

Joint Power and Secret Key Buffer Management to Achieve Delay Limited Secrecy

Onur Gungor, Jian Tan, Can Emre Koksall, Hesham El-Gamal, Ness Shroff

Technical Report, Department of Electrical and Computer Engineering
Ohio State University, Columbus, 43210

I. THEOREM 1 PROOF

The problem is defined as ¹

$$\begin{aligned} R(b, \bar{P}, \alpha_1) &= \max_{P(\mathbf{h})} \mathbb{E}[R_s] \\ \text{subject to: } P(\mathbf{h}) &\geq 0, \\ \mathbb{E}[P(\mathbf{h})] &\leq \bar{P}, \\ \mathbb{P}[R_m^h < b] &\leq \alpha_1, \end{aligned} \quad (1)$$

In the proof of the optimal power control, we assume that b is fixed. ² Since the channel gain vector \mathbf{h} is a well defined random variable, and $P(\mathbf{h})$ is a function of channel gains only, then if we fix the power policy $P(\mathbf{h})$, we know for sure that, for some \mathbf{h} , the main channel rate constraint is satisfied, that is, $R_m^h \geq b$. We define the service set of a power policy $P(\mathbf{h})$ as follows.

$$\mathcal{H}_s(P(\mathbf{h})) : \{\mathbf{h} : R_m^h \geq b\}$$

Also, when the main channel rate constraint is not satisfied, channel outage is declared. Note that, the problem (1) is equivalent to

$$\begin{aligned} \max_{P(\mathbf{h})} \mathbb{E}[R_s] \\ \text{subject to: } P(\mathbf{h}) &\geq 0, \\ \mathbb{E}[P(\mathbf{h})] &\leq \bar{P}, \\ \mathbb{P}[\mathbf{h} \in \mathcal{H}_s] &\geq 1 - \alpha_1, \end{aligned} \quad (2)$$

To solve the problem, we use the lagrangian,

$$R(b, \bar{P}, \alpha_1) = \max_{P(\mathbf{h})} \min_{\lambda, \lambda_2} J(P(\mathbf{h})) \quad (3)$$

where the lagrangian $J(P(\mathbf{h}))$ is

$$\begin{aligned} J(P(\mathbf{h})) &= \int R_s^h f(\mathbf{h}) d\mathbf{h} \\ &\quad - \lambda \left[\int P(\mathbf{h}) f(\mathbf{h}) d\mathbf{h} - \bar{P} \right] \\ &\quad - \lambda_2 \left[\int_{\mathbf{h} \notin \mathcal{H}_s} f(\mathbf{h}) d\mathbf{h} - \alpha_1 \right] \end{aligned} \quad (4)$$

¹(1) is similar to the problem (2) considered in [2], where a point-to-point fading link is considered, and average channel rate is to be maximized the same constraints, but the two problems differ by the objective. In our setting, average *secrecy* rate is maximized, and the power allocation is a function of channel vector, instead of a single channel.

²Note that, in the actual problem of finding $R(b, \bar{P}, \alpha_1)$, the optimal b is found by an iterative algorithm.

where $f(\mathbf{h})$ is the probability density function of channel gains, which we assume is well defined. Note that, the third term in (4) makes the problem challenging, as the integral is over the region ($\mathbf{h} \notin \mathcal{H}_s$), which is a function of the power control policy, hence if we take derivative of $J(P(\mathbf{h}))$ with respect to $P(\mathbf{h})$, discontinuity will arise. To simplify the problem, we use the fact that $\mathcal{H}_s(P)$ is a function of $P(\mathbf{h})$, and

$$\begin{aligned} \arg \max_{P(\mathbf{h})} J(P(\mathbf{h})) &= \arg \max_{P(\mathbf{h})} J'(P(\mathbf{h})) \\ \text{s.t. } \mathbb{P}(\mathbf{h} \in \mathcal{H}_s) &\geq 1 - \alpha_1 \end{aligned} \quad (5)$$

where

$$\begin{aligned} J'(P(\mathbf{h})) &= \int R_s^h f(\mathbf{h}) d\mathbf{h} \\ &\quad - \lambda \left[\int P(\mathbf{h}) f(\mathbf{h}) d\mathbf{h} - \bar{P} \right] \end{aligned} \quad (6)$$

It can be shown that, for fixed α_1 , there is a one to one correspondence between λ and \bar{P} , hence we assume that λ is constant in the next parts.

Lemma 1: For fixed λ , define

$$\begin{aligned} P_1(\mathbf{h}) &= \arg \max_{P(\mathbf{h})} J'(P(\mathbf{h})) \\ \text{s.t } \mathbb{P}(R_m^h \geq b) &\geq 1 - \alpha_1 \end{aligned}$$

and

$$\begin{aligned} P_2(\mathbf{h}) &= \arg \max_{P(\mathbf{h}), \mathcal{G}} J'(P(\mathbf{h})) \\ \text{s.t } R_m^h &\geq b, \quad \forall \mathbf{h} \in \mathcal{G} \\ \mathbb{P}(\mathbf{h} \in \mathcal{G}) &= 1 - \alpha_1 \end{aligned} \quad (7)$$

where \mathcal{G} is a region of channel gains. Then, $P_1 = P_2$, that is, for any \mathbf{h} , $P_1(\mathbf{h}) = P_2(\mathbf{h})$.

Note that, $\mathcal{G} \subseteq \mathcal{H}_s(P_2)$, since there is no converse statement about $\mathbf{h} \notin \mathcal{G}$, as for some $\mathbf{h} \notin \mathcal{G}$, $R_m^h \geq b$ might hold.

Proof: The constraint set of both problems are identical. If $\mathbb{P}(R_m^h \geq b) \geq 1 - \alpha_1$, then there exists a region \mathcal{G} such that $R_m^h \geq b$, for all $\mathbf{h} \in \mathcal{G}$ and $\mathbb{P}(\mathbf{h} \in \mathcal{G}) = 1 - \alpha_1$. Also, if $R_m^h \geq b$ for all $\mathbf{h} \in \mathcal{G}$ where $\mathbb{P}(\mathbf{h} \in \mathcal{G}) = 1 - \alpha_1$, then $\mathbb{P}(R_m^h \geq b) \geq 1 - \alpha_1$. ■

The procedure could be summarized in a two-step approach, as follows.

1) For any arbitrary \mathcal{G} , find

$$\begin{aligned} P_{\mathcal{G}}(\mathbf{h}) &= \arg \max_{P(\mathbf{h})} J'(P(\mathbf{h})) \\ \text{s.t } R_m^h &\geq b, \forall \mathbf{h} \in \mathcal{G} \end{aligned} \quad (8)$$

Note that, in this case, there is no constraint on \mathcal{G} , as in (7).

- 2) Using the result of step 1, we find $P_2(\mathbf{h})$, which is the optimal solution since $P_1 = P_2$, and P_1 is the solution to (1).

We start with step 1.

Lemma 2: Let $\beta = 2^{b+1}/h_m$ and

$$\Gamma(\mathbf{h}) = \frac{1}{h_m} + \frac{\beta^2}{4/\lambda - 2\beta}, \quad (9)$$

then, for $\bar{P} \geq P_{\min}$, $P_{\mathcal{G}}(\mathbf{h})$ is unique for each arbitrary \mathcal{G} , and is equal to

- If $\{\{h_m < \lambda 2^b\} \cup \{1/h_e < \Gamma(\mathbf{h})\}\}$, then,

$$P_{\mathcal{G}}(\mathbf{h}) = P_{inv}(\mathbf{h}) = \frac{2^b - 1}{h_m} \quad (10)$$

- Otherwise,

$$\begin{aligned} P_{\mathcal{G}}(\mathbf{h}) &= P_{wf}(\mathbf{h}) \\ &= \frac{1}{2} \left[\sqrt{\left(\frac{1}{h_e} - \frac{1}{h_m}\right)^2 + \frac{4}{\lambda} \left(\frac{1}{h_e} - \frac{1}{h_m}\right)} \right. \\ &\quad \left. - \left(\frac{1}{h_e} + \frac{1}{h_m}\right) \right]^+, \end{aligned} \quad (11)$$

where λ is determined according to the average power constraint, by solving the equation $\mathbb{E}[P(\mathbf{h})] = \bar{P}$. Note that, if all other parameters are fixed, then there is a one-to-one relation between λ and \bar{P} , and it can be easily shown that $\lambda \rightarrow 0$ as $\bar{P} \rightarrow \infty$.

We define $P_{inv}(\mathbf{h})$ and $P_{wf}(\mathbf{h})$ to be the power allocations used in (10) and (11), as we use those allocations in the preceding parts. $P_{inv}(\mathbf{h})$ is actually called channel inversion power allocation, whereas $P_{wf}(\mathbf{h})$ is called the waterfilling-like power allocation.

Note that, we can combine (10),(11) in a more compact form, as

$$P_{\mathcal{G}}(\mathbf{h}) = P_{wf}(\mathbf{h}) + [P_{inv}(\mathbf{h}) - P_{wf}(\mathbf{h})]^+ \mathbf{1}(\mathbf{h} \in \mathcal{G}) \quad (12)$$

Proof: This is a standard variational optimization problem, and the proof is very similar to the proof in [2]. Firstly, note that, if $\mathbf{h} \in \mathcal{G}$, then the minimum main channel rate has to be b , as

$$R_m^h = \log(1 + P(\mathbf{h})h_m) \geq b, \forall \mathbf{h} \in \mathcal{G}$$

Hence, there is a minimum power constraint,

$$P(\mathbf{h}) \geq \frac{2^b - 1}{h_m}, \forall \mathbf{h} \in \mathcal{G} \quad (13)$$

P_{min} is the minimum average power required to satisfy the minimum main channel rate constraint. P_{min} is found as

$$P_{min} = \int_{\mathcal{G}} \frac{2^b - 1}{h_m} f(\mathbf{h}) d\mathbf{h}$$

Therefore, for any $\bar{P} < P_{min}$, problem (8) does not have a solution. Define non-boundary points $\mathbf{h} \in \bar{\mathcal{G}}_c$ as the set in

which the minimum power constraint (13) is not active, such as

$$\bar{\mathcal{G}}_c = \left\{ \mathbf{h} \in \mathcal{G} : P(\mathbf{h}) > \frac{2^b - 1}{h_m} \right\} \cup \{ \mathbf{h} \notin \mathcal{G} : P(\mathbf{h}) > 0 \}$$

Also, we define the boundary points $\mathbf{h} \in \mathcal{G}_c$, as

$$\mathcal{G}_c = \left\{ \mathbf{h} \in \mathcal{G} : P(\mathbf{h}) = \frac{2^b - 1}{h_m} \right\}$$

First, we focus on the solution in the nonboundary set. Since the optimal solution must satisfy the Euler-Lagrange equations,

$$\frac{dJ'(P(\mathbf{h}))}{dP(\mathbf{h})} = 0, \mathbf{h} \in \bar{\mathcal{G}}_c$$

So, we have for $\mathbf{h} \in \bar{\mathcal{G}}_c$, we get the following condition

$$\frac{h_m}{1 + h_m P(\mathbf{h})} - \frac{h_e}{1 + h_e P(\mathbf{h})} - \lambda = 0$$

whose solution yields

$$\begin{aligned} P(\mathbf{h}) &= \\ &= \frac{1}{2} \left[\sqrt{\left(\frac{1}{h_e} - \frac{1}{h_m}\right)^2 + \frac{4}{\lambda} \left(\frac{1}{h_e} - \frac{1}{h_m}\right)} - \left(\frac{1}{h_e} + \frac{1}{h_m}\right) \right]^+ \end{aligned}$$

Further, showing that the optimal solution satisfies the Karush Kuhn Tucker(K.K.T) equations in the boundary set, which is

$$\frac{dJ'(P(\mathbf{h}))}{dP(\mathbf{h})} \leq 0, \mathbf{h} \notin \bar{\mathcal{G}}_c$$

$$\frac{h_m}{1 + h_m P(\mathbf{h})} - \frac{h_e}{1 + h_e P(\mathbf{h})} - \lambda \leq 0 \quad (14)$$

Note that in boundary points, the main channel constraint is active. Hence, the power control policy in the boundary is, $P(\mathbf{h}) = \frac{2^b - 1}{h_m}$. Placing $P(\mathbf{h})$ in equation (14), the region in which channel inversion is used is found. For $h_e = 0$, we get

$$h_m \leq \lambda 2^b \quad (15)$$

Also, solving for nonzero h_e , we find the results (10),(11). ■

Now, we explain part 2. The problem is to find $P_2(\mathbf{h})$, given that parameter λ is fixed. To proceed, we need to further simplify the lagrangian (6), for the case where $P(\mathbf{h}) = P_{\mathcal{G}}(\mathbf{h})$, where $P_{\mathcal{G}}(\mathbf{h})$ is the solution to (8).

First, to clarify that the achievable secrecy rate R_s is a function of power, we introduce a new notation for achievable secrecy rate.

$$R_s(P(\mathbf{h})) = [\log(1 + P(\mathbf{h})h_m) - \log(1 + P(\mathbf{h})h_e)]^+$$

So, $R_s(P_{wf}(\mathbf{h}))$ corresponds to the achievable secrecy rate given that waterfilling-like power allocation in (11) is used.

Then, we simplify the lagrangian

$$\begin{aligned}
J'(P_{\mathcal{G}}(\mathbf{h})) &= \int_{\mathcal{G}} [R_s^h - \lambda P(\mathbf{h})] f(\mathbf{h}) d\mathbf{h} \\
&+ \int_{\bar{\mathcal{G}}} [R_s^h - \lambda P(\mathbf{h})] f(\mathbf{h}) d\mathbf{h} \\
&= \int [R_s(P_{wf}(\mathbf{h})) - \lambda P_{wf}(\mathbf{h})] f(\mathbf{h}) d\mathbf{h} \\
&+ \int_{\mathcal{G}} \left\{ [R_s(P_{inv}(\mathbf{h})) - R_s(P_{wf}(\mathbf{h}))]^+ \right. \\
&\quad \left. - \lambda [P_{inv}(\mathbf{h}) - P_{wf}(\mathbf{h})]^+ \right\} f(\mathbf{h}) d\mathbf{h} \quad (16)
\end{aligned}$$

Note that, after this simplification, the first term does not depend on \mathcal{G} .

Lemma 3: The solution to (7) is

$$P_2(\mathbf{h}) = P_{\mathcal{G}}(\mathbf{h})$$

where \mathcal{G} is

$$\mathcal{G} = \left\{ \mathbf{h} : [R_s(P_{inv}(\mathbf{h})) - R_s(P_{wf}(\mathbf{h}))]^+ - \lambda [P_{inv}(\mathbf{h}) - P_{wf}(\mathbf{h})]^+ \geq k \right\} \quad (17)$$

where k is a constant that is found by iteratively solving the problem until $\mathbb{P}(\mathbf{h} \in \mathcal{G}) = 1 - \alpha_1$. So, according to lemma 1, this is the optimal solution to problem (1).

Proof: Note that (7) is an extension of (8), where the arbitrary region \mathcal{G} is constrained such that $\mathbb{P}(\mathbf{h} \in \mathcal{G})$ is constant. Note that, for any constant \mathcal{G} , the solution to (8) is $P_{\mathcal{G}}(\mathbf{h})$, hence the power allocation function that maximizes (17) is $P_{\mathcal{G}}(\mathbf{h})$, where \mathcal{G} satisfies $\mathbb{P}(\mathbf{h} \in \mathcal{G}) = 1 - \alpha_1$.

Define $\xi(\mathbf{h}) = [R_s(P_{inv}(\mathbf{h})) - R_s(P_{wf}(\mathbf{h}))]^+ - \lambda [P_{inv}(\mathbf{h}) - P_{wf}(\mathbf{h})]^+$. Then,

$$\mathcal{G} = \arg \max_{\mathcal{G}} \int_{\mathcal{G}} \xi(\mathbf{h}) f(\mathbf{h}) d\mathbf{h}$$

Note that, this problem resembles the bin packing problem. Denote the optimal region in (17) as \mathcal{G}_1 . Then, assume that some other region \mathcal{G}_2 is optimal, where $\mathbb{P}(\mathbf{h} \in \mathcal{G}_1) = \mathbb{P}(\mathbf{h} \in \mathcal{G}_2) = \alpha_1$. Then,

$$\begin{aligned}
&J'(P_{\mathcal{G}_1}(\mathbf{h})) - J'(P_{\mathcal{G}_2}(\mathbf{h})) \\
&= \int_{\mathcal{G}_1} \xi(\mathbf{h}) f(\mathbf{h}) d\mathbf{h} - \int_{\mathcal{G}_2} \xi(\mathbf{h}) f(\mathbf{h}) d\mathbf{h} \\
&= \int_{\mathcal{G}_1 \setminus \mathcal{G}_2} \xi(\mathbf{h}) f(\mathbf{h}) d\mathbf{h} - \int_{\mathcal{G}_2 \setminus \mathcal{G}_1} \xi(\mathbf{h}) f(\mathbf{h}) d\mathbf{h} \\
&\geq 0 \quad (18)
\end{aligned}$$

since

$$\int_{\mathcal{G}_1 \setminus \mathcal{G}_2} f(\mathbf{h}) d\mathbf{h} = \int_{\mathcal{G}_2 \setminus \mathcal{G}_1} f(\mathbf{h}) d\mathbf{h}$$

and

$$\xi(\mathbf{h})|_{\mathbf{h} \in \mathcal{G}_1} \geq \xi(\mathbf{h})|_{\mathbf{h} \in \mathcal{G}_2}, \quad \forall \mathbf{h}$$

by definition. Hence, this contradicts our assumption that \mathcal{G}_2 is optimal. ■

REFERENCES

- [1] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, B. N. Shroff, "Joint Power and Secret Key Buffer Management to Achieve Delay Limited Secrecy", submitted to INFOCOM, 2010
- [2] J. Luo, L. Lin, R. Yates, and P. Spasojevic, "Service outage based power and rate allocation," *Information Theory, IEEE Transactions on*, vol.49, no.1, pp. 323-330, January 2003.