A Fresh Look at Wireless Security and Multimedia

Ashish Khisti

Department of Electrical and Computer Engineering
University of Toronto

February 4, 2013

Talk Outline

Information Theoretic Approaches to Security (ITAS)

- Physical Layer Resources
- Secret-Key Generation
- Multiple Antennas for Secure Communication

Streaming Communications Systems — Fundamental Limits

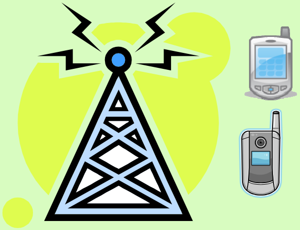
- Error Correction Codes for Streaming Data
- Sequential Compression for Streaming Sources
- Streaming over Wireless Fading Channels
- Deterministic Channel Approximations

Security at PHY-Layer

Use PHY Resources for designing security mechanisms.

Application Layer (Semantics of Information)
Transport Layer (End to End Connectivity)
Network Layer (Routing and Path Discovery)
Data Link Layer (Error Correction Codes)
Physical Layer (Signals, RF hardware)

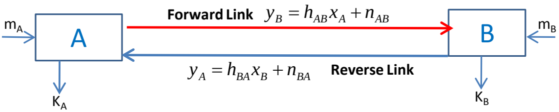
Wireless Systems

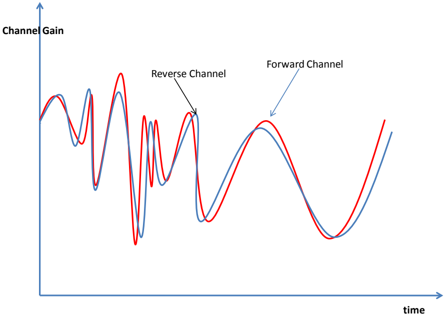


Applications:

- Secret-Key Generation
- Secure Message Transmission
- Physical Layer Authentication
- Jamming Resistance

Secret-Key Generation in Wireless Fading Channels





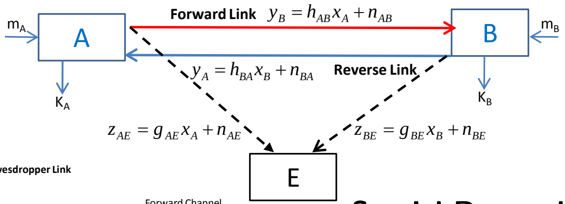
Fading:

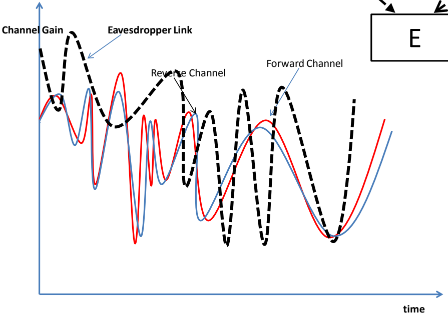
$$y_B(t) = h_{AB}(t)x_A(t)+n_B(t)$$

Reciprocity:

$$y_B(t) = h_{AB}(t)x_A(t) + n_B(t)$$
$$y_A(t) = h_{BA}(t)x_B(t) + n_A(t)$$

Secret-Key Generation in Wireless Fading Channels





Spatial Decorrelation:

$$y_B(t) = h_{AB}(t)x_A(t) + n_B(t)$$
$$y_A(t) = h_{BA}(t)x_B(t) + n_A(t)$$
$$z_A(t) = g_A(t)x_A(t) + n_{AE}(t)$$
$$z_B(t) = g_B(t)x_B(t) + n_{BE}(t)$$

Secret-Key Generation - A Systems Approach

Key Generation in Wireless Systems

- UWB Systems: Wilson-Tse-Scholz ('07), M. Ko ('07), Madiseh-Neville-McGuire('12)
- Narrowband Systems: Azimi Sadjadi- Kiayias-Mercado-Yener ('07), Mathur-Trappe-Mandayam -Ye-Reznick ('10), Patware and Kasera ('07)
- OFDM reciprocity: Haile ('09), Tsouri and Wulich ('09)

Implementations

- Experimental UWB: Measurements for Key Generation Madiseh ('12)
- Software Radio Implementations: Jana et. al. ('09)
- MIMO systems: Wallace and Sharma ('10), Shimizu et al. Zeng-Wu-Mohapatra

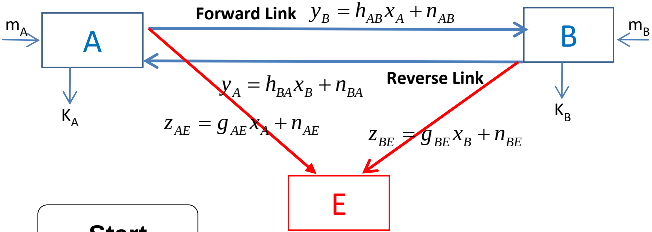
Signal Processing for Secret-Key Generation

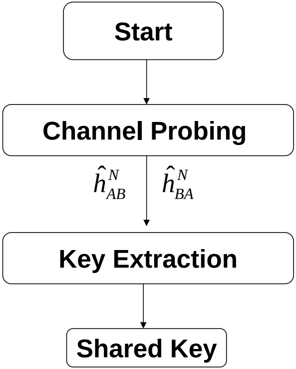
- Quantization Techniques: Ye-Reznik-Shah ('07), Hamida-Pierrot-Castelluccia ('09), Sun-Zhu-Jiang-Zhao ('11)
- Adaptive Channel Probing: Wei-Zheng-Mohapatra ('10)
- Mobility Assisted Key Generation: Gungor-Chen-Koksal ('11)

Attacks

- Active Eavesdroppers: Ebrez et. al ('11) Zafer-Agrawal-Srivatsa ('11),
- Unauthenticated Channels: Mathur et al. ('10), Xiao-Greenstein-Mandayam-Trappe ('07).

Secret-Key Generation: A Systems Approach II





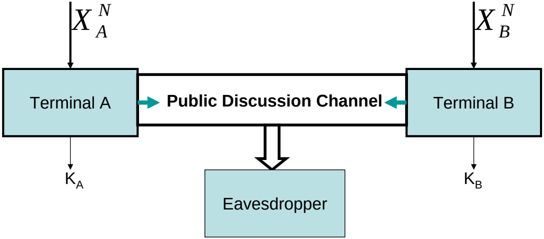
Two Phase Approach:

- **Phase I**: Channel Probing and Estimation: $(\hat{h}_{AB}^N, \hat{h}_{BA}^N)$
- **Phase 2**: Source Reconciliation and Key Extraction

Secret-Key Generation: Capacity Limits

Secret-Key Generation - Source Model

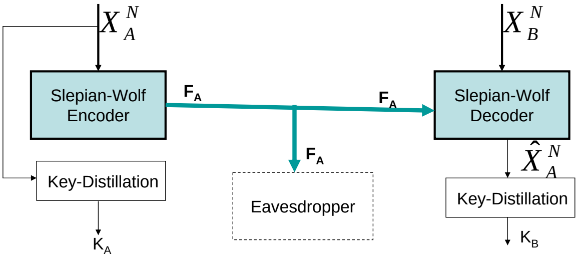
Maurer ('93), Ahlswede-Csiszar ('93)



- DMMS Model: $(x_A^N, x_B^N) \sim \prod_{i=1}^{N} p_{x_A,x_B}(x_A(i), x_B(i))$
- Interactive Public Communication: $\mathbf{F}$
- Key Generation: $k_i = \mathcal{F}_i(x_i^N, \mathbf{F})$, $i \in \{A, B\}$.
- Reliability: $\Pr(k_A \neq k_B) \leq \varepsilon_N$,
- Secrecy: $\frac{1}{N} I(k_A; \mathbf{F}) \leq \varepsilon_N$
- Secret-Key Rate: $R = \frac{1}{N} H(k_A)$

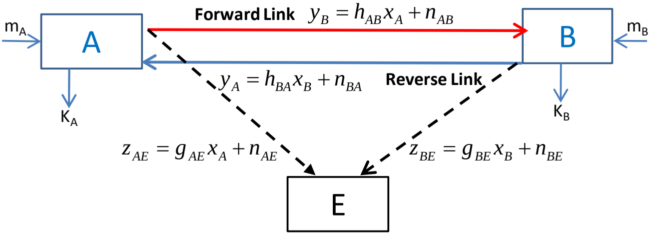
Secret-Key Generation - Source Model

Maurer ('93), Csiszar-Ahlswede ('93)



- Capacity: $C = I(x_A; x_B)$
- One-Round of Communication
- Capacity Unknown when Eavesdropper also observes a source sequence

Problem Setup

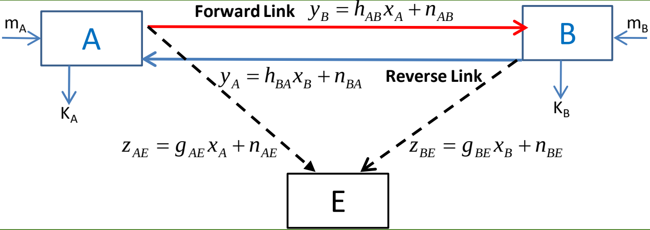


Two-Way Reciprocal Fading Channel

$$y_B(i) = h_{AB}(i)x_A(i) + n_{AB}(i), \qquad y_A(i) = h_{BA}(i)x_B(i) + n_{BA}(i)$$

$$z_A(i) = g_A(i)x_A(i) + n_{AE}(i), \qquad z_B(i) = g_B(i)x_B(i) + n_{BE}(i)$$

Problem Setup



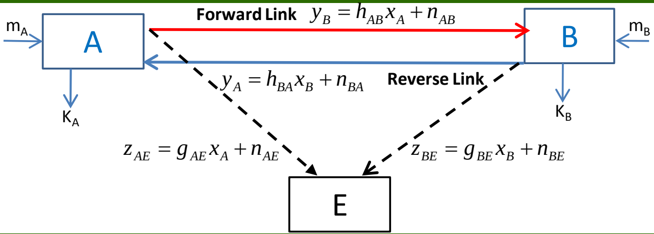
Two-Way Reciprocal Fading Channel

$$y_B(i) = h_{AB}(i)x_A(i) + n_{AB}(i), \qquad y_A(i) = h_{BA}(i)x_B(i) + n_{BA}(i)$$
$$z_A(i) = g_A(i)x_A(i) + n_{AE}(i), \qquad z_B(i) = g_B(i)x_B(i) + n_{BE}(i)$$

Channel Model Assumptions:

- Non-Coherent Model: $h_{AB}(i)$ and $h_{BA}(i)$
- Perfect Eavesdropper CSI: $g_A(i)$ & $g_B(i)$ known to Eve
- Block-Fading Channel with Coherence Period: T.
- Approximate Reciprocity: $(h_{AB}, h_{BA}) \sim p_{h_{AB},h_{BA}}(\cdot,\cdot)$
- Independence: $(g_A, g_B) \perp (h_{AB}, h_{BA})$

Problem Setup



Two-Way Reciprocal Fading Channel

$$y_B(i) = h_{AB}(i) x_A(i) + n_{AB}(i), \qquad y_A(i) = h_{BA}(i) x_B(i) + n_{BA}(i)$$

$$z_A(i) = g_A(i) x_A(i) + n_{AE}(i), \qquad z_B(i) = g_B(i) x_B(i) + n_{BE}(i)$$

Secret-Key Agreement Protocols:

- Interactive: $x_A(i) = f_A(m_A, y_A^{i-1})$, $x_B(i) = f_B(m_B, y_B^{i-1})$
- Average Power Constraints $E[|x_A|^2] \leq P$, $E[|x_B|^2] \leq P$.
- $k_A = \mathcal{K}_A(y_A^N, m_A)$, $k_B = \mathcal{K}_B(y_B^N, m_B)$
- Reliability and Secrecy Constraint.
- Secret-Key Capacity

Outline

- Upper Bound
- Lower Bound — With Public Discussion
- Lower Bound — No Public Discussion
- Asymptotic Regimes and Numerical Results

Secret-Key Capacity — Upper Bound

Khisti'12

Theorem

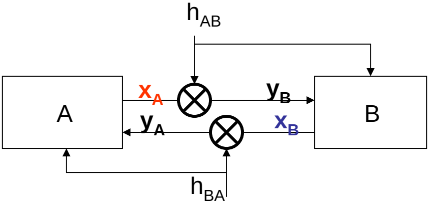
An upper bound on the secret-key capacity is $C \leq R^+$:

$$R^+ = \frac{1}{T} I(h_{AB}; h_{BA}) + \max_{P(h_{AB}) \in \mathcal{P}} E\left[\log\left(1 + \frac{P(h_{AB})|h_{AB}|^2)}{1 + P(h_{AB})|g_A|^2}\right)\right]$$
$$+ \max_{P(h_{BA}) \in \mathcal{P}} E\left[\log\left(1 + \frac{P(h_{BA})|h_{BA}|^2}{1 + P(h_{BA})|g_B|^2)}\right)\right]$$

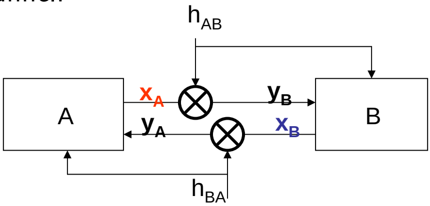
where $P(h_{AB})$ and $P(h_{BA})$ are power allocation function across the fading states.

Secret-Key Capacity — Upper Bound

Genie-Aided Channel:



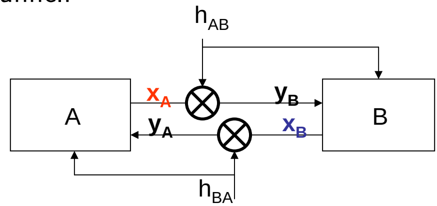
Genie-Aided Channel:



$$NTR \leq I(m_A, h_{BA}^N, y_A^{NT}; m_B, h_{AB}^N, y_B^{NT} | \mathbf{z}^{NT}, \mathbf{g}^N)$$

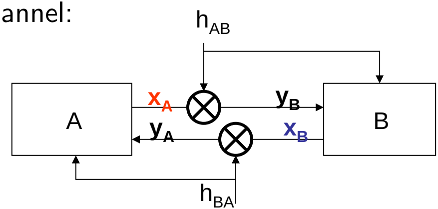
Secret-Key Capacity — Upper Bound

Genie-Aided Channel:



$$
\begin{aligned}
NTR &\le I(m_A, h_{BA}^N, y_A^{NT}; m_B, h_{AB}^N, y_B^{NT} | \mathbf{z}^{NT}, \mathbf{g}^N) \\
&\le I(x_A(NT); y_B(NT) | h_{AB}(N), z_A(NT), g_A(N)) \\
&\quad + I(x_B(NT); y_A(NT) | h_{BA}(N), z_B(NT), g_B(N)) \\
&\quad + I(m_A, h_{BA}^N, y_A^{NT-1}; m_B, h_{AB}^N, y_B^{NT-1} | \mathbf{z}^{NT-1}, \mathbf{g}^N)
\end{aligned}
$$

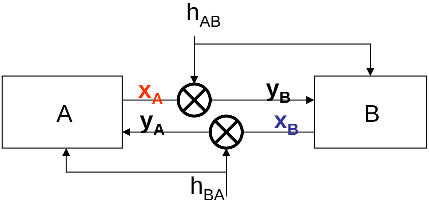
Genie-Aided Channel:



$$
\begin{aligned}
NTR &\le I(m_A, h_{BA}^N, y_A^{NT}; m_B, h_{AB}^N, y_B^{NT} | \mathbf{z}^{NT}, \mathbf{g}^N) \\
&\le \sum_{n=1}^{NT} I(x_A(n); y_B(n) | \bar{h}_{AB}(n), z_A(n), \bar{g}_A(n)) \\
&\quad + \sum_{n=1}^{NT} I(x_B(n); y_A(n) | \bar{h}_{BA}(n), z_B(n), \bar{g}_B(n)) \\
&\quad + NI(h_{AB}; h_{BA})
\end{aligned}
$$

Secret-Key Capacity — Upper Bound

Genie-Aided Channel:

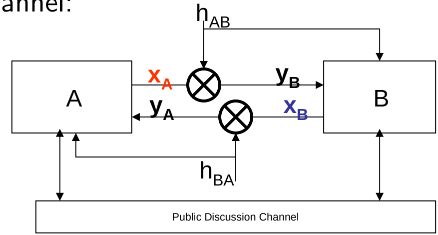


Interpretation of the Upper Bound:

- Channel Reciprocity: $\frac{1}{T} I(h_{AB}; h_{BA})$
- Forward Channel: $I(y_B; x_A | h_{AB}, z_A, g_A)$
- Reverse Channel: $I(y_A; x_B | h_{BA}, z_B, g_B)$

Secret-Key Capacity — Upper Bound

Genie-Aided Channel:



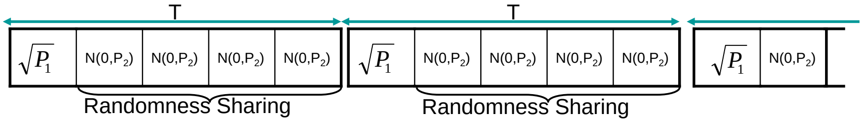
Interpretation of the Upper Bound:

- Channel Reciprocity: $\frac{1}{T}I(h_{AB}; h_{BA})$
- Forward Channel: $I(y_B; x_A | h_{AB}, z_A, g_A)$
- Reverse Channel: $I(y_A; x_B | h_{BA}, z_B, g_B)$

Upper Bound also holds if a public discussion channel is available.

Lower Bound: Separation Based Scheme

Khisti '12

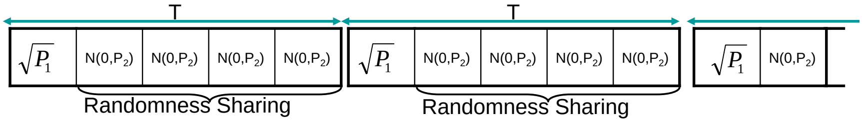


- Training: $x_A(i,1) = \sqrt{P_1}$
- Randomness Sharing: $x_A(i,t) \sim \mathcal{CN}(0, P_2)$ for $t = 2, \ldots, T$
  $\mathbf{x}_A(i) = [x_A(i,2), \ldots, x_A(i,T)] \in \mathbb{C}^{T-1}$.

- Training: $\hat{h}_{AB}(i)$ and $\hat{h}_{BA}(i)$
- Correlated Sources:
  Forward Channel: $\mathbf{y}_B(i) = h_{AB}(i)\mathbf{x}_A(i) + \mathbf{n}_B(i) \in \mathbb{C}^{T-1}$,
  Reverse Channel: $\mathbf{y}_A(i) = h_{BA}(i)\mathbf{x}_B(i) + \mathbf{n}_A(i) \in \mathbb{C}^{T-1}$.

Lower Bound: Separation Based Scheme

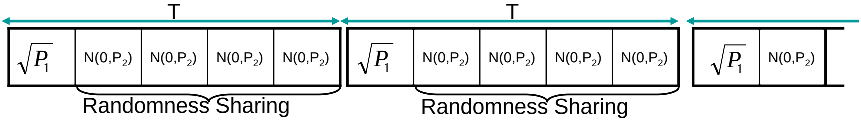
Khisti '12



	A	B	E
Channel State	$\hat{h}_{BA}^K$	$\hat{h}_{AB}^K$	(g_A^K, g_B^K)
Forward Channel	$\mathbf{x}_A^K$	$\mathbf{y}_B^K$	$\mathbf{z}_A^K$
Reverse Channel	$\mathbf{y}_A^K$	$\mathbf{x}_B^K$	$\mathbf{z}_B^K$

Lower Bound: Separation Based Scheme

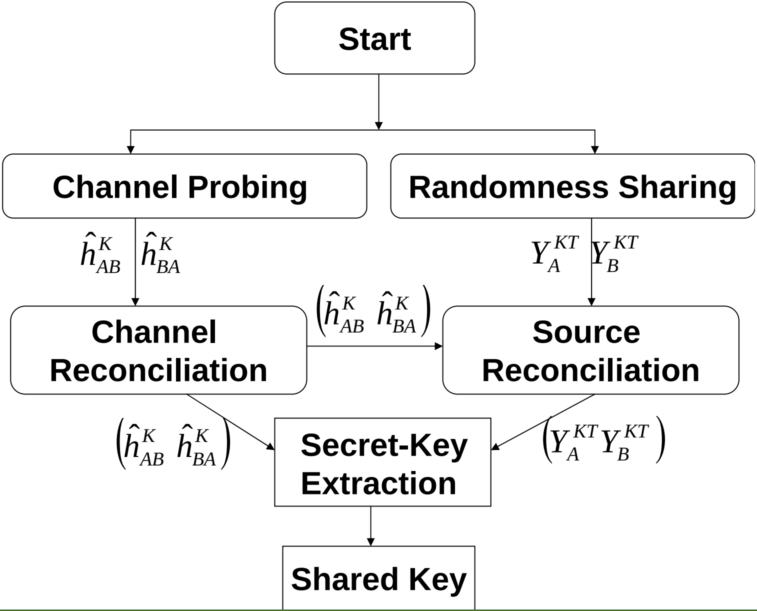
Khisti '12



	A	B	E
Channel State	$\hat{h}_{BA}^K$	$\hat{h}_{AB}^K$	(g_A^K, g_B^K)
Forward Channel	$\mathbf{x}_A^K$	$\mathbf{y}_B^K$	$\mathbf{z}_A^K$
Reverse Channel	$\mathbf{y}_A^K$	$\mathbf{x}_B^K$	$\mathbf{z}_B^K$

Generate a secret-key from these sequences.

Lower Bound — Overview



Achievable Rate with Public Discussion

Theorem (Public Discussion)

An achievable rate when a public discussion channel is available is

$$R_{\text{key}} = \Bigg\{ \frac{1}{T} \underbrace{I(\hat{h}_{AB}; \hat{h}_{BA})}_{\text{Training}} + \frac{T-1}{T} \underbrace{\Big[I(y_B; x_A, \hat{h}_{AB}) - I(y_B; z_A, g_A, h_{AB}) \Big]}_{\text{Forward Channel}} + \frac{T-1}{T} \underbrace{\Big[I(y_A; x_B, \hat{h}_{BA})) - I(y_A; z_B, g_B, h_{BA}) \Big]}_{\text{Reverse Channel}} \Bigg\}$$

Achievable Rate with Public Discussion

Theorem (Public Discussion)

An achievable rate when a public discussion channel is available is

$$R_{\text{key}} = \Bigg\{ \frac{1}{T} \underbrace{I(\hat{h}_{AB}; \hat{h}_{BA})}_{\text{Training}} + \frac{T-1}{T} \underbrace{\Big[I(y_B; x_A, \hat{h}_{AB}) - I(y_B; z_A, g_A, h_{AB}) \Big]}_{\text{Forward Channel}} + \frac{T-1}{T} \underbrace{\Big[I(y_A; x_B, \hat{h}_{BA})) - I(y_A; z_B, g_B, h_{BA}) \Big]}_{\text{Reverse Channel}} \Bigg\}$$

High SNR Regime

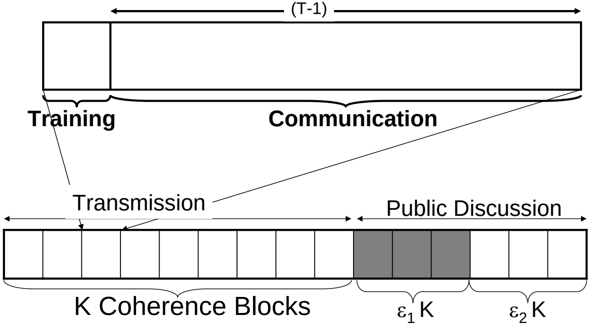
Theorem

In the high SNR regime our upper and lower bound (with public discussion) coincide:

$$\lim_{P\to\infty}\left\{R^{+}(P)-R^{-}_{\mathrm{PD}}(P)\right\}\leq\frac{c}{T}$$

where

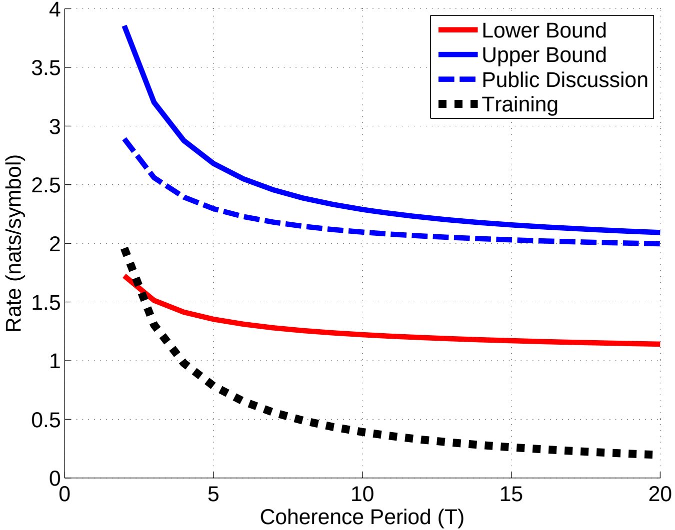
$$c = E\left[\log\left(1+\frac{|h_{AB}|^2}{|g_A|^2}\right)\right] + E\left[\log\left(1+\frac{|h_{BA}|^2}{|g_B|^2}\right)\right]$$



Phase	Coherence Blocks
Probing + Randomness Sharing	K
Channel-Sequence Reconciliation	$\varepsilon_1 \cdot K$
Source-Sequence Reconciliation	$\varepsilon_2 \cdot K$

Numerical Plot

SNR =35 dB, $h_1, h_2 \sim \mathcal{CN}(0,1)$, $\rho = 0.99$.



Symmetric MIMO Extension

M. Andersson, A. Khisti and M. Skoglund, 2012

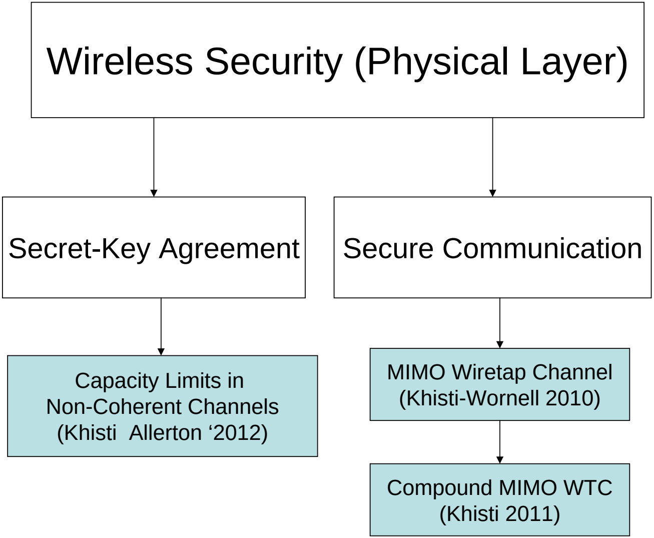
$$\mathbf{y}_B = \mathbf{H}_{AB}\mathbf{x}_A + \mathbf{n}_{AB}, \quad \mathbf{z}_A = \mathbf{G}_{AE}\mathbf{x}_A + \mathbf{n}_{AE}$$
$$\mathbf{y}_A = \mathbf{H}_{BA}\mathbf{x}_B + \mathbf{n}_{BA}, \quad \mathbf{z}_B = \mathbf{G}_{BE}\mathbf{x}_B + \mathbf{n}_{BE}$$

- $\mathbf{H}_A, \mathbf{H}_B \in \mathbb{C}^{M\times M}$, $\mathbf{G}_{AE}, \mathbf{G}_{BE} \in \mathbb{C}^{N_E \times M}$
- Independent Rayleigh Fading, Approximate Reciprocity
- Block Fading with Coherence Period T
- $T \geq M \geq N_E$

Training + Source Emulation achieves degrees of freedom given by:

$$d = \max_{M^\star \in [1,M]} 2\frac{(T - M^\star)(M^\star - N_E)}{T}$$

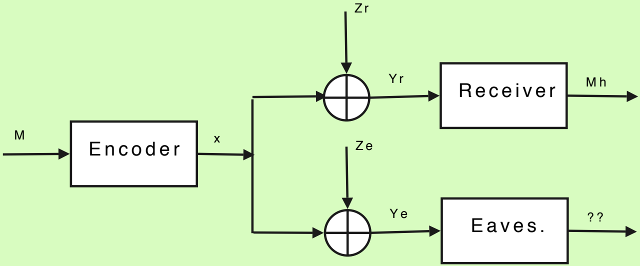
Physical Layer Security



Secure Communication — A Physical Layer Approach

Wyner'75, Csiszar-Korner '78

Wiretap Channel Model



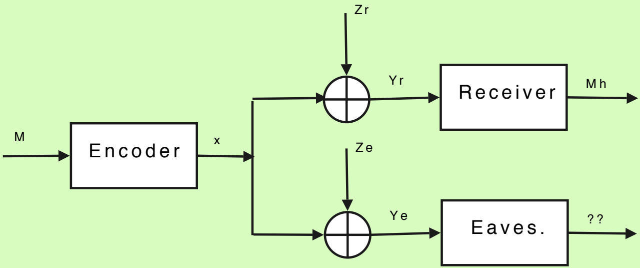
- Reliability Constraint : $\Pr(M \neq \hat{M}) \xrightarrow{n} 0$
- Secrecy Constraint : $\frac{1}{n} H(M|Y_e^n) = \frac{1}{n} H(M) - o_n(1)$

Secrecy Capacity

Secure Communication — A Physical Layer Approach

Wyner'75, Csiszar-Korner '78

Wiretap Channel Model



Csiszar-Korner '78

The Secrecy Capacity of DMC Channels is given by

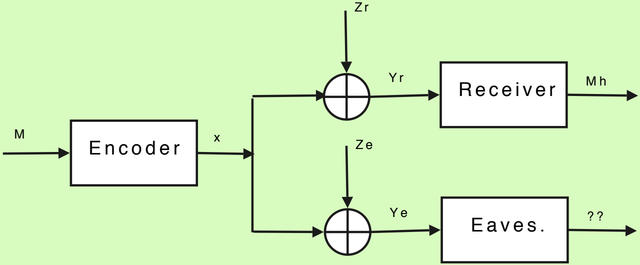
$$C_s = \max_{p_{U,X}} \{I(U;Y_r) - I(U;Y_e)\}$$

where the auxiliary variable U satisfies $U \rightarrow X \rightarrow (Y_r, Y_e)$.

Secure Communication — A Physical Layer Approach

Wyner'75, Csiszar-Korner '78

Wiretap Channel Model



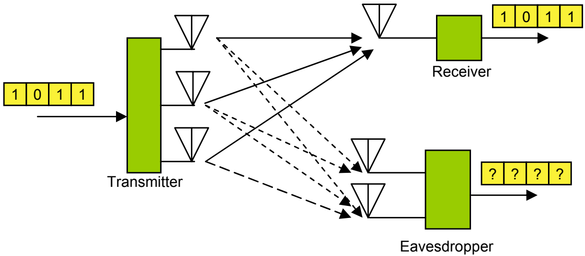
(L. Y. Cheong and M. Hellman '78)

The secrecy capacity of the AWGN Model is:

$$\begin{aligned} C_s &= \log(1 + SNR_r) - \log(1 + SNR_e) \\ &= C(\mathrm{SNR}_r) - C(\mathrm{SNR}_e) \end{aligned}$$

Multiple Antennas

Multi-antenna wiretap channel



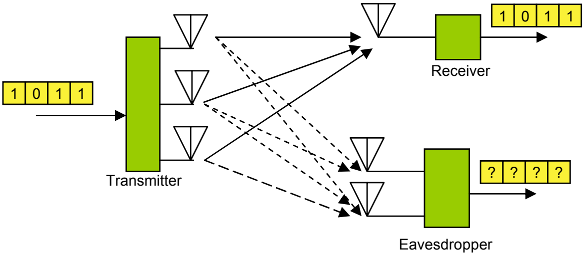
Channel Model

$Y_r = H_r X + Z_r$
$Y_e = H_e X + Z_e$

- Fixed Channel matrices: $H_r \in \mathbb{C}^{N_r \times N_t}$, $H_e \in \mathbb{C}^{N_e \times N_t}$
- AWGN noise

Multiple Antennas

Multi-antenna wiretap channel



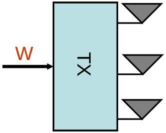
Theorem (Khisti-Wornell (Allerton '07, IT-Trans '10), Oggier-Hassibi (ISIT '08))

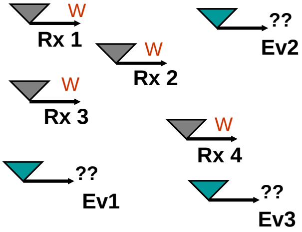
Secrecy capacity of the Multi-antenna wiretap channel is given by,

$$C_s = \max_{Q \succeq 0: Tr(Q) \leq P} \log\det(I_r + H_r Q H_r^\dagger) - \log\det(I_e + H_e Q H_e^\dagger)$$

Lower Bounds: Parada-Blahut '05, Li-Yates-Trappe '07

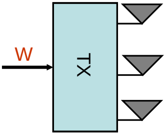
Compound Wiretap Channel

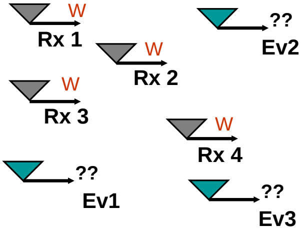




- M transmit Antennas
- Legitimate Receiver:
  $y_j = \mathbf{h}_j^\dagger \mathbf{x} + w_j,$
- Eavesdropper:
  $z_k = \mathbf{g}_k^\dagger \mathbf{x} + w_k,$
- Reliability:
  $\Pr(w \neq \hat{w}_i) \to 0, \; i \in \{1, \dots, J\}$
- Secrecy:
  $\frac{1}{n} I(w; z_j^n) \to 0, \; j \in \{1, \dots, K\}$

Compound Wiretap Channel





Khisti (IT-Trans 2011): Degree of Freedom Analysis

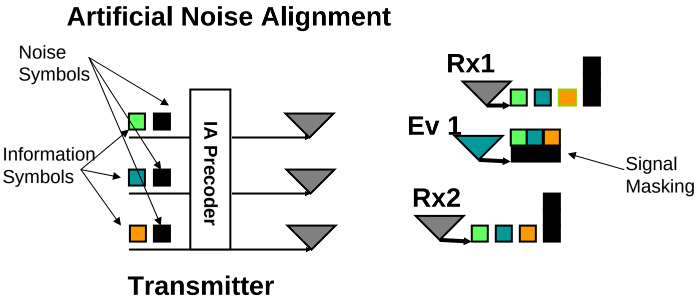
The degrees of freedom of the MISO Compound Wiretap Channel with M Tx antennas and $\min(J, K) \geq M$, satisfy (with high probability) $d_L \leq d \leq d_U$

$$d_L \geq 1 - \frac{1}{M}$$

$$d_U \leq 1 - \frac{1}{M^2 - M + 1}$$

Secure Multi-Antenna Multicast

A. Khisti, "Interference Alignment for Multi-Antenna Wiretap Channel," IEEE Trans. Inf. Theory, Mar. 2011



- Align Noise Symbols at Legitimate Receivers
- Mask Information Symbols at Eavesdroppers
- Only channel knowledge of legitimate receivers is needed.
- Compound Multi-Antenna Wiretap Channel

Talk Outline

Information Theoretic Approaches to Security (ITAS)

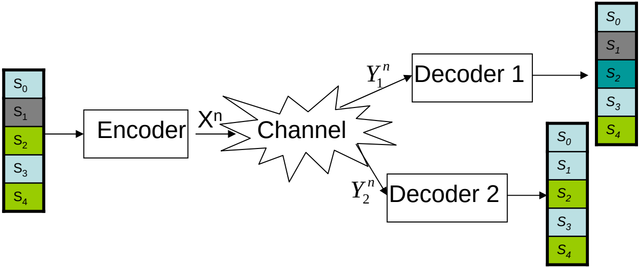
- Physical Layer Resources
- Secret-Key Generation
- Multiple Antennas for Secure Communication

Streaming Communications Systems — Fundamental Limits

- Error Correction Codes for Streaming Data
- Sequential Compression for Streaming Sources
- Streaming over Wireless Fading Channels
- Deterministic Channel Approximations

Joint Source-Channel Coding

Multimedia Streaming over Wireless Links



Model

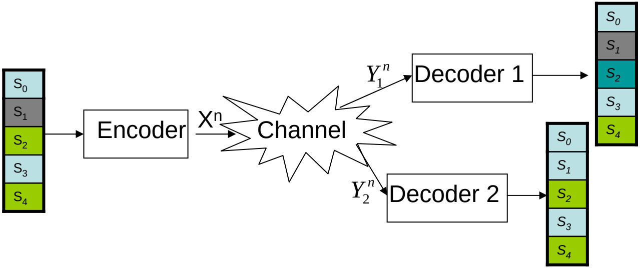
- Source Signal s^n
- Encoder: $s^n \to x^N$
- Decoder: $y_i^N \to \hat{s}_i^n$
- Distortion: $\sum_i d(s_i, \hat{s}_i)$

Architectures

- Separation Theorem
- Unequal Error Protection
- Scalable Video Coding
- Multiple Descriptions

Joint Source-Channel Coding

Multimedia Streaming over Wireless Links

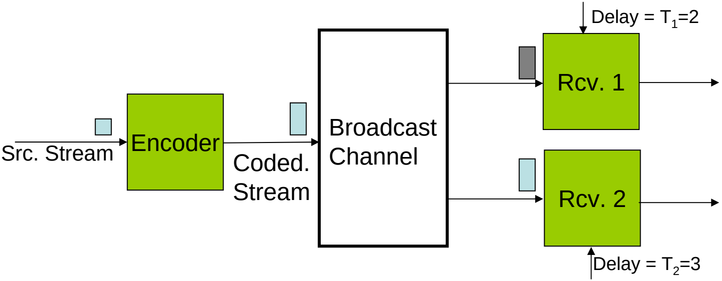


Suitable model for static sources and not streaming

New Models to address:

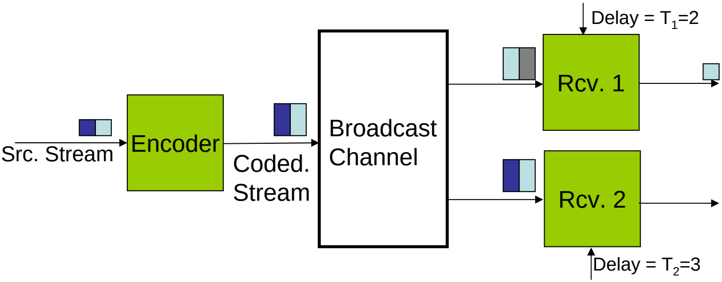
- Streaming Sources
- Delay Constraints

Delay Constrained Streaming



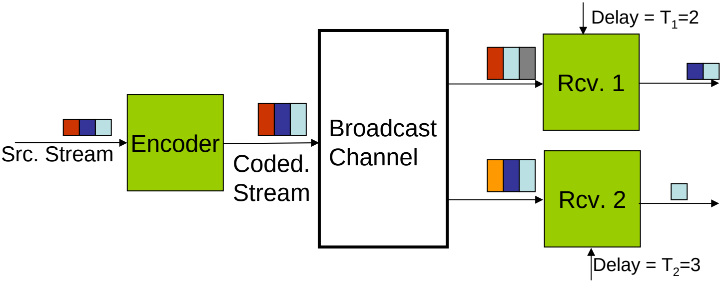
- Common Source
- Streaming Encoder
- Delay Constrained Receivers

Delay Constrained Streaming



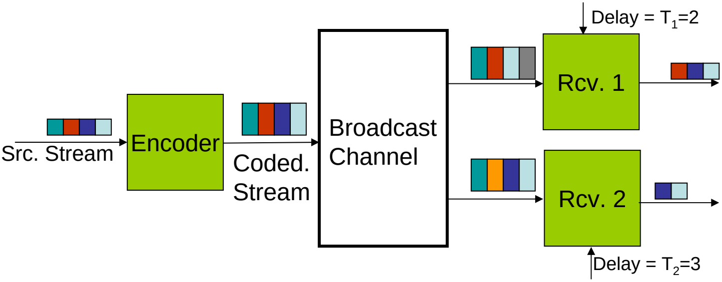
- Common Source
- Streaming Encoder
- Delay Constrained Receivers

Delay Constrained Streaming



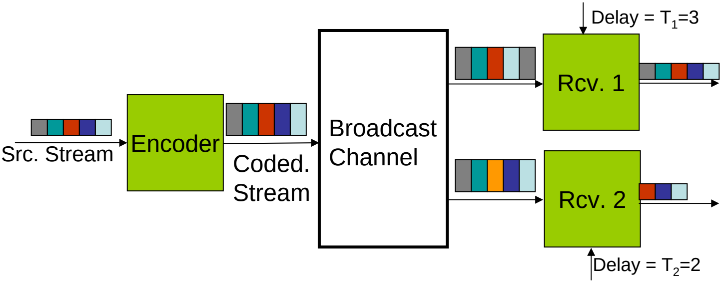
- Common Source
- Streaming Encoder
- Delay Constrained Receivers

Delay Constrained Streaming



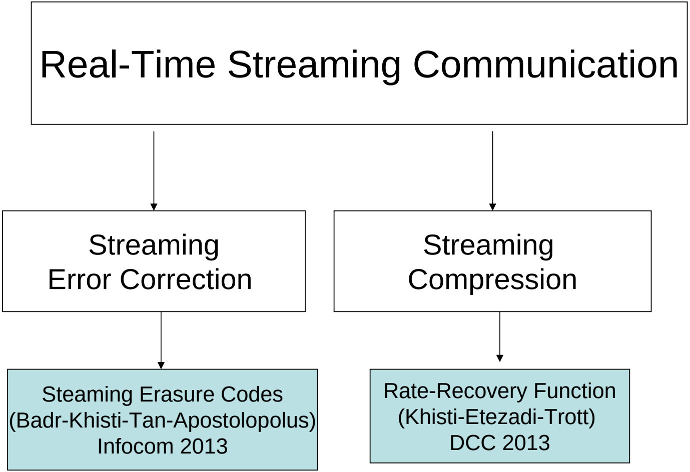
- Common Source
- Streaming Encoder
- Delay Constrained Receivers

Delay Constrained Streaming

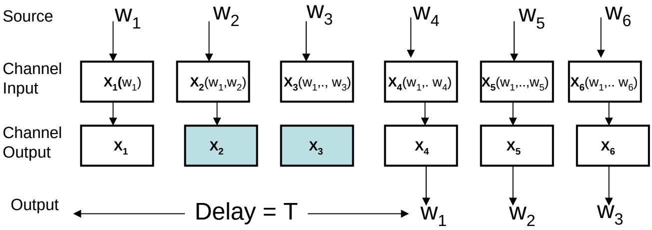


- Common Source
- Streaming Encoder
- Delay Constrained Receivers

Outline


Real-Time Streaming Communication
Streaming Error Correction
Streaming Compression
Steaming Erasure Codes (Badr-Khisti-Tan-Apostolopolus) Infocom 2013
Rate-Recovery Function (Khisti-Etezadi-Trott) DCC 2013

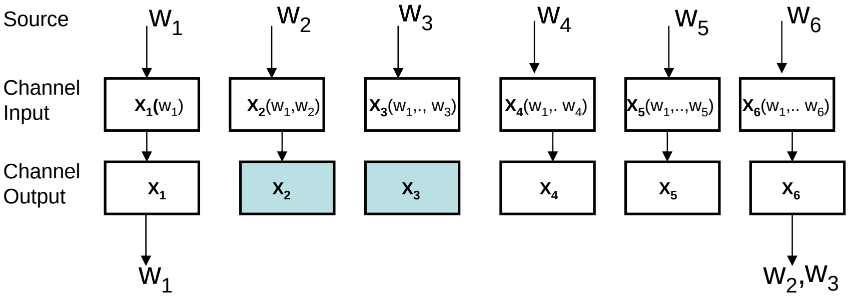
Error-Correction for Streaming Data



Model: Streaming Codes

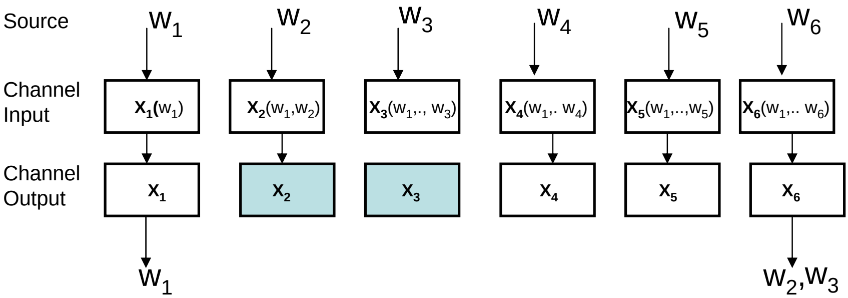
- Source Model : i.i.d. sequence $w[t] \sim p_w(\cdot) = \text{Unif}\{(\mathbb{F}_q)^k\}$
- Streaming Encoder: $x[t] = f_t\,(w[1], \ldots, w[t])$, $x[t] \in (\mathbb{F}_q)^n$
- Erasure Channel
- Delay-Constrained Decoder: $\hat{w}[t] = g_t(y[1], \ldots, y[t+T])$
- Rate $R = \frac{H(w)}{n} = \frac{k}{n}$

"Erasure" Codes



$$x_i = w_i \cdot G_0 + w_{i-1} \cdot G_1 + \ldots + w_{i-M} \cdot G_M, \qquad G_i \in \mathbb{F}_q^{k \times n}$$

“Erasure” Codes



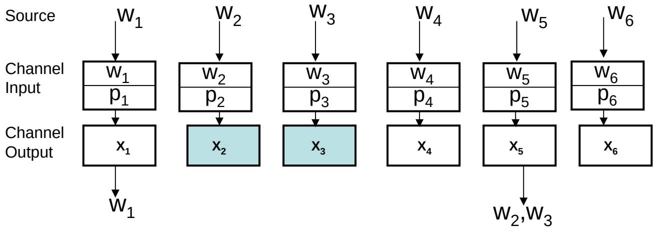
$$x_i = w_i \cdot G_0 + w_{i-1} \cdot G_1 + \ldots + w_{i-M} \cdot G_M, \qquad G_i \in \mathbb{F}_q^{k \times n}$$

$$\begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix} = \underbrace{\begin{bmatrix} G_2 & G_1 & G_0 & 0 & 0 \\ G_3 & G_2 & G_1 & G_0 & 0 \\ G_4 & G_3 & G_2 & G_1 & G_0 \end{bmatrix}}_{\text{full rank}} \begin{bmatrix} w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \end{bmatrix}$$

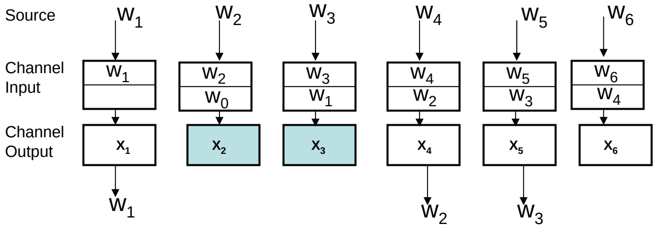
Sequential Recovery

$R = 1/2$

Erasure Codes



Burst-Erasure Codes (Martinian-Sundberg '04)

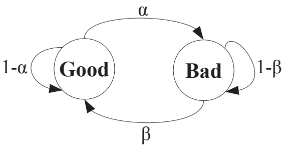


Motivating Questions

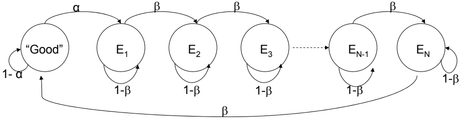
- Can we improve upon "Erasure Codes" for Realistic Channel Models

Motivating Questions

- Can we improve upon "Erasure Codes" for Realistic Channel Models



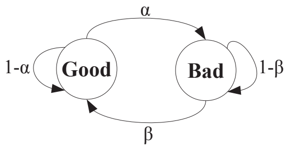
Gilbert-Elliott Model



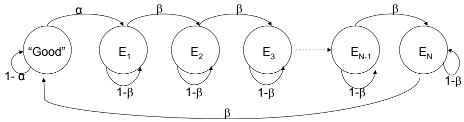
Fritchman Channel Model

Motivating Questions

- Can we improve upon "Erasure Codes" for Realistic Channel Models



Gilbert-Elliott Model

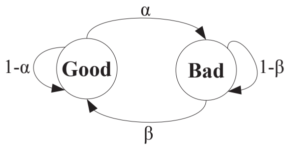


Fritchman Channel Model

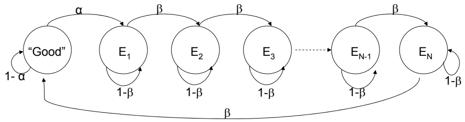
- What are the fundamental metrics for low-delay error correction codes?

Motivating Questions

- Can we improve upon "Erasure Codes" for Realistic Channel Models



Gilbert-Elliott Model



Fritchman Channel Model

- What are the fundamental metrics for low-delay error correction codes?
- How much performance gains can we obtain?

Deterministic Approximation

In any sliding window of length W the channel introduces either

- N erasures in arbitrary locations (or)
- B erasure in a single burst

Deterministic Channel Model $(W = 5, N = 2, B = 3)$

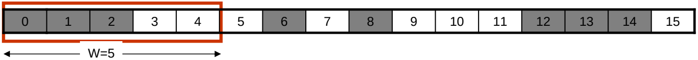
Our Approach:

- Find (nearly) optimal codes for a deterministic approximation.
- Evaluate performance over stochastic models.
- We will take $W = T + 1$

Deterministic Approximation

In any sliding window of length W the channel introduces either

- N erasures in arbitrary locations (or)
- B erasure in a single burst



Deterministic Channel Model $(W = 5, N = 2, B = 3)$

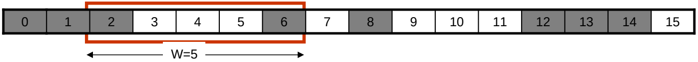
Our Approach:

- Find (nearly) optimal codes for a deterministic approximation.
- Evaluate performance over stochastic models.
- We will take $W = T + 1$

Deterministic Approximation

In any sliding window of length W the channel introduces either

- N erasures in arbitrary locations (or)
- B erasure in a single burst



Deterministic Channel Model $(W = 5, N = 2, B = 3)$

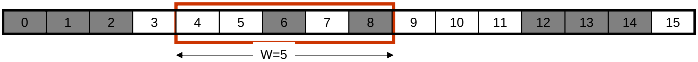
Our Approach:

- Find (nearly) optimal codes for a deterministic approximation.
- Evaluate performance over stochastic models.
- We will take $W = T + 1$

Deterministic Approximation

In any sliding window of length W the channel introduces either

- N erasures in arbitrary locations (or)
- B erasure in a single burst



Deterministic Channel Model $(W = 5, N = 2, B = 3)$

Our Approach:

- Find (nearly) optimal codes for a deterministic approximation.
- Evaluate performance over stochastic models.
- We will take $W = T + 1$

Main Result

Badr-Khisti-Tan-Apostolopoulos '2012

Theorem

For any feasible rate R code, we must have that:

$$N + B\left(\frac{R}{1-R}\right) \leq T+1, \quad N \leq B, \quad N, B \geq 0.$$

There exists a construction that achieves any (N, B) that satisfies:

$$N + B\left(\frac{R}{1-R}\right) \leq T, \quad N \leq B, \quad N, B \geq 0.$$

This characterizes the optimal region to within one erasure.

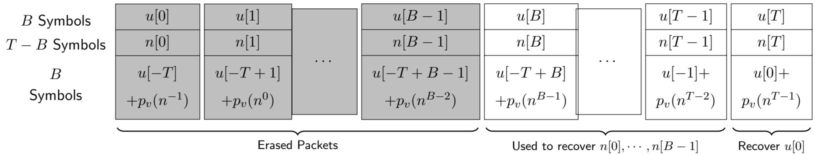
Proposed Coding Scheme

Badr-Khisti-Tan-Apostolopoulos '2012

- Split each source packet into two groups
- Unequal Error Protection

Proposed Coding Scheme
Badr-Khisti-Tan-Apostolopoulos '2012

- Split each source packet into two groups
- Unequal Error Protection



Proposed Coding Scheme-II

$T = 5,\ B = 2.$

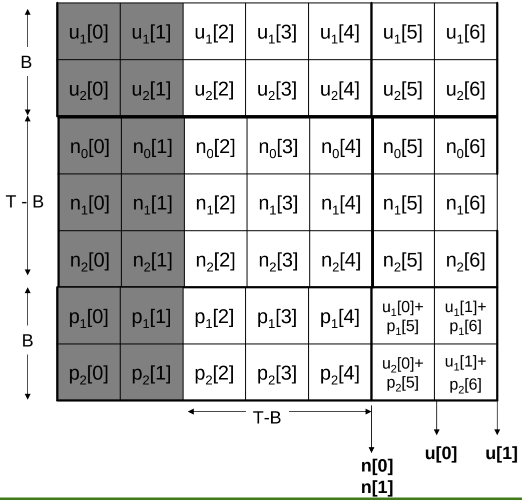
Burst-Erasure Code, $R = \frac{T}{T+B}, \quad N = 1$

B	$u_1[0]$	$u_1[1]$	$u_1[2]$	$u_1[3]$	$u_1[4]$	$u_1[5]$	$u_1[6]$
	$u_2[0]$	$u_2[1]$	$u_2[2]$	$u_2[3]$	$u_2[4]$	$u_2[5]$	$u_2[6]$
	$n_0[0]$	$n_0[1]$	$n_0[2]$	$n_0[3]$	$n_0[4]$	$n_0[5]$	$n_0[6]$
T - B	$n_1[0]$	$n_1[1]$	$n_1[2]$	$n_1[3]$	$n_1[4]$	$n_1[5]$	$n_1[6]$
	$n_2[0]$	$n_2[1]$	$n_2[2]$	$n_2[3]$	$n_2[4]$	$n_2[5]$	$n_2[6]$
B	$p_1[0]$	$p_1[1]$	$p_1[2]$	$p_1[3]$	$p_1[4]$	$u_1[0]+p_1[5]$	$u_1[1]+p_1[6]$
	$p_2[0]$	$p_2[1]$	$p_2[2]$	$p_2[3]$	$p_2[4]$	$u_2[0]+p_2[5]$	$u_1[1]+p_2[6]$

T-B

$T = 5,\ B = 2.$

Burst-Erasure Code, $R = \frac{T}{T+B}, \quad N = 1$



Proposed Coding Scheme-II

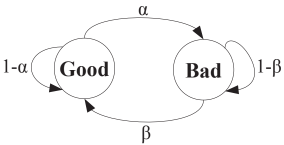
$T = 5,\ B = 2.$

Step III: $R = \frac{T}{T+B+K}, \quad N = \min\left(\frac{K}{K+B}T, B\right)$

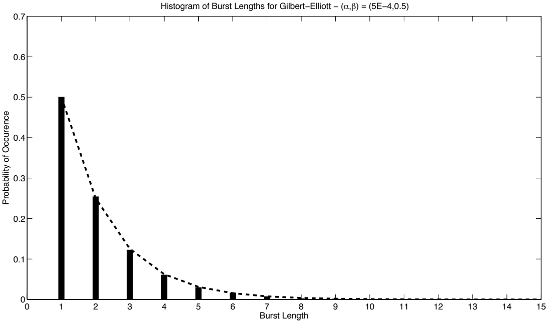
B	$u_1[0]$	$u_1[1]$	$u_1[2]$	$u_1[3]$	$u_1[4]$	$u_1[5]$	$u_1[6]$
	$u_2[0]$	$u_2[1]$	$u_2[2]$	$u_2[3]$	$u_2[4]$	$u_2[5]$	$u_2[6]$
T - B	$n_0[0]$	$n_0[1]$	$n_0[2]$	$n_0[3]$	$n_0[4]$	$n_0[5]$	$n_0[6]$
	$n_1[0]$	$n_1[1]$	$n_1[2]$	$n_1[3]$	$n_1[4]$	$n_1[5]$	$n_1[6]$
	$n_2[0]$	$n_2[1]$	$n_2[2]$	$n_2[3]$	$n_2[4]$	$n_2[5]$	$n_2[6]$
B	$p_1[0]$	$p_1[1]$	$p_1[2]$	$p_1[3]$	$p_1[4]$	$u_1[0]+p_1[5]$	$u_1[1]+p_1[6]$
	$p_2[0]$	$p_2[1]$	$p_2[2]$	$p_2[3]$	$p_2[4]$	$u_2[0]+p_2[5]$	$u_1[1]+p_2[6]$
K	$q[0]$	$q[1]$	$q[2]$	$q[3]$	$q[4]$	$q[5]$	$q[6]$

Simulation Result

Gilbert-Elliott Channel $(\alpha, \beta) = (5 \times 10^{-4}, 0.5)$, $T = 12$ and $R = 12/23$

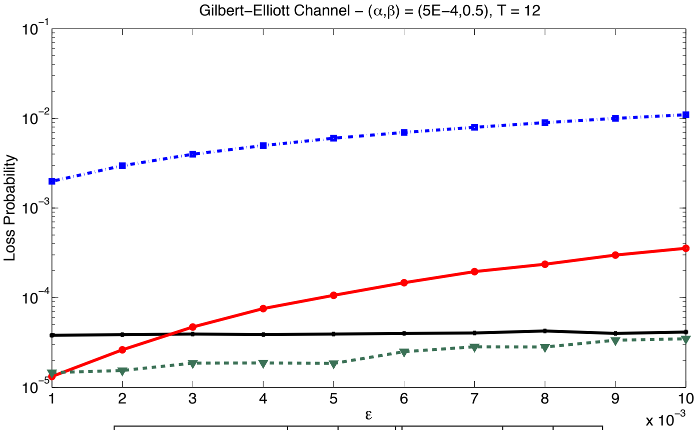


- $\alpha = 5 \times 10^{-4}$
- $\beta = 0.5$



Simulation Result

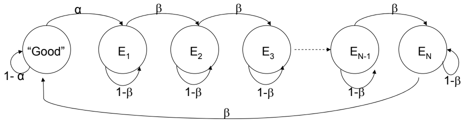
Gilbert-Elliott Channel $(\alpha, \beta) = (5 \times 10^{-4}, 0.5)$, $T = 12$ and $R = 12/23$



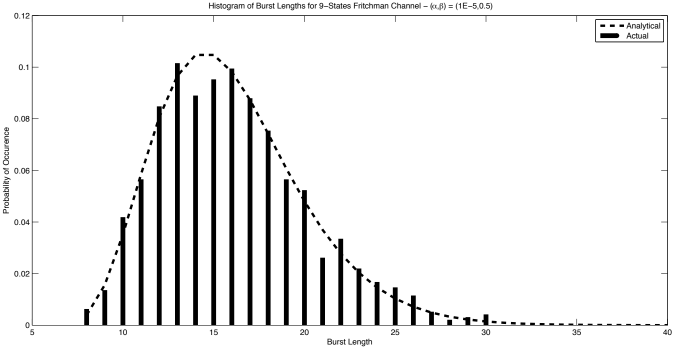
Code	N	B	Code	N	B
RLC	6	6	Hybrid	2	9
Burst-Erasure	1	11			

Simulation Result-II

Fritchman Channel $(\alpha, \beta) = (1e-5, 0.5)$ and $T = 40$ and $R = 40/79$, 9 states

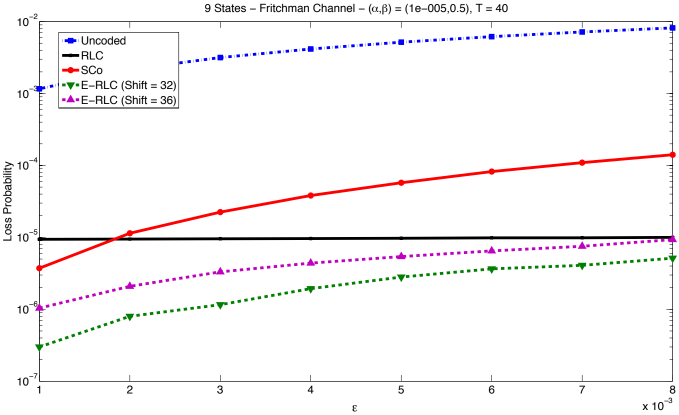


- $\alpha = 1e-5$
- $\beta = 0.5$



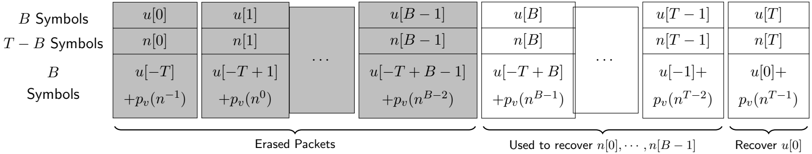
Simulation Result-II

Fritchman Channel $(\alpha, \beta) = (1e-5, 0.5)$ and $T = 40$ and $R = 40/79$, 9 states

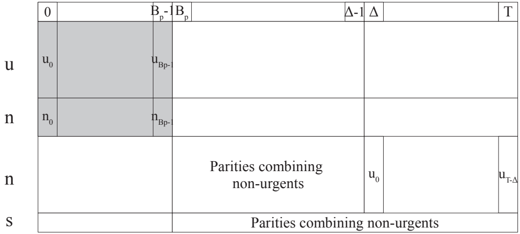


Code	N	B	Code	N	B
RLC	20	20	Hybrid 1	8	31
Burst Erasure	1	39	Hybrid 2	4	35

Original Construction



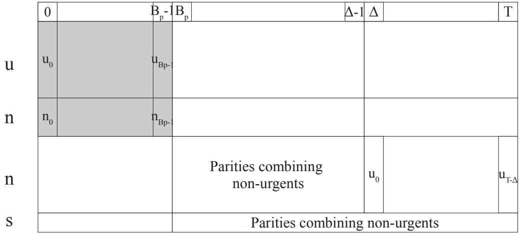
Modified Construction — K_0 erasures



- $(B+1)n \leq (\Delta - B - 1)u + (T-B)s$
- $n \geq s(T + K_0 - \Delta)$
- $R = \frac{u+n}{2u+n+s}$

Extensions — Dealing with Burst+Isolated Erasures

Modified Construction — K_0 erasures

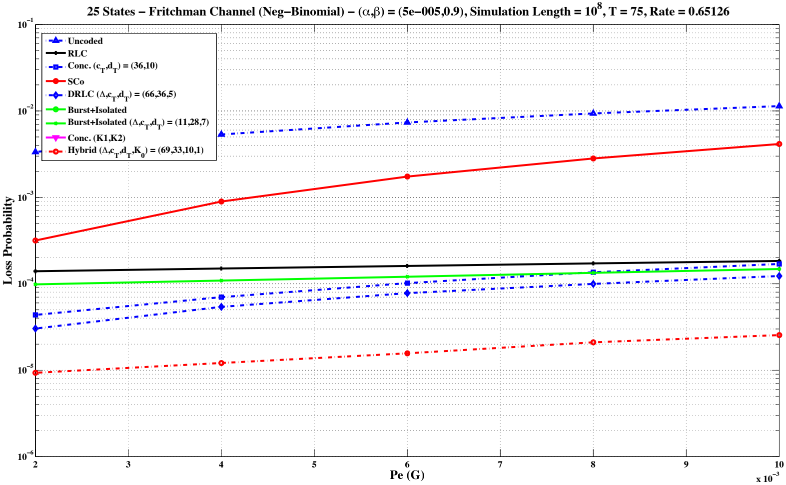


- $(B+1)n \leq (\Delta - B - 1)u + (T - B)s$
- $n \geq s(T + K_0 - \Delta)$
- $R = \frac{u+n}{2u+n+s}$

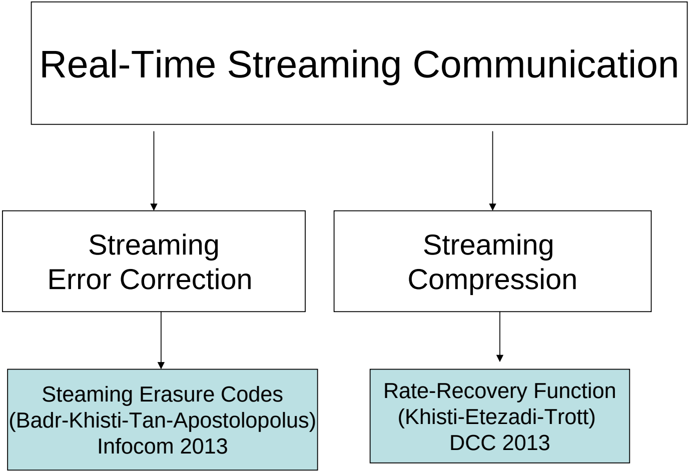
$K_0 = 1$

- $\Delta^\star = T + 1 - \sqrt{T - B}$
- $R = \frac{T+1-2\sqrt{T-B}}{T+B+1-2\sqrt{T-B}}$

Simulations

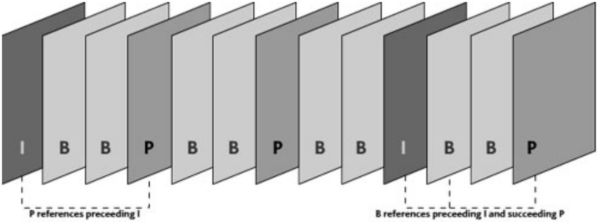


Outline


Real-Time Streaming Communication
Streaming Error Correction
Streaming Compression
Steaming Erasure Codes (Badr-Khisti-Tan-Apostolopolus) Infocom 2013
Rate-Recovery Function (Khisti-Etezadi-Trott) DCC 2013

Compression Vs Error Propagation

GOP Picture Structure[1]

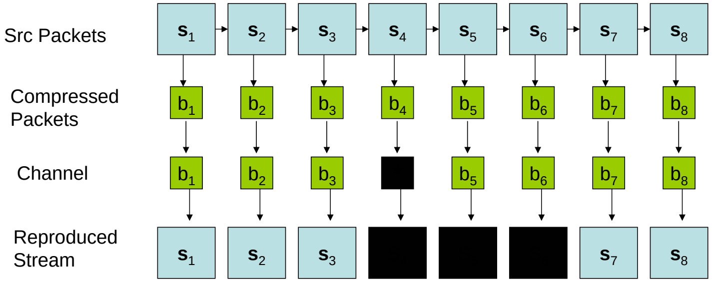


	Compression	Error Propagation
Predictive Coding	$\surd$	$\times$
Still Image Coding	$\times$	$\surd$

- Interleaving Approach
- Error Control Coding

[1]Source : `http://www.networkwebcams.com`

Information Theoretic Model



- Compression Rate: R
- Erasure Burst Length: B
- Recovery Window: W

Rate Recovery Function: $R(B, W)$.

Problem Setup

- Source Model: Sequence of vectors — Temporally Markov and Spatially i.i.d.

$$\Pr(\mathsf{s}_i^n|\mathsf{s}_{i-1}^n, \mathsf{s}_{i-2}^n, \ldots,) = \prod_{j=1}^{n} \Pr(\mathsf{s}_{ij}|\mathsf{s}_{i-1,j})$$

- Channel Model: Burst Erasure Model

$$g_i = \begin{cases} f_i, & i \notin \{j, j+1, \ldots, j+B-1\} \\ \star, & \text{otherwise} \end{cases}$$

Problem Setup

- Source Model: Sequence of vectors — Temporally Markov and Spatially i.i.d.

$$\Pr(\mathsf{s}_i^n | \mathsf{s}_{i-1}^n, \mathsf{s}_{i-2}^n, \ldots,) = \prod_{j=1}^{n} \Pr(\mathsf{s}_{ij} | \mathsf{s}_{i-1,j})$$

- Channel Model: Burst Erasure Model

$$g_i = \begin{cases} f_i, & i \notin \{j, j+1, \ldots, j+B-1\} \\ \star, & \text{otherwise} \end{cases}$$

- Encoder: $\mathcal{F}_i : \{\mathsf{s}_0^n, \ldots, \mathsf{s}_i^n\} \rightarrow f_i \in [1, 2^{nR}]$.
- Decoder: $\mathcal{G}_i : \{g_0, \ldots, g_i\} \rightarrow \hat{\mathsf{s}}_i^n$.

$$\Pr(\hat{\mathsf{s}}_i^n \neq \mathsf{s}_i^n) \leq \varepsilon_n$$

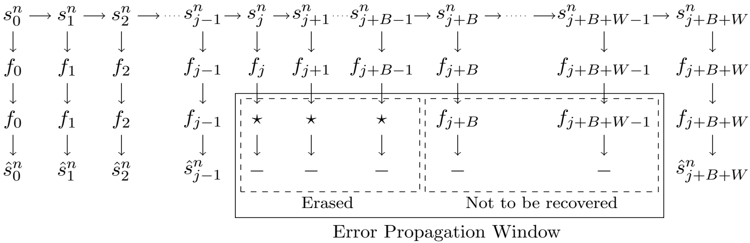
except for $i \in [j, \ldots, j+B+W-1]$.

Rate-Recovery Function

Definition (Rate-Recovery Function)

The minimum compression rate $R(B, W)$ *that is achieved when:*

- *Burst-Erasure Length* $= B$
- *Recovery Window* $= W$



Main Results

Upper and Lower Bounds on $R(B, W)$:

$$R^{+}(B, W) = H(\mathsf{s}_1|\mathsf{s}_0) + \frac{1}{W+1} I(\mathsf{s}_B; \mathsf{s}_{B-1}|\mathsf{s}_{-1})$$
$$R^{-}(B, W) = H(\mathsf{s}_1|\mathsf{s}_0) + \frac{1}{W+1} I(\mathsf{s}_{B+W}; \mathsf{s}_{B-1}|\mathsf{s}_{-1})$$

Main Results

Upper and Lower Bounds on $R(B, W)$:

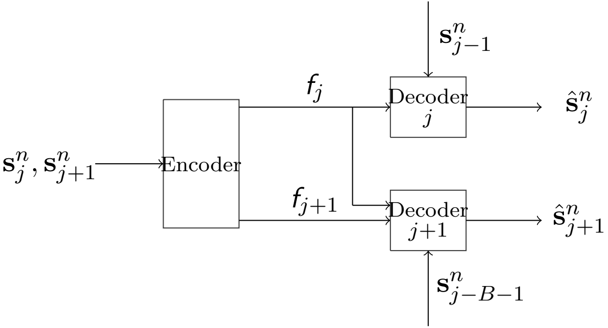
$$R^{+}(B,W) = H(\mathsf{s}_1|\mathsf{s}_0) + \frac{1}{W+1} I(\mathsf{s}_B; \mathsf{s}_{B-1}|\mathsf{s}_{-1})$$

$$R^{-}(B,W) = H(\mathsf{s}_1|\mathsf{s}_0) + \frac{1}{W+1} I(\mathsf{s}_{B+W}; \mathsf{s}_{B-1}|\mathsf{s}_{-1})$$

- Upper bound : Binning based scheme.
- Upper and Lower Bounds Coincide: $W = 0$ and $W \to \infty$.
- Identical Scaling of Upper and Lower Bounds
- Lower Bound is tight for certain models.
- Extensions to Gaussian Case

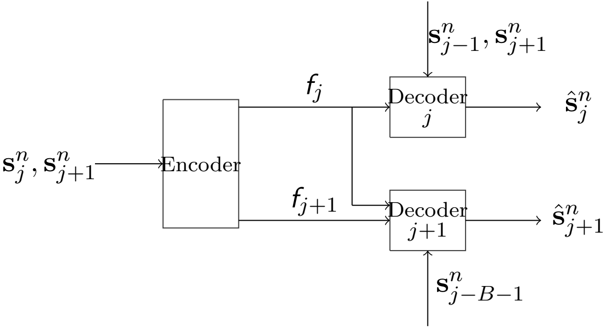
Lower Bound

Let $B = 1$ and $W = 1$.
Encoding of s_j^n, s_{j+1}^n



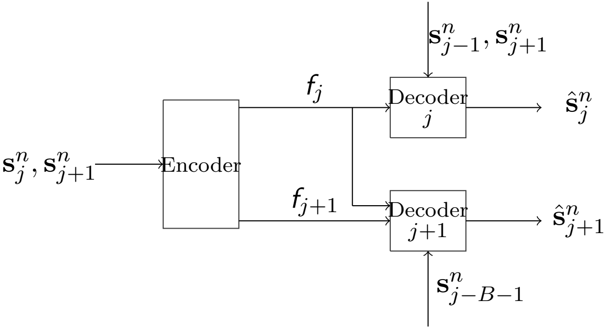
Lower Bound

Let $B = 1$ and $W = 1$.
Encoding of s_j^n, s_{j+1}^n



Lower Bound

Let $B = 1$ and $W = 1$.
Encoding of s_j^n, s_{j+1}^n



Lower Bound $R_j + R_{j+1} \geq H(s_j | s_{j-1}, s_{j+1}) + H(s_{j+1} | s_{j-B-1})$.

Fading Channels

Block Fading Channel

$$\mathbf{y}_i = h_i \mathbf{x}_i + \mathbf{z}_i$$

- Block Fading Channels: n symbols per block
- Source Packet: One in each coherence block nR bits
- Decoding Delay: T coherence blocks

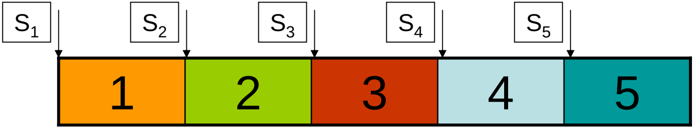
Block Fading Channel Model

Fading Channels

Block Fading Channel

$$\mathbf{y}_i = h_i \mathbf{x}_i + \mathbf{z}_i$$

- Block Fading Channels: n symbols per block
- Source Packet: One in each coherence block nR bits
- Decoding Delay: T coherence blocks

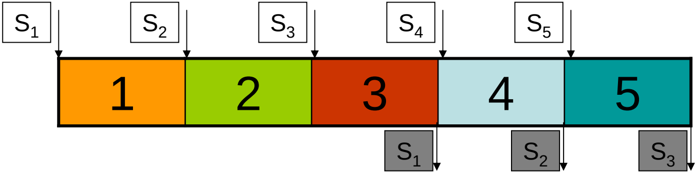


Fading Channels

Block Fading Channel

$$\mathbf{y}_i = h_i \mathbf{x}_i + \mathbf{z}_i$$

- Block Fading Channels: n symbols per block
- Source Packet: One in each coherence block nR bits
- Decoding Delay: T coherence blocks



Diversity-Multiplexing Tradeoff

Quasi-static fading Channels

$$\mathbf{y} = h\mathbf{x} + \mathbf{z}$$

- Quasi-static Channel
- SNR$\equiv \rho$, Rate $= R(\rho)$
- Multiplexing: $r = \lim_{\rho \to \infty} \frac{R(\rho)}{\log \rho}$
- Diversity $d = \lim_{\rho \to \infty} \frac{-\log \Pr(\rho)}{\log \rho}$

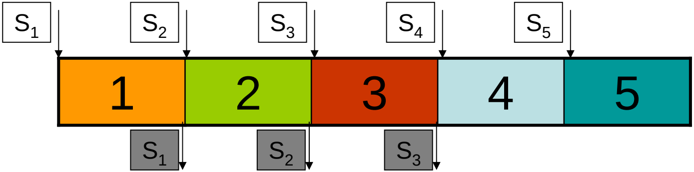
Theorem (Zheng-Tse 2003)

The diversity multiplexing tradeoff for a MIMO Rayleigh Fading channel with N_t transmit antennas and N_r receive antennas is a piecewise constant curve connecting the ponts $(N_t - k)(N_r - k)$ for $k = 0, 1, \ldots, \min(N_r, N_t)$

Quasi-static fading Channels

$$\mathbf{y} = h\mathbf{x} + \mathbf{z}$$

- Quasi-static Channel
- SNR$\equiv \rho$, Rate $= R(\rho)$
- Multiplexing: $r = \lim_{\rho\to\infty} \frac{R(\rho)}{\log \rho}$
- Diversity $d = \lim_{\rho\to\infty} \frac{-\log \Pr(\rho)}{\log \rho}$



Diversity-Multiplexing Tradeoff

Theorem (Khisti-Draper 2011)

The diversity multiplexing tradeoff for streaming source with a delay of T coherence blocks and a block-fading channel model is

$$d(r) = Td_1(r)$$

where $d_1(r)$ is the quasi-static DMT.

- Upper Bound: Outage Amplification Argument
- Lower Bound: Random Tree Codes $\mathbf{X}_i = f_i(\mathbf{S}_0, \ldots, \mathbf{S}_i)$.
- Delay Universal

Conclusions

Physical Layer Security

- Secret-Key Generation Using Channel Reciprocity
- Fundamental Limits of Secret-Key Capacity
- Multiple Antennas for Secure Communication

Fundamental Limits of Streaming Communications

- Error Correction Codes For Streaming Data
- Deterministic Channel Models
- Sequential Compression under Error Propagation Constraints
- Streaming Data over Block Fading Channels (DMT)