The Confidential MIMO Broadcast Capacity

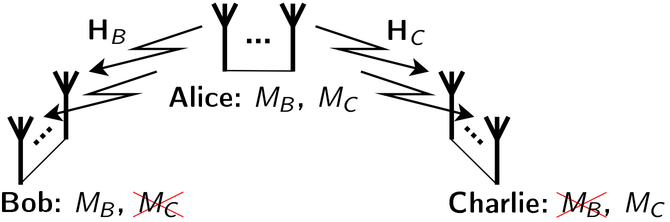
A Simple Derivation

Anatoly Khina, Tel Aviv University

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

IEEEI 2014
Eilat, Israel
December 5, 2014

Model: Confidential Gaussian MIMO Broadcast

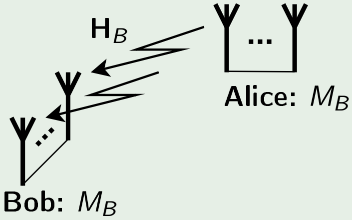


$\mathbf{y}_B = \mathbf{H}_B \mathbf{x}_A + \mathbf{z}_B$ $\qquad$ $\mathbf{y}_C = \mathbf{H}_C \mathbf{x}_A + \mathbf{z}_C$

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

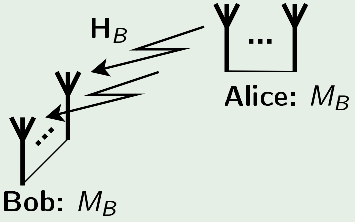
Outline of Talk (Special Cases)

MIMO Without Secrecy (No Charlie)

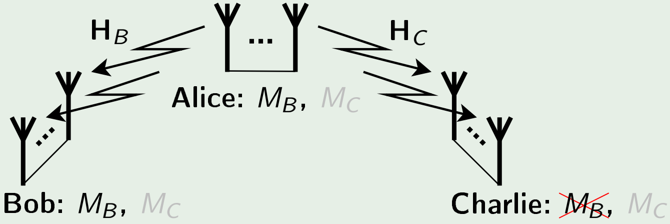


Outline of Talk (Special Cases)

MIMO Without Secrecy (No Charlie)

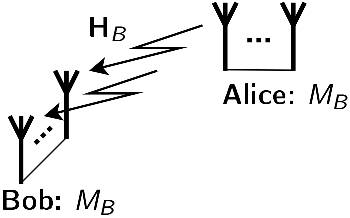


MIMO Wiretap (Maximize Rate to Bob)



MIMO Without Secrecy (No Charlie)

Practical Scheme via Matrix Decompositions



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)
- $$\mathbf{T}_B = \begin{pmatrix} b_1 & * & * & \cdots & * \\ 0 & b_2 & * & \cdots & * \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{N_A-1} & * \\ 0 & 0 & \cdots & 0 & b_{N_A} \end{pmatrix} \Rightarrow \begin{aligned} y_1^{\text{eff}} &= b_1 x_1 + z_1 \\ y_2^{\text{eff}} &= b_2 x_2 + z_2 \\ &\vdots \\ y_{N_A}^{\text{eff}} &= b_{N_A} x_{N_A} + z_{N_A} \end{aligned}$$
- Off-diagonal elements are canceled via either:
  - Successive interference cancellation (SIC)
  - Dirty-paper coding (DPC)

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 or DPC

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: Alice Applies Unitary $\mathbf{V}_A$

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: Alice Applies Unitary $\mathbf{V}_A$

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/DPC needed)

Precoded V-BLAST: Alice Applies Unitary $\mathbf{V}_A$

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

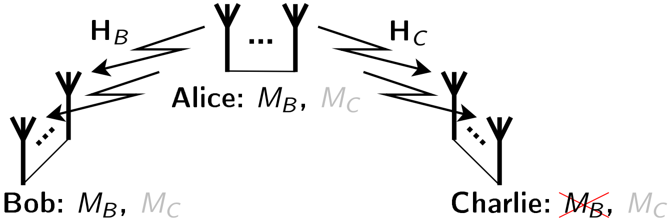
SVD-scheme as MMSE-VBLAST (QR)

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

MIMO Wiretap (Maximize Rate to Bob)



Gaussian MIMO Wiretap: Maximize rate to Bob

Total power constraint [Khisti–Wornell '10][Oggier–Hassibi '11]

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

- $X \sim$ Gaussian
- Maximization over all admissible covariance matrices $\mathbf{K}_A$
- No explicit expression for optimal $\mathbf{K}_A$

Gaussian MIMO Wiretap: Maximize rate to Bob

Total power constraint [Khisti–Wornell '10][Oggier–Hassibi '11]

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

- $X \sim$ Gaussian
- Maximization over all admissible covariance matrices $\mathbf{K}_A$
- No explicit expression for optimal $\mathbf{K}_A$

Input covariance constraint [Liu–Shamai '09]

- Replace $\mathrm{tr}\left\{\mathbf{K}_A\right\} \le P$ with $\mathbf{K}_A \preceq \mathbf{K}$
- Explicit exp. for optimal $\mathbf{K}_A$! [Bustin–Liu–Poor–Shamai '09]

Scheme for General SNR [Kh., Kochman, Khisti ISIT'14]

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

$$\begin{bmatrix} \mathbf{H}_C \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_C \overbrace{\begin{pmatrix} c_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & c_{N_A} \end{pmatrix}}^{\mathbf{T}_C}, \quad c_i^2 = 1 + \mathrm{SNR}_i^E$$

- Use good SISO wiretap codes for SNR-pairs $(b_i^2 - 1, c_i^2 - 1)$
- $\mathbf{V}_A$ of Charlie's SVD $\Rightarrow$ Easy secrecy analysis + strong secrecy
- $\mathbf{V}_A$ of Bob's SVD $\Rightarrow$ No need for V-BLAST
- $\mathrm{diag}\{\mathbf{T}_B\}, \mathrm{diag}\{\mathbf{T}_C\}$ are const. $\Rightarrow$ Same code over all channels

Scheme for General SNR [Kh., Kochman, Khisti ISIT'14]

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

$$\begin{bmatrix} \mathbf{H}_C \mathbf{K}^{1/2} \mathbf{V}_A \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_C \overbrace{\begin{pmatrix} c_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & c_{N_A} \end{pmatrix}}^{\mathbf{T}_C}, \quad c_i^2 = 1 + \mathrm{SNR}_i^E$$

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

Genie-aided secrecy-proof

- Charlie tries to recover messages sequentially (from last to first)
- For the recovery of message i all previous messages are revealed

Dirty-Paper Coding Variant of Scheme [New]

Alice:

- Cancels out off-diagonal elements of Bob via DPC
- Uses good SISO DPC wiretap codes for SNR-pairs $(b_i^2 - 1, c_i^2 - 1)$

Bob: Recovers using DPC decoder (as in MIMO without secrecy)

Genie-aided secrecy-proof

- Similar to secrecy analysis for SIC scheme
- Charlie tries to recover messages sequentially
- Messages this time are Costa-like auxiliaries (U_i)
- For the recovery of message i previous auxiliaries are revealed (from which the signals X_i can be constructed)

Reinterpretation of Optimal K_A Expression of Bustin *et al.* via GSVD

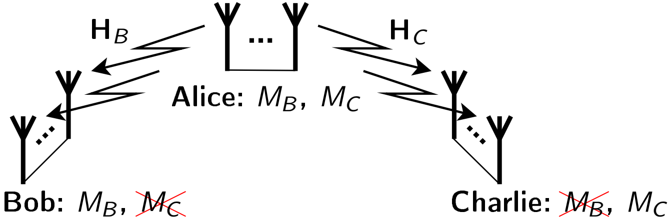
- Apply the *Generalized Singular Value Decomposition* (GSVD) to the "MMSE–VBLAST" matrices:

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_{N_A} \end{pmatrix} \mathbf{V}_A^\dagger$$

$$\begin{bmatrix} \mathbf{H}_C \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_C \begin{pmatrix} c_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & c_{N_A} \end{pmatrix} \mathbf{V}_A^\dagger$$

- $\mathbf{Q}_B$, $\mathbf{Q}_C$, $\mathbf{V}_A$ – Unitary
- $\frac{b_i}{c_i}$ decreases with i and "least balanced" [Kh.-Kochman-Erez '12]
- Choose directions corresponding to $\frac{b_i}{c_i} > 1$ and nullify the rest

Finally... Confidential MIMO Broadcast



Confidential MIMO BC Capacity [Liu–Liu–Poor–Shamai '10]

Total power constraint

Using Lemma 1 of [Weingarten–Steinberg–Shamai '06]:

$$\mathcal{C}\left(\mathbf{H}_B, \mathbf{H}_C, P\right) = \bigcup_{\mathbf{K}_A:\, \mathrm{tr}\{\mathbf{K}_A\} \leq P} \Big(C_B\left(\mathbf{H}_B, \mathbf{H}_C, \mathbf{K}_A\right), C_C\left(\mathbf{H}_B, \mathbf{H}_C, \mathbf{K}_A\right) \Big)$$

$\Rightarrow$ Suffices to determine capacity region under covariance constraint

Covariance constraint

- No tension between users
- Both users achieve optimal wiretap capacities **simultaneously**!
- Rectangular capacity region

Confidential MIMO BC Capacity [Liu–Liu–Poor–Shamai '10]

Method of proof for covariance constraint

Converse: Trivial (both users achieve optimality simultaneously)

Achievable:

- Development of new achievable for MIMO wiretap channel that uses "artificial noise"
- Showing that new techniques achieves capacity (via *channel enhancement* technique)
- Double random-binning schemes and "secret dirty-paper coding"
- Alice $\rightarrow$ Bob: Uses "standard" random binning (standard technique)
- Alice $\rightarrow$ Charlie: Uses random binning with artificial noise (new technique)

Confidential MIMO BC Capacity [Liu–Liu–Poor–Shamai '10]

Connection to [Bustin–Liu–Poor–Shamai '09]

- Generalization of the techniques of Bustin *et al.*
- Capacity region can be represented via "generalized eigenvalues"

Confidential MIMO BC Capacity: New Derivation

- Simple derivation
- Uses standard MIMO wiretap capacity expression
- Builds upon [Bustin–Liu–Poor–Shamai '10]
- Uses standard (Costa) dirty-paper coding
- Explains why dirty-paper coding is required (for at least one of the users)
- Connection to the *generalized singular values* is natural
- Allows construction of a practical scheme

Capacity-Achieving Confidential MIMO Broadcast

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_{N_A} \end{pmatrix} \mathbf{V}_A^\dagger$$

$$\begin{bmatrix} \mathbf{H}_C \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_C \begin{pmatrix} c_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & c_{N_A} \end{pmatrix} \mathbf{V}_A^\dagger$$

- Choosing directions of $b_i > c_i$ is optimal for Bob
- **But...** Choosing directions of $b_i < c_i$ is optimal for Charlie!

$\Longrightarrow$

Allocate $b_i > c_i$ to Bob
Allocate $b_i < c_i$ to Charlie

Capacity-Achieving Confidential MIMO Broadcast

$$\begin{bmatrix} \mathbf{H}_B \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_B \begin{pmatrix} b_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & b_{N_A} \end{pmatrix} \mathbf{V}_A^\dagger$$

$$\begin{bmatrix} \mathbf{H}_C \mathbf{K}^{1/2} \\ \mathbf{I}_{N_A} \end{bmatrix} = \mathbf{Q}_C \begin{pmatrix} c_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & c_{N_A} \end{pmatrix} \mathbf{V}_A^\dagger$$

Scheme

Charlie: Uses SIC or DPC over elements satisfying $c_i > b_i$

Bob: Uses DPC scheme over elements satisfying $b_i > c_i$

- Alice pre-cancels interference also from Charlie's signals
- Bob can gain no info. of Charlie's message from DPC

Capacity-Achieving Confidential MIMO Broadcast

Decoupling the Modulation

- Alice can apply additional unitary block-matrix operations:

$$\tilde{\mathbf{T}}_B = \overbrace{\begin{pmatrix} \mathbf{Q}^\dagger_{B;B} & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}^\dagger_{B;C} \end{pmatrix}}^{\text{Bob}} \begin{pmatrix} \mathbf{B}_B & * \\ \mathbf{0} & \mathbf{B}_C \end{pmatrix} \overbrace{\begin{pmatrix} \mathbf{V}_B & \mathbf{0} \\ \mathbf{0} & \mathbf{V}_C \end{pmatrix}}^{\text{Alice}}$$

$$\tilde{\mathbf{T}}_C = \overbrace{\begin{pmatrix} \mathbf{Q}^\dagger_{C;B} & \mathbf{0} \\ \mathbf{0} & \mathbf{Q}^\dagger_{C;C} \end{pmatrix}}^{\text{Charlie}} \begin{pmatrix} \mathbf{C}_B & * \\ \mathbf{0} & \mathbf{C}_C \end{pmatrix} \overbrace{\begin{pmatrix} \mathbf{V}_B & \mathbf{0} \\ \mathbf{0} & \mathbf{V}_C \end{pmatrix}}^{\text{Alice}}$$

- SVD of Charlie's "block" $\mathbf{C}_C$ allows him to avoid SIC or DPC
- Other decompositions with desired properties can be applied (SVD of $\mathbf{B}_C$, 2-GMD of $(\mathbf{B}_B, \mathbf{B}_C)$, 2-GMD of $(\mathbf{C}_B, \mathbf{C}_C)$, etc.)

Summary

- Simple derivation of capacity region of confidential MIMO BC
- Simple extension of the result of Bustin *et al.* for MIMO WTC
- Connection to generalized singular values is immediate
- Explicitly shows why DPC by at least one user is required