Robust Power Allocation and Outage Analysis for Secrecy in Independent Parallel Gaussian Channels

Siddhartha Sarma, Kundan Kandhway, and Joy Kuri

Abstract—This letter studies parallel independent Gaussian channels with uncertain eavesdropper channel state information (CSI). First, we evaluate the probability of zero secrecy rate in this system for 1) given instantaneous channel conditions and 2) a Rayleigh fading scenario. Second, when nonzero secrecy is achievable in the low SNR regime, we aim to solve a robust power allocation problem, which minimizes the outage probability at a target secrecy rate. We bound the outage probability and obtain a linear fractional program that takes into account the uncertainty in eavesdropper CSI while allocating power on the parallel channels. Problem structure is exploited to solve this optimization problem efficiently. We find the proposed scheme effective for uncertain eavesdropper CSI in comparison with conventional power allocation schemes.

Index Terms—Imperfect CSI, outage analysis, physical layer security, robust power allocation.

I. INTRODUCTION

BY USING inherent random noise in communication channels, physical layer security achieves information theoretically secure communications. Researchers have studied and characterized secrecy capacity for different communication systems and channel scenarios ranging from single antenna single hop [1] to multi-antenna multi-hop systems [2]. Later, to improve secrecy capacity, researchers have proposed schemes like MIMO with artificial noise generation, jammer assisted transmission [3], cooperative relaying and combined relaying-jamming [4] in the context of physical layer security.

However, most of the existing literature on physically secure communications considers perfect knowledge of eavesdroppers’ channel state information (CSI)—a far fetched assumption. For real world scenarios, e.g., border surveillance, we can only expect partial eavesdropper CSI (e.g. estimated path loss). Recently a few papers have discussed power allocation to improve secrecy for single channel scenarios when no CSI or partial CSI for the eavesdropper’s channel is available, either with the help of a jammer or using beamforming or both [2], [3], [5]. But studies involving (robust) optimal power allocation for parallel Gaussian channels with imperfect eavesdropper CSI have received little attention.

The parallel channels serve as a model for wideband wireless communications, channels with inter-symbol interference, block fading channels and multi-antenna systems. The secrecy capacity of parallel channels was studied in [6] and optimal power allocation for the Gaussian scenario was evaluated in [7]. But none of them addressed the imperfect eavesdropper CSI scenario. In the current article, we propose a robust power allocation scheme which ensures minimum secrecy outage when partial eavesdropper CSI is available.

Robust power allocation has appeared in [8] for relay channels without secrecy, in [3] for MISO systems, and in [9] for amplify and forward relaying in the context of secrecy. However, these works did not consider parallel Gaussian channels. Our contributions are summarized below.

- Approximate instantaneous complete secrecy outage probability for partial eavesdropper CSI. Closed form expression for average complete secrecy outage for fading channels.
- When non-zero secrecy is possible, optimal power allocation to minimize $\Pr(R_s < R_s^{(0)})$, where $R_s^{(0)}$ is the target secrecy rate. The proposed technique for this robust power allocation problem bounds the outage probability and leads to a linear fractional program.
- Computationally efficient technique to solve the formulated linear fractional program by exploiting the problem structure. Comparison of this power allocation technique with several conventional schemes with respect to secrecy outage.

II. SYSTEM MODEL

We consider a single transmitter (source)–receiver (destination) pair in presence of an eavesdropper. The source can transmit information to the destination using $N$ parallel channels indexed by $i \in \mathbb{N} = \{1, 2, \ldots, N\}$. The eavesdropper is passively listening to the source–destination transmission. The $i$th channel gains for the source to destination channel and the source to eavesdropper channel are denoted by complex numbers $h_i$ and $g_i$, respectively. The incomplete CSI for the eavesdropper’s channel is modeled as: $g_i = \hat{g}_i + \tilde{g}_i$, where, $\hat{g}_i$ and $\tilde{g}_i$ are the estimated channel gain and the unknown error term, respectively. For $i, j \in \mathbb{N}$, $\hat{g}_i$ and $\hat{g}_j$ are independent. The error $\tilde{g}_i$ is a circularly symmetric Gaussian random variable, i.e., $\tilde{g}_i \sim \mathcal{CN}(0, \sigma^2_i)$. Upon transmitting the vector source signal $x = [x_1, x_2, \ldots, x_N]^T$, the destination and the eavesdropper receive the following signals:

$y_{d,i} = h_i x_i + z_{d,i}$ and $y_{e,i} = g_i x_i + z_{e,i}$, $\forall i \in \mathbb{N}$.

The noise variables $z_{d,i}$ and $z_{e,i}$ are i.i.d. across the $N$ parallel channels, the channel uses over time, and independent of the source signal. All noise variables are circularly symmetric Gaussian random variables with mean 0 and variance 1. Also,
for practical reasons, we have a common power constraint over the parallel channels, i.e., \( \sum_{i=1}^{N} E[|x_i^2|] \leq P \).

For parallel independent Gaussian channels, secrecy capacity is attained when each source signal is distributed according to the Gaussian distribution, i.e., \( x_i \sim \mathcal{CN}(0, P_i) \). Therefore we can write [6]:

\[
C_s = \max_{P \in \mathcal{P}} \sum_{i=1}^{N} \left[ \frac{1}{2} \log (1 + |h_i|^2 P_i) - \frac{1}{2} \log (1 + |g_i|^2 P_i) \right] \tag{1}
\]

where \( \mathcal{P} := \{ P : \sum_{i=1}^{N} P_i \leq P, P_i \geq 0, \forall i \}, P = [P_1, P_2, \ldots, P_N]^T \) and \( |x|^+ = \max\{0, x\} \).

### III. COMPLETE SECRECY OUTAGE ANALYSIS

In Sec. III-A, we evaluate the instantaneous complete outage probability \( \Pr(C_s = 0| h_i, \tilde{g}_i, \forall i) \)—a consequence of imperfect information about eavesdropper’s CSI. Sec. III-B computes the same for fading channels.

#### A. Complete Secrecy Outage for Instantaneous Channel Gains, \( \Pr(C_s = 0| h_i, \tilde{g}_i, \forall i) \)

Complete secrecy outage occurs when the receiver’s absolute channel gain is less than the corresponding eavesdropper’s absolute channel gain, for all channels, i.e., \( |h_i| \leq |g_i|, \forall i \in N \). This scenario leads to zero secrecy rate irrespective of the power allocated.

\[ \Pr(C_s = 0| h_i, \tilde{g}_i, \forall i) = \Pr(|h_i| < |g_i|, \forall i) = \prod_{i=1}^{N} \Pr(|h_i| < |\tilde{g}_i + \tilde{g}_i|). \]

The last equality is true because channels are independent. We define random variables \( X_{1i} := \mathfrak{R}(\tilde{g}_i + \tilde{g}_i) \sim \mathcal{N}(\mathfrak{R}(\tilde{g}_i), \frac{1}{2} \epsilon_i^2) \) and \( X_{2i} := \mathfrak{I}(\tilde{g}_i + \tilde{g}_i) \sim \mathcal{N}(\mathfrak{I}(\tilde{g}_i), \frac{1}{2} \epsilon_i^2) \), where \( \mathfrak{R}(.) \) and \( \mathfrak{I}(.) \) are real and imaginary parts of a complex number, respectively. For each channel, the probability can be calculated in the following manner:

\[ \Pr(|h_i| < |\tilde{g}_i + \tilde{g}_i|) = \Pr(|h_i|^2 < |\tilde{g}_i + \tilde{g}_i|^2) = \Pr \left( \left| X_{1i} \right|^2 < \left( \frac{2X_{1i}^2 + 2X_{2i}^2}{2} \right) \right) = \Pr \left( |h_i|^2 < X_i^2 \right). \]

Here, \( X_i^2 \) is a non-central chi-square random variable with degrees of freedom (d.o.f) 2 and non-centrality parameter \( \lambda_i^2 = 2 \left( \frac{\mathfrak{R}(\tilde{g}_i)^2}{\epsilon_i^2} \right) + 2 \left( \frac{\mathfrak{I}(\tilde{g}_i)^2}{\epsilon_i^2} \right) \). A non-central chi-square random variable can be approximated by a central chi-square random variable as follows [10]:

\[ \Pr \left( X_i^2 < n_i \right) \approx \Pr \left( X_{i,0}^2 < \frac{n_i}{1 + \lambda_i^2/2} \right) = 1 - e^{-\frac{n_i}{2(1 + \lambda_i^2/2)}}. \]

For small values of centrality parameter \( \lambda_i^2 < 0.4 \), this approximation is quite accurate and for higher values it is conservative. The last equality is because a central chi-square

\[1\text{The precise expression is: } \Pr(C_s = 0| h_i, \tilde{g}_i, \forall i) = \Pr(|h_i| < |g_i|, \forall i), \text{ where } H_i \text{ and } G_i = \tilde{g}_i + \tilde{g}_i \text{ are the random variables corresponding to the source-destination and the source-eavesdropper channels respectively.} \]

#### B. Complete Secrecy Outage for Fading Channels \( \Pr(C_s = 0) \)

When \( h_i \) and \( \tilde{g}_i \) are sampled from circularly symmetric Gaussian distributions \( \mathcal{CN}(0, \sigma_{m,i}^2) \) and \( \mathcal{CN}(0, \sigma_{e,i}^2) \), respectively, then \( |h_i| \) and \( |g_i| \) have Rayleigh distributions with parameters \( \sigma_{m,i}/\sqrt{2} \) and \( \sigma_{e,i} + \epsilon_i/\sqrt{2} \). As \( |h_i|^2 \) and \( |g_i|^2 \) are exponentially distributed with parameters \( 1/\sigma_{m,i}^2 \) and \( 1/(\sigma_{e,i} + \epsilon_i)^2 \), respectively, following [1]:

\[ \Pr(C_s = 0) = \prod_{i=1}^{N} \left( \frac{1}{1 + \rho_i} \right), \text{ where } \rho_i = \frac{\sigma_{m,i}^2}{(\sigma_{e,i} + \epsilon_i)^2}. \]

### IV. ANALYSIS FOR NON-ZERO SECRECY RATE

In Sec. III, non-zero secrecy is not possible (irrespective of the power allocation). In contrast, in Sec. IV-A, we formulate and provide the optimal solution for a robust power allocation problem to minimize the outage probability for a target secrecy rate, \( R_{s}^{(0)} \), i.e., \( \Pr(R_s < R_{s}^{(0)}| h_i, \tilde{g}_i, \forall i) \). An expression for main channel outage for a target rate \( R_{s}^{(0)} \) is also provided (Sec. IV-B). Only for this section, we use a low SNR approximation of Eq. (1). This is valid for small values of \( P \)—typical in low power devices, such as, small sensor nodes deployed for surveillance.

#### A. Robust Optimal Power Allocation

Using \( \ln(1 + x) \approx x \), for \( x \to 0 \), we can approximate the secrecy rate in Eq. (1) as:

\[ R_s = \frac{1}{2 \ln(2)} \sum_{i=1}^{N} \left[ |h_i|^2 - |\tilde{g}_i + \tilde{g}_i| \right]^+ P_i. \tag{2} \]
For scenarios when non-zero secrecy is possible, we minimize the outage with respect to a target secrecy rate, $R^0_s$. As eavesdropper’s CSI is imperfect, we can not directly maximize $R_s$; therefore, we need a robust power allocation approach to minimize the outage probability. The optimization problem can be written as:

$$\min \Pr(R_s < R^0_s|h_i, \hat{g}_i, \forall i), \quad \text{subject to: } P \in \mathcal{P}. \quad (3)$$

This optimization is needed only when the main channel, i.e., source to destination channel can sustain a rate $R^0_s$. Otherwise, the secrecy rate is assured to be less than $R^0_s$ and the objective $\Pr(R_s < R^0_s) = 1$ everywhere in the feasible set, $P \in \mathcal{P}$. For small SNR, the main channel can sustain a rate $R^0_s$ when

$$\sum_{i=1}^{N} |h_i|^2 P_i - 2 \ln(2) R^0_s > 0. \quad (4)$$

Here, the secrecy outage can be calculated from Eq. (2) as:

$$\Pr(R_s < R^0_s|h_i, \hat{g}_i, \forall i) \leq \Pr\left(\sum_{i=1}^{N} |h_i|^2 P_i - 2 \ln(2) R^0_s < \sum_{i=1}^{N} |\hat{g}_i|^2 P_i\right) \quad (5)$$

$$= \Pr\left(\sum_{i=1}^{N} |h_i|^2 P_i - 2 \ln(2) R^0_s < \sum_{i=1}^{N} \chi_i^2 \frac{P_i}{c_i^2}\right) \quad (6)$$

As discussed in Sec. III-A, $\chi_i^2$ is a non-central chi-square random variable (d.o.f. 2). Therefore, the mean of $\chi_i^2 \frac{P_i}{c_i^2}$ is $\mathbb{E}[\chi_i^2 \frac{P_i}{c_i^2}] = \frac{\mu_i}{c_i^2} = \frac{\mu_i}{\chi^2(\infty)} = \frac{1}{2} \mathbb{E}[\chi_i^2 (2 + \chi_i^2)] = \frac{1}{2} \mathbb{E}[\chi_i^2 \chi_i^2] P_i$.

Using the Markov inequality, we can bound the outage probability as follows:

$$\Pr\left(\sum_{i=1}^{N} \chi_i^2 \frac{P_i}{c_i^2} > \sum_{i=1}^{N} |h_i|^2 P_i - 2 \ln(2) R^0_s\right) \quad (7)$$

$$\leq \frac{\mathbb{E}\left[\sum_{i=1}^{N} \chi_i^2 \frac{P_i}{c_i^2}\right]}{\sum_{i=1}^{N} |h_i|^2 P_i - 2 \ln(2) R^0_s} = P \quad (8)$$

The validity of Markov bound requires $\Delta \geq 0$ in Eq. (7); this is ensured by Eq. (4).

To minimize the outage, we propose to minimize this upper bound. This leads to the following equivalent linear fractional program (approximation to Problem (3)):}

$$\min \frac{c^T P}{d^T P - 2 \ln(2) R^0_s}, \quad \text{subject to: } P \in \mathcal{P}. \quad (9)$$

Here, $c_i = \chi_i^2 + |\hat{g}_i|^2$, $d_i = |h_i|^2$, and $c$, $d$ are vectors of these elements. The denominator $d^T P - 2 \ln(2) R^0_s \neq 0$ from the earlier discussion. This linear fractional program can be solved numerically by reformulating it as a linear program using the Charnes-Cooper transformation. However, due to the simplex constraint and only a few variables (the number of parallel channels, $N$), we propose the following easy to compute solution.

**Proposition 1:** The optimal solution to Problem (9) lies in one of the corners of the set $\mathcal{P} := \{P : \sum_{i=1}^{N} P_i = P, P_i \geq 0, \forall i\}$, i.e., $P_i = P$ for some $i \in \mathcal{N}$ and $P_j = 0, \forall j \neq i$.

**Proof:** We provide an outline of the proof here. One can verify that, at the optimum, the objective function of Problem (2) will converge the total budget $P$ (when at least one of the coefficients of $P_i$ is non-zero). Therefore, we can use equality in the sum constraint. From [11], a linear fractional program attains its optimum at the basic feasible solution of the constraint set. The corners of the constraint hyperplane—only $N$ in number—are the basic feasible solutions and the one that minimizes the objective function is the optimum.

Note that, unlike a general linear (fractional) program where calculating the corner points is computationally costly, in our case, the corners are known and fixed over the parameter set (specified in Proposition 1). Thus, the optimum is computed by enumerating the objective value at each corner point and selecting the best channel—computationally efficient even for a sensor node.

**B. Main Channel Outage for Fading Scenarios (for Small SNR)**

For completeness, we evaluate the probability of the event when the optimization problem (8) need not be solved, as the main channel capacity itself is less than the target rate. The fading coefficients $|h_i| \sim \text{Rayleigh} (\sigma_m^2, i \sqrt{2})$, $\forall i$. The outage occurs when the strongest of the $N$ parallel channels cannot sustain the target rate, i.e.,

$$\Pr\left(\max_i |h_i|^2 P < 2 \ln(2) R^0_s\right) \quad (10)$$

$$= \Pr\left(\sum_{i=1}^{N} |h_i|^2 P < 2 \ln(2) R^0_s\right) \quad (11)$$

$$\sum_{i=1}^{N} \left(1-e^{-\frac{2 \ln(2) R^0_s}{P \sigma_m^2}}\right) \quad (12)$$

$(u)$ and $(v)$ are true because $h_i$, $\forall i$ are independent and $|h_i|^2$ follows the exponential distribution.

**V. NUMERICAL RESULTS**

In this section, we compare several power allocation schemes for parallel independent Gaussian channels and show the effectiveness of our proposed scheme that considers eavesdropper’s channel uncertainty (optimization problem (8)). We consider three conventional power allocation strategies for comparison: (a) **Equal Power**—allocates equal power on every channel, $P_i = P/N$, $\forall i \in \mathcal{N}$. (b) **Optimum Capacity** power allocation—maximizes the Shannon capacity in the main channel, i.e., $P^*_e = \arg max \sum_{i=1}^{N} |h_i|^2 P_i$ (assuming small SNR), where $P^*_e \in \mathcal{P}$. It allocates the power budget $P$ to the strongest main channel. (c) **Optimum secrecy** power allocation—maximizes secrecy rate for the estimated eavesdropper channel gain without considering uncertainty. $P^*_s = \arg max \sum_{i=1}^{N} |h_i|^2 P_i$, where $P^*_s \in \mathcal{P}$. It allocates $P$ to the channel that has largest value of $|h_i|^2/|\hat{g}_i|^2$.

For simulations, we have generated the main channel $h_i$, and the estimated eavesdropper channel $\hat{g}_i$, from $\mathcal{CN}(0, \sigma_{m,i}^2)$ and $\mathcal{CN}(0, \sigma_{e,i}^2)$, respectively with $\sigma_{m,i}^2 = 0.6$ and $\sigma_{e,i}^2 = 0.3$ for all parallel channels. The power budget considered is $P = 0.1$. We use the default parameters for the target secrecy rate $R^0_s = 0.625 P \times \sigma_{m,i}^2/2 \ln(2)$ and the number of parallel channels.
instances of
SARMA et al.: ROBUST POWER ALLOCATION AND OUTAGE ANALYSIS FOR SECRECY

![Image of graphs](https://via.placeholder.com/150)

Fig. 2. Comparison of secrecy outage with respect to different system parameters. Default parameter values (except the one varied): $P = 0.1$, $\sigma^2_{\text{e}_i} = 0.6$, $\sigma^2_{\text{e}_i} = 0.3$, $R_{s}^{(0)} = 0.625P \times \sigma^2_{m,i}/2 \ln(2)$, $\epsilon^2_{s} = 0.3$ for $i \in \{1, 2, \ldots, [N/2]\}$ and $\epsilon^2_{s} = 0.09$ for $i \in \{[N/2] + 1, \ldots, N\}$.

$N = 10$. Uncertainty in the $i$th eavesdropper’s channel is generated from $CN(0, \epsilon^2_{s})$ with $\epsilon^2_{s} = 0.3$ for $i \in \{1, 2, \ldots, [N/2]\}$ and $\epsilon^2_{s} = 0.09$ for $i \in \{[N/2] + 1, \ldots, N\}$.

Fig. 2 plots the variation of the objective function, secrecy outage Pr($R_s < R_s^{(0)}$), with respect to variation of the system parameters (left y-axis); and the main channel outage for the same target rate $R_s^{(0)}$ (right y-axis). In all the three figures, “Optimum secrecy with uncertainty” identifies the proposed scheme. The plot Pr($R_s < R_s^{(0)}$) is calculated, for example, for the proposed scheme as follows.

We generate $h_i$, $\tilde{g}_i$, $i \in \mathbb{N}$. Given this channel, we calculate the power allocation of the proposed scheme $P_p$ using the optimization problem (8). Note that, we only need the variance of the uncertainty of the eavesdropper’s channel, $\epsilon^2_{s}$, $\forall i$ and not the exact value of $\tilde{g}_i$ to calculate $P_p$. Now, the conditional outage probability given $h_i$ and $\tilde{g}_i$, $\forall i$, i.e., Pr($R_s < R_s^{(0)}|h_i, \tilde{g}_i, \forall i$) is calculated by Monte-Carlo averaging over $10^4$ values of $\tilde{g}_i, \forall i$ using (6) for $P_p$. We obtain the final objective function, Pr($R_s < R_s^{(0)}$), as follows: $10^4$ instances of $h_i$ and $\tilde{g}_i$ are generated, (6) is averaged over the instances for which the main channel is not in outage, i.e., $\max\{|h_i|^2, \forall i\} P > 2 \ln(2) R_s^{(0)}$. The same is carried out for the three conventional power allocation strategies.

Fig. 2a demonstrates the effectiveness of the proposed scheme when the target secrecy rate $R_s^{(0)}$ is varied, specially for small values of $R_s^{(0)}$. The effect of variation of eavesdropper’s channel uncertainty is shown in Fig 2b. As expected, when uncertainty is small, performance of the “Optimum secrecy” power allocation is comparable to the proposed scheme. However, as the uncertainty increases, the proposed scheme outperforms the others. Finally, we vary the number of channels, $N$ in Fig 2c. The proposed scheme exploits the uncertainty parameter $\epsilon^2_{s}$ in addition to the channel gains, and therefore, outperforms “Optimum secrecy” (and others). The improvements are prominent for higher values of $N$.

VI. CONCLUSION

We study the effect of a single eavesdropper’s channel uncertainty in a parallel independent Gaussian channel communications system. We evaluate complete secrecy outage probability for instantaneous and fading channels. Further, we propose a robust power allocation scheme to minimize secrecy outage probability at a target rate in the low SNR regime. Our techniques involve (1) approximating non-central chi-square random variables by corresponding central ones to evaluate instantaneous outage; and (2) bounding outage probabilities for robust power allocation, which leads to a linear fractional program. Exploiting the structure of the problem, we propose an easy-to-compute solution. Numerical results show the superiority of the proposed scheme compared to the conventional schemes that do not consider uncertainty.

REFERENCES

[1] J. Barros and M. Rodrigues, “Secrecy capacity of wireless channels,” in Proc. IEEE Int. Symp. Inf. Theory, Jul. 2006, pp. 356–360.
[2] D. Ng, E. Lo, and R. Schober, “Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks,” IEEE Trans. Wireless Commun., vol. 10, no. 10, pp. 3528–3540, Oct. 2011.
[3] J. Huang and A. Swindlehurst, “Robust secure transmission in MISO channels based on worst-case optimization,” IEEE Trans. Signal Process., vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
[4] K.-H. Park, T. Wang, and M.-S. Alouini, “On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1741–1750, Sep. 2013.
[5] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, “Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no Eavesdropper’s CSI,” IEEE Signal Process. Lett., vol. 20, no. 1, pp. 39–42, Jan. 2013.
[6] Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” in Securing Wireless Communications at the Physical Layer, R. Liu and W. Trappe, Eds. New York, NY, USA: Springer, 2010, pp. 1–18.
[7] E. Jorswieck and A. Wolf, “Resource allocation for the wire-tap multi-carrier broadcast channel,” in Proc. Int. Conf. Telecommun. (ICT’08), Jun. 2008, pp. 1–6.
[8] S. Mallick, R. Devarajan, M. Rashid, and V. Bhargava, “Resource allocation for selective reaying based cellular wireless system with imperfect CSI,” IEEE Trans. Commun., vol. 61, no. 5, pp. 1822–1834, May 2013.
[9] L. Li, Z. Chen, and J. Fang, “Robust transmit design for secure AF relay networks based on worst-case optimization,” in Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), May 2014, pp. 2719–2723.
[10] D. R. Cox and N. Reid, “Approximations to noncentral distributions,” Can. J. Statist., vol. 15, no. 2, pp. 105–114, 1987.
[11] K. Sivarup, “Letter to the editor—Linear fractional functionals programming,” Oper. Res., vol. 13, no. 6, pp. 1029–1036, 1965.