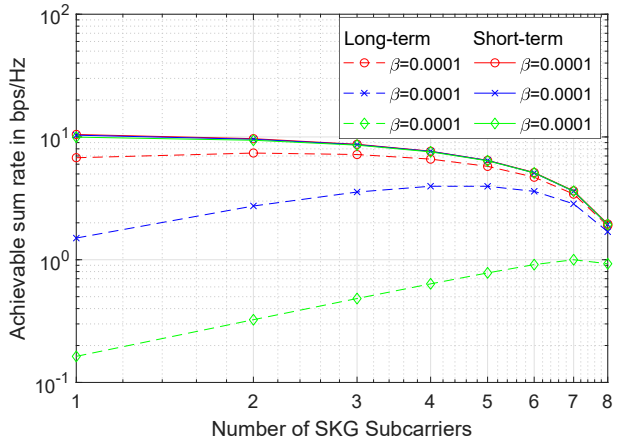

Fig. 3: Case1: Achievable sum rate C_D for different values of β, defined in (12), number of subcarriers used for data transmission and for SKG. Parameters: $(p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1, N = 10$.

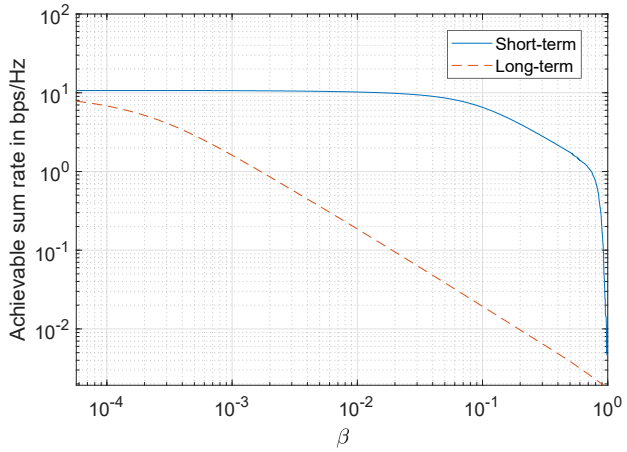

Fig. 4: Case2: Achievable sum rate C_D for different values of β, defined in (12). Parameters: $N = 10, D = 9, (p_1 + \cdots + p_D)/D = 5, \sigma^2 = 1$.

variables, with a pdf that can be expressed as [16]:

$$p(H_N) = \frac{N}{\sigma^2} e^{-\frac{N H_N}{\sigma^2}}. \tag{51}$$

where σ^2 is the variance of channel coefficients.

As a result, the impact of choosing the weakest of N subcarriers for SKG in the long-term is equivalent with scaling the variance of the channel coefficients with a factor of 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.

VI. Jamming attacks on SKG

This section extends our previous results to the case in which an active attacker aims at compromising the SKG process. Our motivation in first examining this scenario lies in the fact that diminishing SKG rates lead to diminishing data rates due to our requirement $\beta C_D = C_K$. The more general scenario in which both data and SKG subcarriers are jammed will be addressed in future work.

The system model includes Alice and Bob and a jammer, Eve. Eve is assumed to be a responsive jammer, i.e., she passively senses the spectrum and jams a specific subcarrier only when the power on it exceeds a certain threshold p_{th}. We consider two scenarios, i.e., when p_{th} is fixed (determined in essence by the carrier sensing capability of Eve's receiver) and when it is variable, i.e., its choice forms part of Eve's strategy. As we will see in the following, in the former scenario the optimal strategies of the legitimate and adversarial parties are independent of each other's choices (can be independently decided), while in the latter case their optimal strategies are depend on the other parties choices. As a result, the first scenario is addressed with standard optimization tools while the latter is analysed using game theoretic tools.

As previously, during the SKG process Alice and Bob observe dependent random variables denoted by $\hat{\mathbf{X}}_A = [\hat{X}_{A,j}]_{j=D+1}^N$ and $\hat{\mathbf{X}}_B = [\hat{X}_{B,j}]_{j=D+1}^N$, respectively, while Eve observes $\hat{\mathbf{X}}_E = [\hat{X}_{E,j}]_{j=D+1}^N$. The rich Rayleigh multipath environment, ensures that Eve's observation $\hat{\mathbf{X}}_E$ is uncorrelated with $\hat{\mathbf{X}}_A$ and $\hat{\mathbf{X}}_A$. We start by reformulating the expressions of Alice's and Bob's observations on the j-th SKG subcarrier as follows:

$$\hat{X}_{A,j} = \sqrt{p_j} H_j + \sqrt{\gamma_j} G_{A,j} + Z_{A,j} \tag{52}$$

$$\hat{X}_{B,j} = \sqrt{p_j} H_j + \sqrt{\gamma_j} G_{B,j} + Z_{B,j}, \tag{53}$$

where p_j is the power level used by Alice and Bob to exchange probe signals on the j-th subcarrier and γ_j is the jamming power on the j-th subcarrier, $N - D + 1 \leq j \leq N$. The fading coefficients are assumed to be Gaussian random variables as follows: in the link between Alice and Eve $G_{A,j} \sim \mathcal{N}(0, \sigma_j^2)$, and in the link between Bob and Eve $G_{B,j} \sim \mathcal{N}(0, \sigma_j^2)$[2]. The noise variables $Z_{A,j}, Z_{B,j}$ are assumed as in Section II to be i.i.d. Gaussian random variables with unit variance and zero mean.

A simple calculation reveals that the SKG rate on the j-th subcarrier can, in the presence of the jammer, be expressed as a function of p_j and $\gamma_j, j = N - D + 1, \ldots, N$ as [10]:

$$\hat{R}(p_j, \gamma_j) = I(\hat{X}_{A,j}; \hat{X}_{B,j}) = \log_2 \left(1 + \frac{p_j \sigma^2}{2w_j + \frac{w_j^2}{p_j \sigma^2}} \right), \tag{54}$$

[2]The assumption that the Rayleigh coefficients in the links Alice-Eve and Bob-Eve share the same statistics is reasonable given that small scale fading roughly depends on the central frequency and the bandwidth, which here are the same in the two links [15].

where

$$w_j = 1 + \sigma_j^2 \gamma_j. \tag{55}$$

The SKG sum rate can then be expressed as follows:

$$\hat{C}_K = \sum_{j=N-D+1}^{N} \log_2 \left(1 + \frac{p_j \sigma^2}{2w_j + \frac{w_j^2}{p_j \sigma^2}} \right). \tag{56}$$

From the discussion in the previous section we need to account for two cases, depending on the average available power for SKG denoted by p_s. The case for $p_s > \frac{w_j}{\sqrt{2}\sigma^2}$ for $j \in \{N-D+1, \ldots, N\}$ when $\hat{R}(p_j, \gamma_j)$ takes concave form and the case for $p_s < \frac{w}{\sqrt{2}\sigma^2}$ when $\hat{R}(p_j, \gamma_j)$ takes convex form. Denoting the average available power for jamming by Γ, we assume the following short-term power constraints:

$$\sum_{j=N-D+1}^{N} p_j \leq (N-D)p_s, \;\; p_j \geq 0, \tag{57}$$

$$\sum_{j=N-D+1}^{N} \gamma_j \leq (N-D)\Gamma, \;\; \gamma_j \geq 0 \tag{58}$$

Our goal is to identify the optimal power allocation for Alice, Bob and Eve in this setting. We begin our analysis with the introduction of two subsets of subcarrier indices. The first subset $\hat{\mathcal{M}}$, with cardinality $|\hat{\mathcal{M}}| = M$, is for the subcarriers that are sensed to be 'ON' by the jammer, i.e., whose power exceeds p_{th} and the second subset $\check{\mathcal{M}}$, with cardinality $|\check{\mathcal{M}}| = N - D - M$, for the subcarriers that are sensed to be 'OFF', i.e., whose power is less or equal to p_{th}:

$$\hat{\mathcal{M}} = \{\hat{m} : p_{\hat{m}} > p_{th}, N-D+1 \leq \hat{m} \leq N\}, \tag{59}$$

$$\check{\mathcal{M}} = \{\check{m} : p_{\check{m}} \leq p_{th}, N-D+1 \leq \check{m} \leq N\}. \tag{60}$$

According to our system model:

$$\gamma_{\check{m}} = 0, \forall \check{m} \in \check{\mathcal{M}}. \tag{61}$$

In the following the objective of Alice and Bob is to maximize $\hat{C}_K$ subject to (57), while Eve's objective is to minimize $\hat{C}_K$ subject to (58).

Lemma 3. *The power allocation γ_j^* that minimizes $\hat{C}_K$ is the equidistribution of the available jamming power on subset $\hat{\mathcal{M}}$, i.e.,*

$$\gamma_j^* = \begin{cases} \Gamma_{on} = (N-D)\Gamma/M, & j \in \hat{\mathcal{M}}, \\ 0, & \textit{otherwise}. \end{cases} \tag{62}$$

Proof: Let us note that $\hat{C}_K$, the SKG sum rate that Eve tries to minimize, is a convex function w.r.t γ_j for any fixed $p_j > 0, j = N-D+1, \ldots, N$. This problem is equivalent to maximizing the $-\hat{C}_K$ s.t. (58). Noting that $-\hat{C}_K$ is a concave function and following similar steps to those in the proof of Lemma 2, it is straightforward to see see, in order to maximize the concave function $-\hat{C}_K$ Eve has to distribute her power as in (62). ∎

In light of the previous discussion, the SKG sum rate can be expressed as follows:

$$\hat{C}_K = \sum_{\hat{m} \in \hat{\mathcal{M}}} \hat{C}_K(p_{\hat{m}}, \Gamma_{\text{on}}) + \sum_{\check{m} \in \check{\mathcal{M}}} \hat{C}_K(p_{\check{m}}, 0). \tag{63}$$

Furthermore, from Lemma 2 in Section III we know that in absence of the jammer Alice and Bob should equally distribute their available power resources on the SKG subcarriers.

Lemma 4. *From all the of possible power levels, Alice and Bob will optimally use only two. They will use either $p_{\check{m}} = P_{off} = p_{th}$ or $p_{\hat{m}} = P_{on} = ((N-D)p_s - (N-D-M)P_{off})/M$.*

Proof: This is a result of the fact that $\hat{C}_K$ is increasing and concave function with p_j. Because of the concavity, the power in subsets $\hat{\mathcal{M}}$ and $\check{\mathcal{M}}$ should be equally distributed. Because it is monotonically increasing we have that:

$$\arg\max_{p_{\hat{m}}} \hat{C}_K(p_{\hat{m}}, \Gamma_{\text{on}}) = P_{\text{on}}, \tag{64}$$

$$\arg\max_{p_{\check{m}}} \hat{C}_K(p_{\check{m}}, \Gamma_{\text{on}}) = P_{\text{off}}. \tag{65}$$

∎

Using Lemmas 3 and 4, the SKG sum rate $\hat{C}_K$ takes a special form; in the following it is denoted by the utility function u:

$$u = MR(P_{\text{on}}, \Gamma_{\text{on}}) + (N-D-M)R(P_{\text{off}}, 0). \tag{66}$$

Given the above we can reformulate the short-term power constraint (57) as follows:

$$\sum_{j=N-D+1}^{N} p_j \leq (N-D)p_s, \;\; p_j \geq P_{\text{off}} = p_{th}. \tag{67}$$

Theorem 3. *Depending on the available power for SKG, either all SKG subcarriers should be set to P_{on} or all of them to P_{off}, i.e.,*

$$M^* = \begin{cases} N-D, & \textit{if } p_s > P_T \\ 0, & \textit{otherwise}. \end{cases} \tag{68}$$

where

$$P_T = P_{off}(\Gamma\sigma_j^2 + 1) \tag{69}$$

is the root of

$$R(P_{on}, \Gamma_{on}) = R(P_{off}, 0). \tag{70}$$

that satisfies constraint (57).

Proof: We first show that P_T is the unique root of (70) that satisfies constraint (67). We can do this by demonstrating that equation (70) is quadratic on P_{on} and therefore on p_s. For simplicity we write the polynomial as a function of P_{on} only:

$$\log_2 \left(1 + \frac{\sigma^2 P_{\text{on}}}{2w_j + \frac{w_j^2}{\sigma^2 P_{\text{on}}}} \right) = \log_2 \left(1 + \frac{\sigma^2 P_{\text{off}}}{2 + \frac{1}{\sigma^2 P_{\text{off}}}} \right)$$

$$\frac{\sigma^4 P_{\text{on}}^2}{2w_j \sigma^2 P_{\text{on}} + w_j^2} = \frac{\sigma^4 {P_{\text{off}}}^2}{2\sigma^2 P_{\text{off}} + 1}$$

$$P_{\text{on}}^2(2\sigma^2 P_{\text{off}} + 1) - P_{\text{on}}(2w_j \sigma^2 {P_{\text{off}}}^2) - w_j^2 {P_{\text{off}}}^2 = 0. \tag{71}$$

Equation (71) proves that (70) has quadratic form in p_s, i.e., it has two roots in p_s. The first is given as P_T while if

$$\Gamma\sigma_j^2 < 1 + 2\sigma^2 P_{\text{off}} + \frac{2M(1+\sigma^2 P_{\text{off}})}{D-N}, \tag{72}$$

we have one further possible solution, expressed as:

$$P_{T'} = -\frac{P_{\text{off}}((D-N)\Gamma\sigma_j^2 - 2M(\sigma^2 P_{\text{off}}+1))}{(D-N)(2\sigma^2 P_{\text{off}}+1)} + P_{\text{off}} < P_{\text{off}}, \tag{73}$$

but with few simple mathematical operations it can be shown that $P_{T'} < P_{\text{off}}$, i.e., the second root does not satisfy the short-term power constraint presented in (67). This results in only one root that is of interest for our study given by P_T.

Given the above we will now show that depending on the available power the optimal value for M is either 0 or $N-D$. Due to the fact R is monotonically increasing function with p_s it can be can seen that when $p_s > P_T$:

$$R\left(P_{\text{on}}, \Gamma_{\text{on}}\right) > R(P_{\text{off}}, 0) \Rightarrow u(M) > u(M-1) > \cdots > u(0), \tag{74}$$

which shows that in order to increase the utility for this case the legitimate users have to set all of the subcarriers devoted for SKG as ON. On the other hand, if $p_s \leq P_T$ we have that:

$$R\left(P_{\text{on}}, \Gamma_{\text{on}}\right) \leq R(P_{\text{off}}, 0) \Rightarrow u(M) \leq u(M-1) \leq \cdots \leq u(0). \tag{75}$$

which shows that in order to increase u for this case Alice and Bob have to set their power level on all of the subcarriers to be equal to P_{off}. In other words, if $p_s > P_T$, (66) is monotonically increasing with M, if $p_s = P_T$ (66) is constant for M and if $p_s < P_T$ (66) is monotonically decreasing with M. Due to the above Theorem 3 follows. ■

A. Fixed p_{th}

In the following we assume that Eve is not able to adjust p_{th}. The optimization problem that identifies the optimal subcarrier allocation for the legitimate parties is formulated, i.e., which strategy maximizes $\hat{C}_K$. The legitimate users may transmit the useful information with power $P_{\text{on}} > p_{\text{th}}$ by taking the risk to be sensed and jammed by Eve, or they may stay conservative and transmit the SKG pilots with power $P_{\text{off}} = p_{\text{th}}$ at the expense of reduced SKG rates. So, for Alice and Bob, the overall problem reduces to finding finding M^* that maximizes the utility function u.

In the light of the previous section we can account two cases depending on p_s. The case when $p_s > \frac{w_j}{\sqrt{2\sigma^2}}$ is a consequence of Lemma 2 and Theorem 3 and it is straightforward to see that the optimal choice for M is given in (68). On the other hand again as a consequence of Lemma 2 and Theorem 3 we can simply see that when $p_s < \frac{w_j}{\sqrt{2\sigma^2}}$ we have that:

$$M^* = \begin{cases} 1, & \text{if } (N-D)p_s > P_T, \\ 0, & \text{otherwise.} \end{cases} \tag{76}$$

B. Adjustable p_{th}

In the following we assume Eve can adjust p_{th}. This means u now becomes a function of both M, which is decided by Alice and Bob, and p_{th}, which is decided by Eve. As a result, each other's choices affect the optimal strategy of the other party and the problem can no longer be addressed with standard optimization tools but rather with game theoretic tools. Since $P_{\text{off}} = p_{\text{th}}$ we can now reformulate the expression for u as follows:

$$u(M, p_{\text{th}}) = MR\left(P_{\text{on}}, \Gamma_{\text{on}}\right) + (N-D-M)R(p_{\text{th}}, 0). \tag{77}$$

A zero-sum game that presents the interaction between the legitimate users and the jammer is investigated. As a non-cooperative game it has 3 components. Firstly, there are two players: player L representing the legitimate users (Alice and Bob are considered to be a single player) and player J representing the jammer (Eve). Secondly, both players have corresponding sets of possible actions $\mathcal{A}_{\text{L}} = M$ with $M \in \{0, 1, \ldots, N-D\}$ and $\mathcal{A}_{\text{J}} = p_{\text{th}}$ with $p_{\text{th}} \in [0, \infty]$ (the indices correspond to the players). Finally, both players have utility functions: u_{L} and $u_{\text{J}} = -u_{\text{L}}$, that measure the payoff for each player and for any set of actions. In other words, whatever first player's gain is, is equal to the second player's loss. The game is then defined as: $\mathcal{G}\{\mathcal{A}_{\text{L}}, \mathcal{A}_{\text{J}}, u(M, p_{\text{th}})\}$.

Letting p_{th} in (77) to become a variable we can identify the objectives of both players, i.e., player J aims to minimize the SKG utility $u(M, p_{\text{th}})$, whereas player L aims to maximize it. The optimal strategy of each player depends on the choice of their opponent and cannot be determined unilaterally. The profile $(M^{\text{NE}}, p_{\text{th}}^{\text{NE}}) \in \mathcal{A}_{\text{L}} \times \mathcal{A}_{\text{J}}$ is a Nash Equilibrium (NE) if none of the players can benefit by deviating from this profile.

Referring to theorem 3 we already know there are two possibility for M that maximizes $u(M, p_{\text{th}})$. Depending on their available power Alice and Bob should transmit at maximim power if $p_s > P_T$ or with constant power p_{th} if $p_s \leq P_T$. On the other hand, when we check the sign of the first derivative of (77) w.r.t. p_{th}, assuming that the short-term power constraint (67) is satisfied, it is easy to see that for any fixed M, the utility function is monotonically decreasing with p_{th}, i.e.:

$$\underset{p_{\text{th}} \in [0,\infty)}{\arg} \min u(M, p_{\text{th}}) = 0. \tag{78}$$

Equation (78) shows that the jammer optimal action is to set $p_{\text{th}} = 0$, so she could detect and jam any ongoing transmission. Eve's optimal action agrees with the work presented in [REFERENCE].

The results given in (68) and (78) present the optimal actions for each of the players. Given that, if each of them is trying to increase their utility, it is straightforward to see that no one can benefit from deviating from the optimal state. In other words player J has to use $p_{th} = 0$ in order to detect and jam any ongoing transmissions while player L has to use all the available power for SKG P_s. This gives the game's state $(N-D, 0)$, which is in fact the unique NE of $\mathcal{G}$.

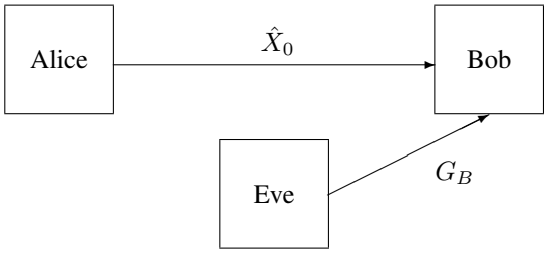

Fig. 5: System model with two legitimate nodes and a single adversary. Alice sends an encrypted message to Bob while Eve tries to compromise $\hat{X}_0$ and jams the recipient.

VII. Jamming attacks on data subcarriers

A. Adjustable threshold of detection

Similarly as in the game formulation the optimal action from Eve is to set $p_{\text{th}} = 0$, but in the previous case, due to the the independence of g_i the optimal power allocation was to use all the available power and to uniformly distribute it. For this case we can not assume that. The system model is presented in Fig. 5 and the objective function can be obtained by reformulating Eq. 10 as:

$$\hat{C}_D = \log_2\left(1 + \frac{g_i p_i}{1 + h_i \gamma_i}\right). \tag{79}$$

Again the legitimate users are trying to maximize $\hat{C}_D$ whereas Eve is aiming at minimizing it.

1) Optimal jammer's model: Assuming the worst case scenario where the gains on each of the subcarriers between the legitimate users and between the jammer and the recipient are know to Eve, while unknown to Alice and Bob. Given that we can find the optimal power allocation for Eve. This can be done by solving the following minimization problem:

$$\max_{\gamma_i, i\in\mathcal{D}} -\sum_{i=1}^{D} \log_2\left(1 + \frac{g_i p_i}{1 + h_i \gamma_i}\right) \tag{80}$$

s.t.

$$\sum_{i=1}^{D} \gamma_i \leq D\Gamma, \;\; \gamma_i \geq 0 \tag{81}$$

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

$$\mathcal{L}_\gamma = -\sum_{i=1}^{D} \log_2\left(1 + \frac{g_i p_i}{1 + h_i \gamma_i}\right) - \nu\left(\sum_{i=1}^{D} \gamma_i - D\Gamma\right). \tag{82}$$

By taking the first derivative and equate it to zero we can find the optimal allocation for the jammer. It is given by:

$$\gamma_i^* = \frac{-g_i p_i \nu \ln(2) - 2\nu \ln(2)}{2 h_i \nu \ln(2)} + \frac{\sqrt{(g_i p_i \nu \ln(2))^2 + 4 g_i p_i h_i \nu \ln(2)}}{2 h_i \nu \ln(2)}. \tag{83}$$

If we substitute (83) into (79) we get:

$$\frac{\ln\left(\ln(2)\, g_i \nu p_i + \sqrt{\ln(2)}\sqrt{g_i}\sqrt{\nu}\sqrt{p_i}\sqrt{\ln(2)\, g_i \nu p_i + 4\, h_i}\right)}{\ln(2)} + \frac{\ln\left(\left(\sqrt{\ln(2)}\sqrt{g_i}\sqrt{\nu}\sqrt{p_i}\sqrt{\ln(2)\, g_i \nu p_i + 4\, h_i} - \ln(2)\, g_i \nu p_i\right)^{-1}\right)}{\ln(2)} \tag{84}$$

2) Optimal model for the legitimate users: In this subsection we assume the opposite scenario, the legitimate users have the full channel state information (CSI) between each other and in the links to the jammer, while the information is unknown to Eve. Given Eq. (79) with average power constraint:

$$\sum_{i=1}^{D} p_i \leq DP, \tag{85}$$

in order to find the optimal p_i when Eve can adjust the threshold we reformulate the Lagrangian from (42), which in this case has the form:

$$\begin{aligned}\mathcal{L}_p =& \left(\sum_{i=1}^{D} \log_2\left(1 + \frac{p_i g_i}{1 + h_i \gamma_i}\right)\right)(1 - \mu\beta) \\ & - \lambda\left(\sum_{i=1}^{D} p_i - DP\right) \\ & + \mu\left((N - D)\log_2\left(1 + \frac{\sigma^2 p_s}{2 + \frac{1}{\sigma^2 p_s}}\right)\right),\end{aligned} \tag{86}$$

Theorem 4. *The optimal power allocation for data transmission, when Eve can adjust the threshold of detection, is expressed as:*

$$p_i^* = \left[\frac{1 - \beta\mu}{\ln(2)\,\lambda} - \frac{1 + h_i \gamma_i}{g_i}\right]^+. \tag{87}$$

If we substitute we get:

$$\hat{C}_D = \frac{\ln\left(\frac{g_i}{1 + h_i \gamma_i}\right) + \ln\left(\frac{1 - \mu\beta}{\lambda \ln(2)}\right)}{\ln(2)} \tag{88}$$

3) Robust jammer's model: In this subsection we are looking for the jammer's best performance under the worst case scenario for her, assuming that the legitimate users always chooses their optimal allocation. This can be written as min-max problem: $\min_\gamma \max_p \hat{C}_D$. The inner max problem has be solved and the solution is given in Eq. (87). We can find the optimal action for the jammer by substituting (87) into (82). This result in:

$$\gamma_{i,0}^* = \left[\frac{1}{\nu \ln(2)} - \frac{1}{h_i}\right]^+ \tag{89}$$

4) Robust legitimate users' model: In this subsection we are looking for the legitimate users' best performance under the worst case scenario for them, assuming that the jammer always chooses her optimal allocation. This can be written as a max-min problem: $\max_p \min_\gamma \hat{C}_D$. The inner min problem has be solved and the solution is given in Eq. (83). We can find the optimal action for the legitimate users by substituting (83) into (86). This result in:

$$p_{i,0}^* = \frac{-2\,\lambda h_i \pm \sqrt{\beta^2 {g_i}^2 \nu^2 \mu^2 - 2\,\beta {g_i}^2 \nu^2 \mu + 4\,\lambda^2 {h_i}^2 + {g_i}^2 \nu^2}}{\ln(2)\, g_i \nu \lambda} \tag{90}$$

B. Fixed threshold of detection

Due to the fact the achievable data transmission rate is dependent on g_i we can not identify unique value of p_i, which can determine the optimal action of the legitimate users for all data subcarriers. Instead, we can find such value for each subcarrier separately.

Theorem 5. *Depending on the available power for data transmission, if p_{th} is fixed, either all data subcarriers should be set to ON or all them to OFF.*

Proof: The proof is analogous to the proof of theorem 3. The value of γ_i that determines the optimal allocation is:

$$\Gamma_{T,i} = -\frac{p_{\text{th}} \ln(2)\, \lambda g_i + \beta g_i \mu + \ln(2)\, \lambda - g_i}{\ln(2)\, h_i \lambda \left(g_i p_{\text{th}} + 1\right)}, \tag{91}$$

which is the solution in γ_i for:

$$\log_2\left(1 + \frac{g_i p_i^*}{1 + h_i \gamma_i}\right) = \log_2\left(1 + g_i p_{\text{th}}\right), \tag{92}$$

and is unique for each subcarrier. Here h_i and γ_i represent the fading coefficient and the power level used for jamming in the link between Eve and the legitimate recipient. Which results in the following; if $\Gamma > \Gamma_{T,i}$, the corresponding subcarrier has to be set OFF, if $\Gamma \leq \Gamma_{T,i}$, the corresponding subcarrier has to be set ON. ■

VIII. Jamming on SKG and data transmission

Either if Eve can or cannot adjust the threshold the results from the previous sections holds true.

IX. 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 depended on the overall available power and might not have been 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 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," *Proc. IEEE*, vol. 103, no 10, Oct. 2015.

[2] A. Yener, S. Ulukus, "Wireless Physical-Layer Security: Lessons Learned From Information Theory," *Proc. IEEE*, vol. 103, No. 10, October 2015.

[3] K. McKay *et al.*, "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. Maurer. "Secret key agreement by public discussion based on common information," *IEEE Trans. Inf. Theory*, Vol. 39, No. 5, pp. 733-742, May 1993.

[6] R. Ahlswede and I. Csiszar. "Common randomness in information theory and cryptography part I: Secret sharing," *IEEE Trans. Inf. Theory*, Vol. 39, No. 7, pp. 1121-1132, July 1993.

[7] Qian Wang, and Hai Su and Kui Ren and Kwangjo Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks", *Proc. IEEE Int. Conf. Computer Commun. (INFOCOM)*, 2011, pp. 1422–1430,

[8] C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness", *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2015, pp. 113-118, Florence, Italy,

[9] C. Ye, A. Reznik and Y. Shah. "Extracting secrecy from jointly Gaussian random variables," 2006 IEEE International Symposium on Information Theory. pp. 2593 - 2597, July 2006.

[10] 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, Nov. 2017.

[11] G. Caire, G. Taricco and E. Biglieri "Optimum Power Control Over Fading Channels," *IEEE Trans. Inf. Theory.* Vol. 45, No. 5, pp. 1468 - 1489, July 1999.

[12] R. Bellman, and R. Kalaba, *"Dynamic Programming and Modem Control Theory"*, Academic Press, New York; 1965.

[13] O. Hölder, *"Ueber einen Mittelwertsatz"*, Gttinger Nachr. (1889) pp. 3847.

[14] J.L. Jensen, *"Sur les fonctions convexes et les ingualits entre les valeurs moyennes"*, Acta Math. , 30 (1906) pp. 175193.

[15] Andrea Goldsmith *" Wireless Communications "*, Cambridge University Press, 2005

[16] H.-C. Yang and M.-S. Alouini, *Order Statistics in Wireless Communicatiobs*, Cambridge University Press, NY, 2011.