Resource Allocation for Parallel Gaussian MIMO Wire-tap Channels

Vincent Le Nir, Bart Scheers

***Abstract*—Wire-tap channels are able to provide perfect secrecy when a receiver exhibits a better channel than its wire-tapping opponent. In this letter, we extend the perfect secrecy principle to parallel Gaussian multiple input multiple output (MIMO) wire-tap channels with independent sub-channels. Assuming $N_r \geq N_t$ and $N_e \geq N_t$, mathematical derivations show that a sub-optimal solution can be given in closed-form considering either secrecy rate maximization subject to a total power constraint or power minimization subject to a secrecy rate constraint. Although sub-optimal for MIMO systems, simulation results show that the proposed algorithm allows to reach higher secrecy rates with substantial gains in power consumption compared to the single input single output (SISO) system.**

***Index Terms*—MIMO systems, optimization methos, wire-tap channel**

I. Introduction

The wire-tap channel has been introduced in 1975 by Wyner [1]. The purpose of a wire-tap channel is to provide reliable communication between a transmitter and its legitimate receiver and to prevent an eavesdropper to read the message. In practice, as the channel state information (CSI) of both links is known at the transmit side, wire-tap channels apply to voice or data networks in which a transmitter sends a confidential message to a particular receiver with perfect secrecy.

The resource allocation problems for parallel Gaussian SISO wire-tap channels with independent sub-channels and a single Gaussian MISO wire-tap channel are studied in [2], [3], [4], [5]. Recently, the optimal power allocation in a single Gaussian MIMO wire-tap channel has been investigated in various articles [6], [7], [8], [9]. The MIMO wiretap channel can be characterized as the saddle point of a minimax problem [6] or based on an enhanced channel [7], [8]. The global optimum solution requires a branch and bound with reformulation linearization technique (BB/RLT) [9], which might be relatively complex when considering parallel Gaussian MIMO wire-tap channels. In this letter, we extend the perfect secrecy principle to parallel Gaussian MIMO wire-tap channels with independent sub-channels. Assuming $N_r \geq N_t$ and $N_e \geq N_t$, mathematical derivations show that a sub-optimal solution can be given in closed-form considering either secrecy rate maximization subject to a total power constraint or power minimization subject to a secrecy rate constraint. Although sub-optimal for MIMO systems, simulation results show that the proposed algorithm allows to reach higher secrecy rates with substantial gains in power consumption compared to the SISO system.

V. Le Nir and B. Scheers are with the Royal Military Academy, Dept. Communication, Information Systems & Sensors (CISS), 30, Avenue de la Renaissance B-1000 Brussels BELGIUM. E-mail: bart.scheers@rma.ac.be vincent.lenir@rma.ac.be

This research work was carried out in the frame of the Belgian Defense Scientific Research & Technology Study C4/19 funded by the Ministry of Defense (MoD). The scientific responsibility is assumed by its authors.

In Section II, we give the power allocation for parallel Gaussian MIMO wire-tap channels with independent sub-channels. In Section III, simulation results are given. Finally, Section IV concludes this letter.

II. Power allocation for parallel Gaussian MIMO wire-tap channels with independent sub-channels

We consider the parallel Gaussian MIMO wire-tap channel with independent sub-channels as shown in Figure 1. The sender has N_t antennas, the receiver and the eavesdropper have $N_r \geq N_t$ and $N_e \geq N_t$ antennas respectively. These two conditions are necessary for the existence of the matrices $\mathbf{A}_i$ and $\mathbf{B}_i$ later defined in this letter. The secured data information is sent on N_c parallel sub-channels. The received signal can be modeled as

$$\begin{aligned} \mathbf{y}_{ik} = \mathbf{H}_{ik}\mathbf{x}_i + \mathbf{n}_{ik} \qquad & k = r, e \\ & i = 1 \dots N_c \end{aligned} \tag{1}$$

with $\mathbf{n}_{ik}$ the additive noise vector of length N_k with autocorrelation matrix $\mathbf{R}_{ik}$ and $\mathbf{H}_{ik}$ the $N_k \times N_t$ channel matrix seen by receiver k on tone i. As the autocorrelation matrix $\mathbf{R}_{ik}$ is Hermitian and positive definite, it can be decomposed into $\mathbf{R}_{ik} = \mathbf{L}_{ik}\mathbf{L}_{ik}^H$ (Cholesky decomposition) with $\mathbf{L}_{ik}$ a lower triangular matrix. The secrecy rate maximization of a parallel Gaussian MIMO wire-tap channel with independent sub-channels subject to a total power constraint P^{tot} is

$$\begin{aligned} \max_{\underline{\mathbf{\Phi}}} \sum_{i=1}^{N_c} \left(\log_2|\mathbf{I} + \tilde{\mathbf{H}}_{ir}\mathbf{\Phi}_i\tilde{\mathbf{H}}_{ir}^H| - \log_2|\mathbf{I} + \tilde{\mathbf{H}}_{ie}\mathbf{\Phi}_i\tilde{\mathbf{H}}_{ie}^H| \right) \\ \text{subject to } \begin{array}{l} \sum_{i=1}^{N_c} \text{Tr}(\mathbf{\Phi}_i) = P^{tot} \\ \mathbf{\Phi}_i = \mathbf{\Phi}_i^H \ \forall i \\ \mathbf{\Phi}_i \succeq 0 \ \forall i \end{array} \end{aligned} \tag{2}$$

with $\mathbf{\Phi}_i = E[\mathbf{x}_i\mathbf{x}_i^H]$ the variance of the input signal on sub-channel i, $\underline{\mathbf{\Phi}}$ the power allocation among all sub-channels, $\tilde{\mathbf{H}}_{ik} = \mathbf{L}_{ik}^{-1}\mathbf{H}_{ik}$ $(k = r, e)$, P^{tot} the total power constraint, $|.|$ the determinant operator, $\text{Tr}(.)$ the trace operator and $(.)^H$ the Hermitian operator. As the objective function is neither convex nor concave, the standard Karush-Kuhn-Tucker (KKT) conditions are necessary but not sufficient [10]. The Lagrangian function which includes the total power constraint is given by

$$\begin{aligned} L(\lambda, \underline{\mathbf{\Phi}}) = \sum_{i=1}^{N_c} \Bigg(\log_2|\mathbf{I} + \tilde{\mathbf{H}}_{ir}\mathbf{\Phi}_i\tilde{\mathbf{H}}_{ir}^H| - \log_2|\mathbf{I} + \tilde{\mathbf{H}}_{ie}\mathbf{\Phi}_i\tilde{\mathbf{H}}_{ie}^H| \\ -\lambda\text{Tr}(\mathbf{\Phi}_i) \Bigg) + \lambda P^{tot} \end{aligned} \tag{3}$$

with λ the Lagrange multiplier associated with the total power constraint. Using the property $|\mathbf{I} + \mathbf{AB}| = |\mathbf{I} + \mathbf{BA}|$, the Lagrangian function can be rewritten as

$$\begin{aligned} L(\lambda, \underline{\mathbf{\Phi}}) = \sum_{i=1}^{N_c} \Bigg(\log_2|\mathbf{A}_i + \mathbf{\Phi}_i| - \log_2|\mathbf{B}_i + \mathbf{\Phi}_i| + \log_2|\mathbf{A}_i^{-1}| \\ -\log_2|\mathbf{B}_i^{-1}| - \lambda\text{Tr}(\mathbf{\Phi}_i) \Bigg) + \lambda P^{tot} \end{aligned} \tag{4}$$

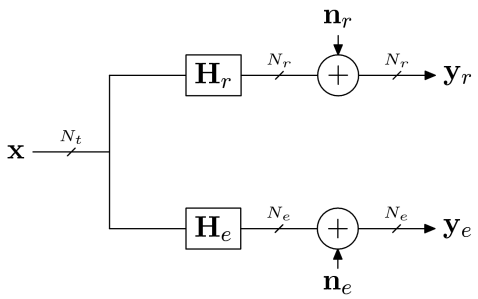

Fig. 1. Gaussian MIMO wire-tap channel

with two Hermitian matrices $\mathbf{A}_i = (\tilde{\mathbf{H}}_{ir}^H \tilde{\mathbf{H}}_{ir})^{-1}$ and $\mathbf{B}_i = (\tilde{\mathbf{H}}_{ie}^H \tilde{\mathbf{H}}_{ie})^{-1}$. The existence of the matrices $\mathbf{A}_i$ and $\mathbf{B}_i$ requires $N_r \geq N_t$ and $N_e \geq N_t$. Moreover, we assume $\mathbf{B}_i \succeq \mathbf{A}_i$. In order to derive the closed-form power allocation associated with the necessary conditions, we define two Hermitian matrices $\tilde{\mathbf{\Phi}}_i = \mathbf{\Phi}_i + \dfrac{\mathbf{A}_i + \mathbf{B}_i}{2}$ and $\mathbf{C}_i = \dfrac{\mathbf{A}_i - \mathbf{B}_i}{2}$, leading to the following Lagrangian function

$$L(\lambda, \underline{\mathbf{\Phi}}) = \sum_{i=1}^{N_c} \left(\log_2|\tilde{\mathbf{\Phi}}_i + \mathbf{C}_i| - \log_2|\tilde{\mathbf{\Phi}}_i - \mathbf{C}_i| + \log_2|\mathbf{A}_i^{-1}| - \log_2|\mathbf{B}_i^{-1}| - \lambda \mathrm{Tr}(\mathbf{\Phi}_i) \right) + \lambda P^{tot} \tag{5}$$

The derivative of the Lagrangian function which includes the total power constraint with respect to $\mathbf{\Phi}_i$ is given by

$$\frac{\partial L(\lambda, \underline{\mathbf{\Phi}})}{\partial \mathbf{\Phi}_i} = \frac{1}{\ln 2} \left((\tilde{\mathbf{\Phi}}_i + \mathbf{C}_i)^{-1} - (\tilde{\mathbf{\Phi}}_i - \mathbf{C}_i)^{-1} \right) - \lambda \mathbf{I}. \tag{6}$$

Nulling the derivative gives

$$\begin{aligned} \frac{\partial L(\lambda, \underline{\mathbf{\Phi}})}{\partial \mathbf{\Phi}_i} = 0 \quad &\Rightarrow (\tilde{\mathbf{\Phi}}_i + \mathbf{C}_i)^{-1} - (\tilde{\mathbf{\Phi}}_i - \mathbf{C}_i)^{-1} = \tilde{\lambda} \mathbf{I} \\ &\Rightarrow -2\mathbf{C}_i = \tilde{\lambda} (\tilde{\mathbf{\Phi}}_i + \mathbf{C}_i)(\tilde{\mathbf{\Phi}}_i - \mathbf{C}_i) \\ &\Rightarrow -2\mathbf{C}_i = \tilde{\lambda} (\tilde{\mathbf{\Phi}}_i^2 - \mathbf{C}_i^2 + \mathbf{C}_i \tilde{\mathbf{\Phi}}_i - \tilde{\mathbf{\Phi}}_i \mathbf{C}_i) \end{aligned} \tag{7}$$

with $\tilde{\lambda} = \lambda \ln 2$. By taking Hermitian conjugates on both sides, we get

$$\begin{aligned} &-2\mathbf{C}_i = \tilde{\lambda} (\tilde{\mathbf{\Phi}}_i^2 - \mathbf{C}_i^2 + \mathbf{C}_i \tilde{\mathbf{\Phi}}_i - \tilde{\mathbf{\Phi}}_i \mathbf{C}_i) \\ &\overset{(.)^H}{\Longleftrightarrow} -2\mathbf{C}_i = \tilde{\lambda} (\tilde{\mathbf{\Phi}}_i^2 - \mathbf{C}_i^2 + \tilde{\mathbf{\Phi}}_i \mathbf{C}_i - \mathbf{C}_i \tilde{\mathbf{\Phi}}_i) \end{aligned} \tag{8}$$

leading to the following system of equations

$$\begin{cases} \mathbf{C}_i \tilde{\mathbf{\Phi}}_i - \tilde{\mathbf{\Phi}}_i \mathbf{C}_i = 0 \\ -2\mathbf{C}_i = \tilde{\lambda} (\tilde{\mathbf{\Phi}}_i^2 - \mathbf{C}_i^2) \end{cases}. \tag{9}$$

Since $\mathbf{C}_i$ is Hermitian, we need to work in a basis in which $\mathbf{C}_i$ is diagonalized. Therefore, we use the eigenvalue decomposition (EVD) $\mathbf{C}_i = \mathbf{W}_i \mathbf{D}_i \mathbf{W}_i^H$ which leads to the following developments of the system of equations

$$\begin{cases} \mathbf{W}_i \mathbf{D}_i \mathbf{W}_i^H \tilde{\mathbf{\Phi}}_i - \tilde{\mathbf{\Phi}}_i \mathbf{W}_i \mathbf{D}_i \mathbf{W}_i^H = 0 \\ -2\mathbf{W}_i \mathbf{D}_i \mathbf{W}_i^H = \tilde{\lambda} (\tilde{\mathbf{\Phi}}_i^2 - \mathbf{W}_i \mathbf{D}_i^2 \mathbf{W}_i^H) \end{cases} \tag{10}$$

$$\Rightarrow \begin{cases} \mathbf{D}_i \mathbf{W}_i^H \tilde{\mathbf{\Phi}}_i \mathbf{W}_i - \mathbf{W}_i^H \tilde{\mathbf{\Phi}}_i \mathbf{W}_i \mathbf{D}_i = 0 \\ -2\mathbf{D}_i = \tilde{\lambda} (\mathbf{W}_i^H \tilde{\mathbf{\Phi}}_i^2 \mathbf{W}_i - \mathbf{D}_i^2) \end{cases}. \tag{11}$$

Making the variable change $\mathbf{Z}_i = \mathbf{W}_i^H \tilde{\mathbf{\Phi}}_i \mathbf{W}_i$, the final system of equations to be solved is

$$\begin{cases} \mathbf{D}_i \mathbf{Z}_i - \mathbf{Z}_i \mathbf{D}_i = 0 \\ -2\mathbf{D}_i = \tilde{\lambda} (\mathbf{Z}_i^2 - \mathbf{D}_i^2) \end{cases}. \tag{12}$$

The system of equations implies $\mathbf{Z}_i$ to be diagonal since $\mathbf{D}_i$ is diagonal. The power allocation is a type of water-filling strategy given by the solution of the parallel quadratic equation

$$\tilde{\lambda} \mathbf{Z}_i^2 + 2\mathbf{D}_i - \tilde{\lambda} \mathbf{D}_i^2 = 0 \tag{13}$$

with $\mathbf{Z}_i$ diagonal. The discriminant of this quadratic equation is given by

$$\Delta = 4\tilde{\lambda}^2 \mathbf{D}_i^2 - 8\tilde{\lambda} \mathbf{D}_i. \tag{14}$$

As $\tilde{\mathbf{\Phi}}_i$ is Hermitian, $\mathbf{Z}_i$ should have real diagonal elements. The solution is given by the positive root

$$\mathbf{Z}_i = \left(\left[\mathbf{D}_i^2 - \frac{2}{\tilde{\lambda}} \mathbf{D}_i \right]^+ \right)^{1/2}. \tag{15}$$

Knowing that $\tilde{\mathbf{\Phi}}_i = \mathbf{W}_i \mathbf{Z}_i \mathbf{W}_i^H$ and $\mathbf{\Phi}_i = \tilde{\mathbf{\Phi}}_i - \dfrac{\mathbf{A}_i + \mathbf{B}_i}{2}$, the power allocation is given by

$$\mathbf{\Phi}_i = \mathbf{W}_i \left(\left[\mathbf{D}_i^2 - \frac{2}{\tilde{\lambda}} \mathbf{D}_i \right]^+ \right)^{1/2} \mathbf{W}_i^H - \frac{\mathbf{A}_i + \mathbf{B}_i}{2}. \tag{16}$$

The difference operation prevents to obtain positive semi-definite matrices. Therefore, after the calculation of the $\mathbf{\Phi}_i$ matrices, a new EVD must be performed on $\mathbf{\Phi}_i = \mathbf{T}_i \mathbf{\Theta}_i \mathbf{T}_i^H$ with $\mathbf{T}_i$ the unitary matrix containing the eigenvectors and $\mathbf{\Theta}_i$ the diagonal matrix containing the eigenvalues. As the negative eigenvalues of $\mathbf{\Theta}_i$ must be set to zero to have positive semi-definite matrices, the power allocation becomes

$$\mathbf{\Phi}_i = \mathbf{T}_i [\mathbf{\Theta}_i]^+ \mathbf{T}_i^H. \tag{17}$$

The SNR gap Γ which measures the loss with respect to theoretical performance [11] can be introduced in (2) giving $\dfrac{1}{\Gamma} \tilde{\mathbf{H}}_{ik} \mathbf{\Phi}_i \tilde{\mathbf{H}}_{ik}^H$. Then, formula (16) becomes

$$\mathbf{\Phi}_i = \mathbf{W}_i \left(\left[\Gamma^2 \mathbf{D}_i^2 - \frac{2\Gamma}{\tilde{\lambda}} \mathbf{D}_i \right]^+ \right)^{1/2} \mathbf{W}_i^H - \frac{\Gamma(\mathbf{A}_i + \mathbf{B}_i)}{2}. \tag{18}$$

A pseudocode, providing the power allocation for secrecy rate maximization subject to a total power constraint P of N_c parallel Gaussian MIMO wire-tap channels with independent sub-channels, is presented in Algorithm 1 from line 3 to line 7 referred to as the inner loop of the algorithm. An outer loop can be added to find the minimum amount of power that is needed to support a given secrecy rate constraint. Algorithm 1 provides the power allocation for power minimization subject to a secrecy rate constraint R^{sec} of N_c parallel Gaussian MIMO wire-tap channels with independent sub-channels (the bisection method is used to update the parameters λ and P).

Algorithm 1 Minimization of the power subject to a secrecy rate constraint

initialize $P = 10^{-9}$, $\lambda = 10^{-9}$, $\mathbf{\Phi}_i = 0 \ \forall i$
repeat
  repeat
    Calculate $\mathbf{\Phi}_i \ \forall i$ according to (17)
    if $\sum_{i=1}^{N_c} Tr(\mathbf{\Phi}_i) < P$ decrease λ
    if $\sum_{i=1}^{N_c} Tr(\mathbf{\Phi}_i) > P$ increase λ
  until the desired accuracy is reached
  Calculate $R = \sum_{i=1}^{N_c} \left(\log_2|\mathbf{I} + \mathbf{H}_{ir}\mathbf{\Phi}_i\mathbf{H}_{ir}^H\mathbf{R}_{ir}^{-1}| - \log_2|\mathbf{I} + \mathbf{H}_{ie}\mathbf{\Phi}_i\mathbf{H}_{ie}^H\mathbf{R}_{ie}^{-1}|\right)$
  if $R < R^{sec}$ increase P
  if $R > R^{sec}$ decrease P
until the desired accuracy is reached

III. Simulation results

In this Section, we study the performance of the proposed power allocation for a SISO system with $N_t = N_r = N_e = 1$ antenna and MIMO systems with $N_t = N_r = N_e = 2, 3$, or 4 antennas. The log-distance path loss model is used to measure the path loss between the transmitter and the receivers [12]. The transmitter is placed at the origin, the receiver is placed randomly in a quarter circle of radius 1 km and the eavesdropper is placed randomly in a quarter circle band of radius 3 and 4 km. For the simulations, $N_c = 4$ sub-channels are considered. The carrier frequency is chosen to be in the VHF band ($f_c = 80$ MHz). The SNR gap $\Gamma = 9.8$ dB corresponds to an uncoded quadrature amplitude modulation (QAM) at symbol error rate 10^{-7}. The bandwidth of each sub-channel is $\Delta f = 25$ kHz, the path loss exponent in the log-distance path loss model is $n = 4$, reference distance $d_0 = 20$ meters and thermal noise with variance $\sigma^2 = -204\text{dB/Hz} + 10\log_{10}(\Delta f)$.

Figure 2 shows the results of the power minimization subject to a secrecy rate constraint and ranging from $R^{sec} = 4$ kbps to $R^{sec} = 1024$ kbps. These results are expressed in Watts and averaged over 10^3 Monte Carlo trials. The SISO and MIMO4x4 secrecy algorithms are compared with the standard SISO and MIMO4x4 waterfilling algorithms (to the intended receiver only) to provide a lower bound for the optimal secrecy algorithms presented in [6], [7], [8], [9]. Figure 2 and Table 1 show that the proposed algorithm allows to obtain higher secrecy rates and lower power consumption when the number of antennas increases. Although sub-optimal for MIMO systems, the MIMO4x4 secrecy algorithm requires only a small power augmentation compared to the standard MIMO4x4 waterfilling algorithm.

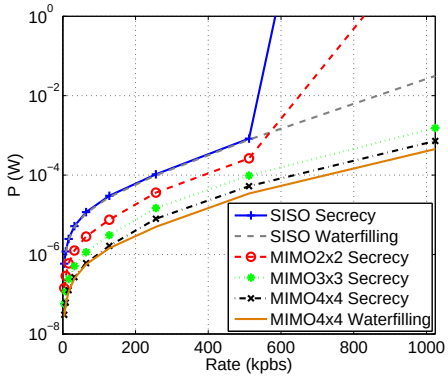

Fig. 2. Results on the power minimization subject to a secrecy rate constraint

64 kbps	SISO Secrecy	SISO Waterfilling	MIMO2x2 Secrecy	MIMO3x3 Secrecy	MIMO4x4 Secrecy	MIMO4x4 Waterfilling
P (W)	1.17e-5	1.11e-5	2.84e-6	1.15e-6	6.07e-7	5.66e-7
Gain (dB)	-	0.23	6.15	10.07	12.85	13.15

TABLE I
NUMERICAL RESULTS AND GAINS FOR THE POWER MINIMIZATION SUBJECT TO A SECRECY RATE CONSTRAINT $R^{sec} = 64$ kbps

IV. Conclusion

In this letter, we have extended the perfect secrecy principle to parallel Gaussian multiple input multiple output (MIMO) wire-tap channels with independent sub-channels. Assuming $N_r \geq N_t$ and $N_e \geq N_t$, mathematical derivations have shown that a sub-optimal solution can be given in closed-form considering either perfect secrecy rate maximization subject to a total power constraint or power minimization subject to a perfect secrecy rate constraint. Although sub-optimal for MIMO systems, simulation results have shown that the proposed algorithm allows to obtain higher secrecy rates and substantial gains in power consumption compared to the SISO system, and is not far from the optimum solution.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journal*, vol. 54, pp. 1355–1387, 1975.

[2] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," *44th Annual Allerton Conference on Communication, Control, and Computing, Allerton House, USA*, Sep. 2006.

[3] Y. Liang and H. V. Poor, "Secure communication over fading channels," *44th Annual Allerton Conference on Communication, Control, and Computing, Allerton House, USA*, Sep. 2006.

[4] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," *15th International Conference on Telecommunications, ICT'08, Saint-Petersburg, Russia*, Jun. 2008.

[5] S. Shaifee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," *IEEE International Symposium on Information Theory, ISIT'07, Nice, France*, Jun. 2007.

[6] A. Khisti and G. Wornell, "The MIMOME Channel," *45th Annual Allerton Conference on Communication, Control, and Computing, Allerton House, USA*, Oct. 2007.

[7] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, Jun. 2009.

[8] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel," *EURASIP Journal on Wireless Communications and Networking Volume 2009, Article ID 370970, 8 pages doi:10.1155/2009/370970*, 2009.

[9] J. Liu, Y. T. Hou, and H. D. Sherali, "Optimal Power Allocation for Achieving Perfect Secrecy Capacity in MIMO Wire-Tap Channels," *43rd Annual Conference on Information Sciences and Systems, CISS'09, Baltimore, USA*, Mar. 2009.

[10] S. Boyd and L. Vandenberghe, "Convex Optimization," *Cambridge University Press*, 2004.

[11] J. M. Cioffi, "A Multicarrier Primer," *ANSI Contribution T1E1.4/91-157*, Nov. 1991.

[12] T. S. Rappaport, "Wireless Communications: principles and practice," *Prentice Hall*, 1996.