Subcarrier Scheduling for Joint Data Transfer and Key Generation Schemes in Multicarrier Systems

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*—In computational complexity and latency constrained emerging 5G applications, e.g., autonomous vehicles, haptic communications and enhanced reality, secret key generation (SKG) at the physical layer could be considered as an alternative to currently used key agreement schemes. In this framework, we study the optimal subcarrier scheduling in multicarrier systems when a subset of the subcarriers are used for SKG and the rest for data transmission, under both security and power constraints. The amount of data that can be transmitted with a single key is determined by the cryptographic suites used, so that realistic key rate constraints can be identified. This allows us to formulate the subcarrier allocation as a subset-sum $0-1$ knapsack optimization problem that we solve using i) the standard dynamic programming approach and ii) a greedy heuristic approach of linear complexity. We show that the proposed heuristic induces virtually no loss in performance. Furthermore, a comparison with a baseline scheme in which SKG and data transfer are performed sequentially, shows that the proposed parallel approach offers gains in terms of efficiency.**

I. Introduction

Many standard cryptographic schemes, particularly those in the realm of public key encryption (PKE), are computationally intensive, incurring considerable overheads and can rapidly drain the battery of power constrained devices [1], [2]. For example, in ultra reliable low latency communication systems (URLLC) it is noted that ”for a URLLC service with higher speed than 65kbps, the 3GGP Release 15 radio access network (RAN) cannot fulfill the quality of service (QoS) requirement while enforcing user plane integrity protection” [3]. Others also point to using physical layer security to reduce the resource overhead in URLLC [4].

As a consequence, the employment of physical layer security (PLS) approaches is currently being considered for beyond fifth generation (B5G) systems. In this direction, a promising alternative to PKE for key agreement is offered by secret key generation (SKG) from shared randomness [5]. The task of SKG from correlated observations was first studied in [6] and [7]. A straightforward SKG approach can be built by exploiting the reciprocity of the wireless fading coefficients between two terminals during the channel coherence time [8]. Since this early work to propose such an SKG approach, there have been implementations showing that the technique is indeed practicable [9].

Focusing in this work on the scheduling of the physical layer resources, we investigate the possibility of jointly performing SKG and data transfer. The motivation behind this study is to increase the transmission efficiency as data could be immediately transmitted whenever they become available without having to “wait” for key agreement to take place. In future work we will explicitly incorporate latency estimates.

In the system model introduced in this work, we assume that a block fading additive white 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. The specific contributions of this work are: i) *determining the optimal subcarrier allocation under security and power constraints* by formulating a subset-sum $0-1$ knapsack problem [10], which is solved using dynamic programming techniques [11], and ii) *proposing a heuristic solution* with linear complexity. We show that the heuristic approach – according to which the strongest subcarriers in terms of SNR should be used for data transfer and the weakest for SKG – only induces a negligible penalty in terms of performance for any realistic set of parameters. Our findings are supported by numerical results, while the efficiency of the proposed scheme is shown to be greater or similar to the efficiency of an alternative approach in which SKG and data transfer are sequentially performed, depending on the exact values of the system parameters.

The paper is organized as follows: the general system model is introduced in Section II, the data transfer and SKG scheme is described in Section III. In Section IV, the efficiency of the proposed hybrid approach is evaluated against that of an alternative sequential approach, while conclusions and directions for future work are presented in Section V.

II. SKG System Model

In the basic SKG system model, depicted in Fig. 1 we assume that two legitimate parties, referred to as Alice and Bob in the following, wish to establish a symmetric secret key using as a source of shared randomness the wireless fading coefficients. Throughout our work a rich Rayleigh multipath environment is assumed, such that the fading coefficients rapidly decorrelate over short distances [8]. Furthermore, Alice and Bob communicate over a block fading AWGN channel that

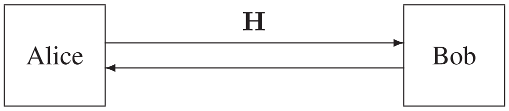

Fig. 1: Alice and Bob exchange pilot signals over a Rayleigh fading channel with realization $\mathbf{H} = [H_1, \ldots, H_N]$ in order to distill a shared secret key.

comprises N orthogonal subcarriers. The fading coefficients, denoted by $H_j, j = 1, \ldots, N$, are assumed to be independent and identically distributed (i.i.d), $H_j \sim \mathcal{CN}(0, \sigma^2)$. Although in actual multicarrier systems neighbouring subcarriers will typically experience correlated fading, in the present work this effect is neglected as its impact on SKG has been treated in numerous contributions in the past [12]–[14] and will not enhance the problem formulation in the following Sections.

The SKG procedure encompasses three phases [6], [7]:

1) Advantage distillation: This phase takes place over two periods. The legitimate nodes sequentially exchange constant probe signals with power P on all subcarriers[1], to obtain estimates of their reciprocal CSI. Commonly, the received signal strength (RSS) has been used as the source of shared randomness for generating the shared key, but it is possible to use the full CSI [15]. At the end of this phase, Alice and Bob obtain observations $X_{A,j}, X_{B,j}$, respectively, on the j-th subcarrier that can be expressed as:

$$X_{A,j} = \sqrt{P} H_j + Z_{A,j}, \tag{1}$$

$$X_{B,j} = \sqrt{P} H_j + Z_{B,j}, \tag{2}$$

$j = 1, \ldots, N$, where by $Z_{A,j}, Z_{B,j}$ we denote zero-mean, unit variance circularly-symmetric complex AWGN random variables, $(Z_{A,j}, Z_{B,j}) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_2)$. At the end of this phase the observations $X_{A,j}, X_{B,j}, j = 1 \ldots, N$ are quantized [16], so that Alice and Bob distill binary vectors $\mathbf{r}_{A,j}, \mathbf{r}_{B,j}, j = 1, \ldots, N$ respectively.

2) Information reconciliation: Due to the presence of noise, $\mathbf{r}_{A,j}, \mathbf{r}_{B,j}, j = 1, \ldots, N$ will differ. To reconcile discrepancies in the quantizer local outputs, side information needs to be exchanged via a public channel. Using the principles of Slepian Wolf encoding, the distilled binary vectors can be reconciled to corresponding codewords $\mathbf{c}_j, j = 1, \ldots, N$, with

$$\mathbf{r}_{A,j} = \mathbf{c}_j + \mathbf{e}_{A,j}, \tag{3}$$

$$\mathbf{r}_{B,j} = \mathbf{c}_j + \mathbf{e}_{B,j}. \tag{4}$$

Numerous practical information reconciliation approaches using standard forward error correction codes (e.g., LDPC, BCH, etc.,) have been proposed [8], [15]. As an example, if a block encoder with parity check matrix $\mathbf{Q}$ is used, then for the errors in the local observations the following hold [15]:

$$\mathbf{Q}\mathbf{e}_{A,j}^T = \mathbf{S}_{A,j}, \tag{5}$$

$$\mathbf{Q}\mathbf{e}_{B,j}^T = \mathbf{S}_{B,j}, \tag{6}$$

where $\mathbf{S}_{A,j}, \mathbf{S}_{B,j}$ denote the syndromes of $\mathbf{r}_{A,j}, \mathbf{r}_{B,j}$ with respect to the codeword $\mathbf{c}_j$ for $j = 1, \ldots, N$. To perform reconciliation, Alice (or Bob) transmit their corresponding syndrome $\mathbf{S}_{A,j}$ ($\mathbf{S}_{B,j}$), so that both parties can reconcile $\mathbf{r}_{A,j}, \mathbf{r}_{B,j}$ to $\mathbf{c}_j, j = 1, \ldots, N$. In this work, we assume that the reconciliation information (e.g., the transmission of syndromes in the previous example) takes place on the same subcarrier index, i.e., the syndrome $\mathbf{S}_{A,j}$ is sent from Alice to Bob on subcarrier with index j.

3) Privacy amplification: The secret key is generated by hashing $[\mathbf{c}_1 \| \ldots \| \mathbf{c}_N]$, where $[\cdot\|\cdot]$ denotes concatenation of the corresponding binary vectors. To this end, modern hash functions can be employed, e.g., SHA-256. The privacy amplification step ensures that the generated keys are completely unpredictable by an adversary and that they have maximum entropy (i.e., are uniformly distributed). Note that the final step of privacy amplification, is executed locally without any further information exchange.

Under the system model in Fig. 1, the SKG rate on any subcarrier is (note that the noise variances are here normalized to unity for simplicity) [8], [17]:

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

while the corresponding *minimum* necessary reconciliation rate has been show to be $h(H_{B,j}|H_{A,j})$ [7]. In the following, we will focus on optimizing the allocation of resources (frequency and power) in multicarrier systems in which keys are generated at the physical layer as described above.

III. Hybrid SKG and Data Transfer System Model

We have discussed in Section II how Alice and Bob can distill secret keys from estimates of the fading coefficients in their wireless link. At the same time CSI estimates are prerequisite in order to optimally allocate power across the subcarriers and achieve high data rates[2]. As a result, a question naturally arises: *should the CSI estimates (obtained at the end of the pilot exchange phase) be used towards the generation of secret keys or towards the reliable data transfer, and, furthermore, whether the SKG and the data transfer can be inter-weaved?*

In this paper, we are interested in answering this question and shed light into whether following the exchange of pilots Alice should transmit reconciliation information on all subcarriers so that she and Bob can generate (potentially) a long sequence of key bits, or, alternatively, perform information reconciliation only over a subset of the subcarriers and transmit data over the rest. We will call the former approach a *sequential* scheme, while we will refer to the latter as a *parallel* scheme. The two will be compared in terms of their efficiency with respect to the achievable data rates

[1] An explanation of the optimality of this choice under different attack scenarios is discussed in [5].

[2] As an example, despite the extra overhead, in URLLC systems advanced CSI estimation techniques are employed in order to be able to satisfy the strict reliability requirements.

As discussed in Section II, our physical layer system model assumes Alice and Bob exchange data over a Rayleigh BF-AWGN channel with N orthogonal subcarriers. Without loss of generality the variance of the AWGN in all links is assumed to be unity. During channel probing, constant pilots are sent across all subcarriers [8], [17] with power P. Using the observations (1), Alice estimates the channel coefficients as

$$\hat{H}_j = H_j + \tilde{H}_j, \tag{8}$$

for $j = 1, \dots, N$ where $\tilde{H}_j$ denotes an estimation error that can be assumed to be Gaussian, $\tilde{H}_j \sim \mathcal{CN}(0, \sigma_e^2)$ [18]. Under this model, the following rate is achievable on the j-th subcarrier from Alice to Bob when the transmit power during data transmission is p_j [18]:

$$R_j = \log_2\left(1 + \frac{g_j p_j}{\sigma_e^2 P + 1}\right) = \log_2(1 + \hat{g}_j p_j), \tag{9}$$

where we set $\hat{g}_i = \frac{g_i}{\sigma_{i,e}^2 P + 1}$. As a result, the channel capacity $C = \sum_{j=1}^{N} R_j$ under the short term power constraint:

$$\sum_{j=1}^{N} p_j \leq NP, \;\; p_j \geq 0, \; \forall j \in \{1, \dots, N\}, \tag{10}$$

is achieved with the well known waterfilling power allocation policy $p_j = \left[\frac{1}{\lambda} - \frac{1}{\hat{g}_j}\right]^+$, where the water-level λ is estimated from the constraint (10). In the following, the estimated channel gains $\hat{g}_j$ are – without loss of generality – assumed ordered in descending order, so that:

$$\hat{g}_1 \geq \hat{g}_2 \geq \dots \geq \hat{g}_N. \tag{11}$$

As mentioned above, the advantage distillation phase of the SKG process consists of the two-way exchange of pilot signals during the coherence time of the channel to obtain $\mathbf{r}_{A,j}, \mathbf{r}_{B,j}, j = 1, \dots, N$. On the other hand, the CSI estimation phase can be used to estimate the reciprocal channel gains in order to optimize data transmission using the waterfilling algorithm. In the former case, the shared parameter is used for generating symmetric keys, in the latter for deriving the optimal power allocation. In the parallel approach the idea is to inter-weave the two procedures and investigate whether a joint data transfer and key generation scheme could bear any advantages with respect to the system efficiency. While in the sequential approach the CSI across all subcarriers will be treated as a source of shared randomness between Alice and Bob, in the parallel approach it plays a dual role.

A. Parallel Approach

In the parallel approach, after the channel estimation phase, the legitimate users decide on which subcarrier to send the reconciliation information (e.g., the syndromes as discussed in Section II) and on which data (i.e., the SKG process here is not performed on all of the subcarriers). The total capacity has now to be distributed between data and reconciliation information bearing subcarriers. As a result, 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 reconciliation such that, $\mathcal{D} \cup \bar{\mathcal{D}} = \{1, \dots, N\}$.

Over $\mathcal{D}$ the achievable sum data transfer rate, denoted by C_D is given by

$$C_D = \sum_{j \in \mathcal{D}} \log_2(1 + \hat{g}_j p_j), \tag{12}$$

while on the subset $\bar{\mathcal{D}}$, Alice and Bob exchange reconciliation information at rate

$$C_R = \sum_{i \in \bar{\mathcal{D}}} \log_2(1 + \hat{g}_i p_i) \tag{13}$$

and establish a secret key with rate C_{SKG}

$$C_{SKG} = |\bar{\mathcal{D}}| R_k = (N - D) \log_2\left(1 + \frac{P\sigma^2}{2 + \frac{1}{P\sigma^2}}\right), \tag{14}$$

after privacy amplification. The minimum rate necessary for reconciliation has been theoretically derived in [7]. Here, alternatively, we employ a more practical design approach in the which the rate of the employed encoder is explicitly taken into account. Noting that in a rate $\frac{k}{n}$ block encoder the syndrome rate is $\frac{n-k}{n}$, we define the parameter $\kappa = \frac{n-k}{k}$ that reflects the ratio of the reconciliation rate to the SKG rate. For example, for a rate $\frac{k}{n} = \frac{1}{2}$ encoder, $\kappa = 1$, for $\frac{k}{n} = \frac{1}{3}$, $\kappa = 2$, while for $\frac{k}{n} = \frac{1}{4}$, $\kappa = 3$. Note, in practice κ needs to be chosen depending on the scenario and the channel characteristics. Based on this discussion, we capture the minimum requirement for the reconciliation rate through the following expression:

$$C_R \quad \geq \quad \kappa C_{SKG}. \tag{15}$$

Furthermore, to identify the necessary key rate, we note that 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 or in the Galois counter mode (GCM). In practical systems, a single key of length 128 to 256 bits can be used to encrypt up to gigabytes of data. As a result, we will assume that for a particular application it is possible to identify the ratio of key to data bits, which in the following we will denote by β. Specifically, we assume that the following security constraint should be met

$$C_{SKG} \geq \beta C_D, \;\; 0 < \beta \leq 1, \tag{16}$$

where, depending on the application, the necessary minimum value of β can be identified. We note in passing that the case $\beta = 1$ would correspond to a one-time-pad, i.e., the generated keys could be simply x-ored with the data to achieve perfect secrecy without the need of any cryptographic suites.

Accounting for the reconciliation rate and security constraints in (15) and (16) we formulate the following maximization problem:

$$\max_{p_j, j \in \mathcal{D}} \sum_{j \in \mathcal{D}} R_j \tag{17}$$

$$\text{s.t. } (10), (15), (16),$$

$$\sum_{j \in \mathcal{D}} R_j + \sum_{i \in \bar{\mathcal{D}}} R_i \leq C. \tag{18}$$

(16) can be integrated with (15) to the combined constraint

$$\sum_{j\in\mathcal{D}} R_j \quad \leq \quad \frac{\sum\limits_{i\in\bar{\mathcal{D}}} R_i}{\kappa\beta}. \tag{19}$$

The optimization problem at hand is a mixed-integer convex optimization problem with unknowns both the sets $\mathcal{D}, \bar{\mathcal{D}}$, as well as the power allocation policy $p_j, j \in \{1, \dots, N\}$. These problems are typically NP hard and addressed with the use of branch and bound algorithms and heuristics.

In this work, we propose a simple heuristic to make the problem more tractable by reducing the number of free variables. In the proposed approach, we assume that the constraint (18) is satisfied with equality. The only power allocation that allows this is the water-filling approach that uniquely determines the power allocation p_j and also requires that the constraint (10) is also satisfied with equality. Thus, if we follow that approach, we determine the power allocation vector uniquely and can combine the remanining constraints (18) and (19) into a single one as:

$$\sum_{j\in\mathcal{D}} R_j \leq \frac{C}{\kappa\beta + 1}. \tag{20}$$

The new optimization problem can be re-written as

$$\max_{x_j\in\{0,1\}} \sum_{j=1}^{N} R_j x_j \tag{21}$$

$$\text{s.t.} \sum_{j=1}^{N} R_j x_j \leq \frac{C}{1+\kappa\beta}. \tag{22}$$

The problem in (21)-(22) is a subset-sum problem from the family of $0-1$ knapsack problems, that is known to be NP hard [10]. However, these type of problems are solvable optimally using dynamic programming techniques in pseudo-polynomial time [10], [11]. Furthermore, it is known that greedy heuristic approaches are bounded away from the optimal solution by half [19].

We propose a simple greedy heuristic algorithm with *linear complexity*, as follows. Let us assume that the estimated channel gains, and, consequently, the rates R_j are ordered in descending order (the ordering is a $\mathcal{O}(N \log N)$ operation, so if the gains are not ordered the overall complexity will be dominated by the sorting operation). The data subcarriers are selected starting from the best – in terms of SNR – until (22) is not satisfied. Once this situation occurs the last subcarrier added to set $\mathcal{D}$ is removed and the next one is added. This continues either to the last index N or until (22) is satisfied with equality. The algorithm is described in *Algorithm 1*.

The efficiency of the proposed parallel method – measured as the ratio of the long-term data rate versus the average capacity – is evaluated as:

$$\mathrm{E}_{\text{parallel}} = \frac{\mathbb{E}\left[\sum\limits_{i\in\mathcal{D}} R_i\right]}{\mathbb{E}[C]}. \tag{23}$$

Algorithm 1: Heuristic Greedy Algorithm for (21)-(22)

```
procedure HEURISTIC(start, end, $R_j$)
    $j \leftarrow 1, C_0 \leftarrow 0, R_{N+1} \leftarrow 0$
    while $j \leq N-1$ and $C_j \leq \frac{C}{1+\kappa\beta}$ do
        $C_j \leftarrow C_{j-1} + R_j$
        if $C_j \leq \frac{C}{1+\kappa\beta}$ then
            $j \leftarrow j+1$
        else do $C_j \leftarrow C_j - R_j; R_j \leftarrow 0; j \leftarrow j+1$
        end if
    end while
end procedure
```

This efficiency quantifies the expected back-off in terms of data rates when part of the resources (power and frequency) are used to enable the generation of secret keys at the physical layer. In future work, we will compare the efficiency achieved to that of actual approaches currently used in 5G by accounting for the actual delays incurred due to the PKE key agreement operations [4].

B. Sequential Approach

In the sequential approach data transfer and secret key generation are two separate events; first, the secret keys are generated over the whole set of subcarriers, leading to a sum SKG rate given as

$$C_{SKG} = N \log_2\left(1 + \frac{P\sigma^2}{2 + \frac{1}{P\sigma^2}}\right). \tag{24}$$

To estimate the efficiency of the scheme, we further need to identify the necessary resources for the exchange of the reconciliation information. We can obtain an estimate of the number of transmission frames that will be required for the transmission of the syndromes, as the expected value of the reconciliation rate (i.e., it's long-term value) $\mathbb{E}[C_R]$. The average number of frames needed for reconciliation is then computed as:

$$M = \left\lceil \frac{\kappa C_{SKG}}{\mathbb{E}[C_R]} \right\rceil, \tag{25}$$

where $\lceil x \rceil$ denotes the smallest integer that is larger than x.

The average number of the frames that can be sent while respecting the secrecy constraint is:

$$L = \left\lfloor \frac{C_{SKG}}{\beta\mathbb{E}[C]} \right\rfloor, \tag{26}$$

where $\lfloor x \rfloor$ denotes the largest interger that is smaller than x. The efficiency of the sequential method is then calculated as:

$$\mathrm{E}_{\text{sequential}} = \frac{L}{L+M}. \tag{27}$$

IV. Numerical Results

In this Section we provide numerical evaluations of the efficiency that can be achieved with the presented methods (i.e., sequential and parallel) for different values of the main parameters. With respect to the parallel approach, we provide

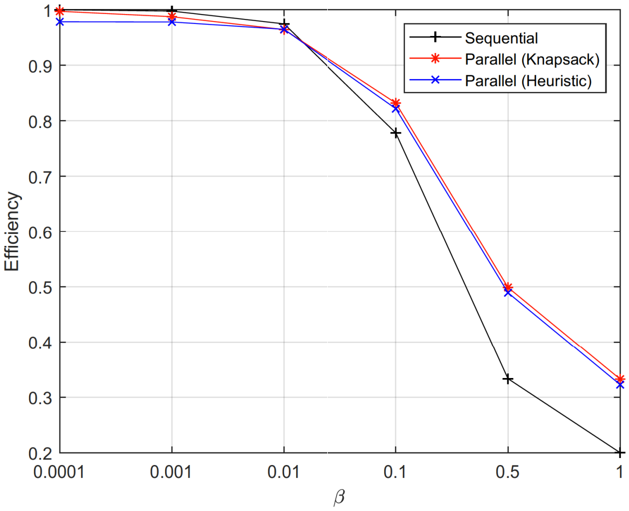

Fig. 2: a) Efficiency comparison for $N = 12$, the transmit SNR=10 dB and $\kappa = 2$.

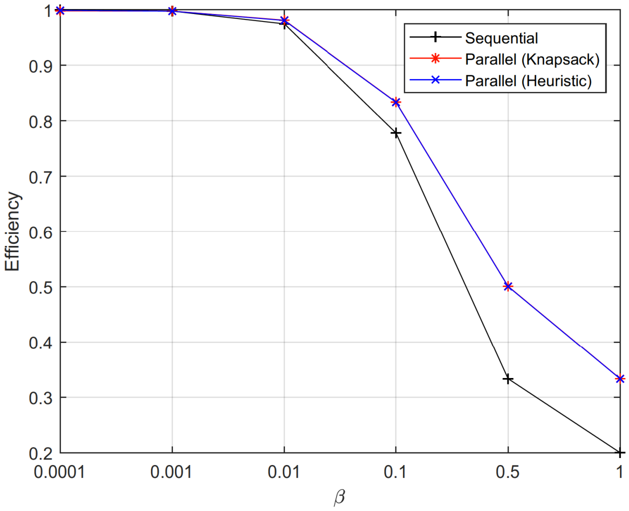

Fig. 2: b) Efficiency comparison for $N = 64$, the transmit SNR=10 dB and $\kappa = 2$.

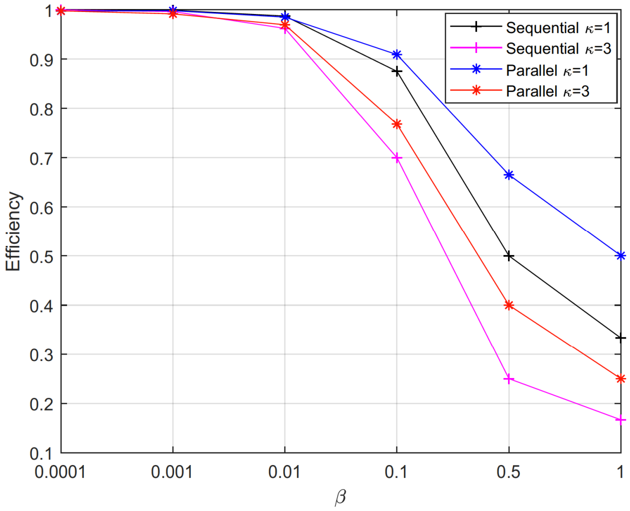

Fig. 3: Efficiency vs κ, for $N = 24$, SNR=10 dB.

numerical results of the optimal dynamic programming solution of the subset-sum $0-1$ knapsack problem, as well as of the greedy heuristic approach presented in *Algorithm 1*.

The two subfigures of Fig. 2 show the efficiency of the methods for $N = 12$, (Fig. 2a) and $N = 64$ (Fig. 2b) while $\kappa = 2$ and $P = 10$. We note that the proposed heuristic algorithm has a near-optimal performance (almost indistinguishable from the red curves achieved with dynamic programming). Due to this fact (which was tested across all scenarios that follow) only the heuristic approach is shown in subsequent figures for clarity in the graphs.

We see that for a small number of subcarriers (N=12, typical for NB-IoT) and small β the efficiency of both the parallel and the sequential approaches are very close to unity, a trend that holds for increasing N. With increasing β, due to the fact that more frames are needed for reconciliation in the sequential approach (i.e., M increases), regardless of the number of subcarriers, the parallel method proves more efficient than the sequential. While the efficiency of the sequential and parallel methods coincide almost until around $\beta = 0.01$ for $N = 12$, for $N = 64$ the crossing point of the curves moves to the left and the efficiency of the two methods coincide until around $\beta = 0.001$. This trend was found to be consistent across many values of N, only two of which are shown here due to restrictions in space.

Next, in Fig. 3 the efficiency of the parallel and the sequential methods are shown for two different values of $\kappa \in \{1, 3\}$ for SNR $= 10$ dB and $N = 24$. It is straightforward to see that they both follow similar trends and when κ increases the efficiency decreases. On the other hand, regardless of the value of κ they both perform identically until around $\beta = 0.001$.

Finally, in Fig.4, focusing on the parallel method, the average size of set $\mathcal{D}$ is shown for different values of σ_e^2 and transmit SNR levels (Fig. 4a) and κ (Fig. 4b), for $N = 24$. As expected, in Fig. 4a we see when the SNR increases the size of the set increases, too. This is due to the fact that more power is used on any single subcarrier and consequently a higher reconcilliation rate can be sustained. Regarding the estimation error σ_e^2 of the CSI, it only slightly affects the performance at high SNR levels. Hence more subcarriers have to be used for reconciliation, and fewer for data. The SNR level in Fig. 4b is set to 10 dB. The figure shows that when increasing κ the size of set $\mathcal{D}$ decreases. This result can be easily predicted from inequality (15), meaning, when κ increases more reconciliation data has to be sent, hence fewer subcarriers can be used for data. In both Fig. 4a and Fig. 4b when β increases the size of set $\mathcal{D}$ decreases; this effect is a consequence of constraint (22) as the data rate is decreasing with β.

V. Conclusions

In this work we investigated the possibility of jointly performing data transfer and SKG in a Rayleigh BF-AWGN

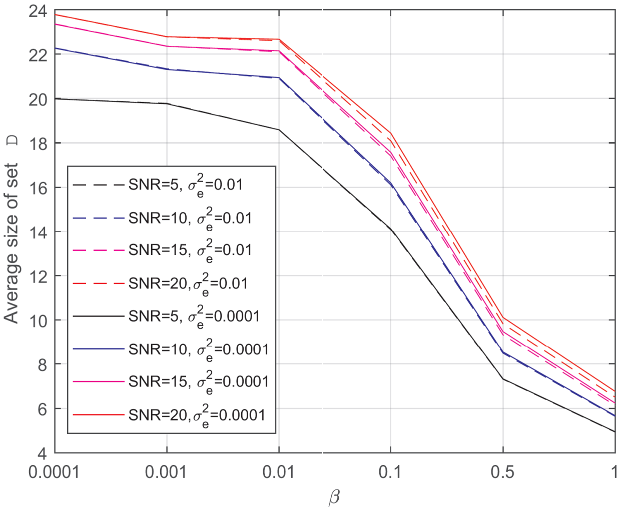

Fig. 4: a) Size of set $\mathcal{D}$ for different SNR levels and σ_e^2 when $N = 24$.

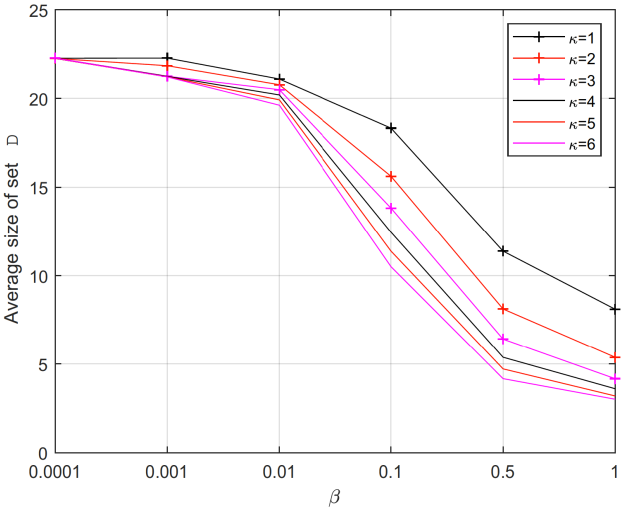

Fig. 4: b) Size of set $\mathcal{D}$ for different values of κ when $N = 24$.

environment. We studied the maximization of the data transfer rate under power and security constraints, captured through the following system parameters: a factor β, representing the minimum ratio of the SKG to the data rate, and, a factor κ representing the maximum ratio of the SKG rate over the reconciliation rate. The proposed parallel method, in which SKG and data transfer are inter-weaved, was shown to perform equally well or better than a sequential approach in which the two operations were separated. Furthermore, a significant result is that although the optimal subcarrier scheduling is a $0-1$ knapsack problem, with a potentially high bound on complexity, it can be solved in linear time using a simple heuristic algorithm with virtually no loss in performance.

Acknowledgements

M. Mitev is supported by the Doctoral Training Programme of CSEE, University of Essex, A. Chorti is supported by the ELIOT ANR-18-CE40-0030 and FAPESP 2018/12579-7 project and M.J. Reed is supported by the project SerIoT which has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement No 780139.

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, pp. 1747–1761, Oct 2015.

[2] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct 2015.

[3] "3GPP TR 33.825 V0.3.0, Study on the Security for 5G URLLC (Release 16)," 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, available online https://www.3gpp.org/ftp/Specs/archive/33_series/33.825/.

[4] A. Weinand, M. Karrenbauer, and H. D. Schotten, "Security Solutions for Local Wireless Networks in Control Applications based on Physical Layer Security," *IFAC-PapersOnLine*, vol. 51, no. 10, pp. 32–39, 2018. [Online]. Available: https://doi.org/10.1016/j.ifacol.2018.06.232

[5] A. Chorti, "A study of injection and jamming attacks in wireless secret sharing systems," in *Proc. of the 2nd Workshop on Communication Security*. Cham: Springer International Publishing, 2018, pp. 1–14.

[6] 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.

[7] 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.

[8] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 2593–2597.

[9] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[10] S. Martello and P. Toth, *Knapsack problems: algorithms and computer implementations*. NY: John Wiley and Sons, 1990.

[11] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems*. Springer-Verlag Berlin Heidelberg, 2004.

[12] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb 2011.

[13] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual ofdm subcarriers," *IEEE Trans. Commun*, vol. 64, no. 6, pp. 2578–2588, June 2016.

[14] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, April 2017.

[15] C. Saiki and A. Chorti, "A novel physical layer authenticated encryption protocol exploiting shared randomness," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 113–118.

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

[17] 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.

[18] M. Medard, "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 933–946, May 2000.

[19] V. Vazirani, *Approximation Algorithms*. Springer-Verlag Berlin Heidelberg, 2003.