Imperfect Information Theoretic Secrecy for Multimode Fiber

Eva C. Song, Emina Soljanin, Kyle C. Guan, Peter J. Winzer
csong@princeton.edu, emina@research.bell-labs.com, {kyle.guan, winzer}@alcatel-lucent.com

Alcatel·Lucent Bell Labs
PRINCETON UNIVERSITY

Motivation

Space-division multiplexing (SDM) is needed for growing demand of optical communication because single mode fiber has been shown to reach its capacity limit (see Fig. 1). SDM can be realized via multimode fiber (MMF). Optical network is vulnerable to physical layer attack (see Fig. 2). The secrecy capacity under equivocation for perfect secrecy was studied in [1] and [2]. In this work, we apply joint source-channel coding and use distortion as the metric for secrecy.

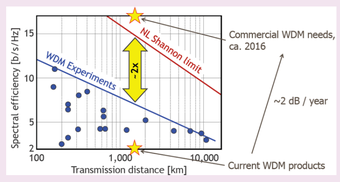


Fig. 1

Fig. 2

System Model

The communication through an M-mode optical SDM system exposed to eavesdropping is modeled as a memoryless complex gaussian MIMO broadcast channel. Eavesdropper suffers from mode dependent loss (MDL).

$$\begin{aligned} \text{Legitimate:} \quad & Y = HX + N \\ \text{Eavesdropper:} \quad & Y^e = H^e X + N^e \end{aligned}$$
$$H = \sqrt{E_0 L}U \quad , \quad H^e = \sqrt{E_0 L^e}\sqrt{V}U^e$$

MMF input have the following per mode power constraint averaged over n uses of channel

$$\frac{1}{n}\sum_{i=1}^{n} |X_i^{(m)}|^2 \quad \leq \quad 1, \forall m \in [1:M]$$

- S^k: i.i.d. source sequence sent by Alice
- $\hat{S}^k$: Bob's reconstruction of source sequence based on his channel output Y^n
- T^k: Eve's estimate of source sequence based on her channel output Z^n and possibly other side information

Definition 1. *For a given distortion function $d(s,t)$, (R,D) is achievable if there exists a sequence of $f_{k,n}$ and $g_{k,n}$ such that*

$$\frac{k}{n} = R, \quad \lim_{n\to\infty} \mathbb{P}[S^k \neq \hat{S}^k] = 0, \qquad (Bob)$$

and

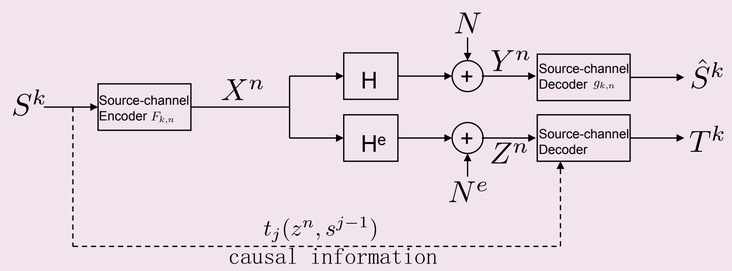
$$\liminf_{n\to\infty} \min_{t^k(z^n)} \mathbb{E}[d(S^k, t^k(Z^n))] \geq D. \quad (Eve)$$

Alternatively, we also consider the case

$$\liminf_{n\to\infty} \min_{\{t^k(z^n, s^{j-1})\}_{j=1}^k} \mathbb{E}[\frac{1}{k}\sum_{j=1}^{k} d(S_j, t_j(Z^n, S^{j-1})] \geq D.$$

- R: rate between Alice and Bob for reliable transmission
- D: distortion between Alice and Eve for security

Main Results



Theorem 1. *For i.i.d. source sequence S^k and memoryless broadcast channel $P_{YZ|X}$, if there exists $V - \square - W - \square - X - \square - YZ$ such that $I(W;Y|V) - I(W;Z|V) > 0$, then (R,D) is achievable if and only if*

$$R < \frac{\max_X I(X;Y)}{H(S)}$$
$$D \leq D_{max}$$

where $D_{max} = \min_t \mathbb{E}[d(S,t)]$.

Theorem 2. *If $\max_{K\in\mathcal{H}^{M\times M}, 0\preceq K\preceq I} \frac{|SNRK+I|}{|SNR^e U^e K U^{e\dagger} V+I|} > 0$, then the following rate distortion pair (R,D) is achievable with **no causal information**:*

$$\begin{aligned} R &< M\log(SNR+1)/H(S) \\ D &\leq D_{max} \end{aligned}$$

Theorem 3. *For i.i.d. source sequence S^k and Hamming distortion, the following distortion rate curve $D(R)$ is in the achievable region **with causal information**[3]:*

$$D = \begin{cases} d(H(S)), & \text{if } R \leq \frac{R_s^*}{H(S)} \\ \alpha(K)D_{max} + (1-\alpha(K))d(\frac{R_s(K)}{R}), & \text{if } \frac{R_s^*}{H(S)} < R \leq \frac{R_p^*}{H(S)} \end{cases}$$

where $d(R_s') \triangleq \min(f(R_s'), 1-\max_s P_S(s))$ and $f(R_s')$ is the linear interpolation of the points $(\log n, \frac{n-1}{n})$, $n = 1,2,3,...$; $\mathcal{K} \triangleq \{K \in \mathcal{H}^{M\times M}, 0 \preceq K \preceq I\}$

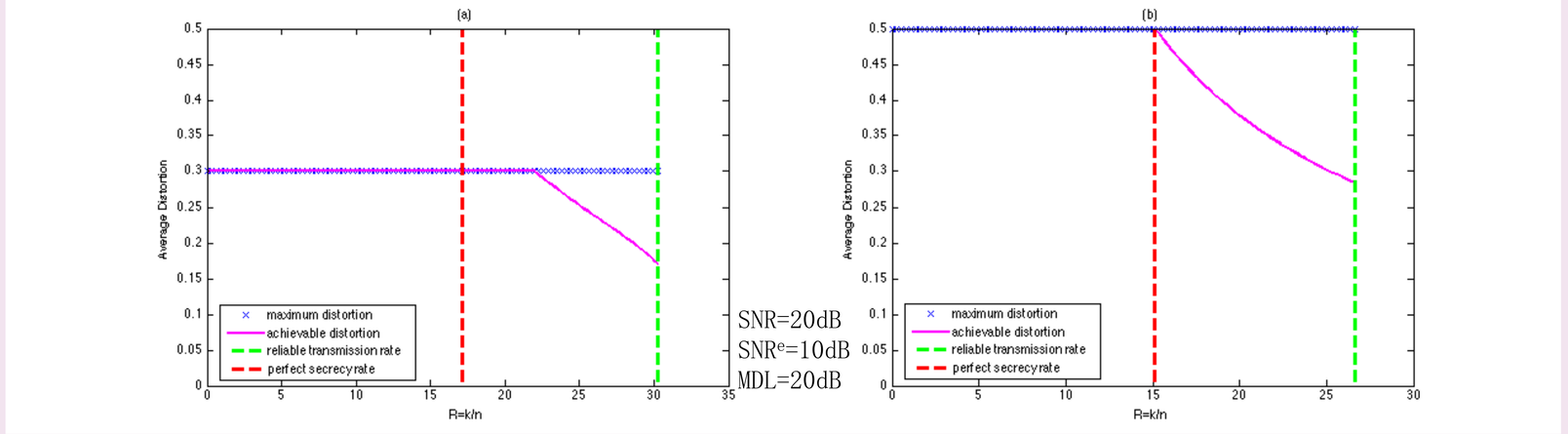
$$R_s^* = \max_{K'\in\mathcal{K}} \log \frac{|SNRK'+I|}{|SNR^e\sqrt{V}U^e K' U^{e\dagger}\sqrt{V}+I|}, \quad R_p^* = M\log(SNR+1),$$

$$R_s(K) = \log \frac{|SNRK+I|}{|SNR^e\sqrt{V}U^e K U^{e\dagger}\sqrt{V}+I|},$$

$$\alpha(K) = \frac{\beta(K)-\gamma(K)}{\beta(K)}, \quad \beta(K) = \log\frac{|(SNR+1)I|}{|SNRK+I|}, \quad \gamma(K) = \log\frac{|SNR^e V+I|}{|SNR^e\sqrt{V}U^e K U^{e\dagger}\sqrt{V}+I|}.$$

Some Numerical Results

Achievable rate-distortion curves of MMF with $Bern(0.3)$ and $Bern(0.5)$ i.i.d. sources [4]:



References

[1] K. Guan, P. J. Winzer, and E. Soljanin, "Information-theoretic security in space-division multiplexed fiber optic networks", ECOC 2012

[2] T. Liu and Y. Liang, "Multiple-input multiple-output gaussian broadcast channels with common and confidential messages", IEEE Trans. Inf Theory, Vol 56, pp. 5477-5487, 2010

[3] C. Schieler, E. C. Song, P. Cuff, and H. V. Poor, "Source-channel secrecy with causal disclosure", Allerton 2012

[4] K. Guan, E. C. Song, E. Soljanin, and P. J. Winzer, "Physical layer security in space-division multiplexed fiber optic communications", Asilomar 2012