Reversible Information Embedding with Compressed Host at the Decoder

Yossef Steinberg

Department of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 32000, Israel

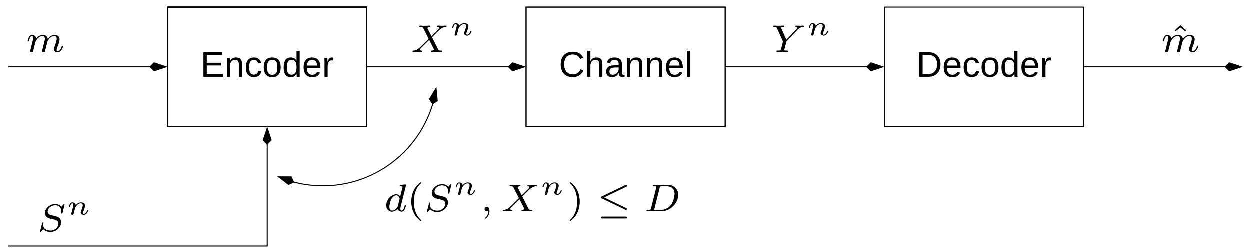
The 2006 Information Theory Symposium—ISIT ‘06:

Seattle, Washington, July 2006

Outline

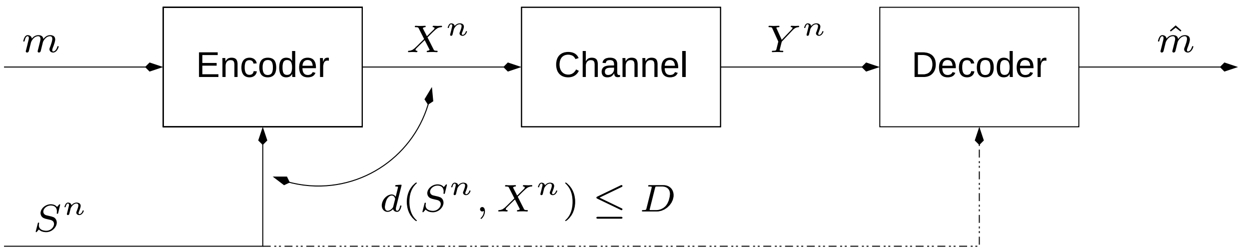
- The general Information Embedding problem
  - Public vs. private
  - The distortion constraint
- Reversible Information Embedding
- Previous work
- Compressed host @ decoder(s)
- Main result
- Extensions and future work

The Information Embedding (IE) Problem



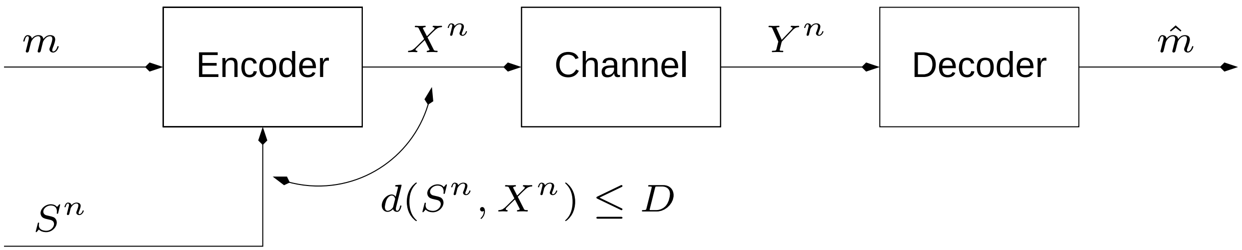
- A message m is embedded into host signal S^n, producing data set X^n
- X^n is transmitted via $P_{Y|X}$ to its destination
- At the destination, a noisy version Y^n of the data set is received, from which m is decoded.
- In IE, m is embedded into S^n in a manner that is transparent to the unintended observer $\Rightarrow$ a distortion constraint between S^n and X^n
- Public IE – The host S^n is known only at the decoder

The Information Embedding (IE) Problem



- A message m is embedded into host signal S^n, producing data set X^n
- X^n is transmitted via $P_{Y|X}$ to its destination
- At the destination, a noisy version Y^n of the data set is received, from which m is decoded.
- In IE, m is embedded into S^n in a manner that is transparent to the unintended observer $\Rightarrow$ a distortion constraint between S^n and X^n
- Public IE – The host S^n is available only at the encoder
- Private IE – The host S^n is available at both, encoder and decoder

The IE Problem (cont'd)



The distortion constraint is imposed in order to:

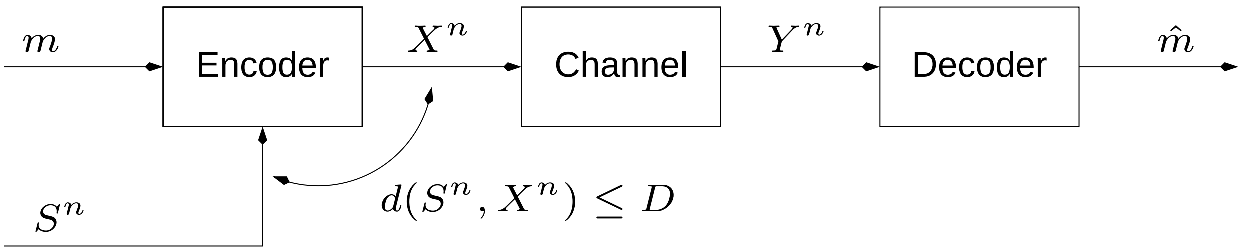
- Hide the fact that communication (beyond that of S^n) is taking place
- Reduce total distortion at the output

Classical IE puts emphasis on embedding rate vs. input distortion D.

Closely related to Gel'fand & Pinsker channel [Moulin & O'Sullivan, 2003], via the constraint. Thus

$$C = \max_{\mathbb{E}d(S,X)\leq D} [I(U;Y) - I(U;S)]$$

The IE Problem (cont'd)



The distortion constraint is imposed in order to:

- Hide the fact that communication (beyond that of S^n) is taking place
- Reduce total distortion at the output

Classical IE puts emphasis on embedding rate vs. input distortion D.

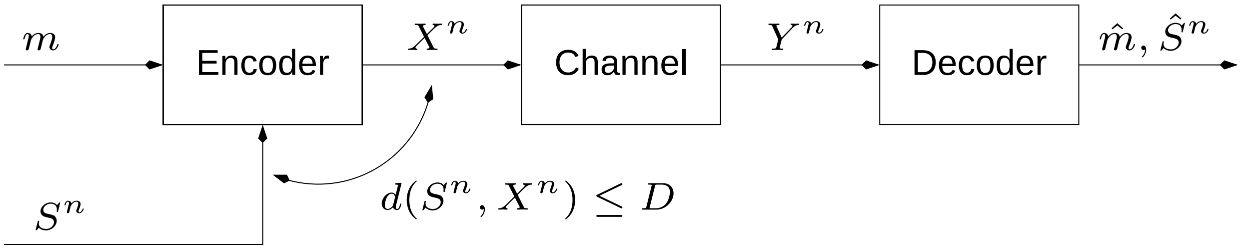
Closely related to Gel'fand & Pinsker channel [Moulin & O'Sullivan, 2003], via the constraint. Thus

$$C = \max_{\mathbb{E}d(S,X) \leq D} [I(U;Y) - I(U;S)]$$

But: Some applications cannot tolerate distortion at the destination (e.g., medical imagery).

Reversible IE

[Fridrich, Goljan, Du *SPIE* 2002], [Kalker & Willems, 2002]

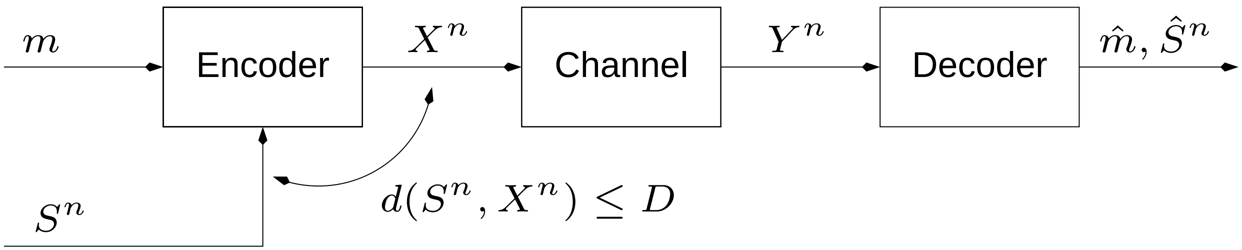


In reversible IE (RIE), an additional constraint is imposed, that S^n can be faithfully restored from Y^n. The constraint $\mathbb{E}d(S, X) \leq D$ is still relevant

$$C = \max H(X) - H(S) \quad \text{(no attack channel, Kalker \& Willems)}$$

$$C = \max I(X;Y) - H(S) \quad \text{(with channel, Kotagiri \& Laneman '05)}$$

Reversible IE (cont'd)



$$C = \max_{\mathbb{E}d(S,X)\leq D} I(X;Y) - H(S)$$

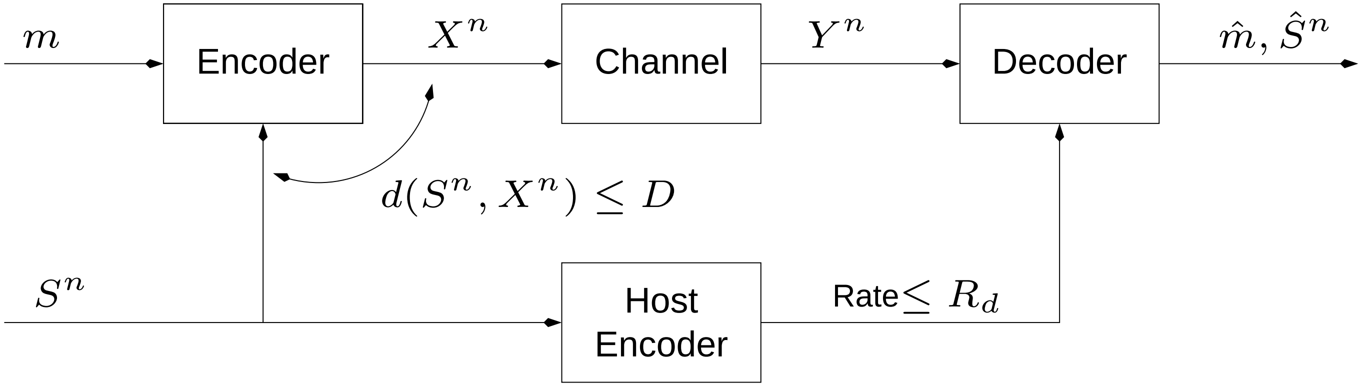
High cost is paid due to the requirement to reproduce the host.

Possible solution – provide the decoder, a priori, with side information on S^n:

- Independent of the embedded messages
- Available before communication (embedding) begins
- Rate limited.

$\Longrightarrow$ Reversible information embedding with compressed host at the decoder (RIEC)

RIEC - Problem formulation



<u>Problem:</u>

Characterize the region of all achievable (R, R_d, D), where:

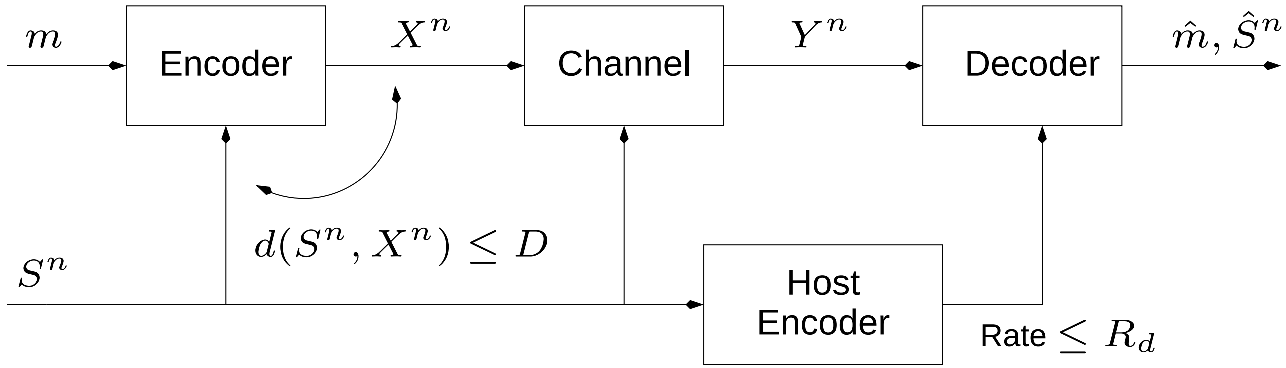
R – Embedding rate,

R_d – rate of compressed SI @ decoder

D – distortion between host and input

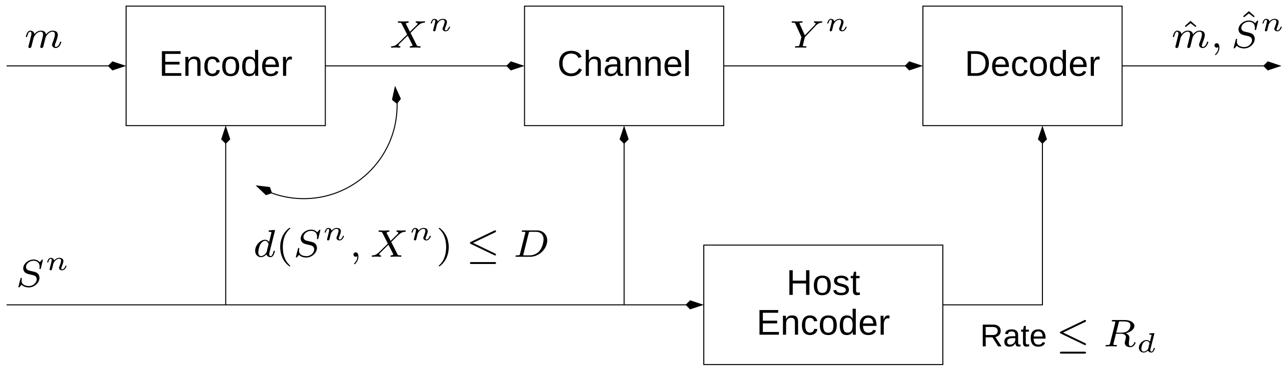
under the requirement of complete reconstruction of the host at the decoder.

Related problems



As the IE problem is closely related to the GP problem we let the channel depend on S.

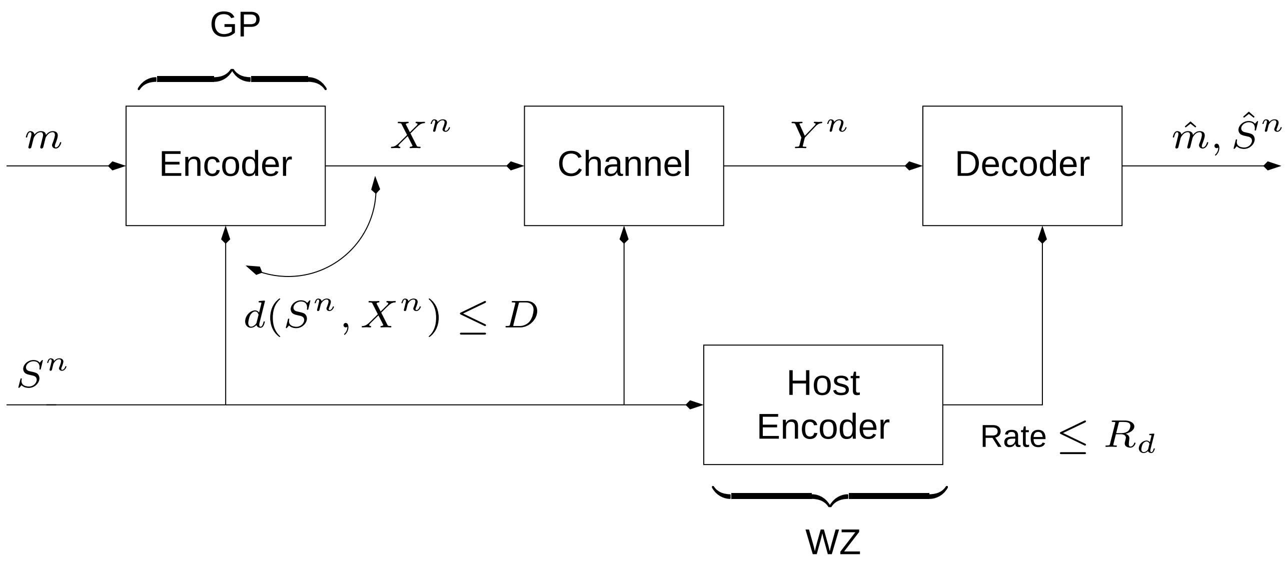
Related problems



- S^n is known noncausally at the encoder $\Rightarrow$ channel coding part is related to the Gel'fand-Pinsker (GP) problem.

- Y^n depends statistically on S^n and can serve as side information (SI) in retrieving the compressed state at the decoder $\Rightarrow$ coding of S^n is related to the Wyner-Ziv (WZ) problem.

Related problems (cont'd)



- For the WZ problem, the SI Y^n is not memoryless
- There is no distortion constraint in retrieving S^n at the decoder (instead, maximize capacity of the main channel)

Previous work

1. Wyner & Ziv, 1976
2. Gel'fand & Pinsker, 1980
3. Fridich, Goljan, & Du 2002. Kalker & Willems 2002.
4. Kotagiri & Laneman, 2005 – RIE in multiuser channels.
5. Heegard & El Gamal, 1983, "On the capacity of computer memory with defects." Introduced coding for state dependent channels with rate limited side information at both ends. Devised an achievable region.
6. Steinberg 2006 – Coding with rate limited SI.

The current model is a combination of 4 and 6.

Main result

$\mathcal{R}^*$ – collection of all (R, R_d, D) satisfying

$$
\begin{aligned}
R &\leq I(X, S; Y|S_d) - H(S|S_d) \\
R_d &\geq I(S; S_d) - I(Y; S_d) \\
D &\geq \mathbb{E}(S, X)
\end{aligned}
$$

for some S_d such that $S_d \multimap (S, X) \multimap Y$. Then

Theorem: For any discrete memoryless (state-dependent) attack channel, with full noncausal SI at the transmitter, and rate-limited SI at the receiver, a triple (R, R_d, Γ) is achievable with perfect reconstruction of S^n at the decoder, if and only if $(R, R_d, \Gamma) \in \mathcal{R}^*$.

Main result (cont'd)

$\mathcal{R}^*$ – collection of all (R, R_d, D) satisfying

$$
\begin{aligned}
R &\leq I(X, S; Y | S_d) - H(S | S_d) \\
R_d &\geq I(S; S_d) - I(Y; S_d) \\
D &\geq \mathbb{E}\big(S, X\big)
\end{aligned}
$$

for some S_d such that $S_d \multimap (S, X) \multimap Y$.

- $\mathcal{R}^*$ is convex
- S_d – A WZ rv, represents the compressed state S^n. Fully decoded, with Y^n as SI.

Main result (cont'd)

$\mathcal{R}^*$ – collection of all (R, R_d, D) satisfying

$$\begin{aligned} R &\leq I(X,S;Y|S_d) - H(S|S_d) \\ R_d &\geq I(S;S_d) - I(Y;S_d) \quad (*) \\ D &\geq \mathbb{E}d(S,X) \end{aligned}$$

for some S_d such that $S_d -\!\!\circ\!\!- (S,X) -\!\!\circ\!\!- Y$.

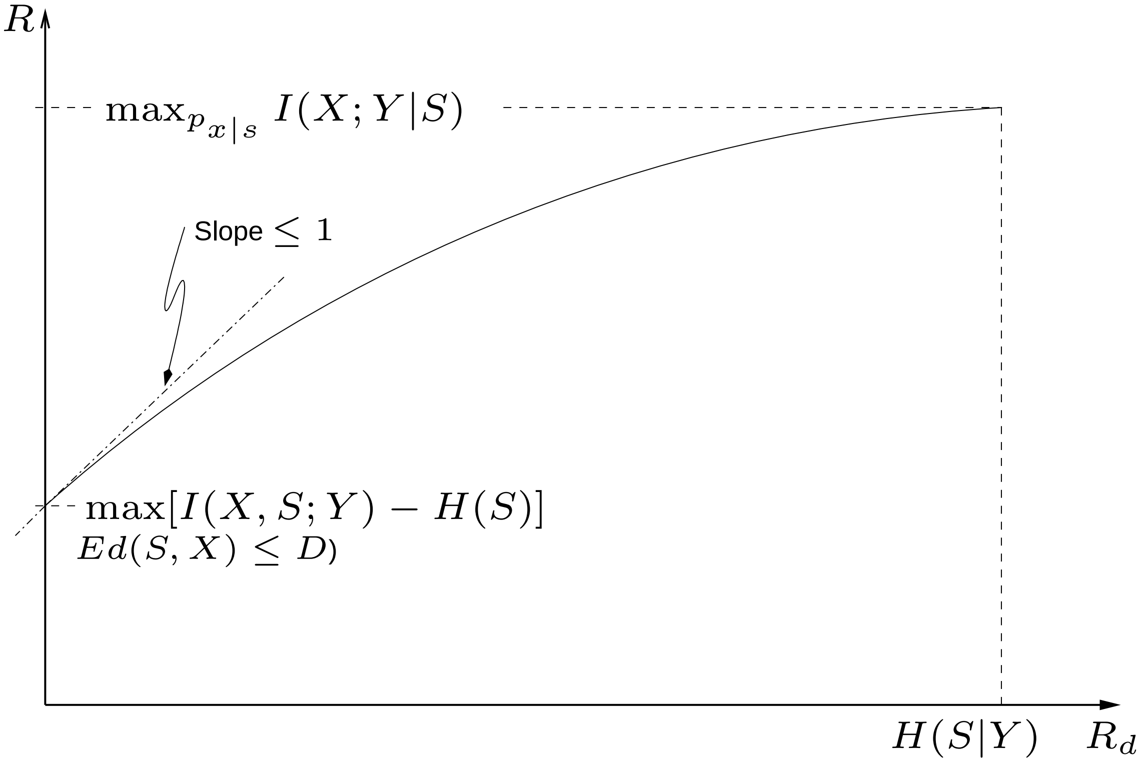
- $S_d -\!\!\circ\!\!- (S,X) -\!\!\circ\!\!- Y$ does not imply $S_d -\!\!\circ\!\!- S -\!\!\circ\!\!- Y$. Therefore $(*)$ is not equivalent to

  $$R_d \geq I(S;S_d|Y),$$

  full duality with GP.
- In classical WZ, $S_d -\!\!\circ\!\!- S -\!\!\circ\!\!- Y$ is needed to guarantee joint typicality of S_d and Y. Here it is guaranteed due to the channel.

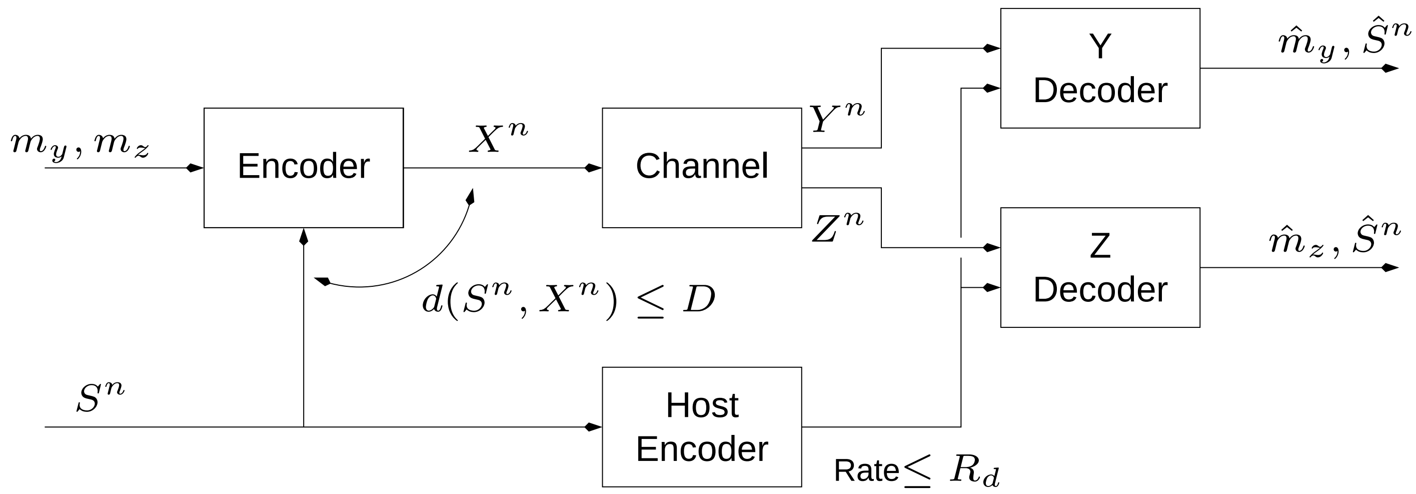
A typical (R, R_d) *curve*

A typical (R, R_d) curve, for fixed D:



- The rate allocated to provide the decoder with compressed host (SI), is always at least as high as the gain in the embedding rate.
- Provide SI to the decoder when the wayside channel cannot be used to transmit embedded data – e.g.
  - Remotely located physical channel
  - IE systems where a compressed host is kept in memory at the decoder, for future use.

RIEC with several stages of attack



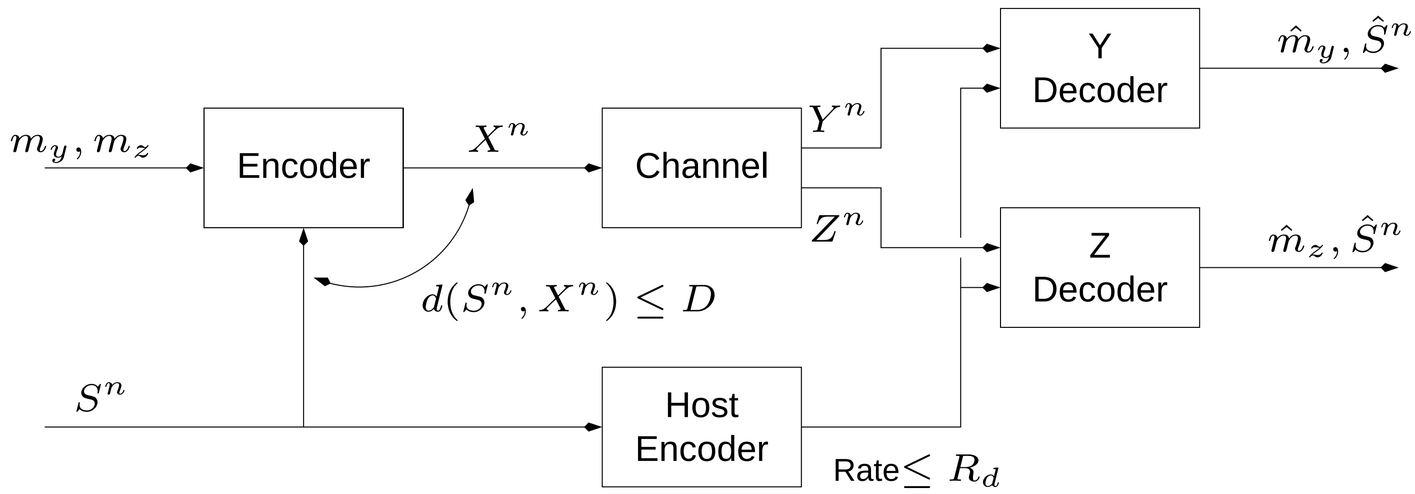
Extension of the Kotagiri & Laneman model.

Assume a degraded broadcast channel:

$$P_{Y,Z|X,S} = P_{Y|X,S} P_{Z|Y},$$

a good model for several stages of attack.

RIEC with several stages of attack



The region of all achievable (R_y, R_z, R_d, D) is given by the set of all quadruples satisfying

$$\begin{aligned} R_y &\le I(X;Y|U,S_d,S) \\ R_z &\le I(U,S;Z|S_d) - H(S|S_d) \\ R_d &\ge I(S_d;S) - I(S_d;Z) \\ D &\ge \mathbb{E}d(S,X) \end{aligned}$$

for some $(U,S_d) \multimap (X,S) \multimap (Y,Z)$.

Future work

- Extensions to other network models
  - MAC
  - Ad hoc networks. Part of the users are silent, and can transmit SI at low cost.
- Specific models. Coding schemes.
- Computational algorithms.