Security and Sensitivity of Space Time Communications

Alfred O. Hero

Dept. EECS

University of Michigan - Ann Arbor

hero@eecs.umich.edu

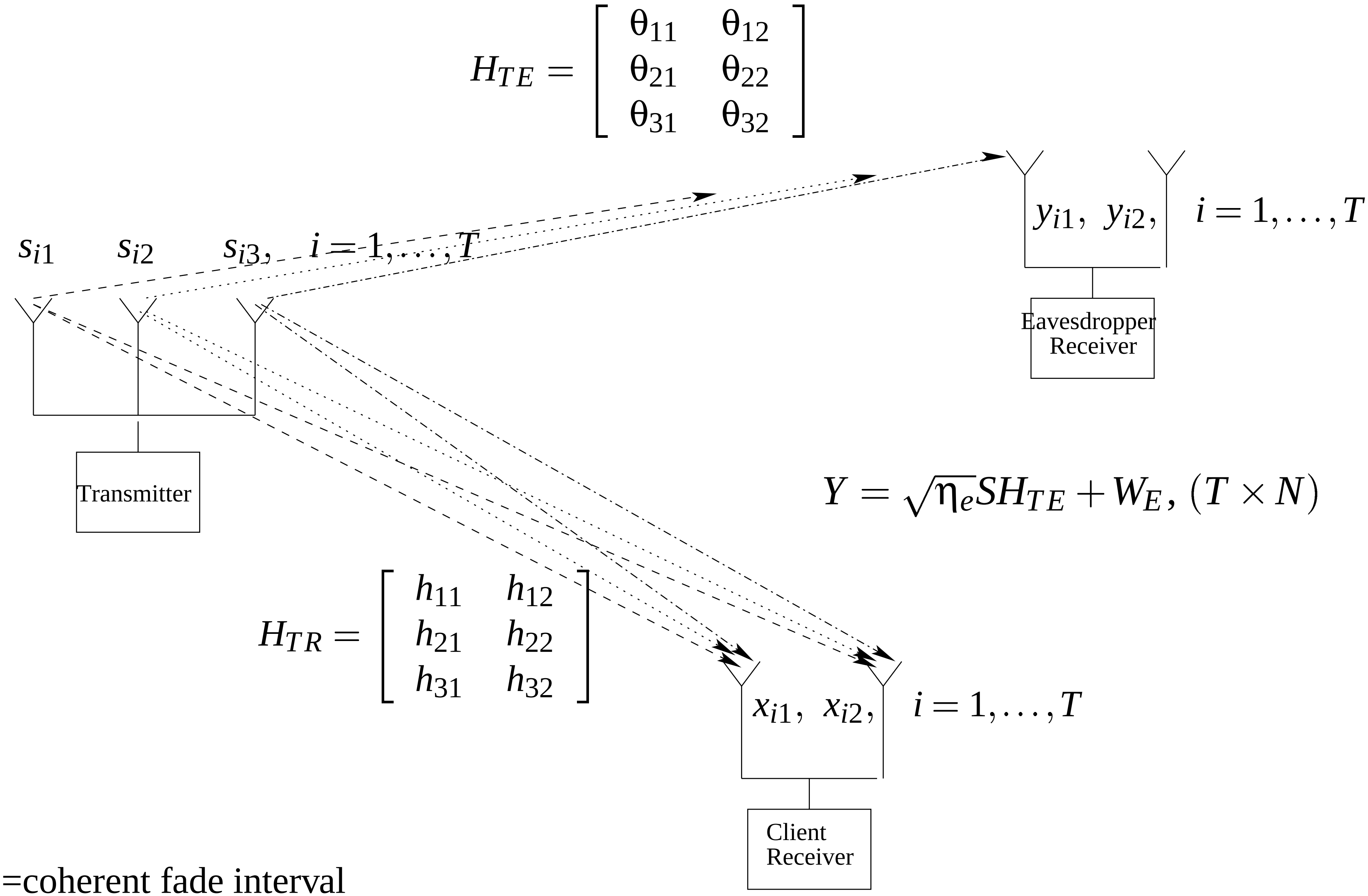
http://www.eecs.umich.edu/~hero

Collaborators:

D. Bliss (MIT-LL), K. Forsythe (MIT-LL), T. Marzetta (Lucent-BL), M. Godavarti (Altrabroadband, Inc)

Outline

1. Wireless network models
2. Performance metrics: capacity vs security
3. Information security: LPD/LPI-constraints
4. Environmental sensitivity



T=coherent fade interval
M=number of transmit antennas
N=number of receive antennas
η_r, η_e= receiver SNR's

$$X = \sqrt{\eta_r} S H_{TR} + W_R, \; (T \times N)$$

Receiver Model

Received signal in l-th frame $(t = 1, \ldots, T)$

$$[x_{t1}^l, \ldots, x_{tn}^l] = \sqrt{\eta}[s_{t1}^l, \ldots, s_{tm}^l] \begin{bmatrix} h_{11}^l & \cdots & h_{1n}^l \\ \vdots & \vdots & \vdots \\ h_{m1}^l & \cdots & h_{mn}^l \end{bmatrix} + [w_{t1}^l, \ldots, w_{tn}^l],$$

or, equivalently

$$X^l = \sqrt{\eta} S^l H^l + W^l$$

- X^l: $T \times N$ received signal matrices
- S^l: $T \times M$ transmitted signal matrices
- H^l: i.i.d. $M \times N$ channel matrices $\sim \mathcal{CN}(0, I_M \bigotimes I_N)$
- W^l: i.i.d. $T \times N$ noise matrices $\sim \mathcal{CN}(0, I_T \bigotimes I_N)$

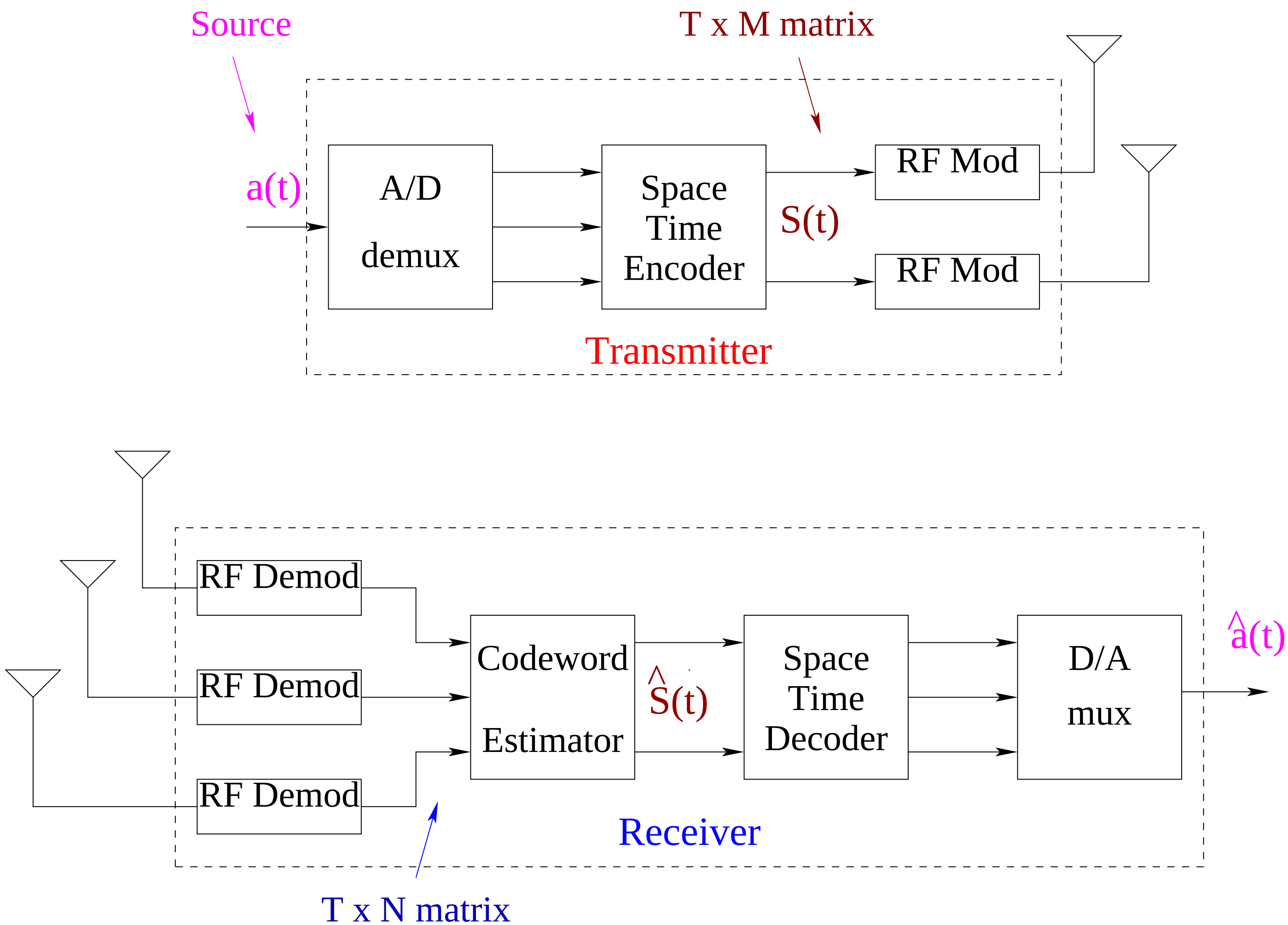


Figure 2. *Space-time transmitter/receiver.*

Space-Time Coding

- **Block coding**: string L codewords over L frames

$$| \; S^1 \; | \; S^2 \; | \; \cdots \; | \; S^L \; |$$

where S^l's are selected from a symbol alphabet $\mathcal{S} \subset \mathbb{C}^{T \times M}$

- **Random Block Coding**: coder generates S^l at random from $\mathcal{S}$ according to probability distribution $P(S) \in \mathcal{P}$.

  - Objective: Find optimal distribution $P(S)$ over $\mathcal{P}$ to:
    - maximize avg. information rate (achieve capacity)

$$C = \max_{P(S)} E[\ln P(X|S)/P(X)]$$

    - maximize sequentially-decodable rate (achieve cut-off rate)

$$R_o = \max_{P(S)} E[\exp\{-ND(S_1 \| S_2)\}]$$

  - Transmitter constraints: average power, peak power, other?

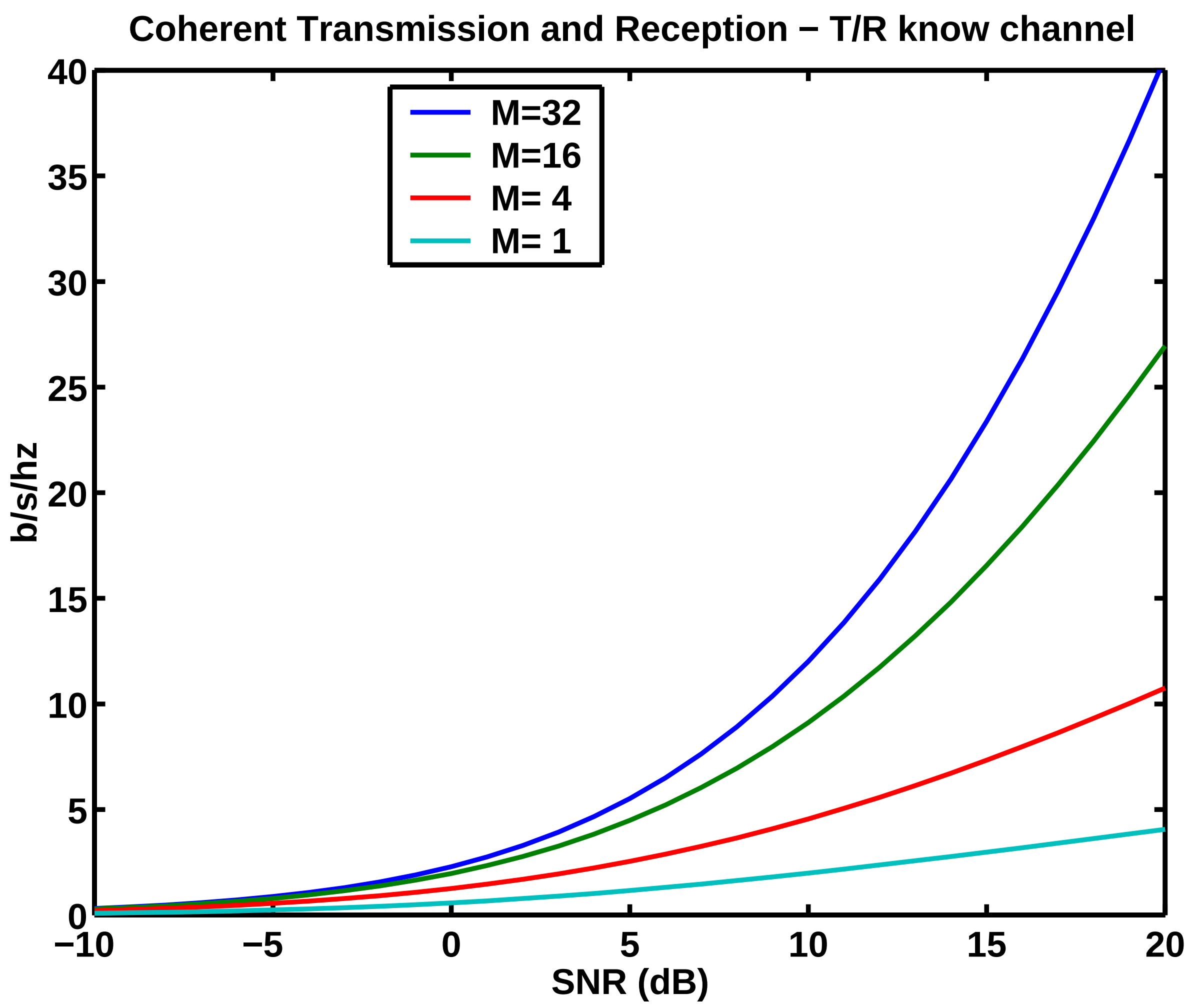


Figure 3. *Capacity for informed transmitter and receiver (IT-IR).*

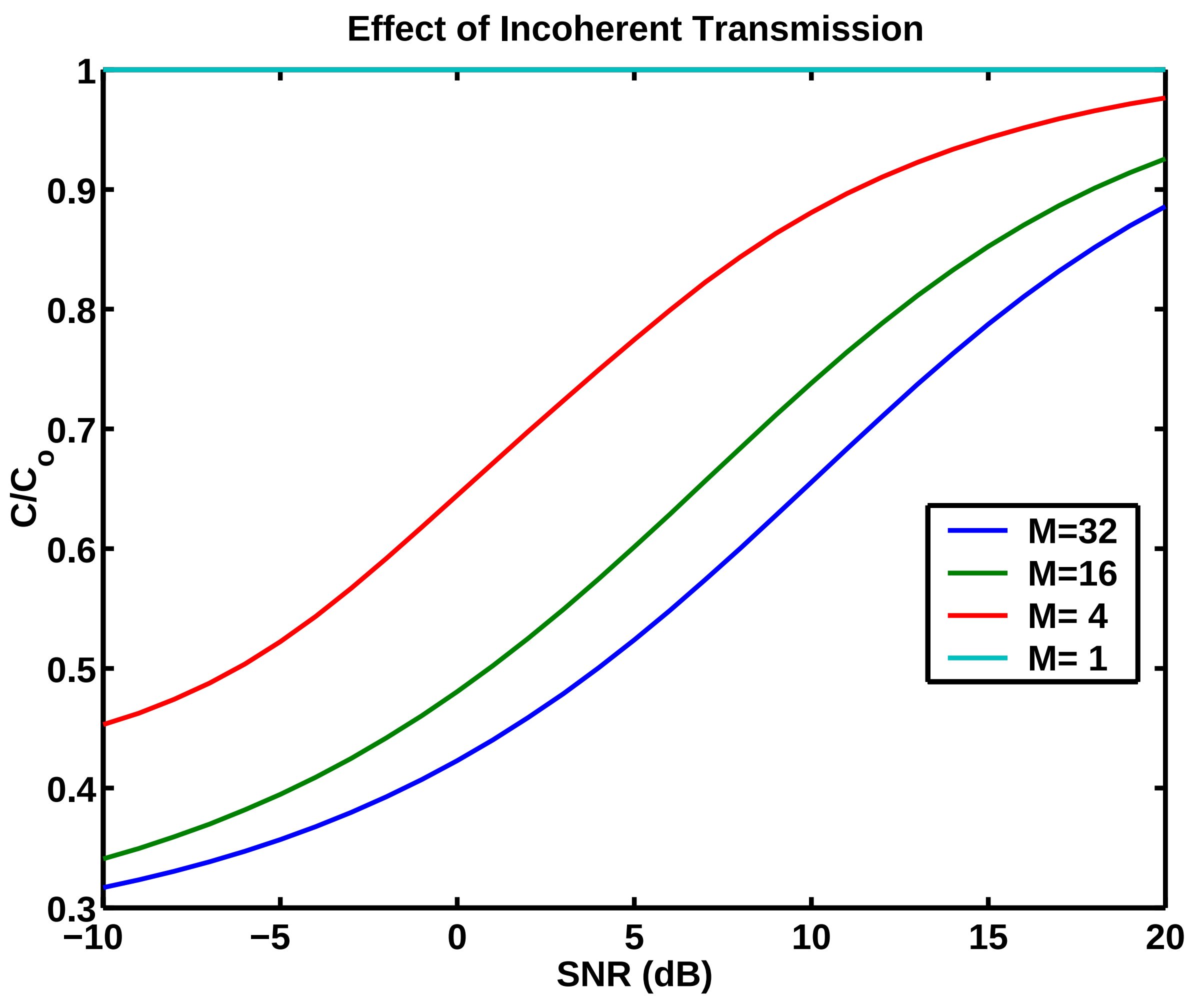


Figure 4. *Capacity loss due to uninformed transmission (UT-IR).*

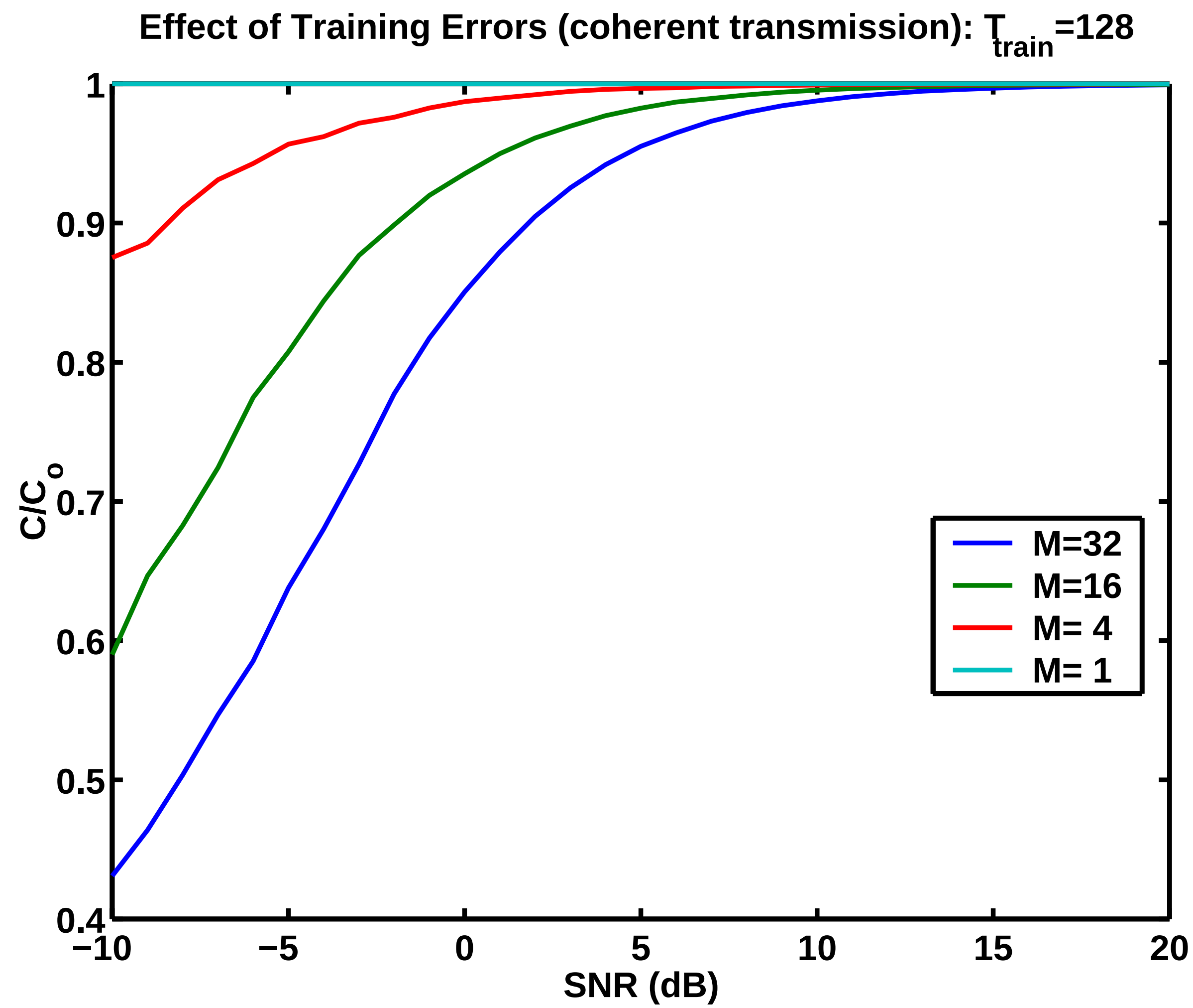


Figure 5. *Capacity loss due to T/R channel estimation errors.*

Link Capacity: avg power constraint: $\mathrm{tr}(E[SS^\dagger]) \leq P_o$

(1): Informed transmitter (IT) and informed receiver (IR) capacity:

$$\begin{aligned} C &= E\left[\sup_{P_S} \log P(X|S,H)/P(X|H)\right] \\ &= TE\left[\sup_{\Sigma:\mathrm{tr}\{\Sigma\}\leq P_o} \ln\left|I_N + \eta H \Sigma H^\dagger\right|\right] \\ &= TE\left[\ln\left|I_N + \eta H \Sigma_{\mathrm{pow}} H^\dagger\right|\right] = T\sum_i E\left[(\log \mu\lambda_i)^+\right] \end{aligned}$$

- Capacity achieving source $S \sim N\left(0,\, I_T \bigotimes \Sigma_{\mathrm{pow}}\right)$

$$\Sigma_{\mathrm{pow}} = UDU^\dagger, \qquad D = \mathrm{diag}\left((\mu - 1/\lambda_i)^+\right)$$

$$\lambda_i = \mathrm{eigs}\left(\eta H H^\dagger\right) \qquad \mu \,:\, \mathrm{tr}(\Sigma_{\mathrm{pow}}) = P_o$$

IT-IR Link

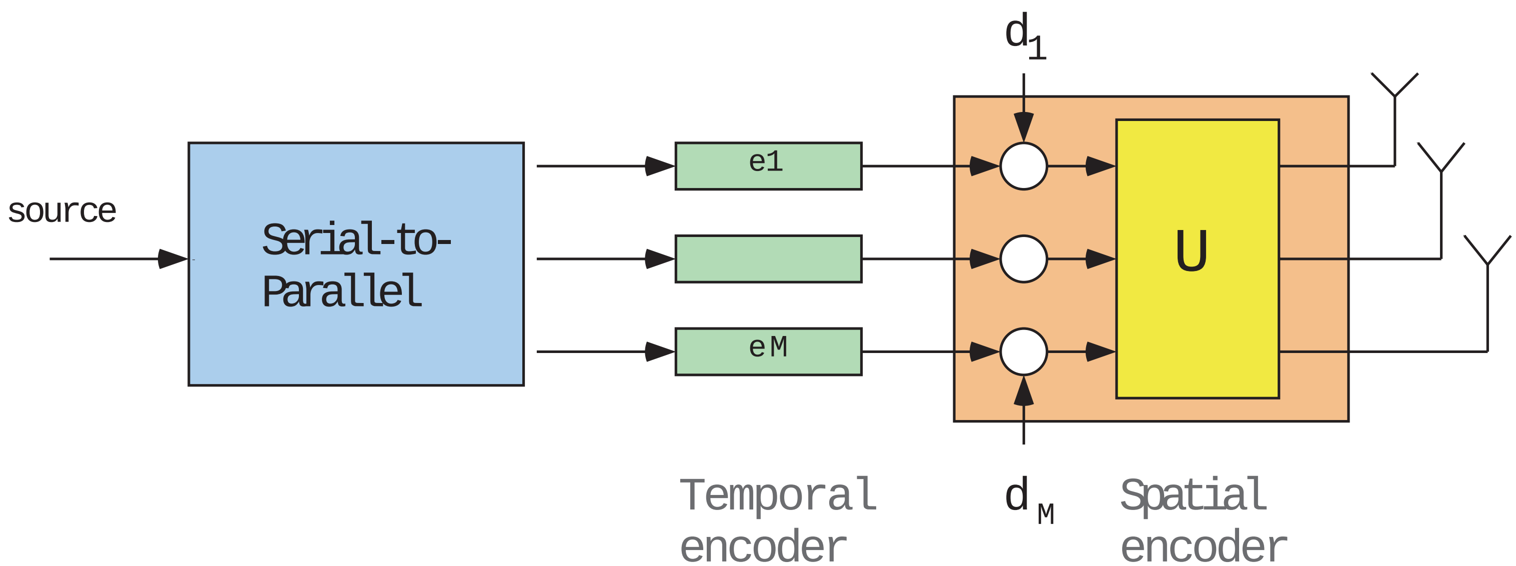


Figure 6. *Optimal STC for informed-transmitter informed-receiver*

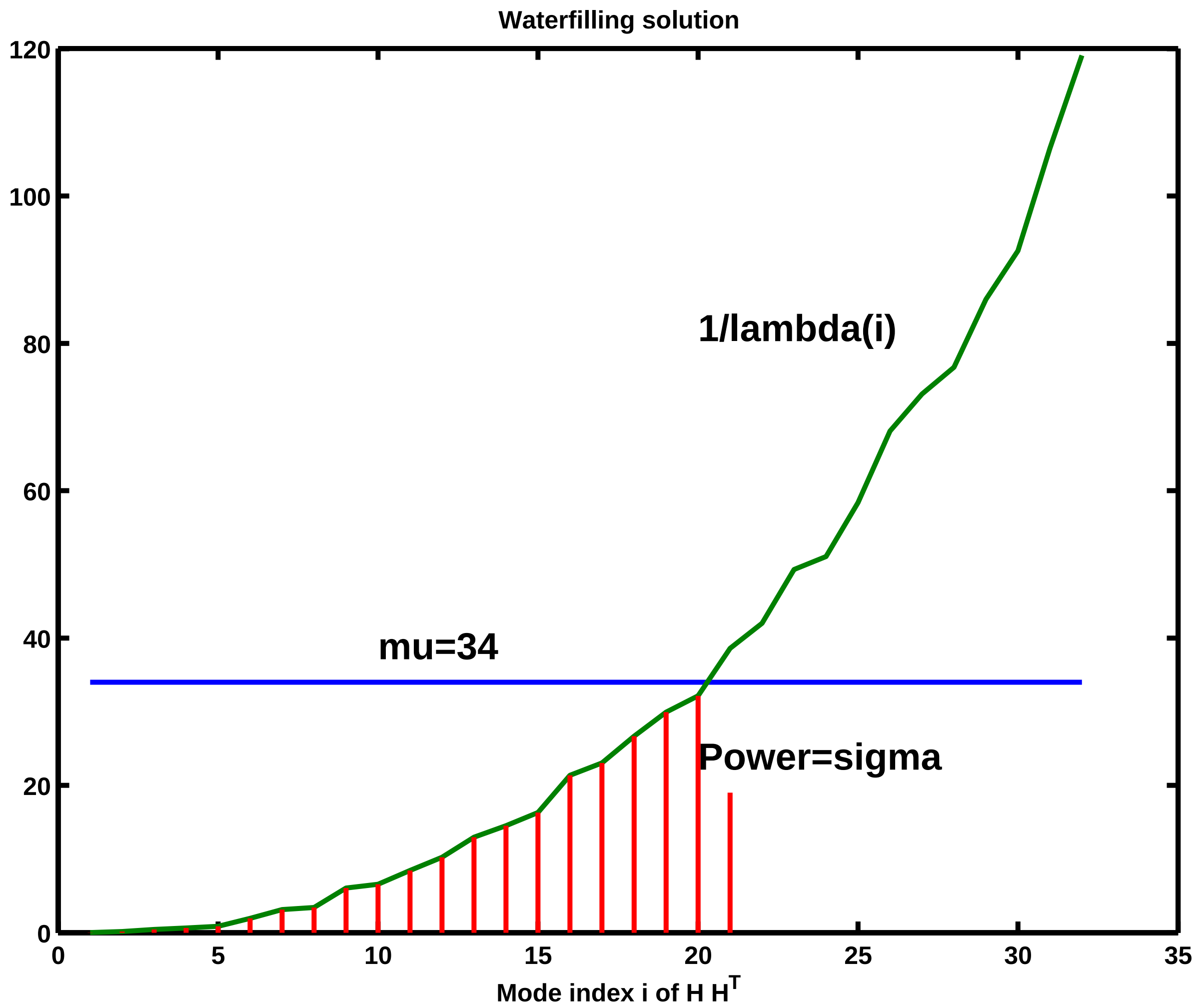


Figure 7. *Waterpouring solution for power-capacity achieving mode allocation($N = M = 32$)*

(2): Uninformed transmitter (UT) and IR capacity

$$\begin{aligned} C &= \sup_{P_S} E[\log P(X|S,H)/P(X|H)] \\ &= \sup_{\Sigma:\mathrm{tr}\{\Sigma\}\leq P_o} TE\left[\ln\left|I_N + \eta H\Sigma H^{\dagger}\right|\right] \\ &= TE\left[\ln\left|I_N + \eta' HH^{\dagger}\right|\right] \end{aligned}$$

where $\eta' = \eta P_o/M$

Capacity achieving source

$$S \sim N\left(0,\ cI_T \bigotimes I_M\right)$$

where $c = P_o/M$

UT-IR Link

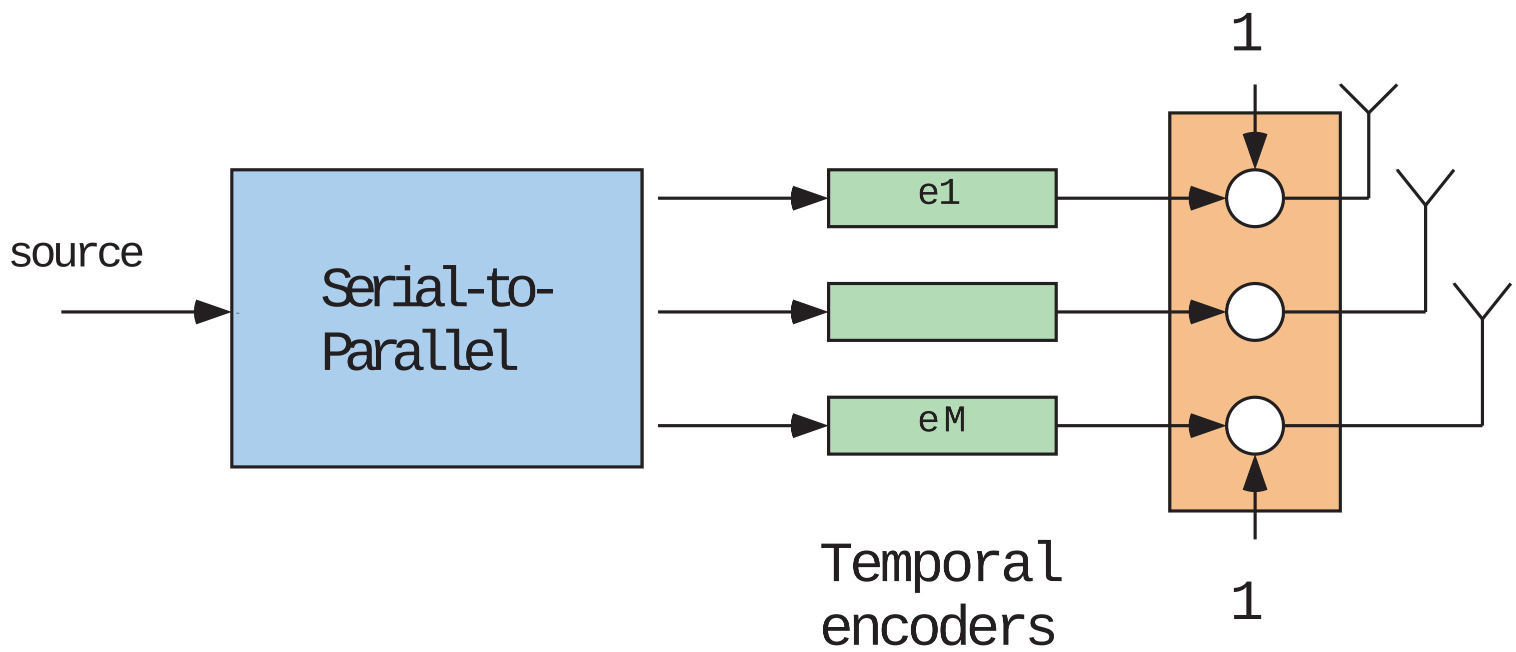


Figure 8. *Optimal STC for uninformed-transmitter informed-receiver*

(3): UT-UR: H unknown to either T/R

$$C_3 = \max_{P_S} E\left[\log P_{X|S}(X|S)/P_X(X)\right]$$

Capacity achieving source

$$S \sim V\Lambda$$

where

*Λ: non-negative $T \times M$ block-diagonal matrix

*V: unitary $T \times T$ matrix

*Λ and V independent

* $\Lambda^\dagger \Lambda = P_o$

UT-UR Link

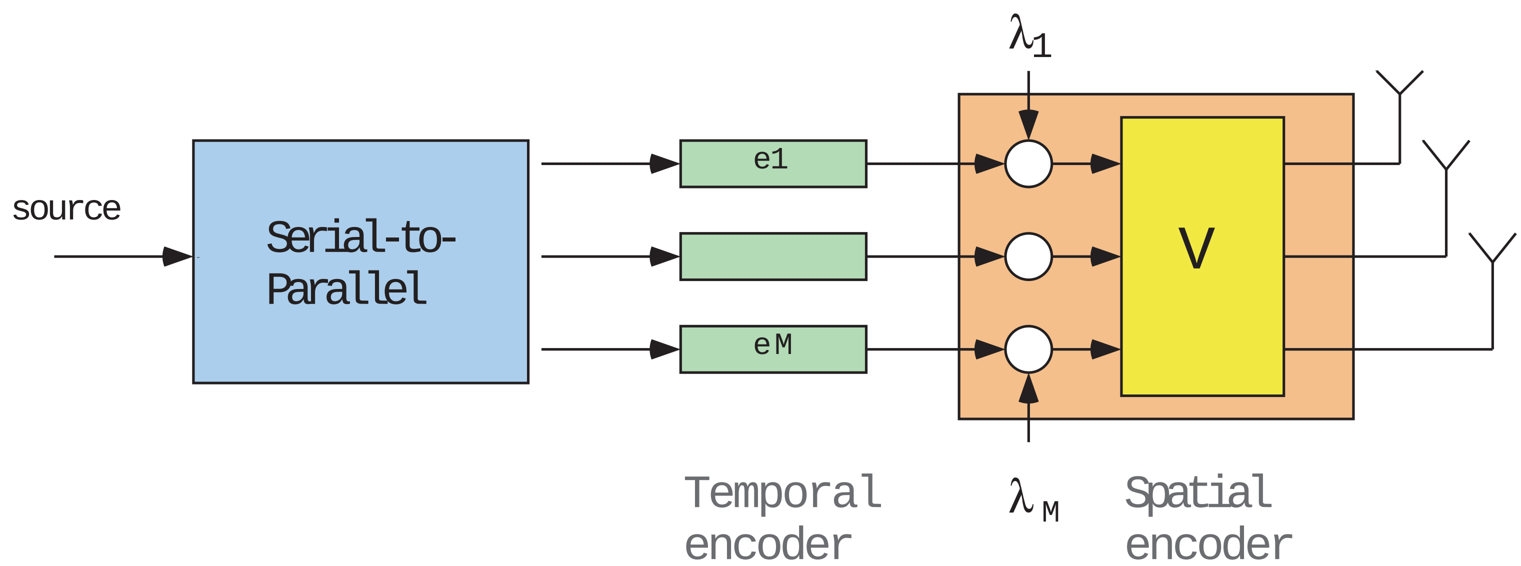


Figure 9. *Optimal STC for uninformed-transmitter uninformed-receiver*

Channel Sensitivity

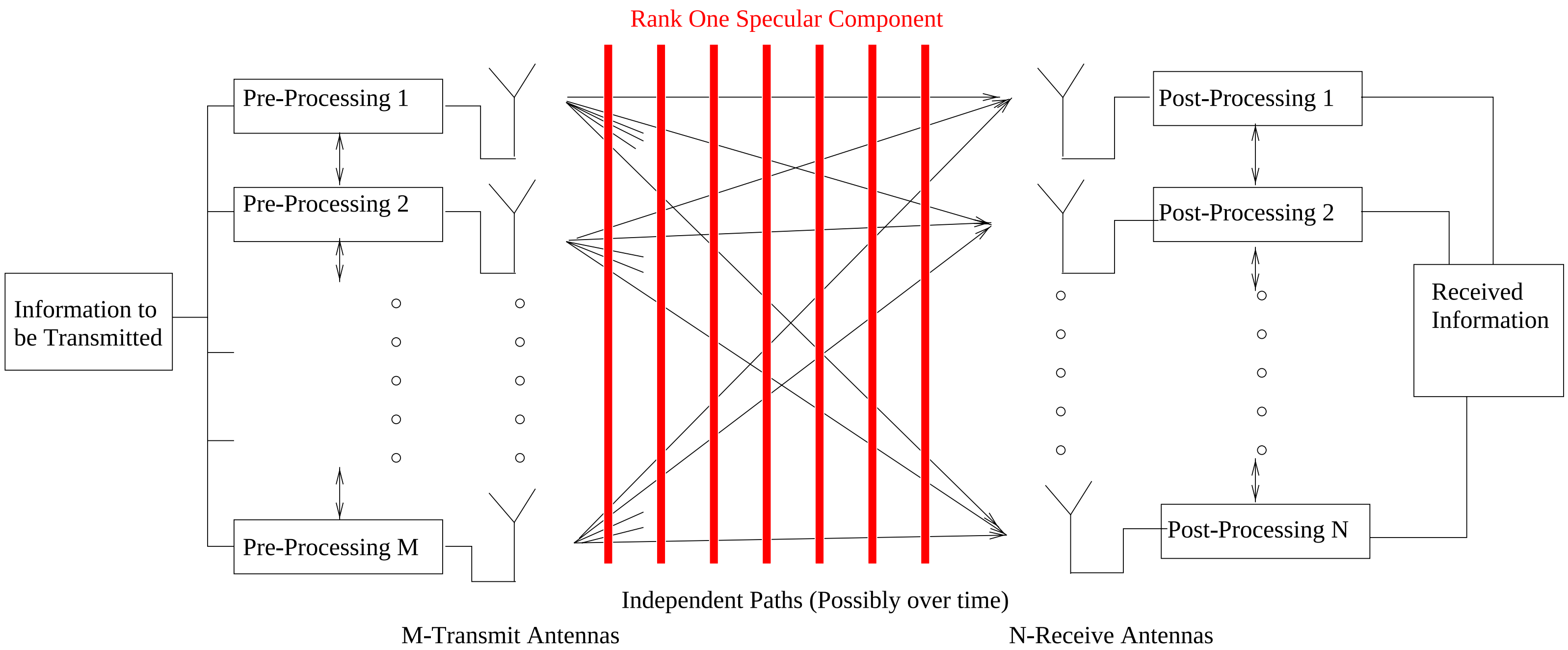


Figure 10. *Diagram of a multiple antenna communication system*

Rician Channel Model

- Combined Rayleigh and Specular Multipath Fading:

$$H = \sqrt{1-r}\, G + \sqrt{r}\, H_m$$

  - G_{mn} are i.i.d. $\mathcal{CN}(0,1)$
  - H_m deterministic matrix such that $\mathrm{tr}\{H_m H_m^\dagger\} = NM$
  - r fraction of channel energy devoted to specular component
  - H_m known to both the transmitter and receiver
  - G not known to the transmitter

- After unitary spatial transformation at T/R: $H_m = [D, 0]$

Rician Capacity: Rank one H_m known to T/R

$$H_m = \sqrt{NM}\, \underline{e}_M \underline{e}_N^T = \begin{bmatrix} \sqrt{NM} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{bmatrix}$$

UT-IR Capacity:

$$C_H = \max_{l,d} TE \log\det[I_N + \eta H \Lambda^{(l,d)} H^\dagger]$$

where

$$\Lambda^{(l,d)} = \begin{bmatrix} M-(M-1)d & l\underline{1}_{M-1} \\ l\underline{1}_{M-1}^\dagger & dI_{M-1} \end{bmatrix}$$

- d is a positive real number such that $0 \leq d \leq M/(M-1)$
- l is a complex number such that $|l| \leq \sqrt{(\frac{M}{M-1} - d)d}$

Optimal UT-IR Rician Link

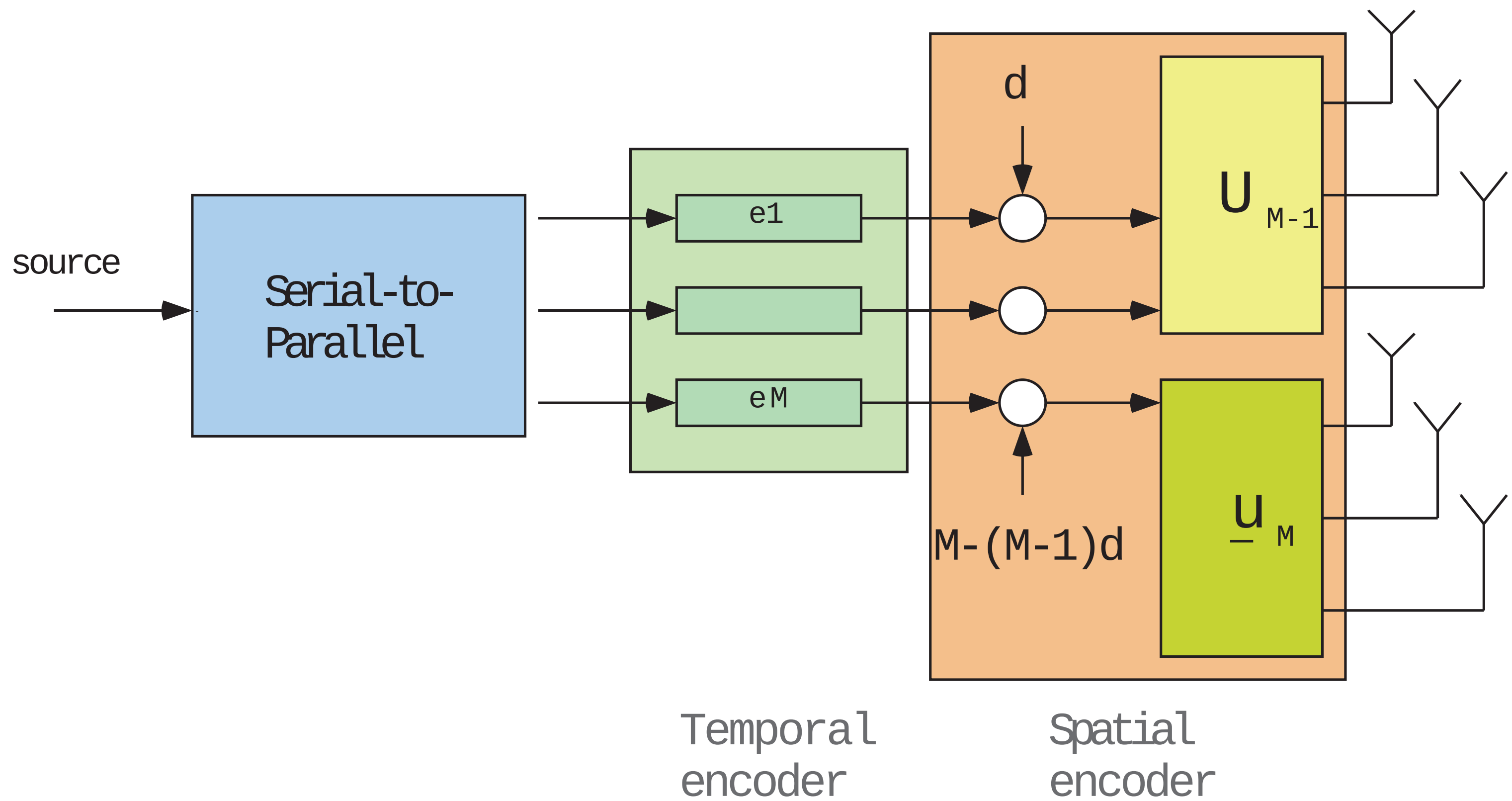


Figure 11. *Optimal STC for Rician uninformed-transmitter informed-receiver*

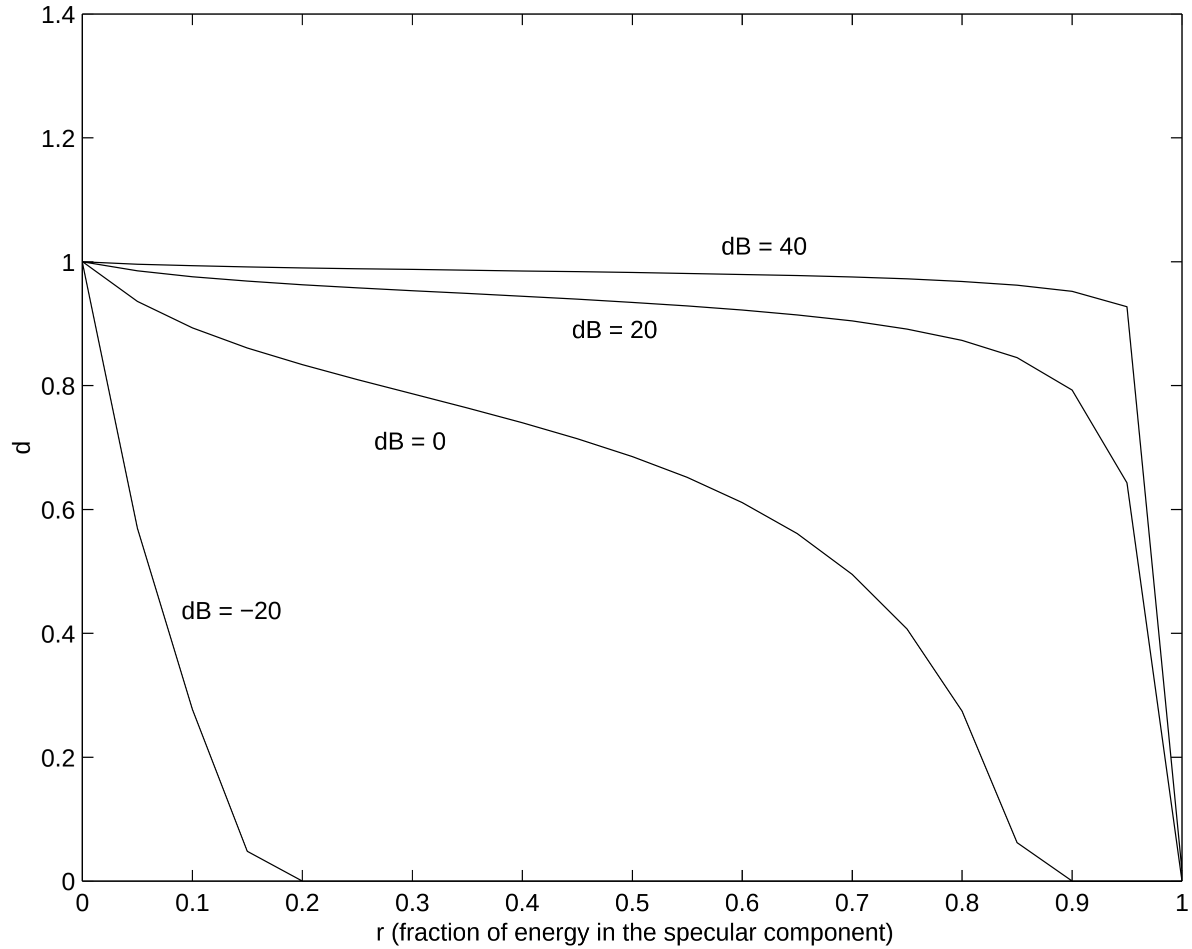
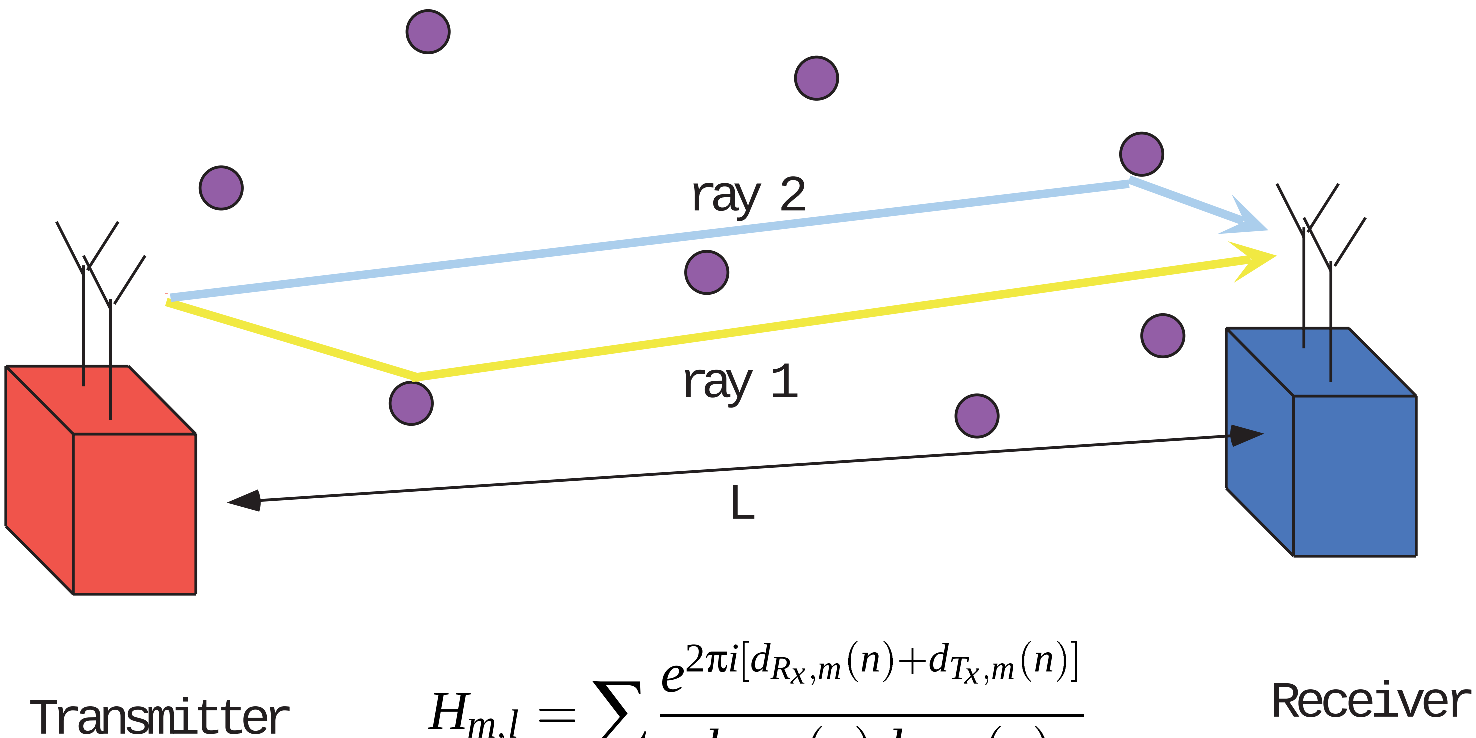


Figure 12. *Numerical optimization yields* $l = 0$ *and values of* d *shown as a function of* r *for different values of* ρ.

Channel Sensitivity: Physical Scatterers



$$H_{m,l} = \sum_n \frac{e^{2\pi i[d_{R_x,m}(n)+d_{T_x,m}(n)]}}{d_{R_x,m}(n)d_{T_x,m}(n)}$$

Figure 13. *Physical point scattering model.*

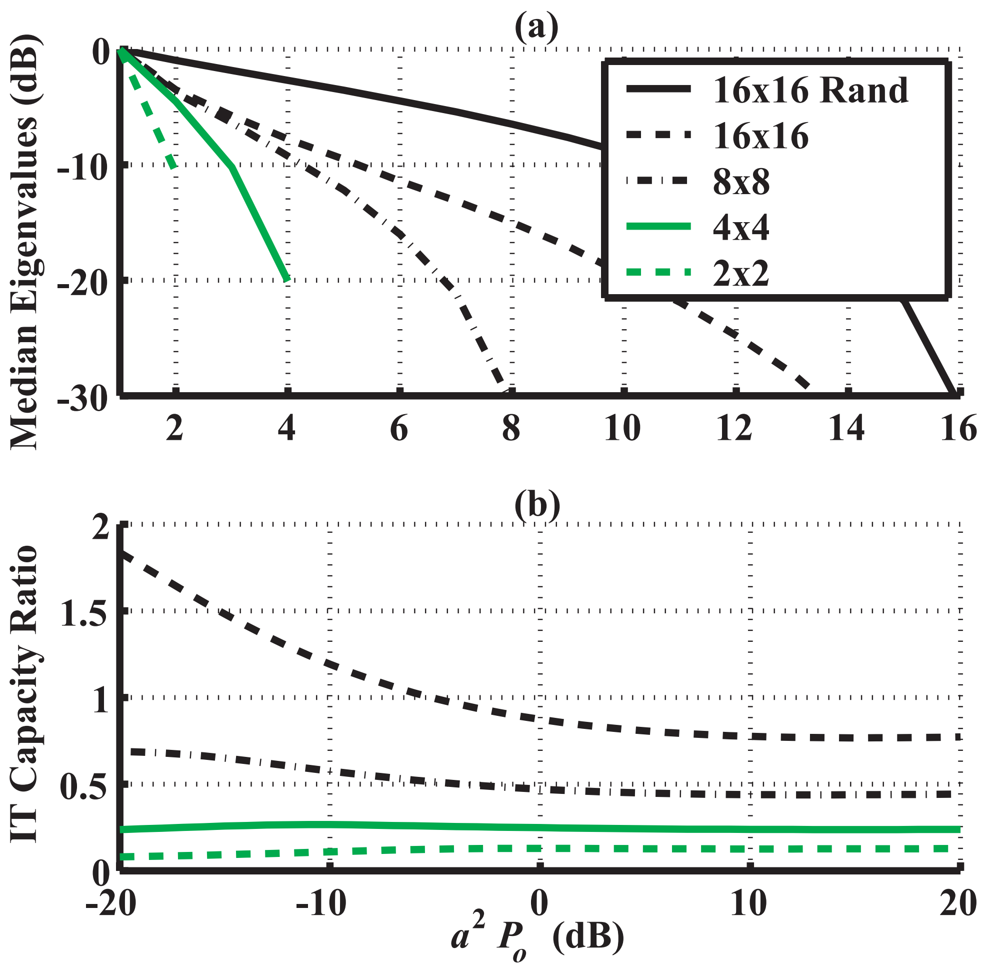


Figure 14. *Eigenvalue dsn and capacity ratio* ($a^2 = \mathrm{tr}\{HH^\dagger\}$)

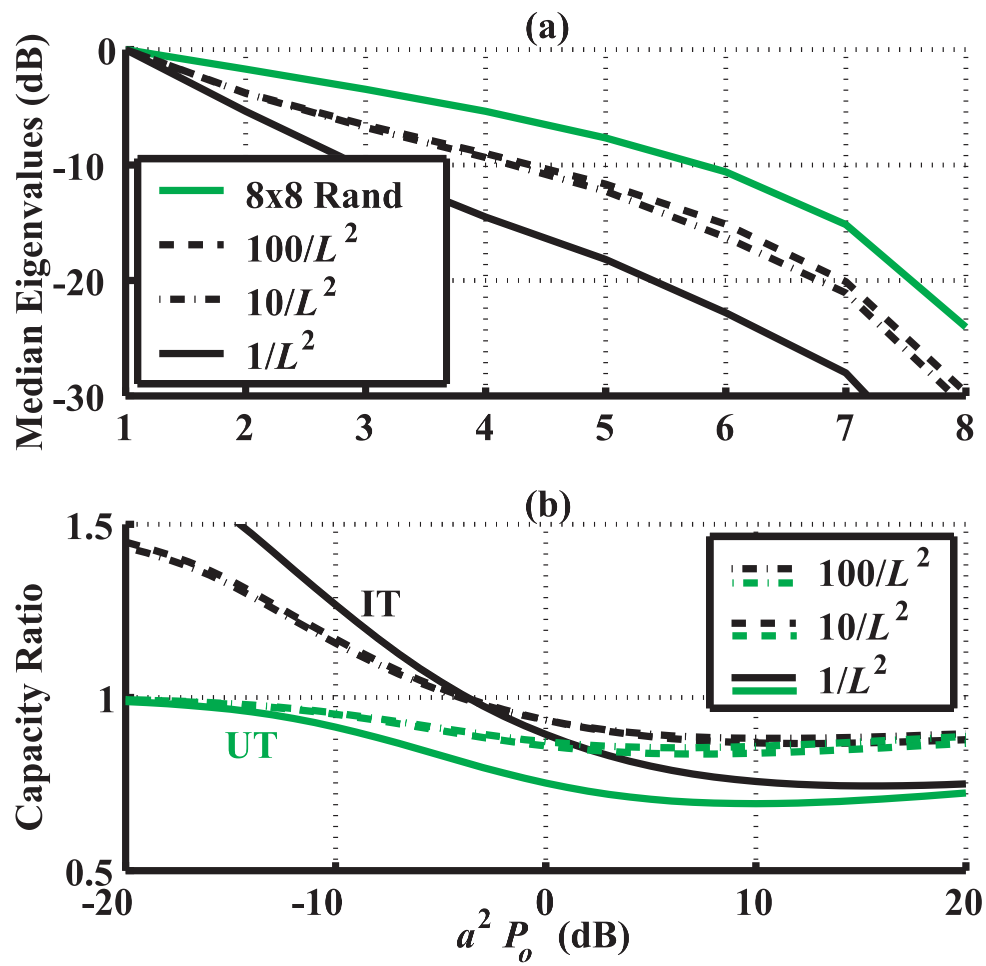


Figure 15. *Median eigenvalue dsn and capacity ratio*

Channel Sensitivity: Interference

Hypothesis: Strong random interferers

Informed Transmitter (IT) and Informed Receiver (IR)

$$C = TE\left[\sup_{\Sigma:\mathrm{tr}\{\Sigma\}\leq P_o} \log\left(I_M + \eta H\,(I+R)^{-\frac{1}{2}}\Sigma(I+R)^{-\frac{1}{2}}\,H^\dagger\right)\right]$$

Uninformed Transmitter (UT) and IR

$$C = T\sup_{\Sigma:\mathrm{tr}\{\Sigma\}\leq P_o} E\left[\log\left(I + \eta H\,(I+R)^{-\frac{1}{2}}\Sigma(I+R)^{-\frac{1}{2}}\,H^\dagger\right)\right]$$

Where R is $N \times N$ interference spatial covariance matrix at receiver

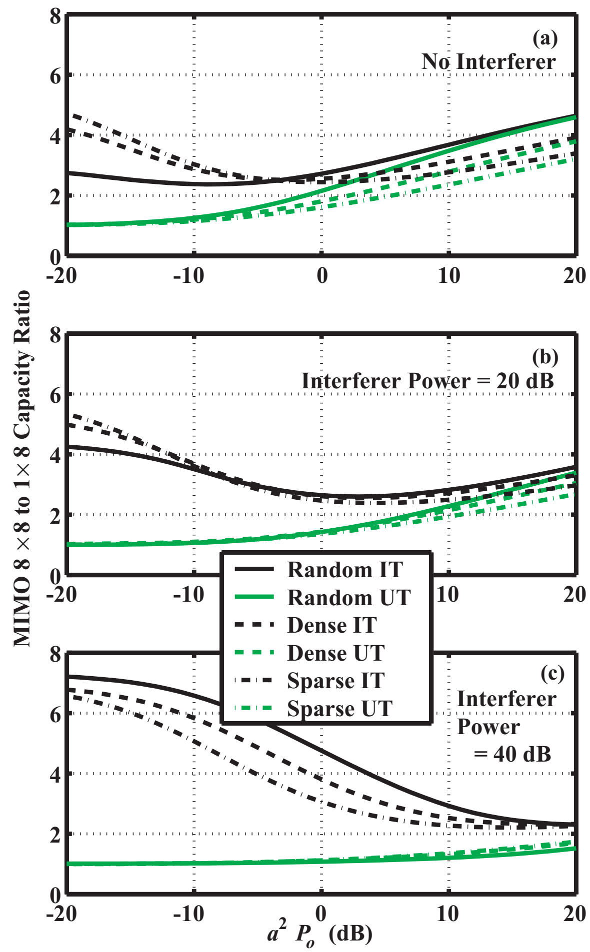


Figure 16. *Spectral efficiency ratio for 8 x 8 system*

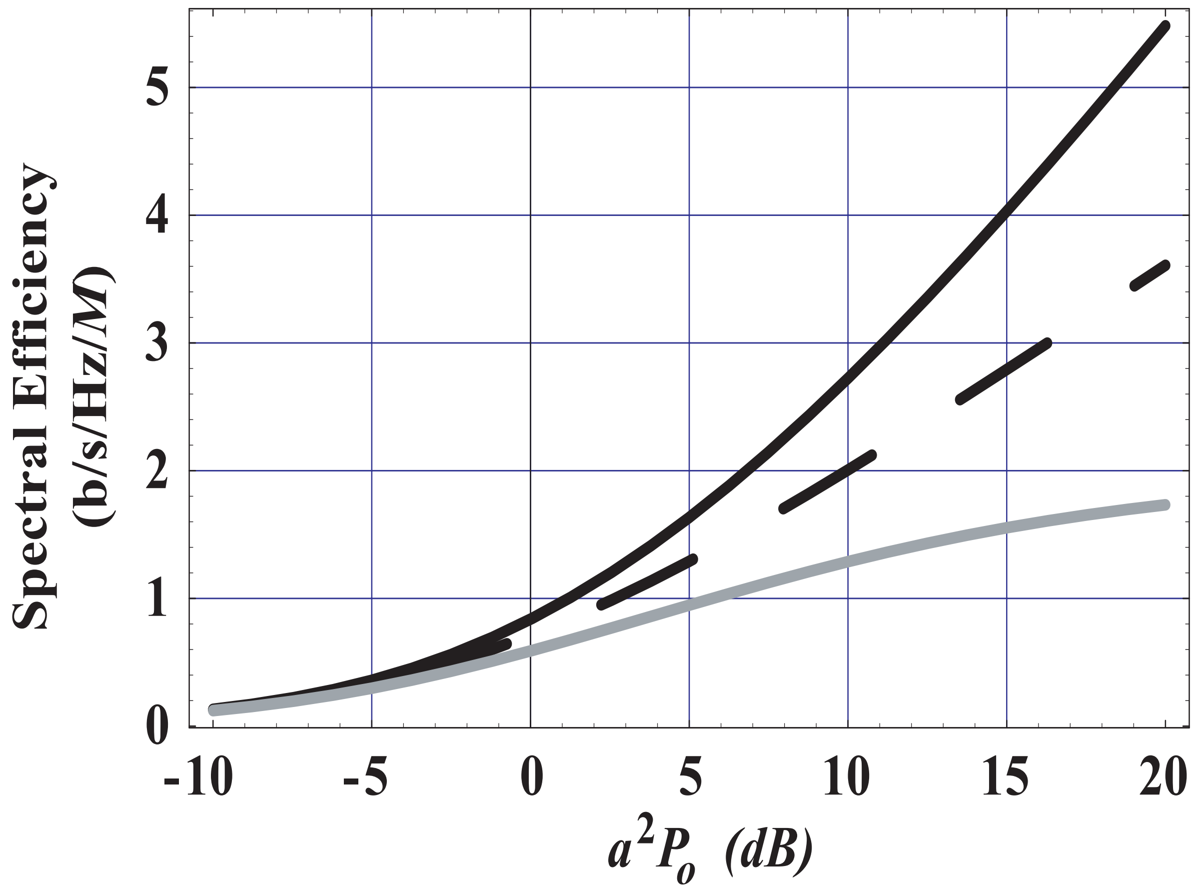


Figure 17. *Normalized capacity for no interferers, cooperative interferers, and un-cooperative interferers.*

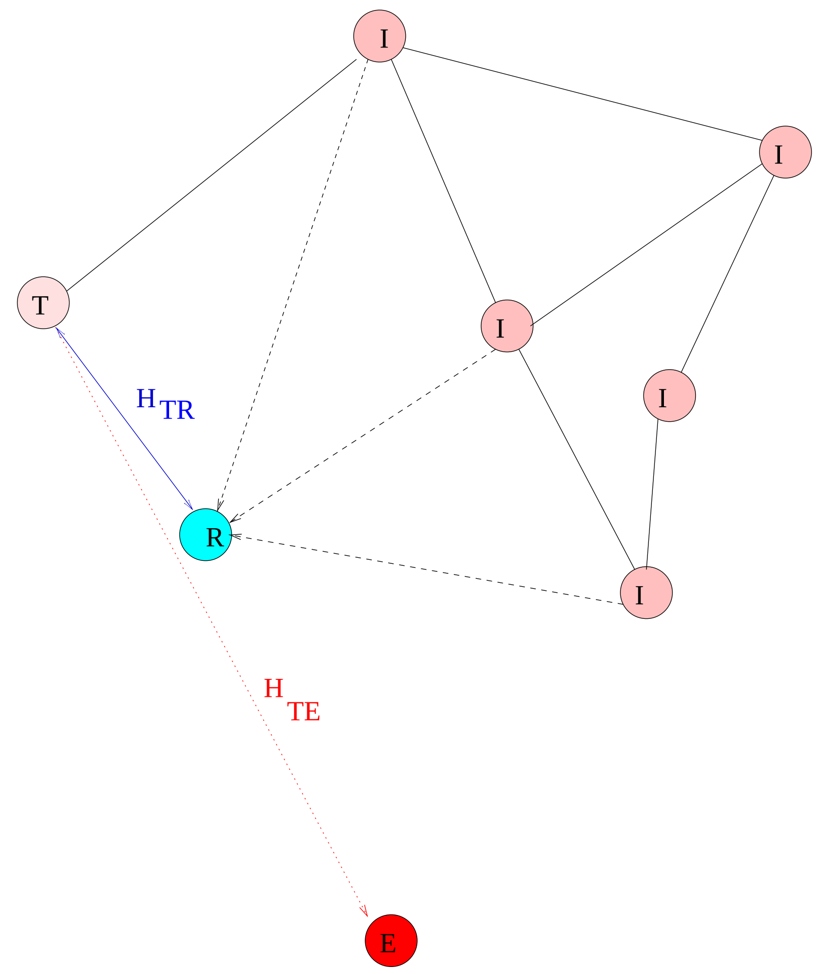


Figure 18. *Wireless network with eavesdropper*

Information Security: Eavesdropper Resistance

Hypotheses:

1. Subscriber links have *informed* transmitters/receivers (IT-IR):
   - H_{TR} is known to both parties over a hop
   - Training generally required to learn channel
   - Feedback required to inform transmitter of channel
2. Eavesdropper link has *uninformed* transmitter (UT)
   - H_{TE} unknown to transmitter
   - S, H_{TE} may be known or unknown to eavesdropper
   - Modulation type, signal constellations, source density, may be known to eavesdropper

Eavesdropper Performance Measures

1. P_e **eavesdropper error rate for detecting known signal** $S = s$ **on link**

$$P_F = P(\Lambda^e > \gamma | S = 0), \quad P_M = P(\Lambda^e < \gamma | S = s)$$

2. $P_F, P_M = 1 - P_D$: **eavesdropper error rates for detecting any activity on link**

$$P_F = P(\Lambda^e > \gamma | S = 0), \quad P_M = P(\Lambda^e < \gamma | S \neq 0)$$

3. $C^e = \max_{P_S} I(S;Y)$: **eavesdropper link capacity**

4. $P^e_{sde}(K)$: eavesdropper symbol intercept error rate

$$P^e_{sde} = P(\hat{S}^e \neq S)$$

Computational Cutoff Rates

$$R_o(H) \quad = \quad \max_{P_{S|H}} - \ln \int\int_{S_1,S_2 \in \mathbb{C}^{T\times M}} dP_{S|H}(S_1) dP_{S|H}(S_2) \quad e^{-ND(S_1\|S_2)}$$

1. T/R Informed cutoff rate: H known to both T/R

$$D(S_1\|S_2) = \frac{\eta}{4} \operatorname{tr}\left(H^\dagger (S_1 - S_2)^\dagger (S_1 - S_2) H\right)$$

2. R informed cutoff rate: H known to R only

$$D(S_1\|S_2) = \ln \left| I_T + \frac{\eta}{4} (S_1 - S_2)(S_1 - S_2)^\dagger \right|$$

3. Uninformed cutoff rate: H unknown to either T/R

$$D(S_1\|S_2) = \ln \frac{\left| I_T + \frac{\eta}{2}(S_1 S_1^\dagger + S_2 S_2^\dagger) \right|}{\sqrt{\left| I_T + \eta S_1 S_1^\dagger \right| \; \left| I_T + \eta S_2 S_2^\dagger \right|}}$$

LPI: Uninformed Eavesdropper Lockout Capacity

Lock out condition: $C_e = 0$

Note: **lock out** occurs if transmitted signal constellation $\{S_i\}$ satisfies:

$$S_i S_i^\dagger = A, \qquad \forall\, i$$

Examples:

- Doubly unitary codes ($T \geq M$):

$$S_i^\dagger S_i = I_M, \quad S_i S_i^\dagger = \begin{bmatrix} I_M & O \\ O & O \end{bmatrix}$$

  Instances

  – Square unitary codes ($T = M$): $S_i S_i^\dagger = S_i^\dagger S_i = I_M$

– Space time QPSK: Quaternion codes ($T = M = 2$):

$$S = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} j & 0 \\ 0 & -j \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix} \right\}$$

- Constant (spatial) modulus (CM) codes $(T = 1)$:

$$S_i = [S_{1i}, \cdots, S_{Mi}]$$

$$\mathrm{tr}\{S_i S_i^\dagger\} = \|\underline{S}_i\|^2 = 1$$

Note 1: Q. How much subscriber capacity does lockout cost?

A. Dimensionality analysis $(T = M)$:

Constraint $S_i S_i^\dagger = A$ reduces coding d.f. by factor

$$\rho = \frac{M(M+1)/2}{M^2} \approx 1/2$$

LPD constraints

The eavesdropper must make a decision between

$$H_0: \qquad X_i = W_i, \qquad i = 1, \ldots, L$$

$$H_1: \quad X_i = S_i H_i + W_i, \quad i = 1, \ldots, L$$

His minimum attainable detection error probability has exponential rate

$$\begin{aligned}
\liminf_{L\to\infty} \frac{1}{L} \ln P_e &= \rho \\
\rho &= \inf_{\alpha\in[0,1]} \lim_{L\to\infty} \frac{1}{L} \ln \int f_{H_1}^{1-\alpha}(X) f_{H_0}^{\alpha}(X) dX
\end{aligned}$$

- ρ is Chernoff error exponent ($\rho \leq 0$)
- ρ is minimal α-divergence between densities f_{H_1} and f_{H_0}
- Chernoff exponent is achieved for Bayes test

SH-informed Eavesdropper

When eavesdropper knows transmitted sequence $S = s = \{s_1, \ldots, s_L\}$ and channel sequence $H_{TE} = \{H_1, \ldots, H_L\}$

$$H_0: \quad S = 0,$$
$$H_1: \quad S = s$$

$$\rho \quad = \quad \lim_{L\to\infty} \frac{1}{L} \sum_{i=1}^{L} \rho(H_i, s_i)$$

where

$$\rho(H_i, s_i) = -\frac{\eta_e^2}{4} \mathrm{tr}\{s_i H_i H_i^\dagger s_i^\dagger\}.$$

LPD transmitter strategy: Attain $E[\max_{P(S)} \ln P(X|H_{TR}, S)/P(X|H_{TR})]$ subject to constraint on LPD (ρ)

• When $H_i = H_{TE}$ are i.i.d. Rayleigh channels:

$$\rho = -\frac{\eta_e^2}{4} E[\mathrm{tr}\{S_i S_i^\dagger\}].$$

Relevant LPD constraints on Transmitter are:

- Peak power constraint:

$$\mathrm{tr}\{s_i s_i^\dagger\} \leq P_{opk}$$

- Average power constraint:

$$\mathrm{tr}\left\{E[S_i S_i^\dagger]\right\} \leq P_o$$

S-Informed Eavesdropper

When eavesdropper knows S, but not H, α-divergence is

$$\ln \int f^{1-\alpha}(X|S=s)\, f_{H_0}^{\alpha}(X|S=0)\, dX \quad = \quad \sum_{i=1}^{L} \ln \frac{|I_T + \eta_e s_i s_i^\dagger|^{1-\alpha}}{|I_T + \eta_e (1-\alpha)\, s_i s_i^\dagger|}$$

Asymptotic development:

$$\ln \frac{|I_T + \eta_e s_i s_i^\dagger|^{1-\alpha}}{|I_T + \eta_e (1-\alpha)\, s_i s_i^\dagger|} \quad = \quad -\frac{\alpha(1-\alpha)\eta_e^2}{2}\, \mathrm{tr}\{s_i s_i^\dagger s_i s_i^\dagger\} + o(\eta_e^2).$$

Low SNR scenario

Low SNR representation for the Chernoff error exponent

$$\rho = -\frac{\eta_e^2}{8}\frac{1}{L}\sum_{i=1}^{L}\mathrm{tr}\{s_i s_i^\dagger s_i s_i^\dagger\} + o(\eta_e^2).$$

Transmitter Strategy:

Attain $E[\max_{P(S)} \ln P(X|H_{TR}, S)/P(X|H_{TR})]$ subject to either

- Peak 4-th moment constraint:

$$\mathrm{tr}\{s_i s_i^\dagger s_i s_i^\dagger\} \le P_{4pk},$$

- Average 4-th moment constraint:

$$\mathrm{tr}\{E[S_i S_i^\dagger S_i S_i^\dagger]\} \le P_{4avg},$$

Uninformed Eavesdropper

When eavesdropper knows neither S nor H

$$H_0: \quad S = 0,$$
$$H_1: \quad S \neq 0$$

- α-divergence not closed form
- Multivariate Edgeworth expansion of $f(X|S \neq 0)$

$$\ln \int f^{1-\alpha}(X|S \neq 0) f^{\alpha}(X|S = 0) dY \tag{1}$$
$$= \ln \frac{\left| I_T + \eta_e \overline{SS^\dagger} \right|^{1-\alpha}}{\left| I_T + \eta_e (1-\alpha) \overline{SS^\dagger} \right|} + \frac{\alpha(1-\alpha)^2 \eta_e^2}{8} \sigma_{t,u} \kappa^{t,u,v,w}(X) \sigma_{v,w} + o(\eta_e^4)$$

$\kappa_{r,s,t,u}(X)$ is received signal kurtosis and

$$\sigma_{t,u}\kappa^{t,u,v,w}(X)\sigma_{v,w}$$
$$= \eta_e^2 3N \sum_{k=1}^{T} \sum_{t,u,v,w=1}^{M} cov(s_{kt}, s_{ku})\mathrm{cov}(s_{kt}s_{ku},\, s_{kv}s_{kw})\mathrm{cov}(s_{kv}, s_{kw})$$

Observe

- Skewness of X is always zero for Gaussian channel
- Kurtosis tensor product depends on 4th moment of source:

$$\mathrm{cov}(s_{kt}s_{ku},\, s_{kv}s_{kw}) = E[s_{kt}s_{ku}s_{kv}s_{kw}] - E[s_{kt}s_{ku}]\, E[\, s_{kv}s_{kw}] \geq 0$$

- First term in (1) dominates for low SNR

Uninformed Eavesdropper: Low SNR

$$\rho = \min_{\alpha\in[0,1]} \left(-\frac{\alpha(1-\alpha)\eta_e^2}{2} \operatorname{tr}\{\overline{SS^\dagger}\;\overline{SS^\dagger}\} + o(\eta_e^2) \right)$$
$$= -\frac{\eta_e^2}{8} \operatorname{tr}\{\overline{SS^\dagger}\;\overline{SS^\dagger}\} + o(\eta_e^2)$$

Transmitter strategy:

Attain $E[\max_{P(S)} \ln P(X|H_{TR},S)/P(X|H_{TR})]$ subject to

$$\operatorname{tr}\{\overline{SS^\dagger}\;\overline{SS^\dagger}\} \leq P_{4avg}$$

• Equivalent to constraining S to Gaussian source with

$$\operatorname{tr}\{\overline{SS^\dagger SS^\dagger}\} \leq P_{4avg}/3$$

LPD-constrained Capacity

Proposition 1 *The LPD-constrained capacity* C_{lpd} *for the T/R informed link is*

$$C_{\text{lpd}} = TE\left[\ln\left|I_M + \eta_r H \Sigma_{\text{lpd}} H^\dagger\right|\right] = TE\left[\log\left(\frac{\sqrt{1+\mu\lambda_i^2}}{2}\right)\right]$$

- Attained by $S \sim N\left(0, I_T \bigotimes \Sigma_{\text{lpd}}\right)$
- $\Sigma_{\text{lpd}} = UDU^\dagger$, $D = \text{diag}(\sigma_i)$,

$$\sigma_i = \frac{\sqrt{1/\lambda_i^2 + \mu} - 1/\lambda_i}{2}, \tag{2}$$

- $\mu > 0$ is a parameter such that $\sum_i \sigma_i^2 = P_{4avg}$.

Note:

- eigenstructure of $\Sigma_{\rm lpd}$ is matched to modes of H.
- power-optimal waterpouring solution is **not** LPD-optimal
- $$\sqrt{M \,\mathrm{tr}\{E[SS^{\dagger}SS^{\dagger}]\}} \geq \mathrm{tr}\left\{E[SS^{\dagger}]\right\}$$

  Conclude: kurtosis constraint also constrains avg power

  However: kurtosis constraint produces qualitatively different optimal source distribution.

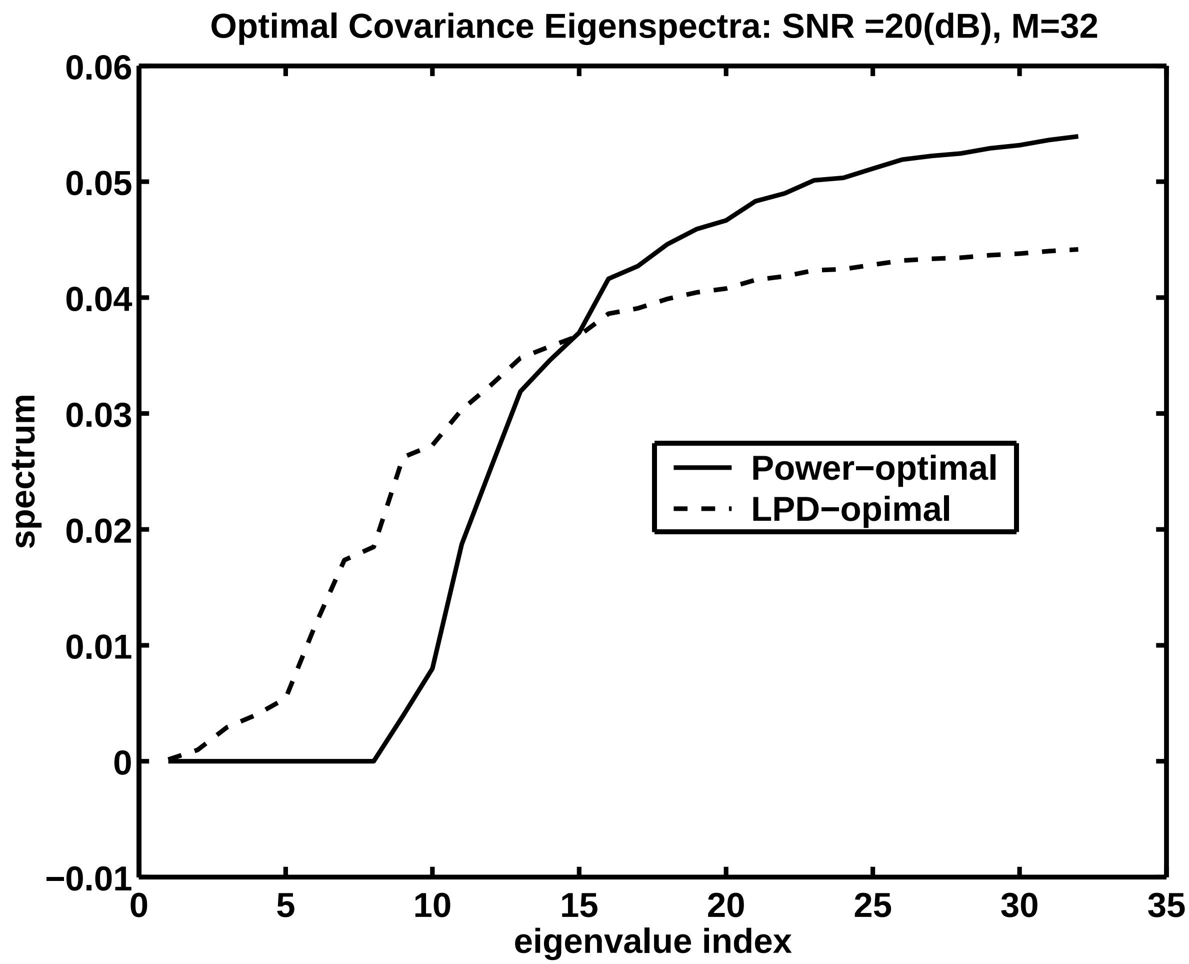


Figure 19. *Optimal source spectra:* $SNR = 20dB, M = N = 32$

LPD: Tradeoff Study

Define

$$I_c(\Sigma) = TE\left[\ln\left|I_M + \eta_r H\Sigma H^\dagger\right|\right]$$

1. IT-IR LPD-Capacity $I_{P_{4avg}}(\Sigma_{\text{lpd}})$
2. Loss in power-constrained capacity due to LPD constraint

$$I_{P_o}(\Sigma_{\text{lpd}})/I_{P_o}(\Sigma_{\text{pow}}) \tag{3}$$

3. Loss in LPD-constrained capacity due to power constraint

$$I_{P_{4avg}}(\Sigma_{\text{pow}})/I_{P_{4avg}}(\Sigma_{\text{lpd}}) \tag{4}$$

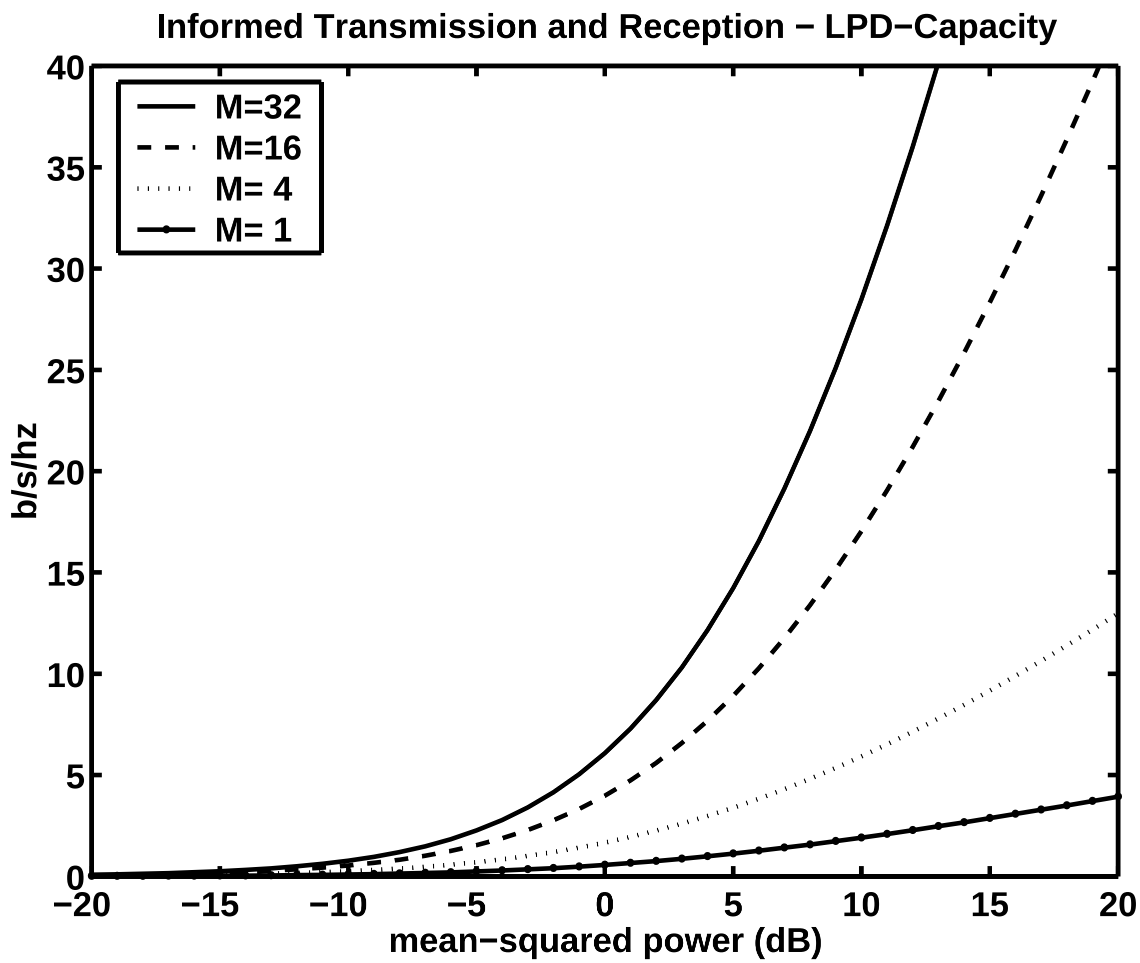


Figure 20. *IT-IR LPD-constrained capacity ($N = M$)*

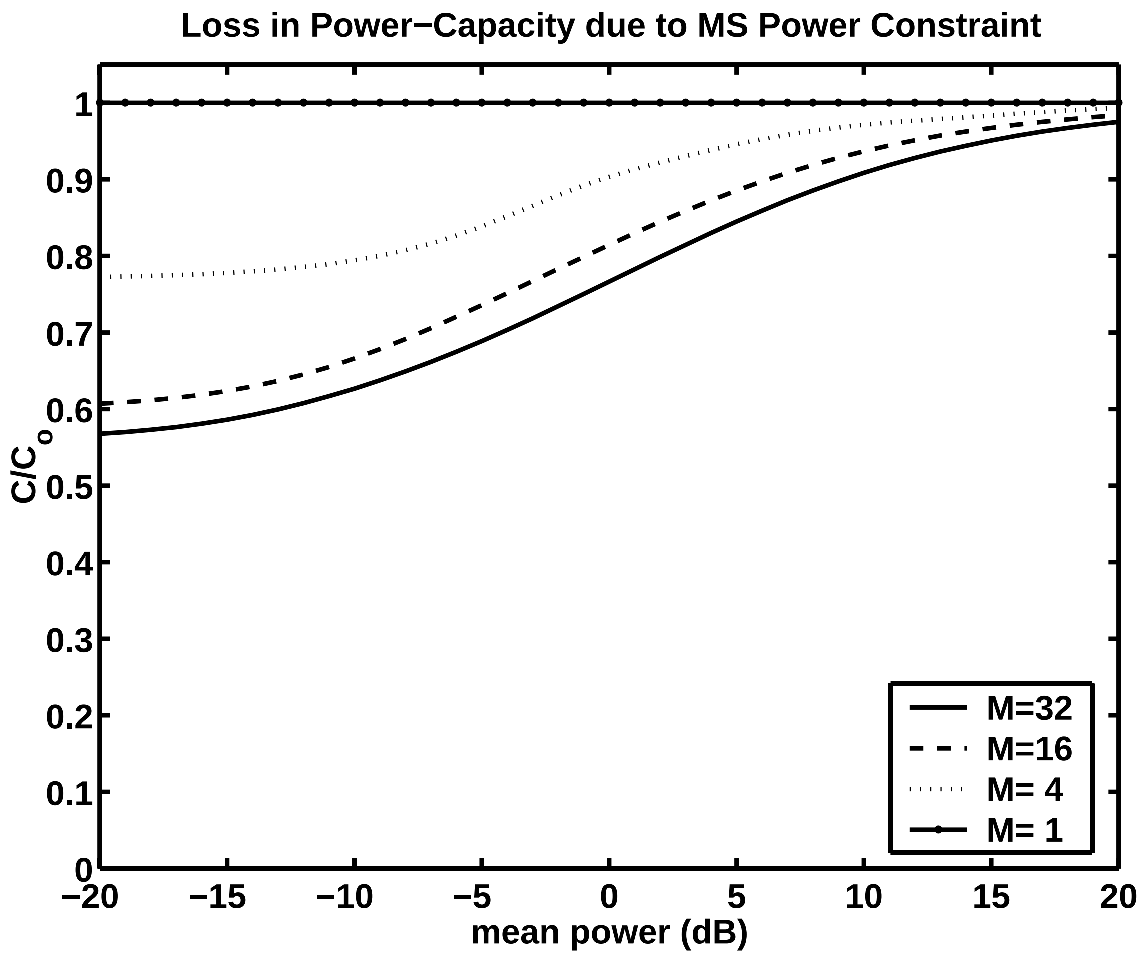


Figure 21. *Loss in power-capacity due to LPD constraint ($N = M$)*

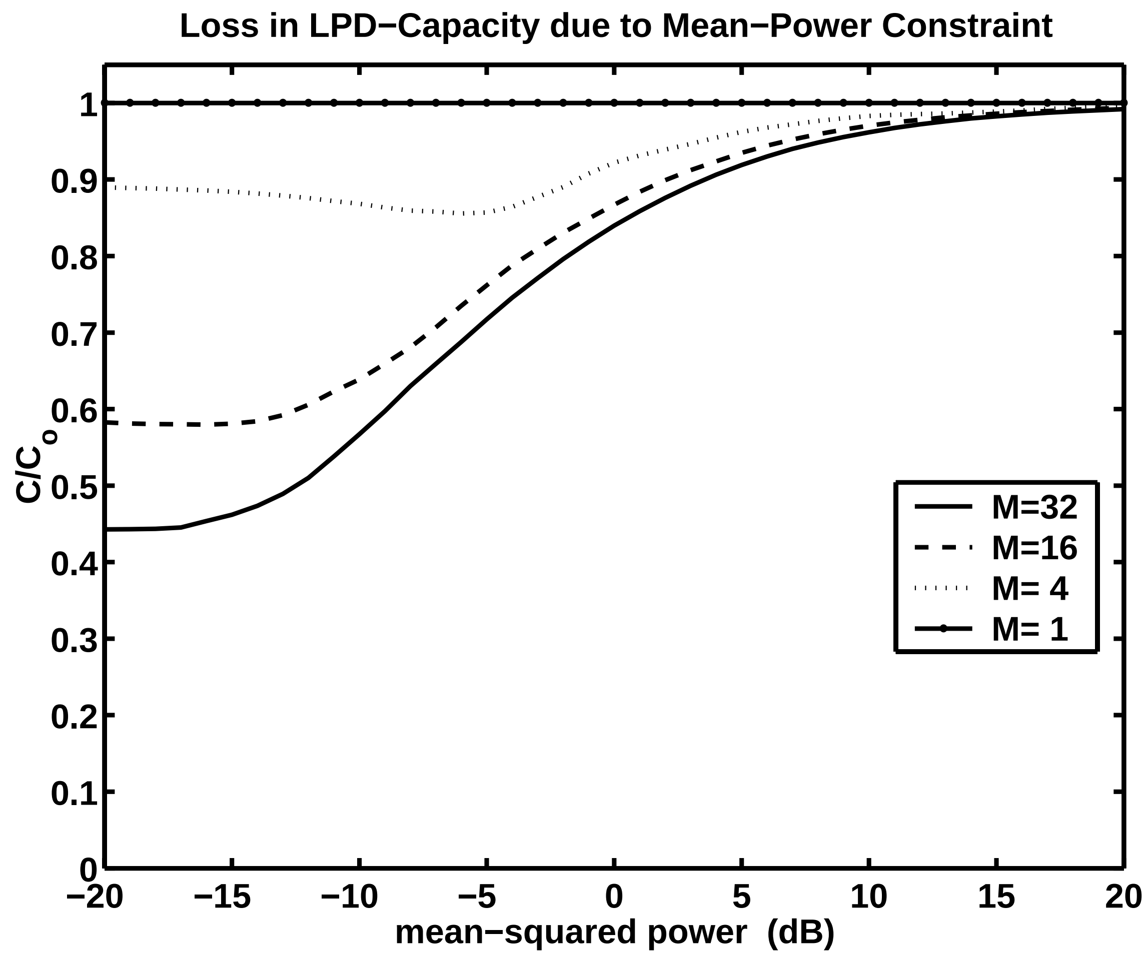


Figure 22. *Loss in LPD-capacity due to Pavg constraint* ($N = M$)

Comments

- For no transmit diversity ($M = 1$) there is no loss in capacity
- loss increases as more antennas M are deployed by eavesdropper and client
- loss decreases as SNR η_r increases
- as η_r decreases to -20 dB loss flattens out.

Conclusions

1. For Rician channel T transmits rank-1 component at low SNR
2. Capacity for physical scattering is less optimistic than for Rayleigh
3. High-power interference reduces degrees of freedom (number of useful channel modes)
4. LPD- and LPI- constrained *secure* channels are different from *open* channels
5. For uninformed eavesdropper 4th moment constraint constrains LPD
6. LPD-constrained information rate advantage increases with M