ON THE SECRECY CAPACITY OF FREQUENCY-SELECTIVE FADING CHANNELS: A PRACTICAL VANDERMONDE PRECODING

Mari Kobayashi, Merouane Debbah

ON THE SECRECY CAPACITY OF FREQUENCY-SELECTIVE FADING CHANNELS : A PRACTICAL VANDERMONDE PRECODING

Mari Kobayashi and Mérouane Debbah

Supelec, 3 rue Joliot-Curie
91192 GIF SUR YVETTE CEDEX, France
Email:{mari.kobayashi,merouane.debbah}@supelec.fr

ABSTRACT

We study the secrecy capacity of the frequency-selective wiretap channel. Assuming that a guard interval of L symbols is inserted to avoid the inter-block interference and these symbols are discarded at the receiver, the single-carrier frequency-selective channel is modeled as a multiple-input multiple-output Toeplitz matrix. For this special case of the MIMO wiretap channel and under the assumption of perfect channel knowledge at transmitter (CSIT), we propose a practical Vandermonde precoding scheme that transmits the confidential messages on the zeros of the eavesdropper channel. It is proved that this Vandermonde precoding achieves the full multiplexing gain offered by the frequency-selective wiretap channel in the high SNR regime. For a more realistic case where the transmitter only knows the legitime channel we consider the "mask beamforming" scheme where the artificial noise is sent on the zeros of the legitime channel via the Vandermonde precoding. This mask beamforming is shown to achieve the same multiplexing gain as the perfect CSIT.

1. INTRODUCTION

We consider the frequency-selective wiretap channel where the legitime transmitter sends confidential messages to the intended receiver in the presence of the eavesdropper. Although recent works have characterized the secrecy capacity of the wiretap fading channel for the scalar case [1], the Multiple-Input Single-Output (MISO) case [2], and Multiple Input Multiple Output (MIMO) case [3], these works only apply to the frequency flat fading channel. To the best of the authors' knowledge, none has explicitly considered the case of the frequency selective channel relevant to current standards (such as IEEE802.11a type). In order to model the frequency selective channel with L paths, we assume that a guard interval of L symbols is inserted at the beginning of each block of N symbols in order to avoid the inter-block interference. By further assuming that each receiver observes N symbols out of $N + L$ by discarding L symbols, the block frequency selective channel can be modeled as a $N + L$ multiple-input N multiple-output Toeplitz matrix[1]. On one hand, it is known that the parallel wiretap fading channels achieve the secrecy capacity which does not scale with the SNR [1]. On other hand, Khisti et al. showed that the capacity of the MIMO wiretap channel grows linearly, i.e. $r \log \mathsf{SNR}$ where r denotes the *effective* degree of freedom (to be specified) [3]. It clearly appears that performing OFDM transmission to convert the frequency-selective channel into a set of N parallel flat fading channels is highly suboptimal in terms of multiplexing gain. Moreover to achieve the secrecy capacity of MISO and MIMO wiretap channel in the high SNR regime, the optimal strategy consists of beamforming in the null space of the eavesdropper's channel [2, 3]. Inspired by this strategy, in the case of perfect CSIT, we propose a practical Vandermonde precoding scheme that nulls the eavesdropper channel in single-carrier frequency selective channels. Since the channel of the legitimate and eavesdropper are statistically independent, this scheme provide L (where L is the number of paths) degrees of freedom to transmit secret information. Note that Vandermonde matrices have already been considered for cognitive radios [4] and CDMA systems [5] to reduce/null interference. One of the appealing aspects of Vandermonde precoding is that it does not require a specific secrecy encoding technique but can be applied to any classical encoding schemes. In a more practical case where the transmitter does not know the eavesdropper' channel, we consider the mask beamforming scheme with Vandermonde precoding. The idea here is to send artificial noise on the zeros of the legitimate channel in such a way that L degrees of freedom of the eavesdropper are jammed. Interestingly, in the high SNR regime, L degrees of freedom for the secrecy capacity can be achieved as for the perfect CSIT case.

In the following, section 2 presents the frequency selective wire-tap channel model. Section 3 introduces the Vandermonde precoding both for the perfect and partial CSIT

[1]The last assumption implies in practice that both the intended receiver and the eavesdropper have the same receiver structure, i.e. the eavesdropper is not allowed/capable to modify its receiver.

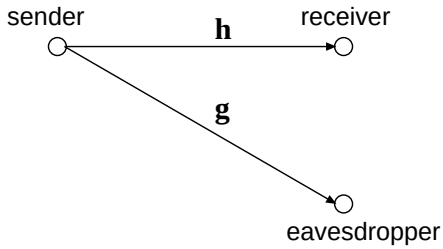

Fig. 1. Wiretap model

cases. The behavior in the high SNR regime is also discussed. Finally, section 4 compares the performance for the various cases.

2. MODEL

2.1. Channel Model

We consider the block frequency-selective fading channel given by

$$\begin{aligned} \mathbf{y}_t &= \mathcal{T}(\mathbf{h})\mathbf{x}_t + \mathbf{n}_t \\ \mathbf{z}_t &= \mathcal{T}(\mathbf{g})\mathbf{x}_t + \boldsymbol{\nu}_t, \quad t = 1, \ldots, T \end{aligned} \tag{1}$$

where $\mathcal{T}(\mathbf{h}), \mathcal{T}(\mathbf{g})$ denotes a $N \times (N+L)$ Toeplitz matrix with $L+1$ i.i.d. Gaussian distributed paths $\mathbf{h}, \mathbf{g} \sim \mathcal{N}_{\mathcal{C}}(\mathbf{0}, \mathbf{I}_{L+1})$ corresponding to the legitime, eavesdropper channel

$$\mathcal{T}(\mathbf{h}) = \begin{bmatrix} h_L & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & h_L & \cdots & h_0 \end{bmatrix}$$

$\mathbf{x}_t \in \mathbb{C}^{N+L}$ denotes the transmit vector at channel use t, and finally $\mathbf{n}_t, \boldsymbol{\nu}_t \sim \mathcal{N}_{\mathcal{C}}(\mathbf{0}, \mathbf{I}_N)$ are independent AWGN. The input matrix is subject to the power constraint given by

$$\frac{1}{T}\sum_{t=1}^{T} \mathbf{x}_t^H \mathbf{x}_t \leq (N+L)P \tag{2}$$

We assume that the channels remain constant over a block length of T channel uses for an arbitrary large T. At each channel use t, we transmit $N+L$ symbols by appending a guard interval of size L larger than the coherence time. This enables to avoid the interference between neighbor channel uses. We assume first that the channels $\mathbf{h}, \mathbf{g}$ are known by all terminals. Then we consider the case where the transmitter knows only the legitime channel $\mathbf{h}$ while the intended receiver and the eavesdropper know both channels.

2.2. Secrecy capacity

The wiretap channel was first introduced by Wyner [6] in the scalar case of degraded channels. The secrecy rate is said to be achievable if there exists a sequence of $(T, 2^{TR})$ codes for w uniformly distributed in $[1, 2, \ldots, 2^{TR}]$ such that the error probability at the intended receiver vanishes and the equivocation rate $\frac{1}{T}H(w|\mathbf{z})$ approaches $\frac{1}{T}H(w)$. Moreover, the secrecy capacity, the supremum of the secrecy rates, of the block frequency selective channel (1) in bps per dimension is given by [7]

$$C = \frac{1}{N+L} \max_{p_u, p_{x|u}} I(\mathbf{u}; \mathbf{y}) - I(\mathbf{u}; \mathbf{z}) \tag{3}$$

for some auxiliary random variable $\mathbf{u}$ satisfying the Markov chain $\mathbf{u} \rightarrow \mathbf{x} \rightarrow (\mathbf{y}, \mathbf{z})$.

2.3. Equivalent MIMO block fading

The frequency-selective wiretap channel (1) is a special case of the MIMO flat-fading wiretap channel with $N+L$ transmit antennas, N receive antennas at the eavesdropper, N antenna at the legitime receiver. It has been proved in [8][9][10] that the MIMO secrecy capacity channel per transmit antenna is given by

$$\max_{\mathbf{S}:\mathrm{tr}(\mathbf{S}) \leq (N+L)P} \frac{1}{N+L} (\log|\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^H| - \log|\mathbf{I} + \mathbf{G}\mathbf{S}\mathbf{G}^H|) \tag{4}$$

where $\mathbf{x}_t \sim \mathcal{N}_{\mathcal{C}}(\mathbf{0}, \mathbf{S})$. Interestingly, the structure of the optimal solution is such as no information is transmitted along any direction where the eavesdropper observes a stronger signal than the intended receiver. In the high SNR regime (where all channels become comparable), the optimal solution imposes to send specifically on the null subspace of the eavesdropper channel [3]. The secrecy degree of freedom (pre-log of (4)) is given by the rank of $\mathbf{H}\mathbf{G}^{\perp}$ where $\mathbf{G}^{\perp}$ denotes the projection matrix onto the null space of $\mathbf{G}$. Unlike previous works, we focus in the next sections on the specific structure (Toeplitz) of the MIMO channel and provide a practical precoding that achieves in the high SNR regime the degrees of freedom of the MIMO secrecy capacity.

3. VANDERMONDE PRECODING

3.1. Perfect CSIT

First we consider the case where the transmitter knows perfectly both the legitime and eavesdropper channels. In order to achieve the linear scaling of the secrecy capacity, we design the precoder such that the transmitter sends in the orthogonal space of the eavesdropper's channel by satisfying

$$\mathcal{T}(\mathbf{g})\mathbf{x}_t = \mathbf{0}_N, \quad \forall t \tag{5}$$

This condition is always satisfied by forming $\mathbf{x}_t$ such that

$$\mathbf{x}_t = \mathbf{V}_g \mathbf{u}_t \tag{6}$$

where $\mathbf{u}_t \in \mathbb{C}^L$ is the symbol vector with covariance $\mathbf{\Phi}$, $\mathbf{V}_g$ is a $(N+L) \times L$ Vandermonde matrix given by

$$\mathbf{V}_g = \begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_L \\ a_1^2 & \cdots & a_L^2 \\ \vdots & \ddots & \vdots \\ a_1^{N+L-1} & \cdots & a_L^{N+L-1} \end{bmatrix} \tag{7}$$

where $\{a_l, \ldots, a_L\}$ are the roots of the polynomial $S(z) = \sum_{i=0}^{L} g_i z^{L-i}$ with $L+1$ coefficients of the eavesdropper's channel $\mathbf{g}$. For later use we let $\mathbf{v}_{g,i}$ denote the i-th column of $\mathbf{V}_g$. It follows immediately that the Vandermonde precoding is one deterministic way of mapping the random symbol vector $\mathbf{u}$ to the transmit vector $\mathbf{x}$ in (3). The power constraint is replaced by

$$\mathrm{tr}(\mathbf{V}_g \mathbf{\Phi} \mathbf{V}_g^H) \leq P \tag{8}$$

The orthogonality between the Vandermonde matrix and the eavesdropper's channel yields

$$I(\mathbf{u}; \mathbf{z}) = \log |\mathbf{I} + \mathcal{T}(\mathbf{g}) \mathbf{V}_g \mathbf{\Phi} \mathbf{V}_g^H \mathcal{T}(\mathbf{g})^H| = 0 \tag{9}$$

as if the eavesdropper channel did not exist. The secrecy capacity of the frequency selective channel (1) with Vandermonde precoding reduces to

$$C_v = \frac{1}{N+L} \max_{\mathrm{tr}(\mathbf{V}_g \mathbf{\Phi} \mathbf{V}_g^H) \leq (N+L)P} \log |\mathbf{I} + \mathbf{H} \mathbf{\Phi} \mathbf{H}^H| \tag{10}$$

where we defined $\mathbf{H} = \mathcal{T}(\mathbf{h}) \mathbf{V}_g \in \mathbb{C}^{N \times L}$. Although the above secrecy capacity concave in $\mathbf{\Phi}$ can be optimized explicitly, here we restrict ourselves to a diagonal input covariance. This is sufficient to achieve the multiplexing gain offered by the channel, as we will see below. In particular, we consider the power allocation $\mathbf{\Phi} = \mathrm{diag}(p_1, \ldots, p_L)$ that equalizes

$$p_i \alpha_i = \frac{(N+L)P}{L}, \quad i = 1, \ldots, L \tag{11}$$

where we let $\alpha_i = ||\mathbf{v}_{g,i}||^2$.

Lemma 1 The secrecy capacity of Vandermonde precoding with the equalized power allocation (11) achieves the multiplexing gain of $\frac{L}{N+L}$.

Sketch of the proof The achievable secrecy capacity with Vandermonde precoding with the power allocation (11) is given by

$$\begin{aligned} C_v(P) &\overset{(a)}{=} \frac{1}{N+L} \log \left| \mathbf{I}_N + \frac{(N+L)P}{L} \mathbf{H} \mathbf{D} \mathbf{H}^H \right| \\ &\overset{(b)}{=} \frac{1}{N+L} \log \left| \mathbf{I}_L + \frac{(N+L)P}{L} \mathcal{T}(\mathbf{h}) \tilde{\mathbf{V}}_g \tilde{\mathbf{V}}_g^H \mathcal{T}(\mathbf{h})^H \right| \\ &= \frac{1}{N+L} \log \left| \mathbf{I}_L + \frac{(N+L)P}{L} \mathcal{T}(\mathbf{h}) \mathcal{T}(\mathbf{h})^H \tilde{\mathbf{V}}_g^H \tilde{\mathbf{V}}_g \right| \\ &\overset{(c)}{=} \frac{L}{N+L} \log P + O(1) \end{aligned}$$

where in (a) we define $\mathbf{D} = \mathrm{diag}\left(\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_L}\right)$, (b) follows by letting $\tilde{\mathbf{V}}_g = \mathbf{V}_g \mathbf{D}^{1/2}$, a scaled Vandermonde matrix whose columns are all unit-norm, (c) follows from

$$\mathrm{rank}(\mathcal{T}(\mathbf{h}) \mathcal{T}(\mathbf{h})^H \mathbf{V}_g^H \mathbf{V}_g) = \mathrm{rank}(\mathbf{V}_g^H \mathbf{V}_g) = L$$

by noticing that $\mathcal{T}(\mathbf{h}) \mathcal{T}(\mathbf{h})^H$ is invertible (since all the columns of the Vandermonde matrix are linearly independent[2]). The last expression shows that the secrecy capacity with the Vandermonde precoding achieves $\frac{L}{N+L}$ degrees of freedom. □

In order to enhance the performance, we can replace the equalized power allocation (11) by the following waterfilling power allocation. Apply singular value decomposition so that

$$\mathbf{H} = \mathbf{U}_h \mathbf{\Lambda}_h \mathbf{P}_h^H$$

where $\mathbf{U}_h \in \mathbb{C}^{N \times N}, \mathbf{P}_h \in \mathbb{C}^{L \times L}$ are unitary matrices and $\mathbf{\Lambda}_h \in \mathbb{C}^{N \times L}$ contains r singular values $\{\lambda_{hi}^{1/2}\}$. Then, the i-th diagonal element is given by

$$p_i = \left[\frac{\mu}{\alpha_i} - \frac{1}{\lambda_{hi}} \right]_+ \tag{12}$$

where μ is determined so as to satisfy the total power constraint $\sum_{i=1}^{r} \alpha_i p_i = (N+L)P$. It is not difficult to see that if $\frac{\alpha_1}{\lambda_{h1}} = \cdots = \frac{\alpha_L}{\lambda_{hL}}$ the waterfilling power allocation coincides with the equalized allocation (11).

3.2. Partial CSIT

We now consider a more realistic scenario where the transmitter only knows the legitimate channel $\mathbf{h}$. We apply the mask beamforming scheme originally proposed by [11] and analyzed in [3]. Let us form the transmit vector $\mathbf{x} \in \mathbb{C}^{N+L}$ such as

$$\mathbf{x} = [\tilde{\mathbf{V}}_h | \mathbf{Q}] \begin{bmatrix} \boldsymbol{\eta} \\ \mathbf{u} \end{bmatrix} \tag{13}$$

where $\mathbf{V}_h \in \mathbb{C}^{(N+L) \times L}$ is the normalized Vandermonde matrix that nulls the roots of $\mathbf{h}$ with unit-norm columns, $\mathbf{Q} \in \mathbb{C}^{(N+L) \times N}$ is unitary matrix obtained by the compact singular value decomposition of $\mathcal{T}(\mathbf{h}) = \mathbf{U}' \mathbf{\Lambda} \mathbf{Q}^H$ such that $\mathbf{Q}^H \mathbf{Q} = \mathbf{I}$, $\boldsymbol{\eta} \sim \mathcal{N}_{\mathcal{C}}(\mathbf{0}, P\mathbf{I}_L)$ is noise, $\mathbf{u} \sim \mathcal{N}_{\mathcal{C}}(\mathbf{0}, P\mathbf{I}_N)$ is the symbol vector. Notice that the precoding matrix $\tilde{\mathbf{V}}_h$ for the artificial noise can be replaced by any matrix that is orthogonal to $\mathcal{T}(\mathbf{h})$, for example by a unitary matrix orthogonal to $\mathbf{Q}$ as considered in [3]. The received signals are given by

$$\mathbf{y} = \mathcal{T}(\mathbf{h}) \mathbf{Q} \mathbf{u} + \mathbf{n} \tag{14}$$

$$\mathbf{z} = \mathcal{T}(\mathbf{g}) \mathbf{Q} \mathbf{u} + \mathcal{T}(\mathbf{g}) \tilde{\mathbf{V}}_h \boldsymbol{\eta} + \boldsymbol{\nu} \tag{15}$$

[2] $\mathrm{rank}(AB) = \mathrm{rank}(B)$ if A is invertible

The secrecy capacity achieved by the mask beamforming is given by

$$C_{\rm mb}(P) = \frac{1}{N+L}\left(\log|\mathbf{I}_N + P\mathcal{T}(\mathbf{h})\mathcal{T}(\mathbf{h})^H| - C_{\rm mb}^{\rm residual}(P)\right) \quad (16)$$

where $C_{\rm mb}^{\rm residual}(P)$ is given by

$$\begin{aligned} C_{\rm mb}^{\rm residual}(P) &= \log\frac{|\mathbf{\Sigma}(P) + P\mathcal{T}(\mathbf{g})\mathbf{Q}\mathbf{Q}^H\mathcal{T}(\mathbf{g})^H|}{|\mathbf{\Sigma}(P)|} \\ &= \log|\mathbf{I}_N + P\mathbf{\Sigma}^{-1}(P)\mathcal{T}(\mathbf{g})\mathbf{Q}\mathbf{Q}^H\mathcal{T}(\mathbf{g})^H| \end{aligned}$$

and we define the covariance of the overall noise seen by the eavesdropper

$$\mathbf{\Sigma}(P) = \mathbf{I}_N + P\mathcal{T}(\mathbf{g})\tilde{\mathbf{V}}_h\tilde{\mathbf{V}}_h^H\mathcal{T}(\mathbf{g})^H.$$

Lemma 2 The secrecy capacity of the mask beamforming achieves the multiplexing gain $\frac{L}{N+L}$.

Sketch of the proof We show that the first term in (16) scales as $N\log(P)$ in the high SNR regime. This can be easily seen by noticing that $\mathcal{T}(\mathbf{h})$ has a rank N, i.e.

$$\log|\mathbf{I}_N + P\mathcal{T}(\mathbf{h})\mathcal{T}(\mathbf{h})^H| = \sum_{i=1}^{N}\log(1+P\lambda_i^h) \quad (17)$$

where λ_i^h are the N non-zero eigenvalues of $\mathcal{T}(\mathbf{h})\mathcal{T}(\mathbf{h})^H$. Next, we consider the scaling of $C_{\rm mb}^{\rm residual}(P)$ as $P\to\infty$. Let $\mathcal{T}(\mathbf{g})\tilde{\mathbf{V}}_h\tilde{\mathbf{V}}_h^H\mathcal{T}(\mathbf{g})^H = \mathbf{U}\Lambda^v\mathbf{U}^H$ where Λ^v contains L eigen values of $\{\lambda_l^v\}$. In this case,

$$\begin{aligned} C_{\rm mb}^{\rm residual}(P) &= \log|\mathbf{I} + P\mathbf{\Sigma}(P)^{-1}\mathcal{T}(\mathbf{g})\mathbf{Q}\mathbf{Q}^H\mathcal{T}(\mathbf{g})^H| \\ &= \log|\mathbf{I} + \mathbf{D}^v(P)\mathcal{T}(\mathbf{g})\mathbf{Q}\mathbf{Q}^H\mathcal{T}(\mathbf{g})^H| \quad (18) \end{aligned}$$

with $\mathbf{D}^v(P) = \text{diag}([P,...P,\frac{P}{1+P\lambda_1^v},...,\frac{P}{1+P\lambda_L^v}])$. In the high SNR regime, the term (18) scales as $(N-L)\log(P)$ whereas (17) scales as $N\log(P)$. The secrecy capacity of the make beamforming scales therefore as $\frac{L}{N+L}\log(P)$, the same as the perfect CSI case. □

4. NUMERICAL EXAMPLES

In this section, we evaluate the secrecy capacity of the proposed Vandermonde precoding as well as the mask beamforming.

For the sake of comparison, we first consider the special case of the MISO wiretap channel where the intended receiver receives a scalar observation while the eavesdropper has N observations. We average the capacity over a large number of randomly generated channels with $N=64$ and $L=16$. In Fig. 2, we compare the secrecy capacity with the Vandermonde precoding, the mask beamforming, and the optimal beamforming strategy [8] as a function of P. We observe that all strategies achieve the same multiplexing gain of $\frac{1}{N+L}$. In fact, the MISO secrecy capacity is given by

$$\frac{1}{N+L}\log\left(1+(N+L)P\max_{\boldsymbol{\phi}:\mathcal{T}(\mathbf{g})\boldsymbol{\phi}=\mathbf{0}}|\mathbf{h}_1^H\boldsymbol{\phi}|^2\right) \quad (19)$$

where $\mathbf{h}_1^H$ denotes the first row of $\mathcal{T}(\mathbf{h})$, while the Vandermonde precoding achieves

$$\frac{1}{N+L}\log(1+(N+L)P\max_l|\mathbf{h}_1^H\mathbf{v}_{g,l}|^2). \quad (20)$$

Clearly, there exists a constant gap between (19) and (20) due to the suboptimal choice of beamforming vector. With the mask beamforming that sends one symbol and $N+L-1$ artificial noise under the MISO setting, it is not difficult to see that $(N+L)C_{\rm mb}(P)$ in the high SNR regime reduces to

$$\left(\log(1+||\mathbf{h}_1||^2P) - \log\left|\mathbf{I} + \frac{1}{||\mathbf{h}_1||^2}\mathbf{\Lambda}^{-1}\mathcal{T}(\mathbf{g})\mathbf{h}_1\mathbf{h}_1^H\mathcal{T}(\mathbf{g})^H\right|\right)$$

where $\mathbf{\Lambda}$ is a diagonal matrix related to the N eigenvalues of $\mathcal{T}(\mathbf{g})\mathbf{Q}'\mathbf{Q}'^H\mathcal{T}(\mathbf{g})$ where $\mathbf{Q}'$ is the unitary matrix orthogonal to $\mathbf{h}_1$.

Next, we consider the MIMO wiretap channel where the transmitter sends $N+L$ signals and both the intended receiver and the eavesdropper receive N observations. We compare the secrecy capacity of Vandermonde precoding (10) and that of the mask beamforming (16). For the Vandermonde precoding we consider both the equalized power (11) and the waterfilling power (12). Figs. 3, 4 show the secrecy capacity in bps/dimension achieved by these schemes for $N=L=64$, $N=64, L=16$ respectively. The latter parameter is inspired by the 802.11a where we aim at sending the confidential messages over a cyclic prefix. It can be remarked that both the Vandermonde precoding and the mask beamforming achieve the same slope in the high SNR regime. The mask beamforming performs closed to the Vandermonde precoding with equal power allocation especially for $N=L$. We observe also a non-negligible gain due to the watefilling power allocation for the Vandermonde precoding. The relative merit between these schemes is out of scope of this paper and remains as a future investigation.

These numerical examples show that the Vandermonde precoding as well as the mask beamforming are able to exploit the full degrees of freedom offered by the frequency-selective wiretap channel. The Vandermonde precoding with waterfilling power allocation yields a substantial gain with respect to the mask beamforming at the price of perfect channel knowledge at the transmitter.

Acknowledgment

The work of was supported partially by Alcatel-Lucent within the Alcatel-Lucent Chair on Flexible Radio at Supelec as

well as the European Commission in the framework of the FP7 Network of Excellence in Wireless COMmunications NEWCOM++.

5. REFERENCES

[1] Y. Liang, H.V. Poor, and S. Shamai, "Secure Communication over Fading Channels," *Arxiv preprint cs/0701024*, 2007.

[2] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel," *Arxiv preprint arXiv:0708.4219*, 2007.

[3] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," *Proc. ISIT'07, Nice, France*.

[4] L. Sampaio, M. Kobayashi, Ø. Ryan, and M. Debbah, "Vandermonde frequency division multiplexing for cognitive radio," *9th IEEE Workshop on Signal Processing Advances for Wireless Communications, Recife, Brazil*, 2008.

[5] A. Scaglione, GB Giannakis, and S. Barbarossa, "Lagrange/Vandermonde MUI eliminating user codes forquasi-synchronous CDMA in unknown multipath," *IEEE Trans. on Signal Process.*, vol. 48, no. 7, pp. 2057–2073, 2000.

[6] A. D Wyner, "The Wiretap Channel," *Bell. Syst. Tech. J.*, vol. 54, 1975.

[7] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inform. Theory*, vol. 24, 1978.

[8] A. Khisti and G. Wornell, "The MIMOME Channel," *Arxiv preprint arXiv:0710.1325*, 2007.

[9] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *Arxiv preprint arXiv:0710.1920*, 2007.

[10] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel," *Arxiv preprint arXiv:0710.4105*, 2007.

[11] R. Negi and S. Goel, "Secret communication using artificial noise," *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 3, 2005.

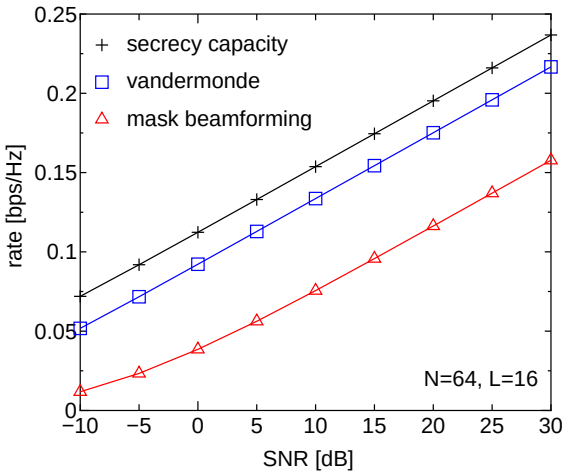

Fig. 2. MISO Secrecy capacity

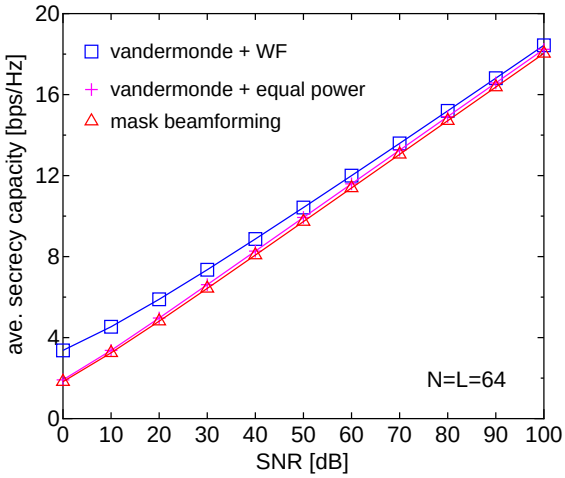

Fig. 3. MIMO Secrecy capacity with $N = L = 64$

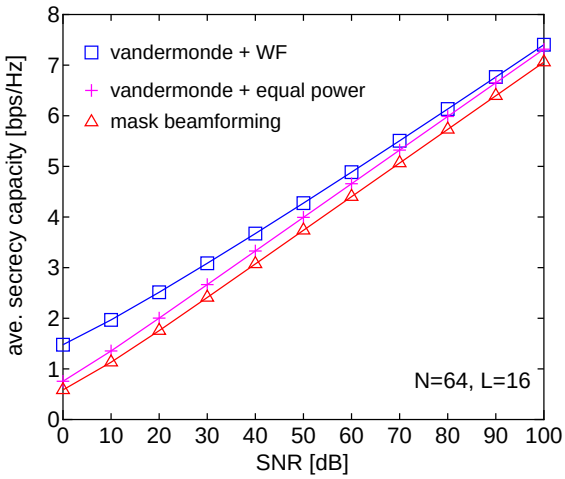

Fig. 4. MIMO Secrecy capacity with $N = 64, L = 16$