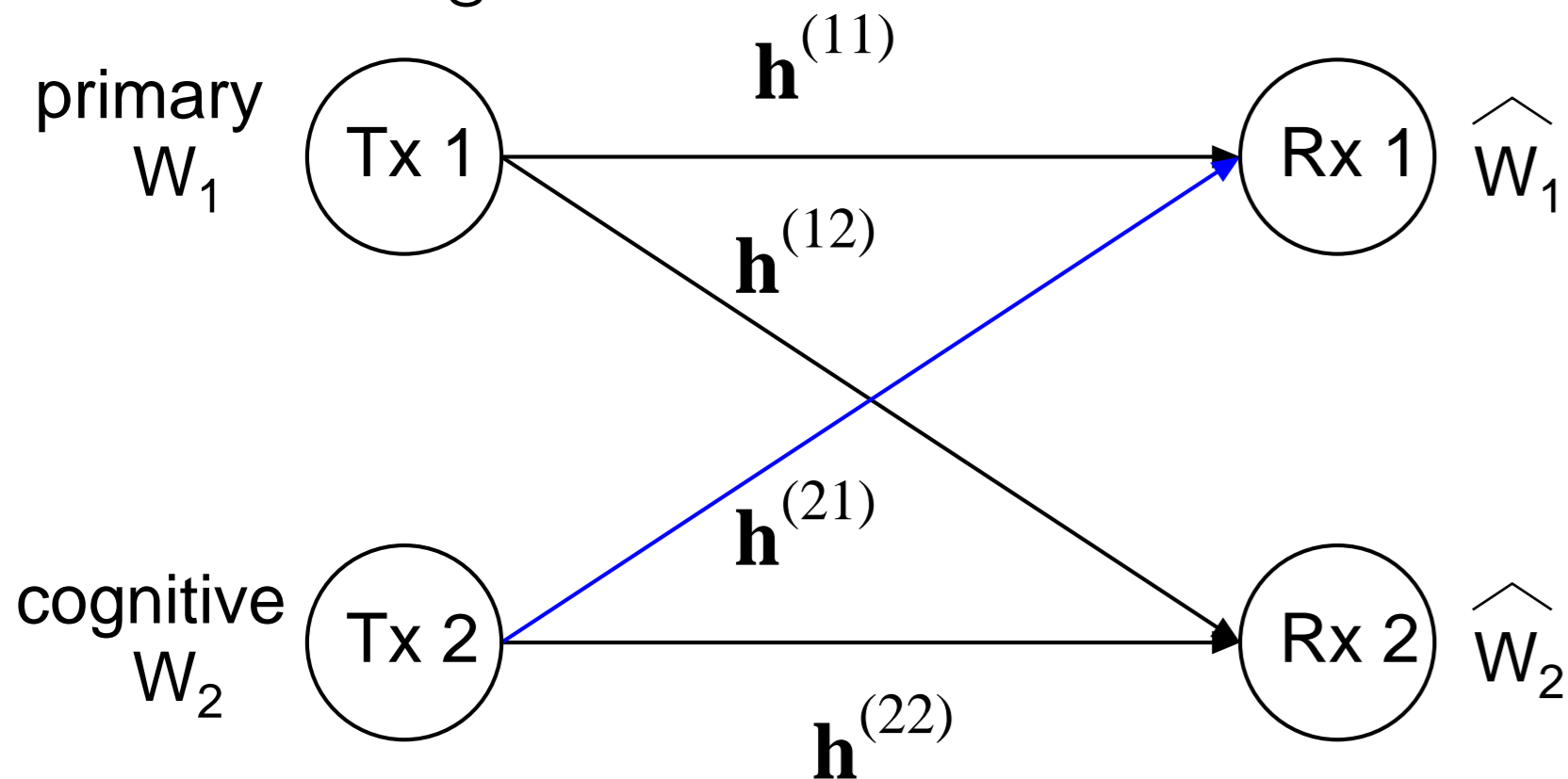


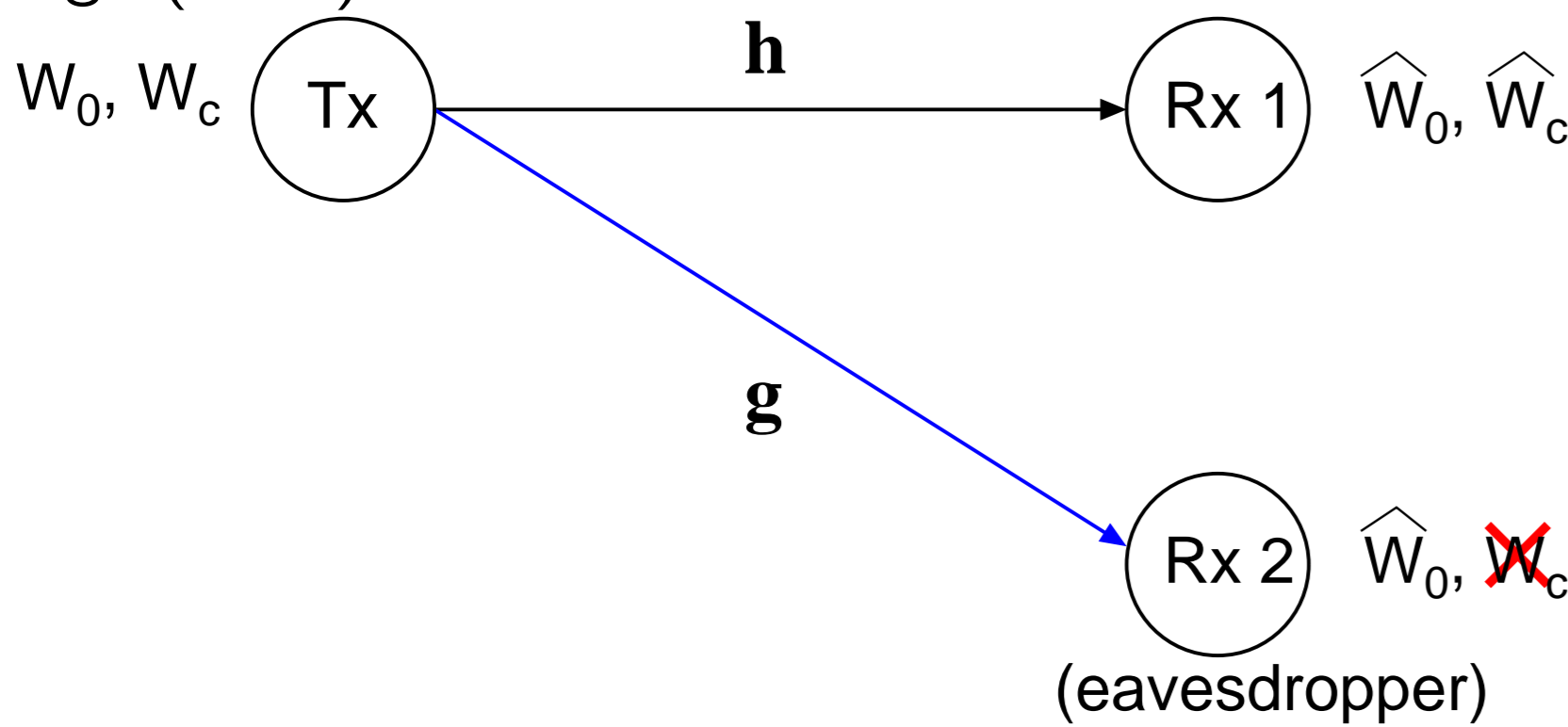
1 Introduction

- **Scenario 1:** cognitive interference channel



- Each transmitter k sends the message W_k to its receiver.
- The primary system is ignorant of the existence of the secondary one.
- Goal : create the cognitive signal transparent to the primary system

- **Scenario 2:** Broadcast channel with confidential message (BCC)



- Transmitter sends a confidential message W_c to Rx 1 and a common message W_0 .
- Goal : minimize the leakage of W_c at Rx 2 (eavesdropper).

- We propose a Vandermonde precoder that yields a practical solution to the two problems.

2 System Model

- Consider the $L+1$ -path frequency-selective fading channel relevant to current standards (WiMax, 802.11 a/g).
- Based on a block transmission of N symbols followed by a guard interval of L symbols, model the channel as a $N \times (N+L)$ Toeplitz matrix, i.e. $\mathcal{T}(\mathbf{h})$

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

- Assume local CSIT (e.g. Tx k knows $\mathbf{h}^{(k1)}$ and $\mathbf{h}^{(k2)}$) and perfect CSIR.
- **Scenario 1:** received signals in frequency domain after FFT operation \mathbf{F} are given by

$$\begin{aligned} \mathbf{r}_1 &= \mathbf{F}(\mathcal{T}(\mathbf{h}^{(11)})\mathbf{x}_1 + \mathcal{T}(\mathbf{h}^{(21)})\mathbf{x}_2 + \mathbf{v}'_1) \\ \mathbf{r}_2 &= \mathbf{F}(\mathcal{T}(\mathbf{h}^{(22)})\mathbf{x}_2 + \mathcal{T}(\mathbf{h}^{(12)})\mathbf{x}_1 + \mathbf{v}'_2) \end{aligned} \quad (1)$$

- $\mathbf{v}'_1, \mathbf{v}'_2$ are mutually independent AWGN (zero mean unit variance)
- power constraint : $\text{tr}(E[\mathbf{x}_k \mathbf{x}_k^H]) \leq (N+L)P_k$ for $k=1,2$.
- the primary system performs OFDM

$$\mathbf{x}_1 = \mathbf{A}\mathbf{F}^H \mathbf{s}_1$$

where \mathbf{A} is appending matrix, \mathbf{s}_1 is N symbol vector.
– The optimal strategy for the (MIMO) interference channel is a long-standing open problem. Some strategies are known when the cognitive transmitter knows perfectly W_1 (see e.g. [1, 2]).

- **Scenario 2:** the model reduces to a special MIMO wiretap channel

$$\begin{aligned} \mathbf{y} &= \mathcal{T}(\mathbf{h})\mathbf{x} + \mathbf{n}_1 \\ \mathbf{z} &= \mathcal{T}(\mathbf{g})\mathbf{x} + \mathbf{n}_2 \end{aligned} \quad (2)$$

- encoder maps W_0, W_c into Gaussian input $\mathbf{x} \sim \mathcal{N}(\mathbf{0}, \mathbf{S})$
- power constraint : $\text{tr}(\mathbf{S}) \leq (N+L)P$.

- The capacity region of the MIMO-BCC has been characterized [3] and given by

$$\begin{aligned} R_0 &\leq \frac{1}{N+L} \min \left\{ \log \frac{|\mathbf{I} + \mathcal{T}(\mathbf{h})\mathbf{S}\mathcal{T}(\mathbf{h})^H|}{|\mathbf{I} + \mathcal{T}(\mathbf{h})\mathbf{K}\mathcal{T}(\mathbf{h})^H|}, \log \frac{|\mathbf{I} + \mathcal{T}(\mathbf{g})\mathbf{S}\mathcal{T}(\mathbf{g})^H|}{|\mathbf{I} + \mathcal{T}(\mathbf{g})\mathbf{K}\mathcal{T}(\mathbf{g})^H|} \right\} \\ R_c &\leq \frac{1}{N+L} \log \frac{|\mathbf{I} + \mathcal{T}(\mathbf{h})\mathbf{K}\mathcal{T}(\mathbf{h})^H|}{|\mathbf{I} + \mathcal{T}(\mathbf{g})\mathbf{K}\mathcal{T}(\mathbf{g})^H|} \end{aligned} \quad (3)$$

for some $\mathbf{0} \leq \mathbf{K} \leq \mathbf{S}$.

The optimal strategy is generally unknown.

- For the special case of sending only W_c , the MIMO-BCC reduces to the MIMO wiretap channel whose secrecy capacity was characterized by [4, 5, 6].
- The degree of freedom (d.o.f.) region is defined

$$(r_0, r_c) \triangleq \lim_{P \rightarrow \infty} \left(\frac{R_0}{\log P}, \frac{R_c}{\log P} \right) \quad (4)$$

where the secrecy d.o.f. is $r_c = \text{rank}(\mathcal{T}(\mathbf{h})\mathcal{T}(\mathbf{g})^\perp)$ with $\mathcal{T}(\mathbf{g})^\perp$ is a projection matrix on a null space of $\mathcal{T}(\mathbf{g})$.

3 Vandermonde precoding

- Albeit suboptimal, a practical solution consists of nulling the signal seen by the unintended receiver, i.e.

$$\mathcal{T}(\mathbf{h}^{(21)})\tilde{\mathbf{V}} = \mathbf{0}, \quad \mathcal{T}(\mathbf{g})\tilde{\mathbf{V}} = \mathbf{0} \quad (5)$$

- One solution to (5) is given by the Vandermonde matrix

$$\tilde{\mathbf{V}} = \begin{bmatrix} 1 & \dots & 1 \\ a_1 & \dots & a_L \\ a_1^2 & \dots & a_L^2 \\ \vdots & \dots & \vdots \\ a_1^{N+L-1} & \dots & a_L^{N+L-1} \end{bmatrix} \quad (6)$$

where $\{a_1, \dots, a_L\}$ are the roots of the polynomial $S(z) = \sum_{i=0}^L h_i^{(21)} z^{L-i}$.

- In order to avoid a rank deficient behavior, consider a unitary Vandermonde matrix \mathbf{V} by orthogonalizing L columns of $\tilde{\mathbf{V}}$ such that $\mathbf{V}^H \mathbf{V} = \mathbf{I}_L$.

- **Scenario 1:** form the cognitive symbol $\mathbf{x}_2 = \mathbf{V}\mathbf{s}_2$. (2) can be rewritten as:

$$\begin{aligned} \mathbf{r}_1 &= \mathbf{H}_{\text{diag}}^{(11)} \mathbf{s}_1 + \mathbf{v}_1 \\ \mathbf{r}_2 &= \mathbf{F}\mathcal{T}(\mathbf{h}^{(22)})\mathbf{V}\mathbf{s}_2 + \underbrace{\mathbf{H}_{\text{diag}}^{(12)} \mathbf{s}_1}_{\boldsymbol{\eta}} + \mathbf{v}_2 \end{aligned} \quad (7)$$

The primary receiver “sees” N interference-free parallel channels.

- **Scenario 2:**

- form \mathbf{x} by Gaussian superposition coding

$$\mathbf{x} = \mathbf{V}_0 \mathbf{u}_0 + \mathbf{V}_c \mathbf{u}_c$$

where $\mathbf{u}_0 \in \mathbb{C}^{(N-L) \times 1}$, $\mathbf{u}_c \in \mathbb{C}^{L \times 1}$ denotes the vector of common, confidential messages for $l \leq L$.

- the received signals are

$$\begin{aligned} \mathbf{y} &= \mathcal{T}(\mathbf{h})\mathbf{V}_0 \mathbf{u}_0 + \mathcal{T}(\mathbf{h})\mathbf{V}_c \mathbf{u}_c + \mathbf{n}_1 \\ \mathbf{z} &= \mathcal{T}(\mathbf{g})\mathbf{V}_0 \mathbf{u}_0 + \mathbf{n}_2. \end{aligned} \quad (8)$$

The eavesdropper observes only the common message.

4 Achievable Rates

- **Scenario 1:** Assuming that the cognitive receiver treats the interference as noise, the following rate tuple (R_1, R_2) is achievable.

$$\begin{aligned} R_1 &\leq \frac{1}{N+L} \max_{\mathbf{p}_1} \sum_{n=1}^N \log(1 + |H_{\text{diag}}^{(11)}(n)|^2 p_{1,n}) \\ R_2 &\leq \frac{1}{N+L} \max_{\mathbf{S}} \log |\mathbf{I} + \boldsymbol{\Sigma}_\eta^{-1} \mathcal{T}(\mathbf{h}^{(22)})\mathbf{V}\mathbf{S}\mathbf{V}^H \mathcal{T}(\mathbf{h}^{(22)})^H| \end{aligned}$$

where $\boldsymbol{\Sigma}_\eta$ denotes the covariance of the noise plus interference given by

$$\boldsymbol{\Sigma}_\eta = \mathbf{H}_{\text{diag}}^{(12)} \text{diag}(\mathbf{p}_1) \mathbf{H}_{\text{diag}}^{(12)H} + \mathbf{I}$$

Both rates can be maximized by a classical waterfilling.

- **Scenario 2:** the rate-tuple (R_0, R_c) is achievable

$$\begin{aligned} R_0 &\leq \frac{1}{N+L} \min\{I(\mathbf{u}_0; \mathbf{y}), I(\mathbf{u}_0; \mathbf{z})\}, \\ R_c &\leq \frac{1}{N+L} \log |\mathbf{I}_N + \mathcal{T}(\mathbf{h})\mathbf{V}_c \mathbf{S}_c \mathbf{V}_c^H \mathcal{T}(\mathbf{h})^H| \end{aligned}$$

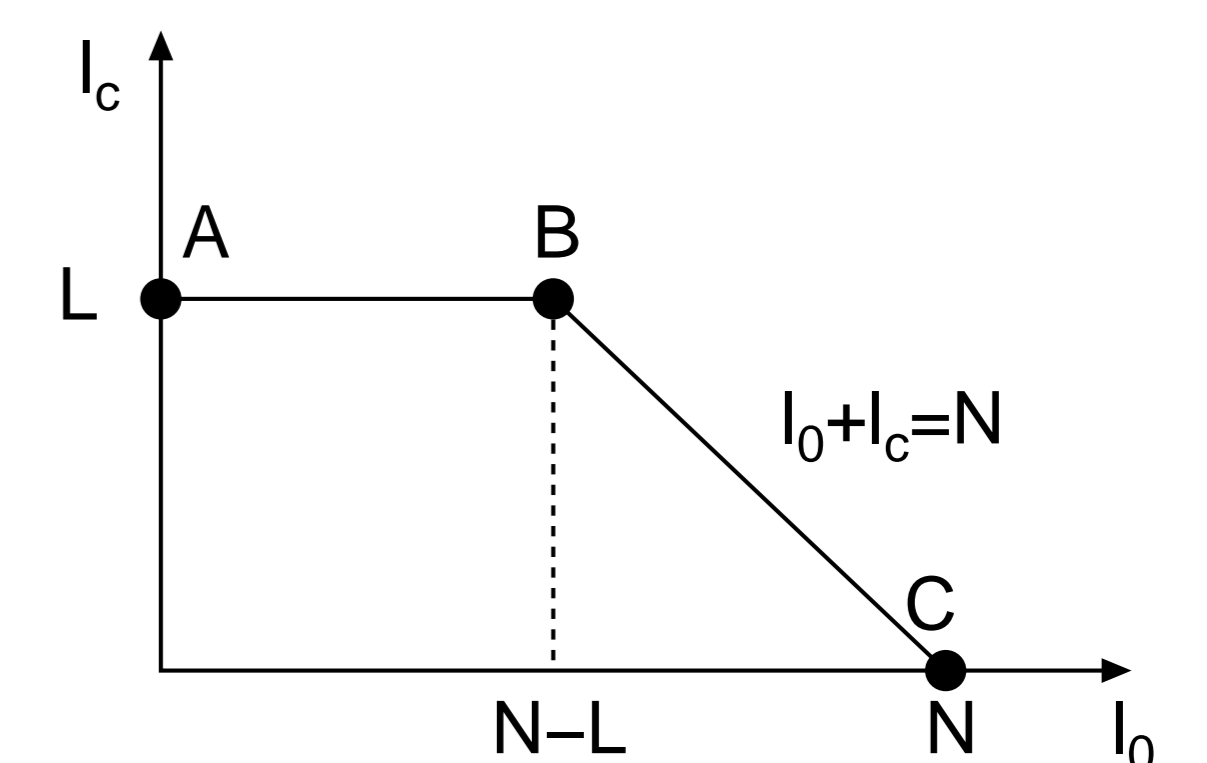
for $\text{tr}(\mathbf{S}_0 + \mathbf{S}_c) \leq P$, where

$$\begin{aligned} I(\mathbf{u}_0; \mathbf{y}) &= \log \frac{|\mathbf{I}_N + \mathcal{T}(\mathbf{h})\mathbf{V}_0 \mathbf{S}_0 \mathbf{V}_0^H \mathcal{T}(\mathbf{h})^H + \mathcal{T}(\mathbf{h})\mathbf{V}_c \mathbf{S}_c \mathbf{V}_c^H \mathcal{T}(\mathbf{h})^H|}{|\mathbf{I}_N + \mathcal{T}(\mathbf{h})\mathbf{V}_c \mathbf{S}_c \mathbf{V}_c^H \mathcal{T}(\mathbf{h})^H|} \\ I(\mathbf{u}_0; \mathbf{z}) &= \log |\mathbf{I}_N + \mathcal{T}(\mathbf{g})\mathbf{V}_0 \mathbf{S}_0 \mathbf{V}_0^H \mathcal{T}(\mathbf{g})^H| \end{aligned}$$

The characterization of $\mathbf{S}_0, \mathbf{S}_c$ is generally difficult except for some special cases of interest.

- secrecy rate R_c when sending only W_c
- maximum sum rate $R_0 + R_c$

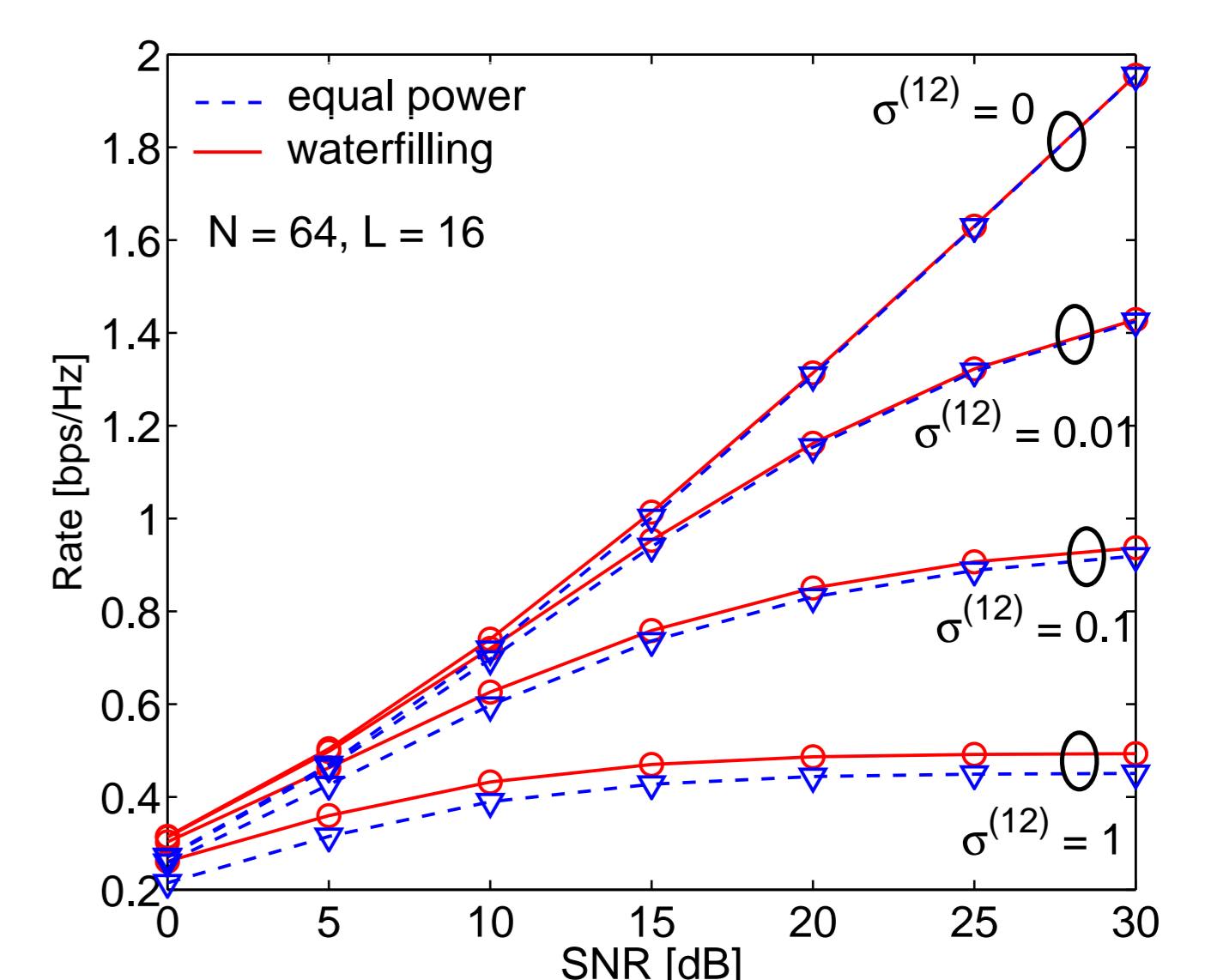
It can be shown that the Vandermonde precoder achieves the optimal d.o.f. region $(r_0, r_c) = \frac{1}{N+L}(l_0, l_c)$.



5 Numerical examples

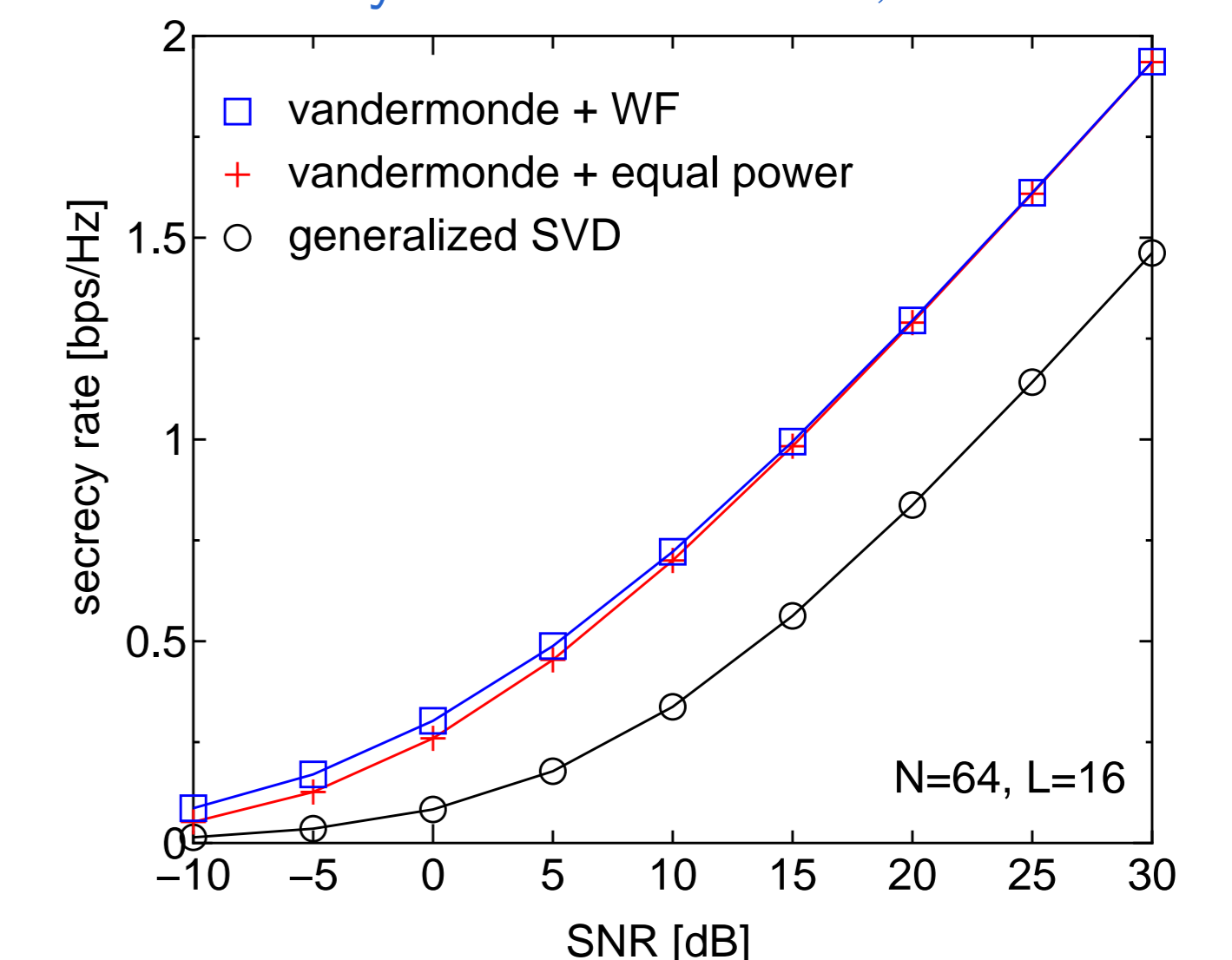
- **Scenario 1:**

Cognitive user's rate



- **Scenario 2:**

Secrecy rate with $N=64, L=16$



The applications to other multiuser scenarios can be found in [7].

References

- [1] N. Devroye, P. Mitran, and V. Tarokh, “Achievable rates in cognitive radio channels,” *IEEE Trans. on Inform. Theory*, vol. 52, no. 5, pp. 1813–1827, 2006.
- [2] Y. Liang, A. Simekh-Baruch, H.V. Poor, S. Shamai, and S. Verdú, “Cognitive Interference Channels with Confidential Messages,” *IEEE Trans. on Inform. Theory*, vol. 55, no. 2, February 2009.
- [3] Hung D. Ly, Tie Liu, and Yingbin Liang, “MIMO Broadcasting with Common, Private, and Confidential Messages,” in *ISITA'2008, New Zealand*, December 2008.
- [4] A. Khisti and G. Wornell, “The MIMOME Channel,” *the 45th Annual Allerton Conference on Communication, Control, and Computing*, also available on Arxiv preprint arXiv:0710.1325, October 2007.
- [5] F. Oggier and B. Hassibi, “The Secrecy Capacity of the MIMO Wiretap Channel,” *Arxiv preprint arXiv:0710.1920*, 2007.
- [6] T. Liu and S. Shamai, “A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel,” *Arxiv preprint arXiv:0710.4105*, 2007.
- [7] M. Kobayashi, M. Debbah, and S. Shamai (Shitz), “Secured communications over frequency-selective fading channels: A practical Vandermonde precoding,” *submitted to Eurasp, Special Issue on Wireless Physical Security*, November 2008.