Smart Antennas for Secure Networks

Alfred O. Hero

Dept. EECS

University of Michigan - Ann Arbor

`hero@eecs.umich.edu`

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

Outline

1. Wireless network model utilizing smart antennas
2. Performance metrics: capacity vs security
3. Maximum LPD-constrained information rates
4. Maximum LPI-constrained information rates
5. Tradeoff study

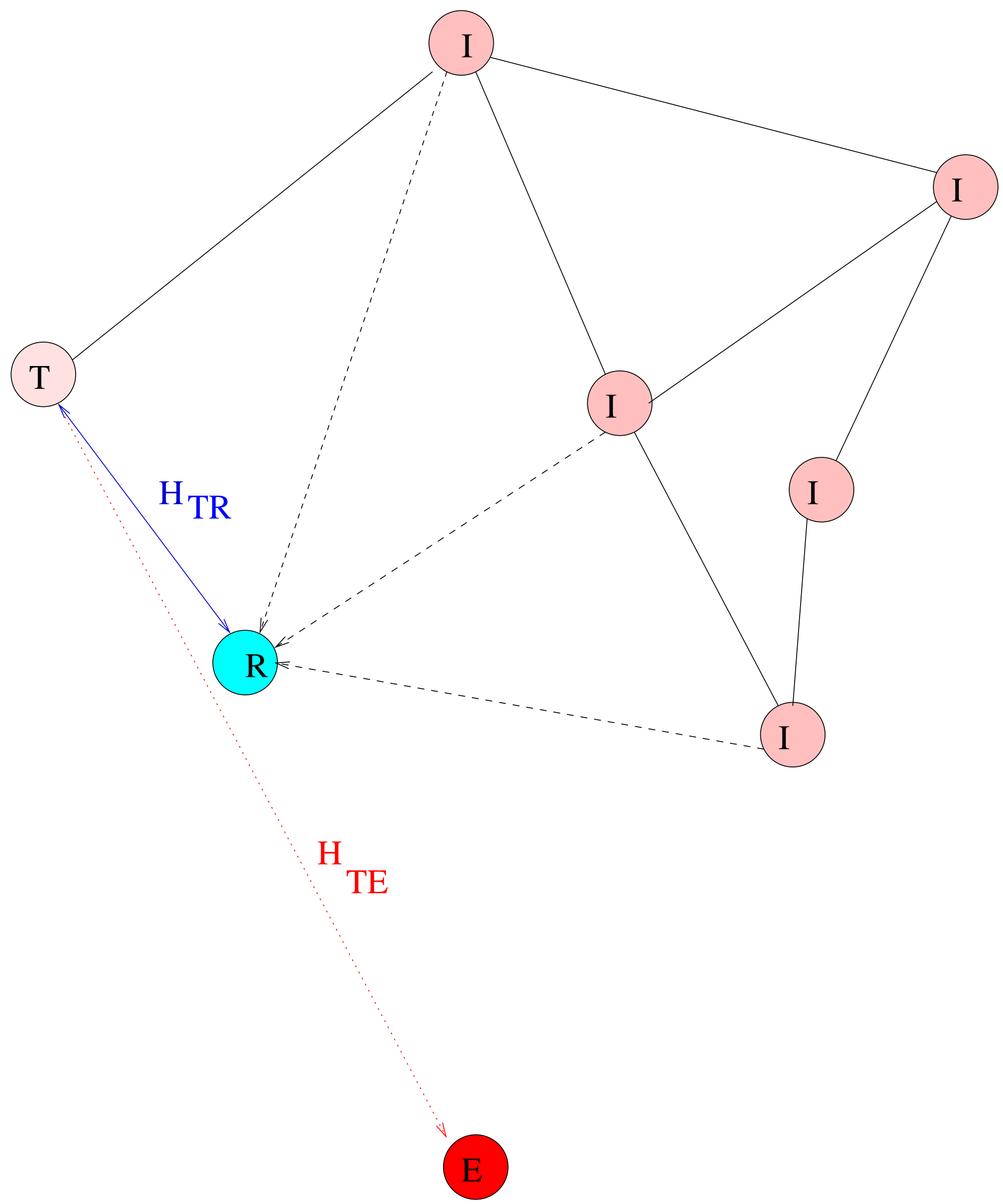

Figure 1. *Wireless network with eavesdropper*

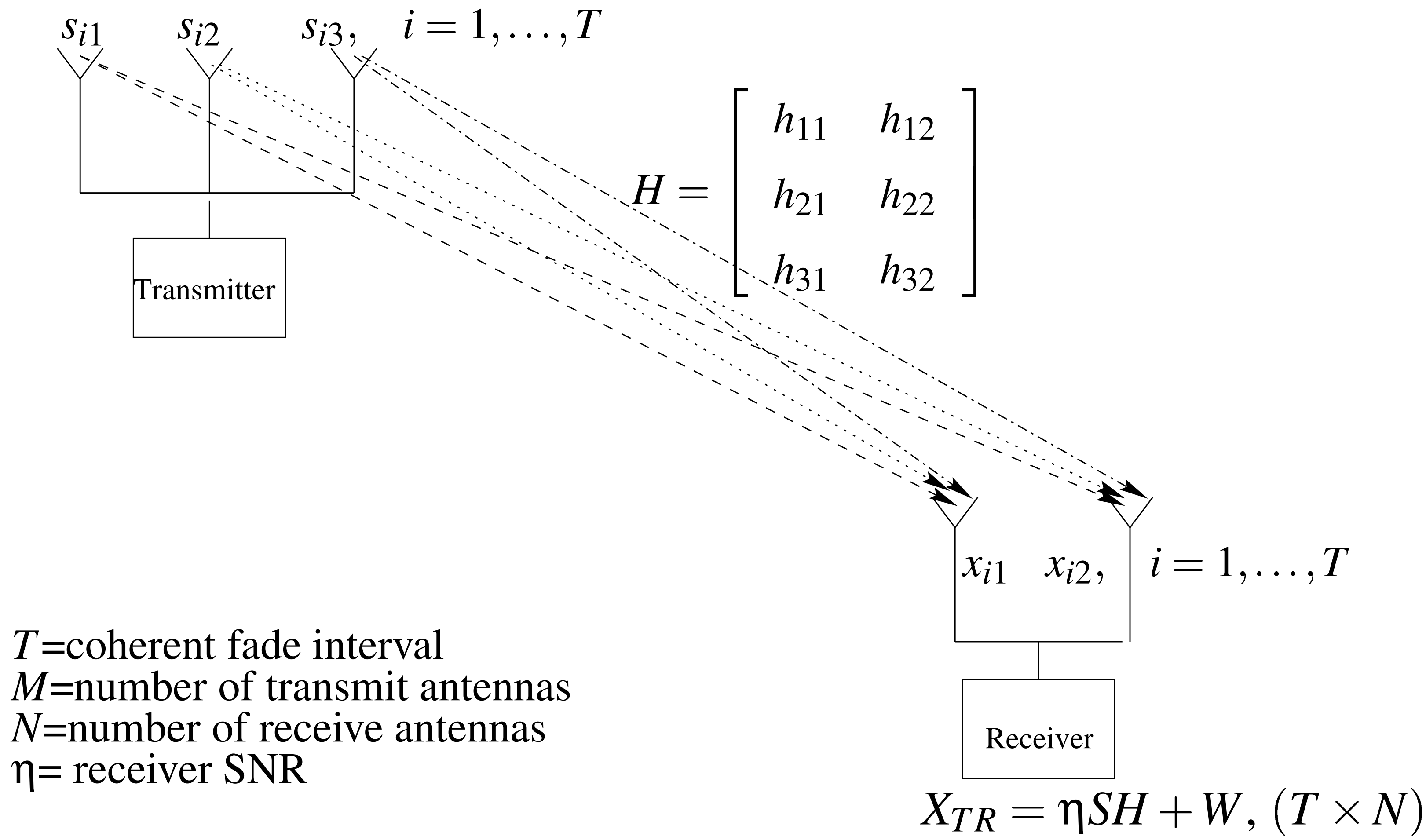

Figure 2. Space-Time channel for $M = 3$, $N = 2$

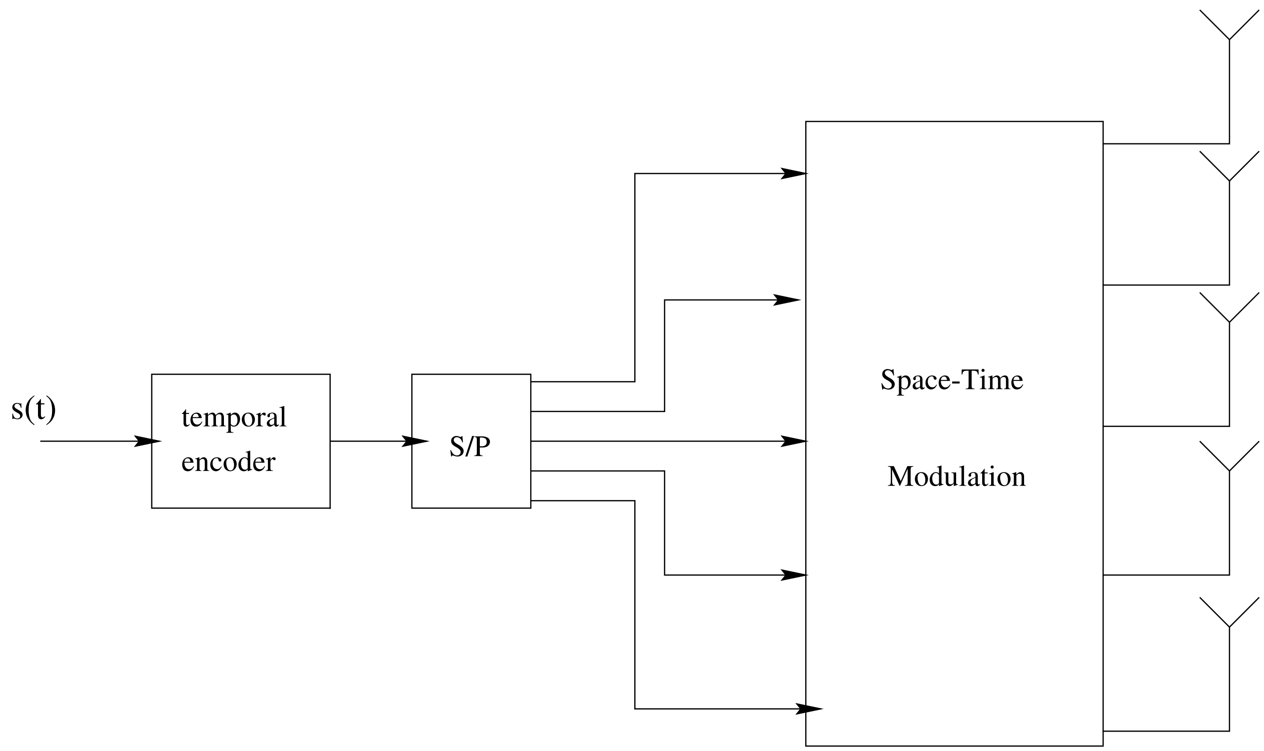

Figure 3. Third generation space-time coding: transmitter

General Rayleigh Fading Receiver Model

Received signal over L symbol blocks is sequence of $T \times N$ matrices

$$
\begin{aligned}
\mathbf{X}(t) &= \sum_{i=1}^{K} \mathbf{S}_k(t;\theta_k)\mathbf{H}_k(t) + \mathbf{N}(t) \\
&= \overbrace{[\mathbf{S}_1(t;\theta_1),\ldots,\mathbf{S}_K(t;\theta_K)]}^{T\times KM} \underbrace{\begin{bmatrix} \mathbf{H}_1(t) \\ \vdots \\ \mathbf{H}_K(t) \end{bmatrix}}_{KM\times N} + \mathbf{N}(t) \\
&= \mathcal{S}_K(t;\underline{\theta}_K)\mathcal{H}_K(t) + \mathbf{N}(t) \\
&= \mathbf{S}_K(t;\theta_K)\mathbf{H}_K(t) + \underbrace{\mathcal{S}_{K-1}(t;\underline{\theta}_{K-1})\mathcal{H}_{K-1}(t)}_{MUI} + \mathbf{N}(t) \quad t = 1,\ldots,L
\end{aligned}
$$

General Model Parameters

1. $\mathbf{S}_k(t;\theta_k)$: k-th user signature matrix ($T \times M$)
2. $\mathbf{H}_k(t)$: k-th user propagation (channel) matrix ($M \times N$)
3. θ_k: k-th user parameters (b_k, τ_k, ν_k)
4. $\mathbf{N}(t)$: zero mean white complex Gaussian noise matrix ($T \times N$)

Saturated/heavily-loaded MUI approximation

$$\text{MUI} \sim \mathcal{N}(0,\ Q_T \otimes Q_N)$$

Secure network conditions

1. Subscriber links have *informed* transmitters/receivers:
   - H_{TR} is known to both parties over a hop
   - Training may be required to learn channel
   - Feedback is required to inform transmitter of channel
2. Eavesdropper link has *uninformed* transmitter/reciever
   - H_{TE} is unknown to both parties over a hop
   - Training sequences, signal constellations, and other attributes may be known

Network QoS metrics

1. $P_{sde}(K)$: symbol decoding error rate of K-th link

$$P_{sde}(K) = P_{\underline{\theta}}(\hat{\underline{\theta}}_K \neq \underline{\theta}_K)$$

2. $C(K)$: **channel capacity of K-th link**

$$C(K) = \max_{P_{S_K}} I(S_K;X), \quad I(S_K;X) = E_{\underline{\theta}}[\ln f_{X|S_K}(X|S_K)/f_X(X)]$$

3. $R_o(K)$: **channel cutoff-rate of K-th link**

4. $C_{out}(K)$: outage capacity of K-th link

$$P(C(H_K) > C_{out}) \geq 1 - \varepsilon, \quad C(H_K) = \max_{P_{S_K}} I(S_K;X|H_K)$$

5. C_{sum}: sum capacity over all links

$$C_{sum} = \max_{P_{S_1,\ldots,S_K}} \sum_{i=1}^{K} R_i$$

6. C_{min}: min capacity of any link

$$C_{min} = \max_{P_{S_1,\ldots,S_K}} \min_i R_i$$

Eavesdropper metrics

1. $P_F(K), P_M(K) = 1 - P_D(K)$: **eavesdropper error rates for detecting presence of K-th user**

$$P_M = P_{H_0}(\Lambda_K^e > \gamma), \quad P_M = P_{H_1,\underline{\theta}_K}(\Lambda_K^e < \gamma)$$

2. $C^e(K) = \max_{P_{S_K}} I(S_K; X^e)$: **eavesdropper link capacity for K-th user**

3. $P_{sde}^e(K)$: eavesdropper K-th user intercept error rate

$$P_{sde}^e(K) = P_{\underline{\theta}}(\hat{\underline{\theta}}_K^e \neq \underline{\theta}_K)$$

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

1. T/R-informed σ-capacity: H known to both T/R

$$C_1 = E[C(H)], \quad (bits/sec/hz)$$

$$\begin{aligned} C(H) &= \max_{P_{S|H}} E[I(S,X|H)] \\ &= T \ln \left| I_M + H\Sigma_S H^\dagger \right| \end{aligned}$$

Capacity achieving source (waterpouring is optimal)

$$S \sim \mathcal{N}(0,\ (I_T + Q_T) \bigotimes \Sigma_S), \qquad \Sigma_S = \mathrm{diag}\left((\mu - 1/\lambda_i)^+\right)$$

$$\lambda_i = \mathrm{eigs}\left(H(I_N + Q_N)^{-1} H^\dagger\right) \qquad \mu\ :\ \mathrm{tr}(\Sigma_S) = \sigma$$

2. R-informed σ-capacity: H known to R only

$$C_2 = \max_{P_S} E[I(X,S|H)]$$

Capacity achieving source

$$S \sim \mathcal{N}(0,\ (I_T + Q_T) \bigotimes I_M)$$

3. Uninformed σ-capacity: H unknown to either T/R

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

Capacity achieving source

$$S \sim (I_T + Q_T)^{\frac{1}{2}} V \Lambda$$

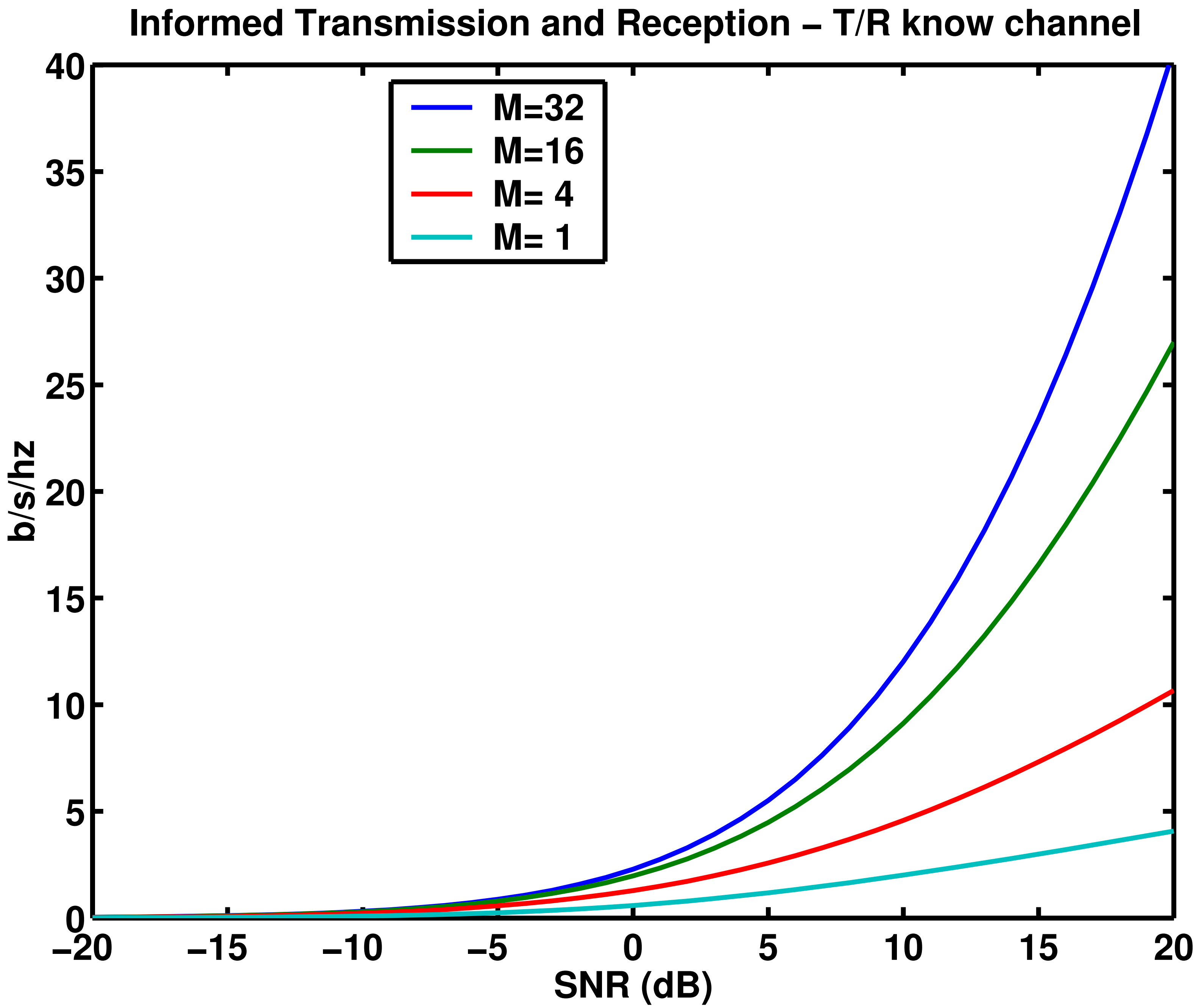

Figure 4. *T/R informed σ-capacity (N = M)*

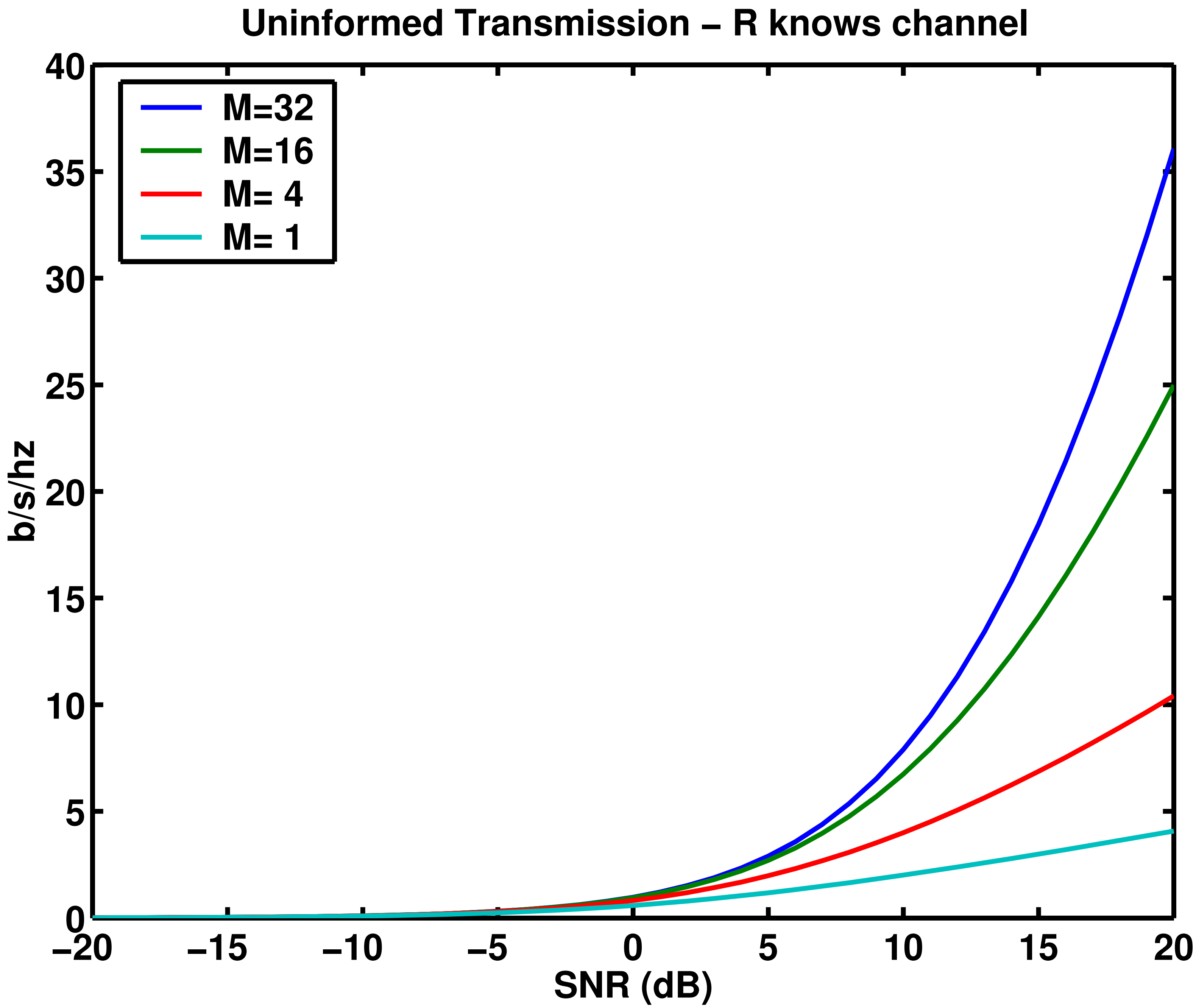

Figure 5. *R informed σ-capacity (N = M)*

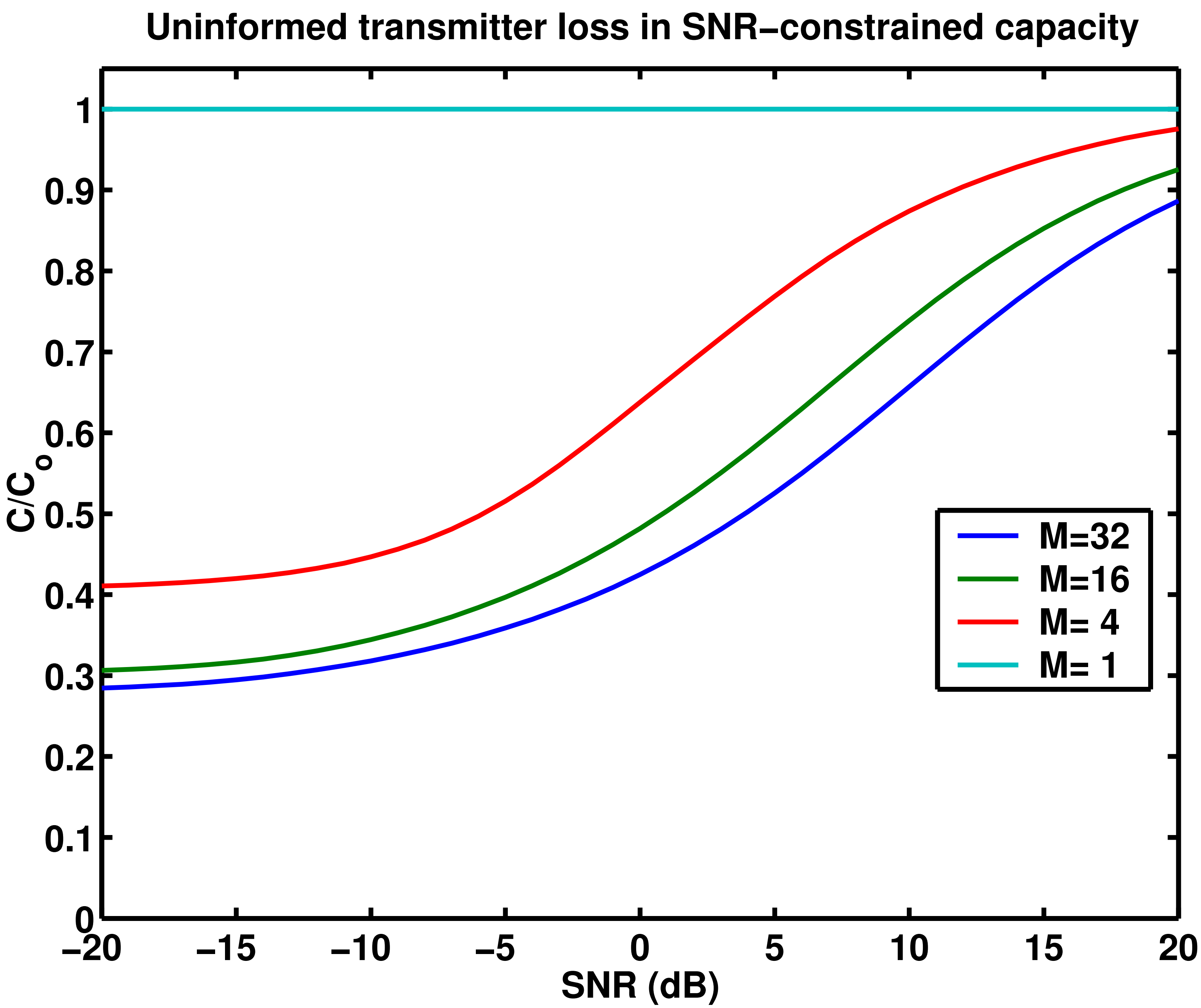

Figure 6. *R informed Capacity loss due to uninformed T (N = M)*

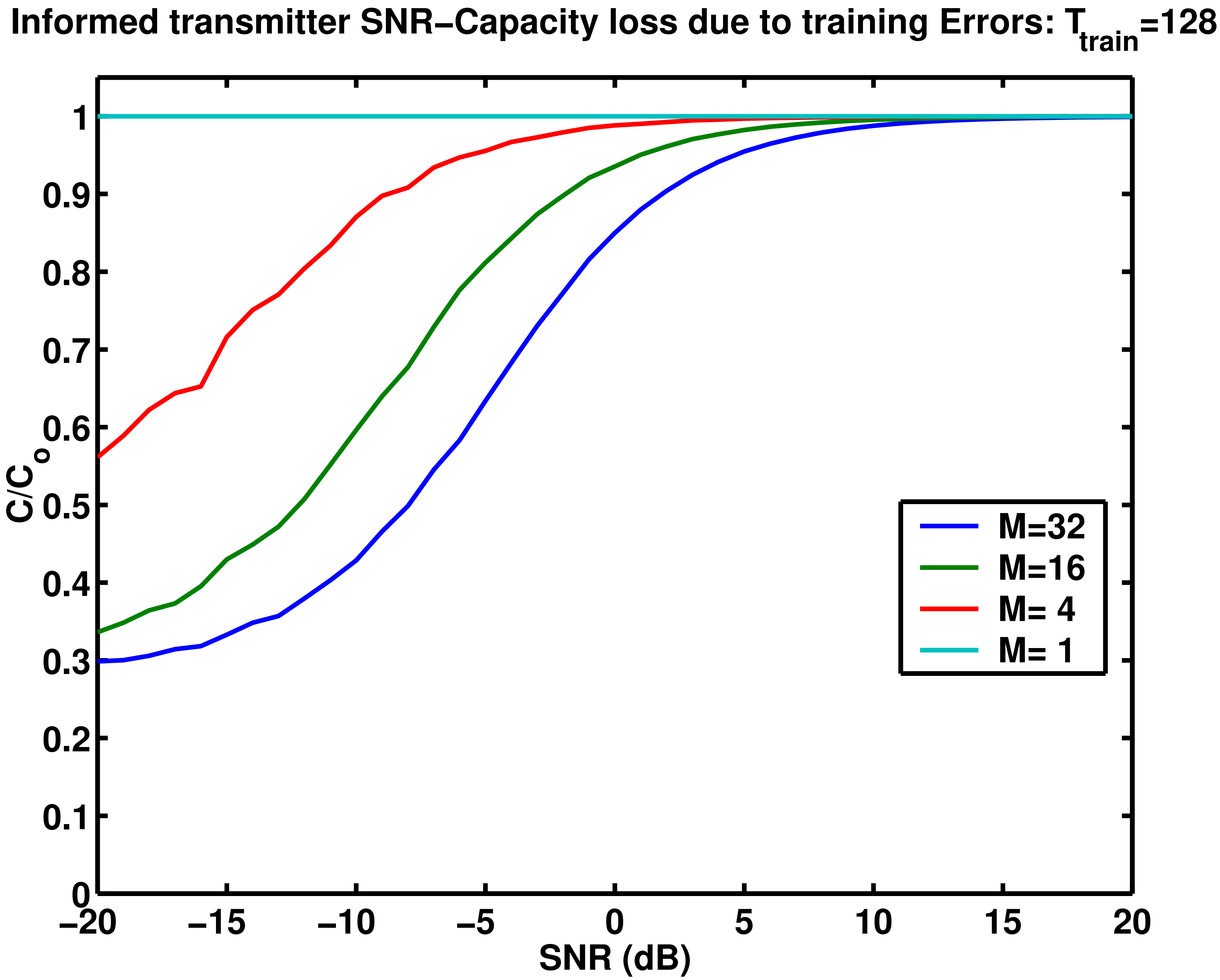

Figure 7. *T/R nformed capacity loss due to training errors (N = M)*

Single Link 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 ($\tilde{S} = (I_T + Q_T)^{-\frac{1}{2}} S$)

$$D(S_1 \| S_2) = \frac{\eta}{4} \operatorname{tr} \left(H^\dagger (\tilde{S}_1 - \tilde{S}_2)^\dagger (\tilde{S}_1 - \tilde{S}_2) H \right)$$

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

$$D(S_1 \| S_2) = \ln \left| I_M + \frac{\eta}{4} (\tilde{S}_1 - \tilde{S}_2)^\dagger (\tilde{S}_1 - \tilde{S}_2) \right|$$

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

$$D(S_1 \| S_2) = \ln \frac{\left| I_T + \frac{\eta}{2} (\tilde{S}_1 \tilde{S}_1^\dagger + \tilde{S}_2 \tilde{S}_2^\dagger) \right|}{\left| I_T + \eta \tilde{S}_1 \tilde{S}_1^\dagger \right| \; \left| I_T + \eta \tilde{S}_2 \tilde{S}_2^\dagger \right|}$$

LPI: Eavesdropper Lockout Capacity

Lock out condition: $R_o^3 = 0$

Note: **lock out** occurs if transmitted signal constellation $\{\tilde{S}_i\}$ satisfies:

$$\tilde{S}_i \tilde{S}_i^\dagger = A, \quad \forall\, i$$

Special case $T = 1$: "constant spatial modulus"

$$\tilde{S}_i \tilde{S}_i^\dagger = \mathrm{tr}\{\tilde{S}_i \tilde{S}_i^\dagger\} = A \;\; \Rightarrow \;\; \text{peak transmit power constraint}$$

Let

$$N \geq M, \quad H = U[\Lambda\; O]V$$

$$S_o(\mathbb{C}^{TM}) = \{\tilde{S} : \tilde{S}\tilde{S}^\dagger = cI_T\}$$

and define for $c > 0$

$$\mathcal{E} = \{\tilde{S} : \tilde{S}\Lambda^{-2}\tilde{S}^\dagger = cI_T\}$$

Proposition 1 *The eavesdropper lockout capacity for a T/R informed in-network link is the statistical expectation of*

$$C_{lockout}(H) = -\int dX \, \mathcal{N}_{TM}(\tilde{S} - X_1) \, \ln \int_{\mathcal{E}} dP^*_{\tilde{S}}(\tilde{S}') \mathcal{N}_{TM}(\tilde{S}' - X_1) - TM \ln \pi e$$

where

- $\mathcal{N}_{TM}(x)$ *is density of standard* TM *complex normal rv*
- $T \times M$ *matrix* X_1 *is defined by:* $[X_1, X_2] = XV$
- $dP^*_{\tilde{S}}$ *is density over* $\mathcal{S}_o(\mathbb{C}^T M)$ *which makes the RHS independent of* $\tilde{S}$

Special case: $H = [I_M, O]$

$\Rightarrow$ Capacity attaining source distribution $dP^*_{\tilde{S}}$ is uniform over the *sphere* $S_o(\mathbb{C}^{TM})$

Conjecture: this is optimal source distribution for any H as SNR gets large and receiver can accurately estimate channel.

LPD: kurtosis constrained capacity

Chernoff Bound on eavesdropper's minimum attainable detection error probability

$$
\begin{aligned}
\liminf_{L\to\infty} \frac{1}{L} P_e &\leq \rho \\
\rho &= \inf_{\alpha\in[0,1]} \ln \int dP_S(s) \int dX\, f_{X|S}^{1-\alpha}(X|s) f_{X|S}^{\alpha}(X|s=0) \\
&= \inf_{\alpha\in[0,1]} \ln \int dP_S(s) \left(\frac{\|I_T + \eta\, SS^\dagger\|^\alpha}{I_T + \alpha\eta\, SS^\dagger\|} \right)^N
\end{aligned}
$$

Low SNR approximation:

$$
\rho = -\frac{N\eta^2}{8} \operatorname{tr}\left(E[SS^\dagger SS^\dagger]\right) + o(\eta^2)
$$

Conclude: LPD constraint $\rho \geq \rho_o$ is captured by *kurtosis* constraint

$$
\operatorname{tr}\left(E[SS^\dagger SS^\dagger]\right) \leq \kappa
$$

Kurtosis-constrained Capacity

Proposition 2 *The kurtosis-constrained capacity* C_κ^3 *for the T/R informed link satisfies the lower bound*

$$C_\kappa^3 \geq E[C_\kappa(H)]$$

$$C(H) \quad = \quad T \ln \left| I_M + H \Sigma_S H^\dagger \right|$$

Capacity-bound achieving source: $S \sim \mathcal{N}(0,\ (I_T + Q_T) \bigotimes \Sigma_S)$

$$\Sigma_S = \mathrm{diag}\left(\frac{\sqrt{1/\lambda_i^2 + \mu} - 1/\lambda_i}{2} \right), \qquad \lambda_i = \mathrm{eigs}\left(H (I_N + Q_N)^{-1} H^\dagger \right)$$

$$\mu \ :\ 3\,(\mathrm{tr}\{\Sigma_S\})^2 = \kappa$$

Note:

1) σ-optimal waterpouring solution is **not** κ-optimal

2) relation between kurtosis and avg power of S

$$\sqrt{M \,\mathrm{tr}\{E[SS^\dagger SS^\dagger]\}} \geq \mathrm{tr}\left\{E[SS^\dagger]\right\}$$

Conclude: kurtosis constraint also constrains avg power

However: kurtosis constraint produces qualitatively different optimal source distribution.

3) Optimal Kurtosis constrained signal covariance is well approximated at high SNR by

$$\Sigma_S \approx \sqrt{\kappa/M}\ \ \mathrm{diag}\left(\frac{\lambda_{max}^2 - \lambda_i^2}{\sum_i(\lambda_{max}^2 - \lambda_i^2)}\right)$$

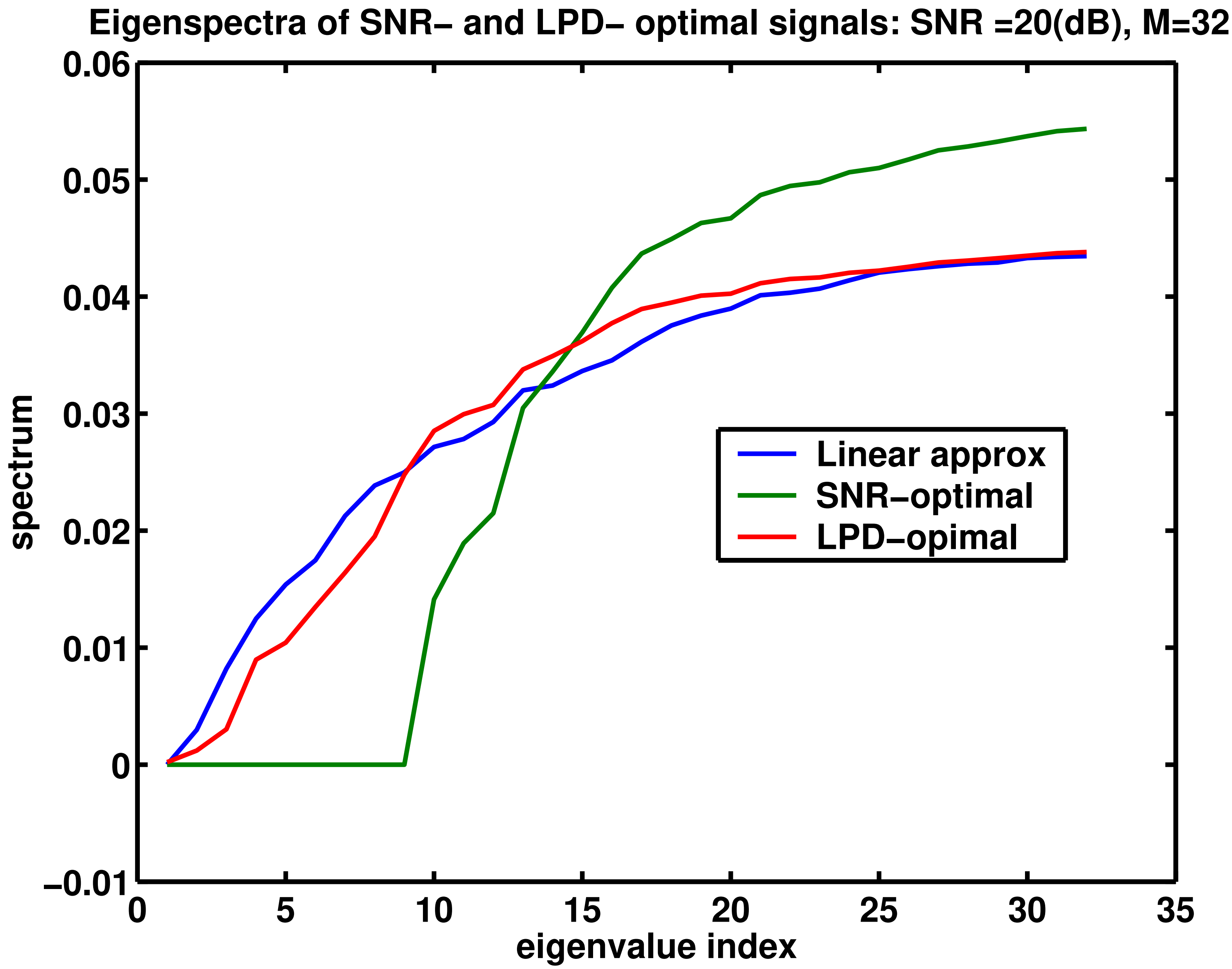

Figure 8. *Spectra of optimal source covariance matrices under LPD and Pavg constraints:* $SNR = 20dB, M = N = 32, Q_T = Q_R = 0$

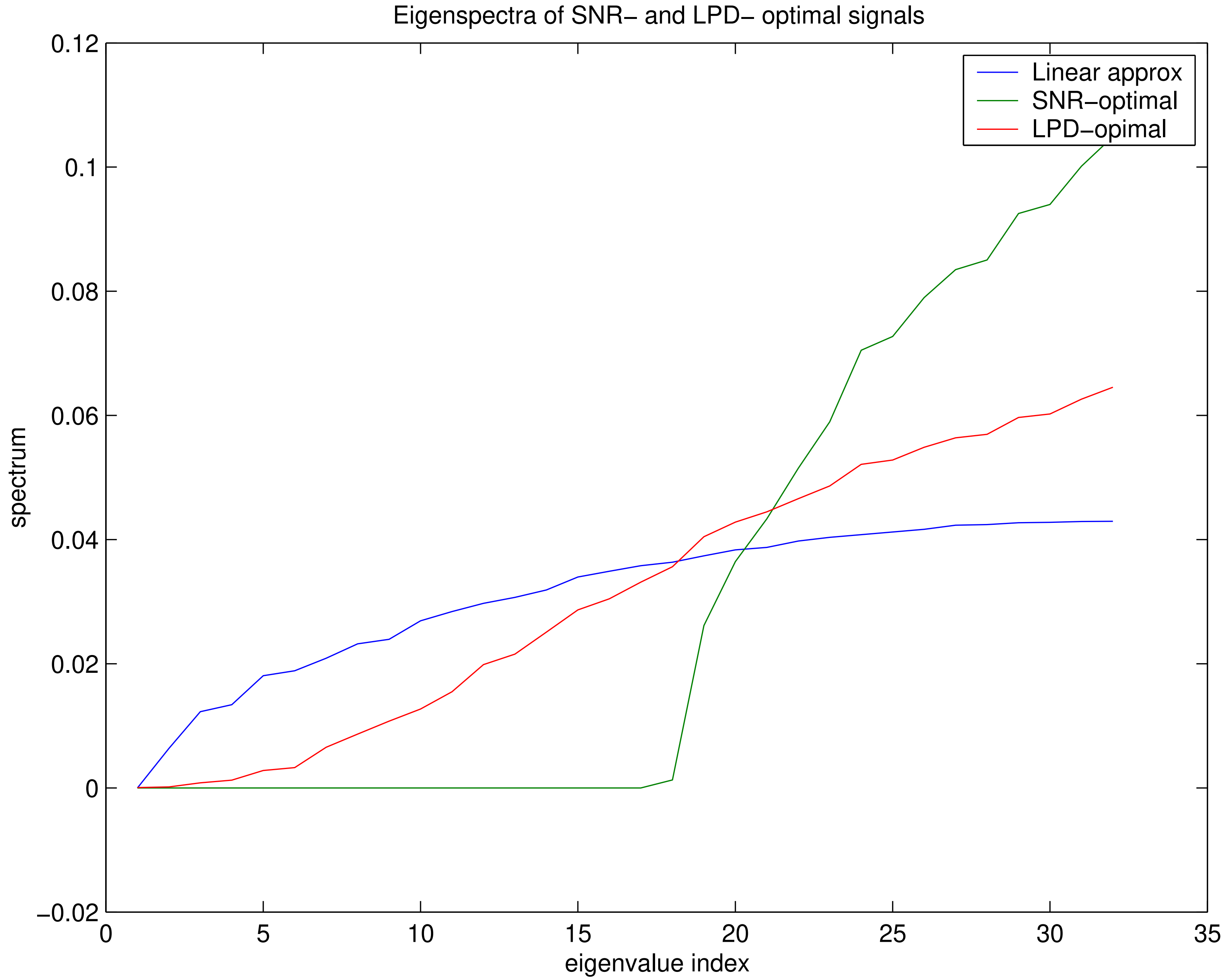

Figure 9. *Spectra of optimal source covariance matrices under LPD and Pavg constraints:* $SNR = 10dB, M = N = 32, Q_T = Q_R = 0$

LPD: Tradeoff Study

1. T/R informed κ-Capacity
2. Loss in σ-capacity due to LPD constraint

$$C_\sigma(dP_\kappa^*)/C_\sigma(dP_\sigma^*)$$

3. Loss in κ-capacity due to Pavg constraint

$$C_\kappa(dP_\sigma^*)/C_\kappa(dP_\kappa^*)$$

4. Loss in κ-capacity due to training errors

$$T = 1024, \quad T_{train} = 128$$

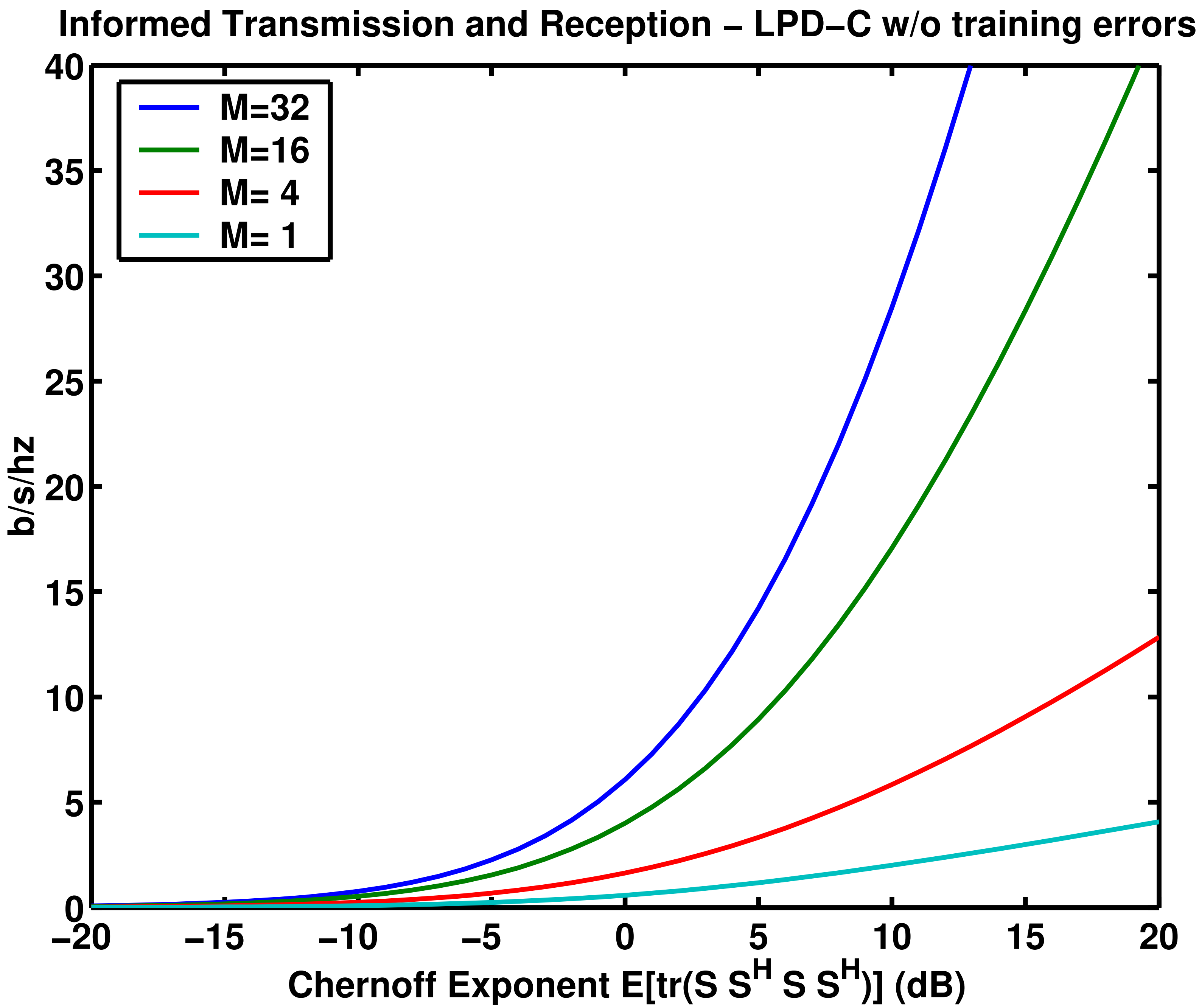

Figure 10. *T/R informed κ-capacity (N = M)*

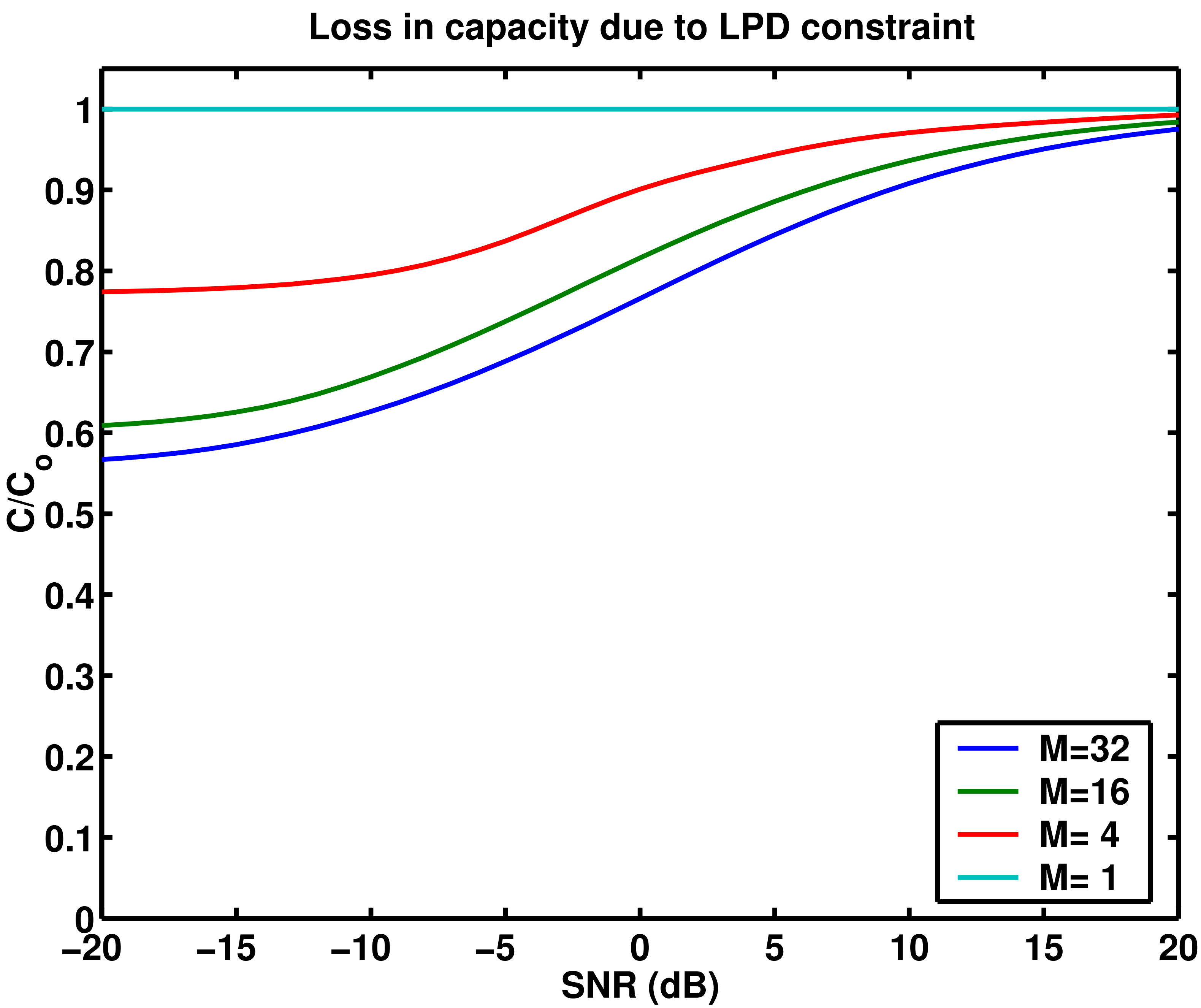

Figure 11. *Loss in σ-capacity due to LPD constraint (N = M)*

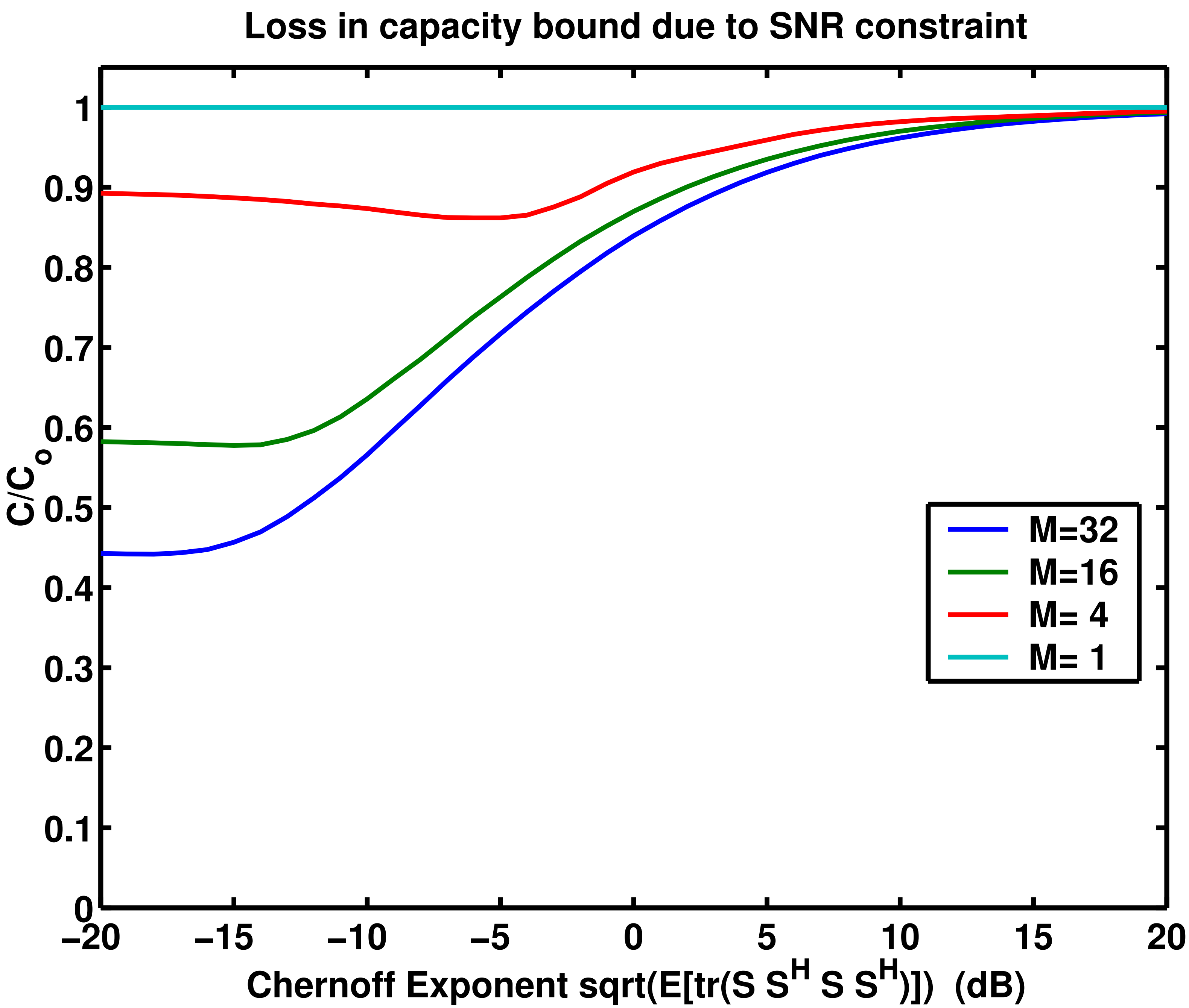

Figure 12. *Loss in κ-capacity due to Pavg constraint (N = M)*

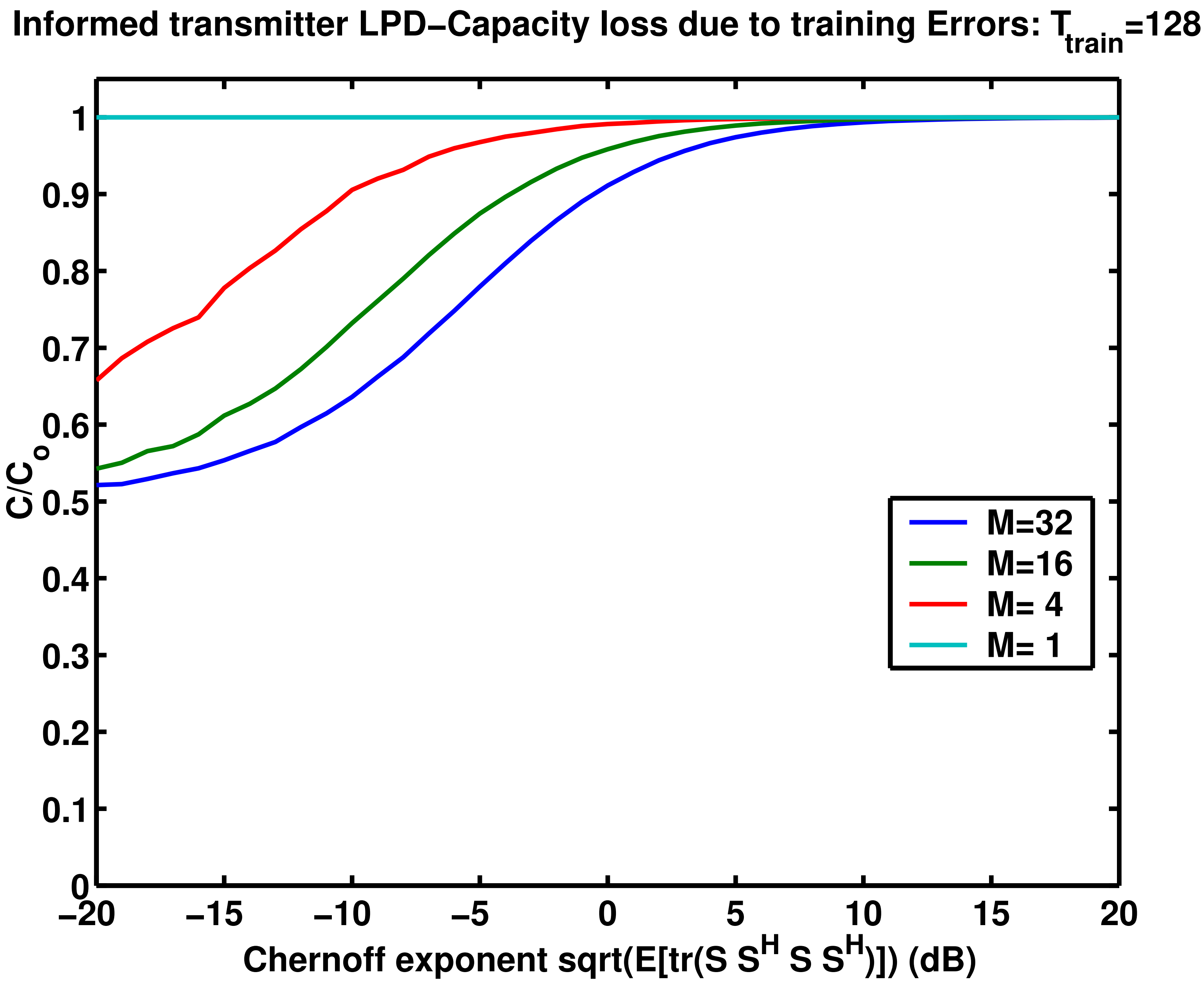

Figure 13. *T/R informed κ-capacity loss due to training errors (N = M)*

Conclusions

1. Capacity and other link level QoS metrics can be analyzed under network security constraints
2. Optimal signalling for LPD- and LPI- constrained *secure* channels is qualitatively different from *open* channels
3. Transmit kurtosis is relevant constraint for ensuring LPD to eavesdropper
4. Smart eavesdropper with info on training sequences can be handled similarly
5. Analogous analysis of R-informed link capacity is of interest
6. Extensions to min and sum capacities will account for network level QoS