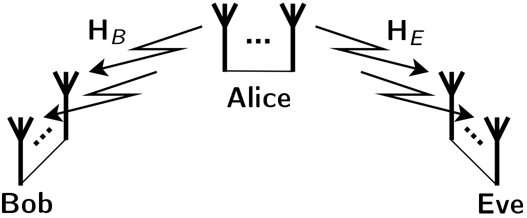
From Ordinary AWGN Codes to Optimal MIMO Wiretap Schemes

Anatoly Khina, Tel Aviv University

Joint work with:
Yuval Kochman, Hebrew University
Ashish Khisti, University of Toronto

ITW 2014
Hobart, Tasmania, Australia
November 05, 2014

Channel Model: Gaussian MIMO Wiretap Channel



$\mathbf{y}_B = \mathbf{H}_B \mathbf{x} + \mathbf{z}_B$ $\mathbf{y}_E = \mathbf{H}_E \mathbf{x} + \mathbf{z}_E$

- $\mathbf{x}$ – $N_A \times 1$ input vector of power P
- $\mathbf{y}_B$, $\mathbf{y}_E$ – $N_B \times 1$, $N_E \times 1$ received vectors
- $\mathbf{H}_B$, $\mathbf{H}_E$ – $N_B \times N_A$, $N_E \times N_A$ channel matrices
- $\mathbf{z}_B \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_B})$, $\mathbf{z}_E \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_E})$ – noise vectors
- "Closed loop" (full channel knowledge everywhere)

Capacity

Gaussian SISO channel capacity [Leung-Yan-Cheong, Hellman '78]

$$C_S(h_B, h_E) = \Big[\overbrace{\log\left(1 + |h_B|^2 P\right)}^{I(X;Y_B)} - \overbrace{\log\left(1 + |h_E|^2 P\right)}^{I(X;Y_E)} \Big]_+$$

Gaussian MIMO channel capacity [Khisti,Wornell '10][Oggier,Hassibi '11]

$$C_S(\mathbf{H}_B, \mathbf{H}_E) = \max_{\mathbf{K}:\, \mathrm{trace}\{\mathbf{K}\} \le P} \Big[\overbrace{\log\left|\mathbf{I} + \mathbf{H}_B \mathbf{K} \mathbf{H}_B^\dagger\right|}^{I(\mathbf{X};\mathbf{Y}_B)} - \overbrace{\log\left|\mathbf{I} + \mathbf{H}_E \mathbf{K} \mathbf{H}_E^\dagger\right|}^{I(\mathbf{X};\mathbf{Y}_E)} \Big]$$

- Maximization over all admissible covariance matrices $\mathbf{K}$
- Power constraint can be replaced with covariance constraint [Liu, Shamai '09]

How to Construct a Practical Capacity-achieving Scheme?

Black box approach

- Construct MIMO Wiretap Codes from "ordinary" SISO ones
- Any good "ordinary" SISO AWGN codes
- Signal processing
  (SVD-based scheme [Telatar '99], V-BLAST [Foschini '96], ...)
- Codeword indexing
- Achieves capacity
- Gap-to-capacity dictated by gap-to-capacity of the SISO codes

How to Construct a Practical Capacity-achieving Scheme?

Two-step procedure

1. Reduce MIMO to SISO (as in "ordinary" MIMO case)
2. Transform "ordinary" (non-secrecy) codes to wiretap ones

Weak/strong secrecy

- Concentrate on achievability of weak secrecy
- One specific structure achieves strong secrecy

“Ordinary” Codes → Wiretap Codes

Good Wiretap Codes for SISO

Two-level AWGN code of rates $(R, \tilde{R})$

- $x^n = g(m, f)$
- $m \in \{1, \ldots, 2^{nR}\}$ – Information message
- $f \in \left\{1, \ldots, 2^{n\tilde{R}}\right\}$ – Fictitious message
- g – Mapping known to all (including Eve!)
- Bob can decode (m, f) and then discard f
- Eve **can** recover f from (y_E, m)

$$\Downarrow$$

Eve **cannot** recover m from y_E: $I(m; y_E) \leq n\epsilon$

Ordinary Codes → Two-level AWGN Codes

Randomized procedure

- Base AWGN codebook $\mathcal{C}_0$ of rate R_0: $R + \tilde{R} < R_0 < C_B$
- $\forall(m, f)$: Draw an index $\theta(m, f) \in \mathrm{Unif}\left(\left\{1, \ldots, 2^{nR_0}\right\}\right)$
- Average codebook = good two-level AWGN codebook
- De-mapping of random indexing is hard!

Practical procedure

- Two-universal hash function
  [Hayashi, Matsumoto 2010][Bellare, Tessaro, Vardy 2012]
- Low-complexity structured approach
- Valid for Gaussian channels [Tyagi, Vardy ISIT2014]

MIMO Without Secrecy (No Eve)

Singular-Value Decomposition (SVD) Scheme [Telatar '99]

- $\mathbf{H}_B = \mathbf{Q}_B \mathbf{D}_B \mathbf{V}_A^\dagger$
- $\mathbf{Q}_B$ and $\mathbf{V}_A$ — unitary
- Alice applies $\mathbf{V}_A$ and Bob applies $\mathbf{Q}_B$
- $$\mathbf{D}_B = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d_{N-1} & 0 \\ 0 & \cdots & 0 & 0 & d_N \end{pmatrix} \Rightarrow \begin{aligned} y_1 &= d_1 x_1 + z_1 \\ y_2 &= d_2 x_2 + z_2 \\ &\vdots \\ y_N &= d_N x_N + z_N \end{aligned}$$
- Results in parallel scalar sub-channels (each sub-channel has a different SNR)
- Apply water-filling to $\{x_1, \ldots, x_N\}$: $\mathbf{x} = \mathbf{V}_A \mathbf{W} \mathbf{c}$

SVD-based scheme for a given input covariance K

- $\mathbf{H}_B\mathbf{K}^{1/2} = \mathbf{Q}_B\mathbf{D}_B\mathbf{V}_A^\dagger$
- $\mathbf{Q}_B$ and $\mathbf{V}_A$ — unitary
- Alice applies $\mathbf{K}^{1/2}\mathbf{V}_A$ and Bob applies $\mathbf{Q}_B$
- $\mathbf{D}_B = \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d_{N-1} & 0 \\ 0 & \cdots & 0 & 0 & d_N \end{pmatrix} \Rightarrow \begin{aligned} y_1 &= d_1 x_1 + z_1 \\ y_2 &= d_2 x_2 + z_2 \\ &\vdots \\ y_N &= d_N x_N + z_N \end{aligned}$
- Results in parallel scalar sub-channels
  (each sub-channel has a different SNR)
- ~~Apply water filling to $\{x_1, \ldots, x_N\}$: $\mathbf{x} = \mathbf{V}_A\mathbf{W}\mathbf{c}$~~ $\mathbf{x} = \mathbf{K}^{1/2}\mathbf{V}_A\mathbf{c}$

SVD-based scheme for a given input covariance $\mathbf{K}$

- SVD scheme with given $\mathbf{K}$ achieves : $R = \log \left| \mathbf{I}_{N_A} + \mathbf{H}_B \mathbf{K} \mathbf{H}_B^\dagger \right|$
- For optimal choice of $\mathbf{K}$ attains capacity
- Can be used to attain capacity for other covariance constraint scenarios (e.g., individual power constraints)

V-BLAST Scheme: QR Decomposition Based Scheme

Zero-forcing V-BLAST [Foschini '96][Wolniansky et al. '98]

- $\mathbf{H}_B = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{Q}_B$ – unitary; $\mathbf{T}_B$ – triangular
- Bob applies $\mathbf{Q}_B^\dagger$ (no SP is required by Alice)
- $$\mathbf{T}_B = \begin{pmatrix} t_1 & * & * & \cdots & * \\ 0 & t_2 & * & \cdots & * \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & t_{N-1} & * \\ 0 & 0 & \cdots & 0 & t_N \end{pmatrix} \Rightarrow \begin{aligned} y_1^{\text{eff}} &= t_1 x_1 + z_1 \\ y_2^{\text{eff}} &= t_2 x_2 + z_2 \\ &\vdots \\ y_N^{\text{eff}} &= t_N x_N + z_N \end{aligned}$$
- Off-diagonal elements are canceled via successive interference cancellation (SIC)

V-BLAST Scheme: QR Decomposition Based Scheme

MMSE-VBLAST for a given covariance K [Hassibi '00]

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{Q}_B$ – unitary; $\tilde{\mathbf{Q}}_B$ – $N_B \times N_A$ submatrix of $\mathbf{Q}_B$
- Bob applies $\tilde{\mathbf{Q}}_B^\dagger$ (no SP is required by Alice)
- $\tilde{\mathbf{Q}}_B^\dagger$ contains Wiener-filtering ("FFE")
- Effective noise has channel noise and "ISI" components
- Effective SNRs satisfy: $t_i^2 = 1 + \mathrm{SNR}_i$

$$\log(t_i^2) = \log(1 + \mathrm{SNR}_i) = I(c_i; \mathbf{y}_B | c_{i+1}^{N_A})$$

- Off-diagonal elements above diagonal canceled via SIC

V-BLAST Scheme: QR Decomposition Based Scheme

- For square invertible $\mathbf{H}$, ZF-VBLAST achieves:

$$R = \log \left| \mathbf{H}_B \mathbf{H}_B^{\dagger} \right|$$

$$\left(\text{Using } \mathbf{K} \text{ at the transmitter achieves: } R = \log \left| \mathbf{H}_B \mathbf{K} \mathbf{H}_B^{\dagger} \right| \right)$$

- MMSE-VBLAST achieves: $R = \log \left| \mathbf{I}_{N_B} + \mathbf{H}_B \mathbf{K} \mathbf{H}_B^{\dagger} \right|$

Precoded V-BLAST

MMSE-VBLAST with precoding for a given covariance $\mathbf{K}$

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{V}_A$ can be used to design diagonal values $\Leftrightarrow$ design SNRs

Precoded V-BLAST

MMSE-VBLAST with precoding for a given covariance $\mathbf{K}$

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{V}_A$ can be used to design diagonal values $\Leftrightarrow$ design SNRs

SVD-scheme as MMSE-VBLAST (QR)

Choosing $\mathbf{V}_A$ of the SVD of $\mathbf{H}_B \mathbf{K}^{1/2}$ $\Rightarrow$ SVD scheme (no SIC needed)

Precoded V-BLAST

MMSE-VBLAST with precoding for a given covariance $\mathbf{K}$

- $\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \mathbf{T}_B$
- $\mathbf{V}_A$ can be used to design diagonal values $\Leftrightarrow$ design SNRs

SVD-scheme as MMSE-VBLAST (QR)

Choosing $\mathbf{V}_A$ of the SVD of $\mathbf{H}_B \mathbf{K}^{1/2}$ $\Rightarrow$ SVD scheme
(no SIC needed)

Geometric-mean decomposition [Jiang et al. '05]/ QRS [Zhang et al. '05]

- $\mathbf{V}_A$ is choosing s.t. all diagonal values (all SNRs) are equal
- The same codebook can be used over all subchannels
- No need for bit-loading

V-BLAST: What Codes Can be Used?

Problem

- **Not any** codebooks can be used!
- At each stage of V-BLAST: Noise = Gaussian noise + ISI
- Aligned codes impair decoding

Alignment phenomenon

For the decoding of sub-stream x_i

- Bob Cancels out $x_{i+1}, \ldots, x_N$
- Applies maximum ratio combining for the recovery of x_i
- Example: Suppose the resulting effective channel is

$$y_i^{\text{eff}} = 2x_i + \underbrace{x_{i-1} + z_i}_{\text{Effective noise}}$$

- If x_i, x_{i-1} belong to same lattice codebook
  $\Rightarrow 2x_i + x_{i-1}$ is **not uniquely decodable!**

V-BLAST: What Codes Can be Used?

- In V-BLAST: Bob observes a MAC channel at each stage i

Multiple-access (MAC) SIC codes

- A collection of AWGN codes that are "sufficiently different"
- No MAC gains can align them
- Relaxation of the "MAC capacity-achieving codes" of [Baccelli, El Gamal, Tse 2011]

How to generate such codes?

Theoretical: Encapsulate in dithered modulo lattice of high dim.

- Not black box! ☹

Practical: Simple randomization process suffice (not rigor!):

- Multiplicative (phase) dithering
- Different interleaving / permutation of each code

Putting It All Together

New Scheme for General SNR [Kh., Kochman, Khisti ISIT2014]

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \quad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \quad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$

New Scheme for General SNR [Kh., Kochman, Khisti ISIT2014]

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \quad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \quad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$
- $\mathbf{V}_A$ of Eve's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy

New Scheme for General SNR [Kh., Kochman, Khisti ISIT2014]

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \quad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \quad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$
- $\mathbf{V}_A$ of Eve's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy
- $\mathbf{V}_A$ of Bob's SVD $\Rightarrow$ No need for V-BLAST

New Scheme for General SNR [Kh., Kochman, Khisti ISIT2014]

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \overbrace{\begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_N \end{pmatrix}}^{\mathbf{T}_B}, \quad b_i^2 = 1 + \mathrm{SNR}_i^B$$

$$\begin{bmatrix} \mathbf{H}_E \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_E \overbrace{\begin{pmatrix} e_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & e_N \end{pmatrix}}^{\mathbf{T}_E}, \quad e_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, e_i^2 - 1)$
- $\mathbf{V}_A$ of Eve's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy
- $\mathbf{V}_A$ of Bob's SVD $\Rightarrow$ No need for V-BLAST
- $\mathrm{diag}\{T_B\}, \mathrm{diag}\{T_E\}$ are const. $\Rightarrow$ Same code over all channels

New Scheme for General SNR [Kh., Kochman, Khisti ISIT2014]

But...

- Proof used random binning $\Rightarrow$ Existence result

New Scheme for General SNR [Kh., Kochman, Khisti ISIT2014]

But...

- Proof used random binning $\Rightarrow$ Existence result

Theorem

Good two-level MAC-SIC codes approach the MIMO WTC capacity.

Two-Level MAC-SIC Codes Achieve MIMO WTC Capacity

Proof idea

- **Bob**'s optimal (?) receiver of sub-message i:
  - Sub-messages $(i+1), \ldots, N$ are known
  - Subtract interference of $x_{i+1}, \ldots, x_N$
  - Treat $x_1, \ldots, x_{i-1}$ as noise
  - Project onto subspace of x_i
- **Eve**'s **genie-aided** optimal (?) receiver of sub-message i:
  - Sub-messages $(i+1), \ldots, N$ are revealed to Eve for decoding x_i
  - Subtract interference of $x_{i+1}, \ldots, x_N$
  - Treat $x_1, \ldots, x_{i-1}$ as noise
  - Project onto subspace of x_i

- Secrecy: Codes need to be two-level
- Optimality: Codes need to be MAC-SIC

End-to-End Scheme

"Nested black-box" type approach

End-to-End Scheme

"Nested black-box" type approach

or

"Матрёшка" ("Matryoshka") type approach

End-to-End Scheme

Modulation

- Apply the MIMO wiretap matrix decomposition scheme
- Bob uses standard V-BLAST for decoding

End-to-End Scheme

Modulation

- Apply the MIMO wiretap matrix decomposition scheme

Coding: Good two-level MAC-SIC codes

- Take *any* good AWGN codes of appropriate rates $\{R_i + \tilde{R}_i\}$
- Transform into "good MAC-SIC codes" via a randomization process (modulo-lattice, interleaving,...)
- Transform into "good two-level codes" via random indexing / two-universal hashing

- Bob uses standard V-BLAST for decoding

End-to-End Scheme

Modulation

- Apply the MIMO wiretap matrix decomposition scheme

Coding: Good two-level MAC-SIC codes

- Take *any* good AWGN codes of appropriate rates $\{R_i + \tilde{R}_i\}$
- Transform into "good MAC-SIC codes" via a randomization process (modulo-lattice, interleaving,...)
- Transform into "good two-level codes" via random indexing / two-universal hashing

- Bob uses standard V-BLAST for decoding

Alignment has a double-bad effect in wiretap

- Bob cannot recover the whole message
- ISI that serves as noise for Eve might align

Complementary

Good Wiretap Codes for SISO

Explanation of last requirement

$$I\left(x^n; y_E^n\right) = I\left(m, f; y_E^n\right) = I\left(m; y_E^n\right) + I\left(f; y_E^n | m\right)$$
$$= I\left(m; y_E^n\right) + \underbrace{H\left(f\right)}_{\substack{= n\tilde{R} \\ \geq n(C_E - \delta_1)}} - \underbrace{H\left(f | y_E^n, m\right)}_{\leq n\delta_2} \leq nC_E$$

$$\Downarrow$$

$$I\left(m; y_E^n\right) \leq n\left(\delta_1 + \delta_2\right)$$