Optimal Signalling Strategies and Power Allocation for Wireless Secret Key Generation Systems in the Presence of a Jammer

Arsenia Chorti
School of Computer Science and Electronic Engineering
University of Essex, Wivenhoe Park, UK
Email: achorti@essex.ac.uk

***Abstract*—Secret key generation (SKG) schemes have been shown to be vulnerable to denial of service (DoS) attacks in the form of jamming. In this paper, a comprehensive study on the impact of correlated and uncorrelated jamming in wireless SKG systems is presented. First, optimal signalling schemes for the legitimate users and jamming approaches for an active adversary launching a DoS attack on the SKG system are derived. It is shown that the legitimate users should employ constant signalling. On the other hand, the jammer should inject either correlated jamming when imperfect channel state information (CSI) regarding the main channel is at their disposal, or, uncorrelated jamming when the main channel CSI is completely unknown. In both cases, optimal power allocation policies are studied under short-term power constrains for M block fading additive white Gaussian noise (BF-AWGN) channels. Numerical evaluations demonstrate that equidistribution of the jamming power is near-optimal in the case of uncorrelated jamming.**

***Index Terms*—Jamming, communication system security, physical layer security.**

I. Introduction

The increasing deployment of wireless networks poses security challenges in next generation dynamic and decentralized networks, consisting of low-cost, low-complexity devices. Over the last two decades alternative/complementary means to secure data exchange in wireless settings have been investigated in the framework of physical layer security (PLS), addressing jointly the issues of reliability and secrecy. One of the most mature topics in PLS is the generation of secret keys via public discussion, based on either the so-called source model [1]–[5] or the so-called channel model [6].

Recently, in [7] the effect of denial of service attacks (DoS) in the form of jamming was demonstrated to substantially decrease SKG rates; with increasing jamming power the SKG rates were shown to asymptotically diminish. In this investigation the adversaries were assumed to inject constant jamming signals and have been shown to have a maximum impact on the SKG system when they were able to evaluate the channel state information (CSI) in the links between themselves and the legitimate nodes (partial CSI availability). However, the optimality of injecting constant jamming signals was not studied, neither was the scenario in which the adversary obtains an imperfect estimate of the main channel CSI. Furthermore, this analysis concerned exclusively narrowband SKG systems while typical anti-jamming techniques such as direct sequence spread spectrum, spread spectrum frequency hopping and uncoordinated hopping/spreading approaches span many parallel subchannels.

As a result, a systematic analysis of the impact of jamming in SKG systems with parallel subchannels when imperfect CSI might be available at the adversarial node is timely. We begin our investigation by determining optimal signalling schemes for the pair of legitimate nodes and the jammer. It is shown that the legitimate nodes should employ a constant signalling scheme, while the jammer – depending on the availability of side information in the form of imperfect main channel CSI – should either inject correlated or uncorrelated jamming. Next, optimal power allocation policies are investigated for SKG systems with M parallel subchannels – modeled as M block fading additive white Gaussian noise (BF-AWGN) channels – under short-term power constraints. In the case of uncorrelated jamming attacks, it is shown through numerical evaluations that equally distributing their power across the available spectrum is near-optimal for active adversaries.

The rest of the paper is organized as follows. The system model is described in Section II. Furthermore, in Section III optimal signalling schemes for the pair of legitimate nodes and the jammer are derived while optimal power allocation schemes over M parallel subchannels under short-term power constraints are investigated in Section IV. Numerical evaluations are presented in Section V while the conclusions of this work are drawn in Section VI.

II. System Model

The system model is shown in Fig.1 with Alice and Bob denoting legitimate nodes and Eve a jammer. The SKG process includes two distinct cycles over which the channel coefficients between Alice and Bob are assumed to be reciprocal and stationary and then to change independently, i.e., both cycles take place within the channel's coherence time[1]. In this work we assume that Eve attempts to obtain an estimate of the main channel CSI over the first cycle and transmit jamming signals over the second. Moreover, given that a common countermeasure for DoS attacks in wireless systems is the

[1]This standard assumption in SKG systems analysis does not affect the nature of the presented results. For more realistic channel models that account for correlation of the fading coefficients see [8] and related works.

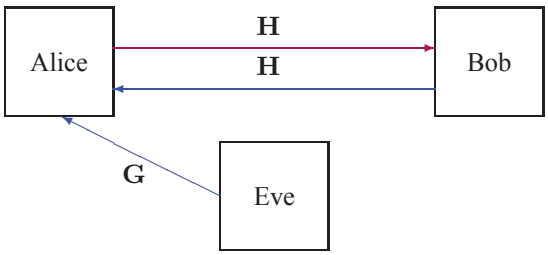

Fig. 1. System model of the SKG process encompassing two cycles. During the first cycle (purple) Alice transmits probe signals and Eve attempts to obtain an estimate of $\mathbf{H}$. During the second cycle (blue) Bob transmits probe signals and Eve jams the communication.

employment of frequency hopping [9], in the SKG system model under investigation Alice and Bob exchange messages over an M BF-AWGN channel with M parallel subchannels. In this framework we use the following notation for the fading coefficients: $\mathbf{H} = \left[H^{(1)}, \ldots, H^{(M)}\right]$ denotes the main channel CSI over the first and second cycles, and, $\mathbf{G} = \left[G^{(1)}, \ldots, G^{(M)}\right]$ the CSI in the link between Eve and Alice over the second cycle. All fading coefficients are modeled to be independent and identically distributed (i.i.d.) complex zero mean Gaussian random variables, i.e., $\mathbf{H} \sim \mathcal{CN}(0, \mathbf{\Sigma}_H)$, $\mathbf{G} \sim \mathcal{CN}(0, \mathbf{\Sigma}_G)$ with $\mathbf{\Sigma}_H = \text{diag}\left(\sigma_H^{2\,(1)}, \ldots, \sigma_H^{2\,(M)}\right)$ and $\mathbf{\Sigma}_G = \text{diag}\left(\sigma_G^{2\,(1)}, \ldots, \sigma_G^{2\,(M)}\right)$. The case of $M = 1$ corresponds to single channel SKG systems.

During the first cycle, Alice broadcast probe signals $\mathbf{X} = \left[X^{(1)}, \ldots, X^{(M)}\right]$ with power $\mathbf{p} = \left[p^{(1)}, \ldots, p^{(M)}\right]$ over the corresponding subchannels subject to (s.t.) a short term power constrain $\sum_{i=1}^{M} p^{(i)} \leq MP$. During this cycle Eve observes the channel and obtains an estimate $\hat{\mathbf{H}}$ of the main channel CSI that satisfies [10], [11]

$$\mathbf{H} = \sqrt{1-\alpha^2}\hat{\mathbf{H}} + \alpha\tilde{\mathbf{H}}, \tag{1}$$

where $\tilde{\mathbf{H}} \sim \mathcal{CN}(0, \mathbf{\Sigma}_H)$ denotes the estimation error and $\alpha \in [0, 1]$. For $\alpha = 0$ Eve has a perfect estimate of the main channel CSI while for $\alpha = 1$ Eve has no main channel CSI. During the second cycle Bob broadcasts $\mathbf{X}$ and Eve injects in the channel a jamming signal $\mathbf{J} = \left[J^{(1)}, \ldots, J^{(M)}\right]$ with power $\gamma = \left[\gamma^{(1)}, \ldots, \gamma^{(M)}\right]$ over the corresponding subchannels s.t. a short term power constraint $\sum_{i=1}^{M} \gamma^{(i)} \leq M\Gamma$.

Based on the above, Alice's and Bob's observations on the i-th subchannel, denoted by $Z_1^{(i)}$ and $Z_2^{(i)}$, respectively, can be expressed as

$$Z_1^{(i)} = H_0^{(i)} X^{(i)} + W_1^{(i)}, \tag{2}$$

$$Z_2^{(i)} = H_0^{(i)} X^{(i)} + G^{(i)} J^{(i)} + W_2^{(i)}, \tag{3}$$

with $\left(W_1^{(i)}, W_2^{(i)}\right) \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_2)$ denoting i.i.d. circularly symmetric complex Gaussian random variables modeling the effect of white noise on the system and $\mathbf{I}_n$ the identity matrix of dimension n. For the establishment of the secret key Alice needs to transmit reconciliation data to Bob at a minimum rate $h(\mathbf{Z}_2|\mathbf{Z}_1)$ [1], [2], [3]. On the other hand, denoting by $\mathbf{Z}_e$ the observation at Eve, the maximum achievable rate for the establishment of the secret key is upper bounded by $C \leq \min\left(I\left(\mathbf{Z}_1, \mathbf{Z}_2\right), I\left(\mathbf{Z}_1, \mathbf{Z}_2|\mathbf{Z}_e\right)\right)$ [1], [2], [3], [4]. Using this model, in [7] the metric employed to evaluate the impact of a jammer on the SKG process was defined by

$$R = \frac{h(\mathbf{Z}_2|\mathbf{Z}_1)}{C}. \tag{4}$$

In this study, for simplicity the derivation of optimal jamming schemes and of the power allocation policies for the jammer employs as objective function the raw rate of reconciliation data $h(\mathbf{Z}_2|\mathbf{Z}_1)$. However, for compatibility with [7] the comparison of different policies through numerical evaluations is performed using as metric R.

III. Optimal Probe and Jamming Signals for Single Channel SKG Systems

For simplicity in the proofs and without loss of generality in the case of multiple parallel subchannels, in this Section we focus on single channel SKG, i.e., we assume that $M = 1$ in the system model. Furthermore, for ease of notation the subscript corresponding to the subchannel index is omitted in the following.

In many studies, e.g., [4], [7] constant probe signals were assumed to be exchanged between the legitimate parties during the SKG procedure; on the other hand in [3] raised cosine pulses where chosen as probe signals. Furthermore, in [7] active adversaries were assumed to inject constant jamming signals over the wireless channel, without any formal proof of their optimality. In this Section we begin by lifting any related ambiguities and formalize the legitimate users' optimal signalling that maximizes the mutual information between their respective observations in the following proposition.

Proposition 1: In absence of active adversaries, i.e., for $J = 0$, the optimal probe signal maximizing $I(Z_1; Z_2)$ is a constant signal satisfying the power constraint with equality, i.e. $X = \sqrt{P}$.

Proof: For $J = 0$ the system model in (2), (3) corresponds to the two-look channel [12, pp. 290] with input variable HX and a power constraint $p \leq P$. As a result, the input distribution that maximizes $I\left(Z_1; Z_2\right)$ is Gaussian [12] while the convexity of the mutual information dictates transmitting with maximum power. Since $H \sim \mathcal{CN}\left(0, \sigma_H^2\right)$, the optimal X reduces to a scalar with $X = \sqrt{P}$. ■

Subsequently, we derive optimal jamming strategies when imperfect main channel CSI might be available at the active adversary. In this investigation we account for the worst case scenario in which a jammer can be closely located to a legitimate user or employ ray tracing techniques to obtain an imperfect estimate of the main channel CSI. The metric to be maximized by the jammer is the minimum rate of reconciliation data that should be exchanged between Alice and Bob, given by $h(Z_2|Z_1)$ [1]–[3]. To this end we focus on two limiting cases: in Subsection III-A the case $\alpha = 0$ corresponding to full CSI availability at Eve and in Subsection III-C $\alpha = 1$ corresponding to the case in which Eve has no CSI

in her disposal. Although when $\alpha = 0$ it is apparent that the SKG capacity is $C = 0$, this limiting scenario will enable us gain valuable intuition regarding the optimal jamming strategy in the realistic scenario with imperfect CSI $\alpha \in (0, 1)$ in Subsection III-B.

A. Full Main Channel CSI at Eve: Correlated Jamming

In the following, we assume that the legitimate users employ constant signalling $X = \sqrt{P}$ as dictated by Proposition 1. In the case of perfect CSI availability at the jammer, it has been shown that correlated jamming is optimal in point-to-point as well as multi-user and multiple input multiple output systems [13], [14]. We will demonstrate that the same is true in the case of SKG systems when $\alpha = 0$. When the jammer has a perfect estimate of the main channel CSI H the SKG capacity is $C = 0$ and it can be argued that jamming is not necessary; however, the following analysis will serve as the basis in deriving the jamming strategy in the realistic scenario $\alpha > 0$.

In this context, following the methodology introduced in [7] we assume that Eve's objective is the disruption of the SKG process (instead of eavesdropping), by increasing the cost of the reconciliation phase, i.e., by maximizing $h(Z_2|Z_1)$. Employing this criterion the following proposition formalizes the jammer's optimal jamming strategy.

Proposition 2: When full CSI is available at the jammer, the optimal jamming signal J that maximizes the minimum required rate of reconciliation data $h(Z_2|Z_1)$ is linear to H.

Proof: The jammer wishes to maximize

$$h(Z_2|Z_1) = h(Z_1, Z_2|H) + h(H) - h(Z_1). \tag{5}$$

The maximization is achieved by maximizing the term $h(Z_1, Z_2|H)$ that is controlled by the jammer; $h(H)$ and $h(Z_1)$ are independent of the jammer's actions. We show that a linear jamming signal achieves this goal.

We have that

$$\begin{aligned} & h(Z_1, Z_2|H) \\ & = h(Z_1, Z_2 - \lambda H|H) \\ & \leq h(Z_1, Z_2 - \lambda H) \qquad (6) \\ & \leq \log\left((2\pi e)^2|\Lambda|\right), \qquad (7) \end{aligned}$$

where (6) holds because conditioning reduces entropy and Λ is the covariance matrix of $(Z_1, Z_2 - \lambda H)$. Regarding (7), we note that for a given autocorrelation matrix the entropy is maximized by a Gaussian distribution [12]. (6) and (7) hold for arbitrary λ; here we choose $\lambda = \frac{\mathbb{E}[Z_2 H^*]}{\sigma_H^2}$.

Now let's assume that the jammer employs linear jamming so that the jamming signal can be expressed as

$$J = \frac{\kappa}{G} H + \sqrt{v}, \tag{8}$$

where $\kappa \in \mathbb{R}$ and $v \in \mathbb{R}^+$. We assume that the following power constraint is met: $\kappa^2/\sigma_G^2\sigma_H^2 + v \leq \Gamma$. Taking into account Proposition 1 and substituting (8) into (2)-(3), the observations at Alice and Bob can then be rewritten as

$$\begin{aligned} Z_1 &= \sqrt{P}H + W_1, \qquad (9) \\ Z_2 &= \left(\sqrt{P} + \kappa\right) H + \sqrt{v}G + W_2. \qquad (10) \end{aligned}$$

Next, suppose that optimal $\tilde{J}$ is found so that $h(Z_1, Z_2|H)$ is maximized, or, equivalently, (7) is satisfied with equality. We define R such that

$$R = \tilde{J} - \frac{\mathbb{E}\left[\tilde{J}H^*\right]}{\sigma_H^2} H, \tag{11}$$

so that R is uncorrelated with H. Exploiting this fact, the power of the optimal jamming signal is found to be

$$\mathbb{E}\left[|\tilde{J}|^2\right] = \frac{\mathbb{E}\left[\left|\tilde{J}H^*\right|^2\right]}{\sigma_H^2} + \mathbb{E}\left[|R|^2\right],$$

and must satisfy the power constraint so that the optimal jamming signal is feasible.

We observe that setting

$$\begin{aligned} \kappa &= \frac{\mathbb{E}\left[\tilde{J}GH^*\right]}{\sigma_H^2}, \qquad (12) \\ v &= \mathbb{E}\left[|R|^2\right], \qquad (13) \end{aligned}$$

results in J having the same power as $\tilde{J}$. Furthermore, the autocorrelation matrix Λ is the same for both J and $\tilde{J}$. Since uncorrelated Gaussian signals are also independent, $\tilde{J}$ achieves (6) and (7) with equality, and therefore so does J. In conclusion, J has power equal to that of the optimal jamming signal and satisfies the same constraints as the optimal jamming signal; as a result, J is optimal. ■

Remark: If $P/\sigma_G^2\sigma_H^2 \leq \Gamma$, the optimal jamming signal can designed so that $\kappa = -\sqrt{P}$, i.e., Bob's transmission during the second cycle can be completely canceled off. On the other hand whenever $P/\sigma_G^2\sigma_H^2 > \Gamma$, the optimal strategy would be to cancel off as much as possible Bob's transmission.

B. Imperfect Main Channel CSI at Eve: Linear Jamming

Now let us assume that Eve has imperfect main channel CSI s.t. $H = \sqrt{1-\alpha^2}\hat{H} + \alpha\tilde{H}$ for some $\alpha \in (0, 1)$ and perfect channel CSI for the link Eve-Alice. Based on the analysis in III-A Eve can simply inject linear jamming in the form

$$J = \frac{\kappa}{G}\sqrt{1-\alpha^2}\hat{H}, \tag{14}$$

so that Bob's observation can be expressed as:

$$Z_2 = (\sqrt{P} + \kappa)H + \tilde{W}_2, \tag{15}$$

with $\tilde{W}_2 = W_2 - \alpha\kappa\tilde{H}$. Similarly to the case of perfect main channel CSI, $h(Z_2|Z_1)$ is maximized for $\kappa = -\sqrt{P}$ if the jammer has sufficient power resources, $P\sqrt{1-\alpha^2}\frac{\sigma_H^2}{\sigma_G^2} \leq \Gamma$.

Corollary 1: When imperfect main channel CSI $\hat{H}$ is at Eve's disposal, the jamming signal that maximizes the rate of reconciliation data $h(Z_2|Z_1)$ is linear to $\hat{H}$.

C. Absence of Main Channel CSI at Eve: Uncorrelated Jamming

Next, the optimal jamming is characterized in absence of main channel CSI, i.e., $\alpha = 1$ in the following proposition.

Proposition 3: For $\alpha = 1$ when no main channel CSI is available at the jammer the optimal jamming signal J is the constant signal $J = \sqrt{\Gamma}$.

Proof: The case of absence of main channel CSI can be treated as a subcase of the full CSI availability case examined in III-A. Based on this observation, as shown in the proof of Proposition 2, the optimal jamming signal can be expressed as $J = \frac{\mathbb{E}[JGH^*]}{\sigma_H^2 G} H + \sqrt{v}$. In absence of knowledge of H, the term JG is *necessarily* uncorrelated with H so that $J = \frac{\mathbb{E}[JG]\mathbb{E}[H^*]}{\sigma_H^2 G} H + \sqrt{v} = \sqrt{v}$. Finally, due to the convexity of the entropy, maximization is achieved when the power constraint is satisfied with equality, i.e., $J = \sqrt{v} = \sqrt{\Gamma}$. ■

IV. Power Allocation Policies over M Parallel Subchannels

In this Section we investigate the power allocation policies, first for the legitimate users and then for the jammer when M parallel subchannels are used in the SKG process. The metric to be optimized by the legitimate users is naturally their mutual information over the M parallel subchannels. On the other hand, assuming that the adversary's goal is the interruption of the SKG process, the metric to be maximized is the rate of the reconciliation data that need to exchanged between the legitimate parties to establish a common secret key $h(\mathbf{Z}_2|\mathbf{Z}_1)$.

For the pair of legitimate users it is straightforward to demonstrate that equidistribution of the power resources is the optimal strategy, denoted henceforth as the "blind" policy. On the other hand, for the jammer the optimal policy depends on α, i.e., on the accuracy of the main channel CSI estimates.

A. Optimal Power Allocation for the Legitimate Users

During the SKG process the legitimate users do not possess any knowledge regarding the fading coefficients they attempt to estimate to establish the secret key. Alice's and Bob's optimal power allocation strategies can be determined by the following optimization problem

$$\arg\max_{\mathbf{p}} \min\left(I\left(\mathbf{Z}_1, \mathbf{Z}_2\right), I\left(\mathbf{Z}_1, \mathbf{Z}_2|\mathbf{Z}_e\right)\right), \tag{16}$$

$$\text{s.t. } \sum_{i=1}^{M} p^{(i)} \leq MP, \tag{17}$$

Irrespective of the type of jamming injected by Eve (correlated or uncorrelated), the objective function is monotone increasing in $\mathbf{p}$ so that in both cases the optimal power allocation policy – denoted by $\mathbf{p}^*$ – is the equidistribution of the power resources, i.e.,

$$\mathbf{p}^* = [P]_{i=1}^{M}. \tag{18}$$

This is a general result for the maximization of monotonically increasing cost functions in blind scenarios. For details on a proof using dynamic programming see Appendix A.

B. Optimal Power Allocation for a Jammer Employing Correlated Jamming

We begin with the case in which Eve has full CSI, i.e., knowledge of $\mathbf{H}, \mathbf{G}$ and of the power allocation policy $\mathbf{p}^*$ (18). We denote the jammer's optimal power allocation $\gamma^* = [\gamma^{(1)*}, \ldots, \gamma^{(M)*}]$ where $\gamma^{(i)*} = \left(\kappa^{(i)*}\right)^2 \frac{\sigma_H^{2\,(i)}}{\sigma_G^{2\,(i)}} + v^{(i)*}$. γ^* is evaluated as the solution of the optimization problem

$$\arg\min_{\gamma} h(\mathbf{Z}_2|\mathbf{Z}_1) = h(\mathbf{Z}_1, \mathbf{Z}_2) - h(\mathbf{Z}_1), \tag{19}$$

$$\text{s.t. } \sum_{i=1}^{M} \gamma^{(i)} \leq M\Gamma. \tag{20}$$

The cost function in (19) is nonnegative and the maximum is achieved when $\mathbf{Z}_2$ is uncorrelated with $\mathbf{Z}_1$, i.e, from the point of view of disruption of the SKG process the worse case is when Eve has enough power to cancel off Bob's transmission. This is feasible only if

$$\Gamma_{min} = \frac{1}{M} \sum_{i=1}^{M} P \frac{\sigma_H^{2\,(i)}}{\sigma_G^{2\,(i)}} \leq \Gamma. \tag{21}$$

If condition (21) is true, then $\kappa^{(i)} = \kappa = -\sqrt{P}$ and $h(\mathbf{Z}_2|\mathbf{Z}_1) = h(\mathbf{Z}_2) = M\log(2\pi e) + \sum_{i=1}^{M} \log\left(1 + v^{(i)} \sigma_G^{2\,(i)}\right)$. The objective function can be further maximized by using the waterfilling algorithm for $\mathbf{v} = [v^{(1)}, \ldots, v^{(M)}]$ over the remaining power $M\Gamma - M\Gamma_{min}$:

$$\text{iff } \sum_{i=1}^{M} P \frac{\sigma_H^{2(i)}}{\sigma_G^{2(i)}} \leq M\Gamma \text{ then } \begin{cases} \kappa^{(i)} = \kappa = -\sqrt{P}, \\ v^{(i)} = \left(\lambda - \frac{1}{\sigma_G^{2\,(i)}}\right)^+, \end{cases} \tag{22}$$

where $(\cdot)^+ = \max(\cdot, 0)$ and λ is the waterlevel chosen to satisfy the constraint $\sum_{i=1}^{M} v^{(i)} \leq M\Gamma - M\Gamma_{min}$ with equality.

If the condition (21) is not satisfied, a heuristic power allocation policy that minimizes the correlation between $\mathbf{Z}_2$ and $\mathbf{Z}_1$ is obtained by

$$\arg\min_{\kappa} \sum_{i=1}^{M} \sqrt{P}\left(\sqrt{P} + \kappa^{(i)}\right) \sigma_H^{2\,(i)} \tag{23}$$

$$\text{s.t. } \sum_{i=1}^{M} (\kappa^{(i)})^2 \frac{\sigma_H^{2\,(i)}}{\sigma_G^{2\,(i)}} \leq M\Gamma, \tag{24}$$

while setting $v^{(i)} = 0, \forall i$. The solution to (23) is given by

$$\kappa^{(i)} = \frac{-\sqrt{P}\sigma_G^{2\,(i)}}{2\mu}, \tag{25}$$

where $\mu > 0$ is chosen such that the power constraint (24) is satisfied with equality, i.e.,

$$\mu = \sqrt{\frac{P}{4M\Gamma} \sum_{i=1}^{M} \frac{\sigma_H^{2\,(i)}}{\sigma_G^{2\,(i)}}}. \tag{26}$$

C. Power Allocation for a Jammer with Imperfect CSI

Extending the previous analysis to the case of $\alpha \in (0,1)$, it is straightforward to see that the optimal jamming signal would cancel off Bob's signal if the jammer's power budget is sufficient, i.e., if

$$\sum_{i=1}^{M} P\sqrt{1-\alpha^2}\frac{\sigma_H^{2(i)}}{\sigma_G^{2(i)}} \leq M\Gamma \tag{27}$$

then $J^{(i)} = \frac{\kappa^{(i)}}{G}\sqrt{1-\alpha^2}\hat{H}^{(i)}$ and $\kappa^{(i)} = \kappa - \sqrt{P}$. If condition (27) is not met, then the power allocation policy $\kappa^{(i)} = \frac{-\sqrt{P}\sigma_G^{2\,(i)}}{2\xi}$ could be adopted where ξ satisfies the power constraint with equality and is given by

$$\xi = \sqrt{\frac{P\sqrt{1-\alpha^2}}{4M\Gamma}\sum_{i=1}^{M}\frac{\sigma_H^{2\,(i)}}{\sigma_G^{2\,(i)}}}. \tag{28}$$

D. Optimal Power Allocation for a Jammer Employing Uncorrelated Jamming

Next, we turn our attention to the scenario of uncorrelated jamming assuming that Eve has knowledge of $\mathbf{G}$ but no information regarding $\mathbf{H}$. Employing uncorrelated jamming as dictated by Proposition 3, Eve's optimal power allocation can be evaluated by maximizing

$$h(\mathbf{Z}_1,\mathbf{Z}_2) - h(\mathbf{Z}_1) = M\log(2\pi e) + \sum_{i=1}^{M}\log\left(1+v^{(i)}\sigma_G^{2\,(i)}\right)$$

i.e., as the solution of the standard waterfilling optimization problem

$$\arg\min_{\mathbf{v}} \sum_{i=1}^{M}\log\left(1+v^{(i)}\sigma_G^{2\,(i)}\right), \tag{29}$$

$$\text{s.t.} \sum_{i=1}^{M} v^{(i)} \leq M\Gamma, \tag{30}$$

with the well know solution $v^{(i)} = \left(\chi - \frac{1}{\sigma_G^{2\,(i)}}\right)^+$ where χ satisfies (30) with equality.

Finally, when neither $\mathbf{H}$ nor $\mathbf{G}$ are available at Eve, the monotonicity of the objective function suggests that the optimal power allocation policy is equidistribution of the power, i.e., "blind" power allocation.

V. Numerical Results

In the following we define the normalized rate of reconciliation data to the upper bound of the SKG capacity as follows for the various cases:

$$R = \frac{h(\mathbf{Z}_2|\mathbf{Z}_1)}{\min\left(I\left(\mathbf{Z}_1,\mathbf{Z}_2\right), I\left(\mathbf{Z}_1,\mathbf{Z}_2|\mathbf{Z}_e\right)\right)} \tag{31}$$

where

$$\mathbf{Z}_e = \hat{\mathbf{H}} \text{ linear jamming,} \tag{32}$$

$$\mathbf{Z}_e = \mathbf{0} \text{ uncorrelated and blind jamming.} \tag{33}$$

The case of correlated jamming is not examined because in this case $\min\left(I\left(\mathbf{Z}_1,\mathbf{Z}_2\right), I\left(\mathbf{Z}_1,\mathbf{Z}_2|\mathbf{Z}_e\right)\right) = 0$. In Fig. 2 R is depicted as a function of the jamming power Γ for $P = 10$, $M = 100$, $\alpha = 0.2$, averaged over 10^4 repetitions. As expected, it is demonstrated that the impact of linear jamming is severely more acute than that of uncorrelated jamming. Interestingly, using uncorrelated jamming (i.e., employing the waterfilling algorithm for the jamming power) versus blind jamming (i.e., equidistribution of the jamming power across all subchannels) bears negligible gains. As a result, a jammer that cannot obtain an estimate of the main channel CSI need not spend resources in estimating the CSI between itself and the legitimate nodes in order to inject uncorrelated jamming.

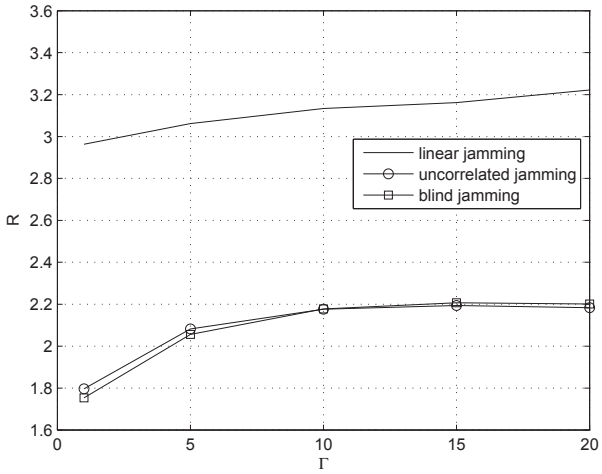

Fig. 2. R vs Γ for $P = 10, M = 100, \alpha = 0.2$.

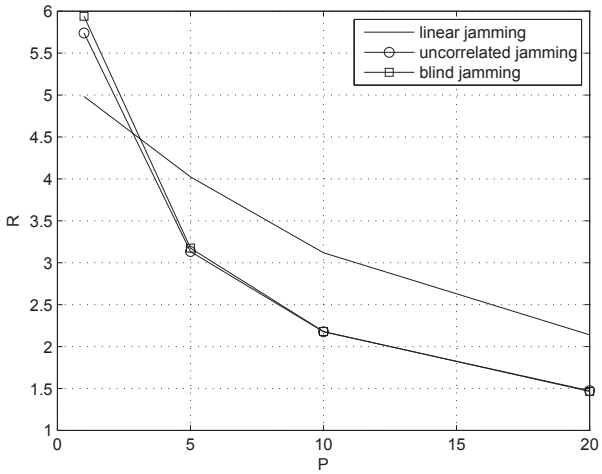

Fig. 3. R vs P for $\Gamma = 10, M = 100, \alpha = 0.2$

Similar conclusions can be reached by examining the numerical evaluations of R versus P in Fig. 3 for $\Gamma = 10$, $P = 100$ and $\alpha = 0.2$. A further point that can be made is that when the jamming power is substantially bigger than the power available at the legitimate nodes, the jammer can benefit from using a simple power allocation policy such as

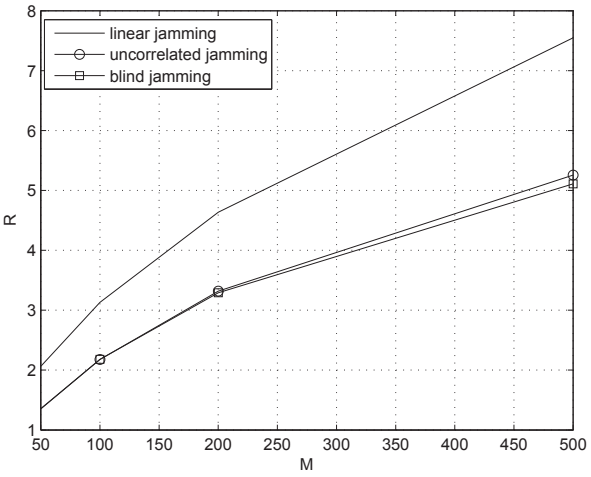

Fig. 4. R vs M for $P = 10, \Gamma = 10, \alpha = 0.2$

blind jamming.

Finally, in Fig. 4 R is depicted as a function of M for $P = \Gamma = 10$ and $\alpha = 0.2$. The cost of reconciliation increases monotonically with M, demonstrating that the impact of jamming grows faster than the rate of the secret key establishment.

VI. Conclusions

In this study optimal signalling and jamming schemes were derived for SKG systems. Furthermore, optimal and heuristic power allocation policies were investigated in M BF-AWGN channels. It was shown that when the jammer has imperfect main channel CSI at his disposal the injection of linear jamming can severely impact SKG systems. When no main channel CSI is available at the jammer, it was shown that equidistibution of the jamming power is nearly optimal.

Appendix A
Legitimate Users Optimal Power Allocation

Proof: Following the proof in [15], the stochastic optimization objective function can be written as follows:

$$\max_{\mathbf{p}} f(\mathbf{p}) \text{ s.t. } \sum_{i=1}^{M} p^{(i)} \leq MP, \tag{34}$$

where we define $f(\mathbf{p}) \equiv \min\left(I\left(\mathbf{Z}_1, \mathbf{Z}_2\right), I\left(\mathbf{Z}_1, \mathbf{Z}_2 | \mathbf{Z}_e\right)\right)$.

We introduce the auxiliary variables $p_i, i = 1, \ldots, M$ to denote the remaining power at step i of the dynamic program (DP). Then, the problem in (34) can be written as a stochastic DP as follows: We let $V_i(p_i)$ be the SKG capacity gained from block i to the end of the horizon if the optimal power allocation policy is used. Then the DP equations can be written as:

$$\begin{aligned} V_i(p_i) &= \max_{0 \leq p^{(i)} \leq p_i} f(p^{(i)}) + V_{i+1}(p_i - p^{(i)}), i \leq M-1 \\ V_M(p_M) &= 0. \end{aligned}$$

We perform backward DP starting the recursion at block $i = M$, where the optimality equations are:

$$V_M(p_M) = \max_{0 \leq p^{(M)} \leq p_M} f(p^{(M)}). \tag{35}$$

Since f is nondecreasing, the maximization in (35) is achieved at $p^{(M)} = p_M$. Thus, we have: $p^{(M)} = p_M$ and $V_M(p_M) = f(p_M)$. Thus, at block $i = M-1$ the optimality equations are:

$$\begin{aligned} V_{M-1}(p_{M-1}) = &\max_{0 \leq p^{(M-1)} \leq p_{M-1}} f(p^{(M-1)}) \\ &+ f(p_{M-1} - p^{(M-1)}). \end{aligned} \tag{36}$$

In (36) the maximum is achieved at $p^{(M-1)} = \frac{p_{M-1}}{2}$ and therefore $V_{M-1}(p_{M-1}) = 2f(\frac{p_{M-1}}{2})$. Continuing the recursion we get

$$V_{M-n}(p_{M-n}) = (n+1) f\Big(\frac{p_{M-n}}{n+1}\Big) \tag{37}$$

and the optimal decision is $p^{(M-n)} = \frac{p_{M-n}}{n+1}$. This implies that if we have no information about the channel the optimal thing to do is to divide the power into as many equal parts as there are periods remaining, i.e., $p^{(i)} = P, \forall i$. ■

References

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[2] 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.

[3] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–154, Jun. 2010.

[5] T.-H. Chou, S. Draper, and A. M. Sayeed, "Key generation using external source excitation: Capacity, reliability and secrecy exponent," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2455–2474, Apr. 2012.

[6] L. Lai, Y. Liang, and H. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[7] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, Oct. 2012.

[8] C. Chen and M. 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.

[9] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. Electronic Ed.: McGraw Hill, Inc., 2002.

[10] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[11] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, Jun. 2014.

[12] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ: John Wiley and Sons, Inc., 2006.

[13] M. Médard, "Capacity of correlated jamming channels," in *Proc. 35th Annu. Allerton Conf. Commun., Control Comp.*, Monticello, IL, Sep.-Oct. 1997.

[14] S. Shafiee and S. Ulukus, "Mutual information games in multiuser channels with correlated jamming," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4598–4607, Oct. 2009.

[15] A. Chorti, K. Papadaki, and H. Poor, "Optimal power allocation in block fading channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 4708–4719, Sep. 2015.