Jamming MIMO Communications

Rutgers, The State University of New Jersey

www.winlab.rutgers.edu

Contact: Rob Miller

rdmiller@winlab.rutgers.edu

So just what is this guy talking about?

- Multi-Input Multi-Output (MIMO) Overview
- Channel State Information (CSI)
- MIMO Channel Capacity
- Jamming Results and Observations
  - Singular Value Decomposition (SVD)-based MIMO
  - Alamouti Space-Time Block Code (STBC)
- Conclusions and Questions

Introducing the MIMO channel…

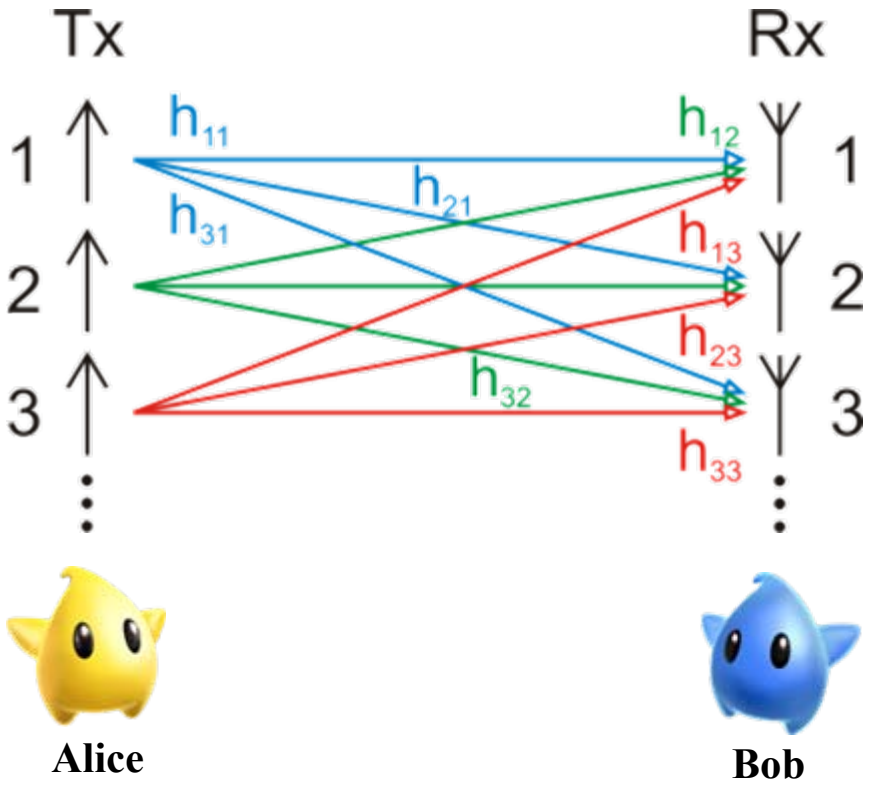
- Alice sends **x** using n_t transmit antennas
- Bob sees **r** with n_r receive antennas

$$\mathbf{r} = \mathbf{H}\mathbf{x} + \mathbf{n}$$

where,

H is n_r by n_t channel matrix

n is additive channel noise

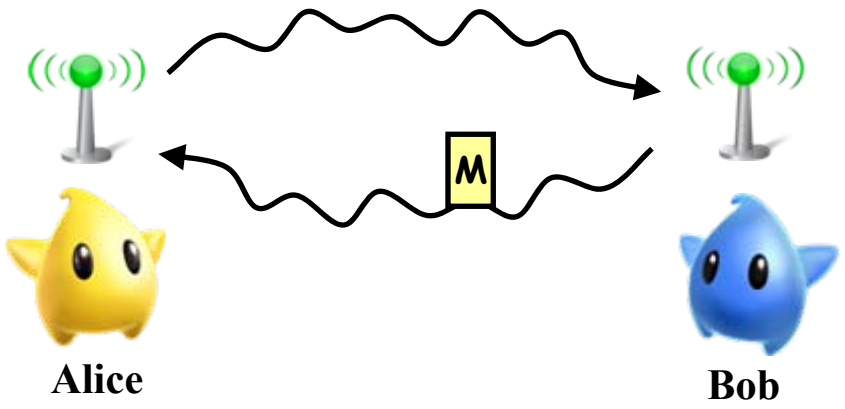


Three main sub-categories of MIMO exist…

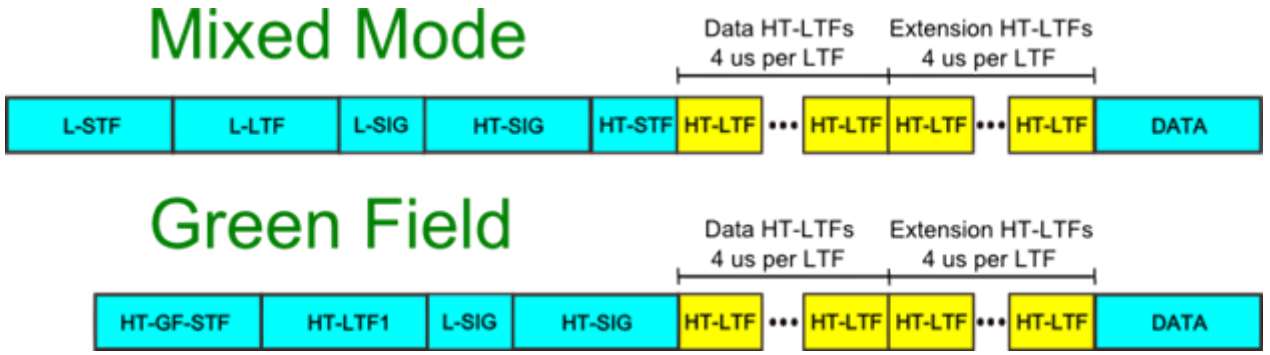
- Spatial Multiplexing
  - Low-rate streams are created from a high-rate signal and transmitted from different antennas
  - Does not always require Channel State Information (CSI)
  - Can be combined with Pre-coding or Diversity Coding
- Pre-coding
  - Ranges from multi-layer beamforming to all spatial processing
  - Requires CSI at the transmitter
- Diversity Coding
  - Includes space-time coding (STC) techniques
  - Does not require CSI at the transmitter

Most MIMO schemes involve some level of Channel State Information (CSI).

- Channel State Information is utilized by the transmitter, the receiver, or both.
  - Bob to Alice
  - Alice to Bob
  - Alice to Bob and then back
    - *estimation*
    - *messaging*



- 802.11n packet structure lets Bob estimate the CSI.



Attacking only the CSI procedure is efficient, effective, and covert.

CSI Training Sequences (TS) are shorter than data transmissions

- ***Efficient***

  Jamming only during the CSI is energy conservative

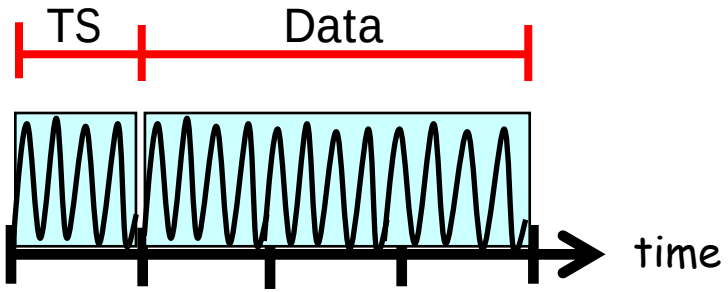
- ***Effective***

  Jamming the CSI causes errors in decoding the data

- ***Covert***

  Jamming only the CSI is more inconspicuous

Eve



A commonly studied MIMO technique is SVD-based MIMO.

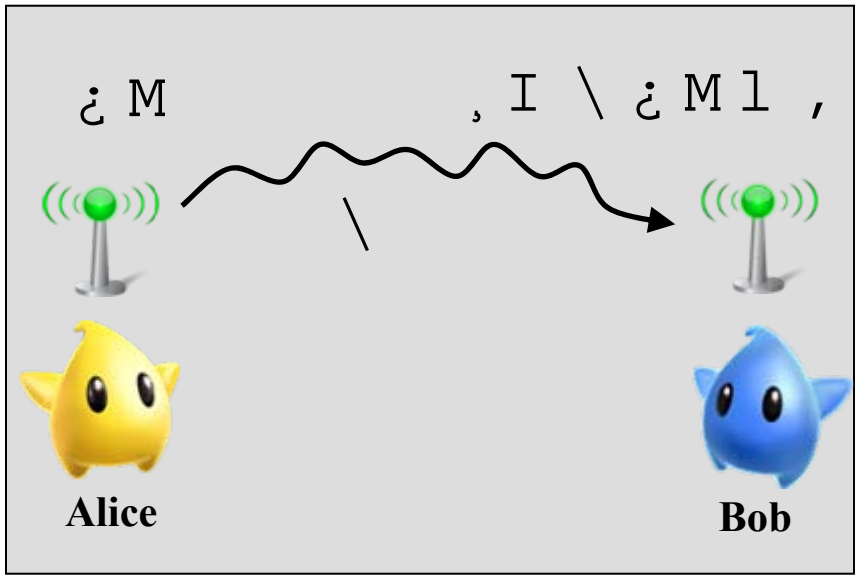
- Recall, the SVD of **H** yields \ I] * ¿ \

  U and **V** are the left and right singular vectors

  Singular values found in diag(∑)

- Bob and Alice compute the SVD
  - Alice transmits (**Vx**)
  - Bob receives **r**,
    and operates on it with ($\mathbf{U}^H$)

i I] \ ¸
I] \ \ ¿ M l] \ ,
I] \ ] * ¿ \ ¿ M l] \ ,
I *M l] \ ,



Results in min(n_r, n_t) parallel SISO channels

SVD-based MIMO can achieve capacity by waterfilling over the best channel eigenmodes.

- Mutual Information

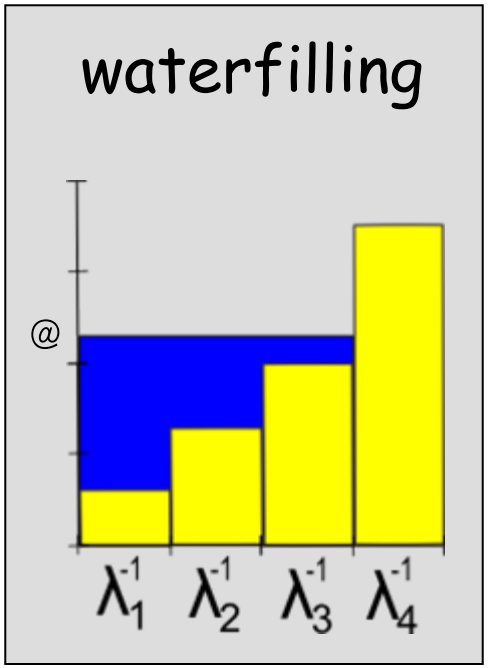
- Maximization:

- Capacity:

- Power Distribution:

, where

Power Constraint



Jamming SVD-based MIMO is complicated as there are many degrees of freedom.

The rabbit hole deepens…

- CSI knowledge:
  - Perfect, Estimated, None
- Perturbation Ability:
  - Perfect, Estimated, Random
- Target:
  - Alice, Bob, Alice *and* Bob
- Equipment:
  - Single/Multiple antenna
  - Power constraints (J/S)

General CSI jamming

$$\begin{aligned} \mathbf{s}_J &= \hat{\mathbf{U}}_B^H \mathbf{H} \hat{\mathbf{V}}_A \mathbf{x} + \hat{\mathbf{U}}_B^H \mathbf{n} \\ &= \hat{\mathbf{U}}_B^H \mathbf{U} \Sigma \mathbf{V}^H \hat{\mathbf{V}}_A \mathbf{x} + \hat{\mathbf{U}}_B^H \mathbf{n} \end{aligned}$$

With ample control, Eve may force Alice and Bob to perform opposite waterfilling.

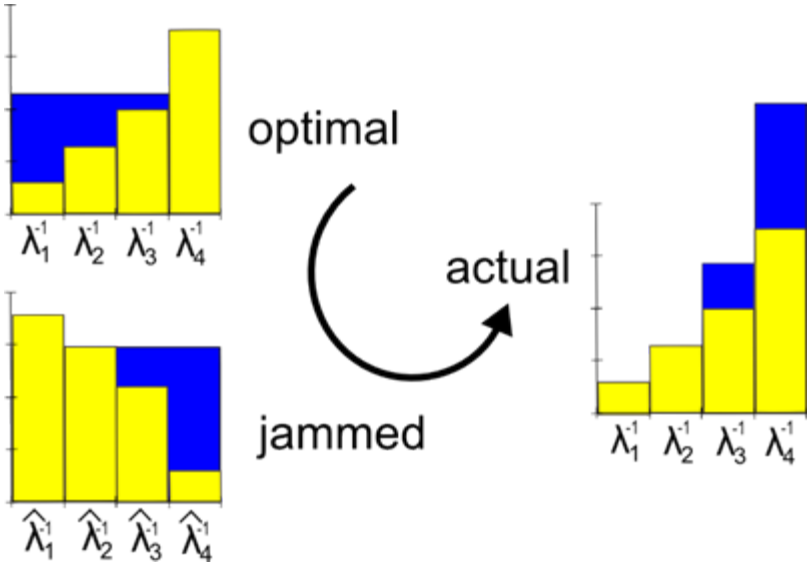
- Eve can force opposite waterfilling
  - Compute the SVD of **H**

    \ I] * ¿ \
  - Reverse the singular values

    5W I 5,1 W
  - Reconstruct the new channel

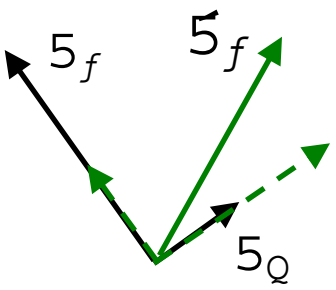
    \´ I] *´ ¿ \
  - Disseminate the new info

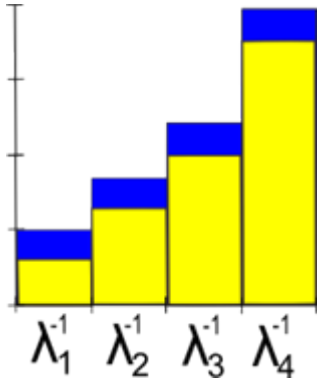
    Alice and Bob use \´



Without CSI or complete RF control, Eve can still effectively jam SVD-based MIMO.

- Random perturbations of **H** make small singular values larger
- If Alice and Bob use the same estimate
  - Emphasize a physical channel to create a random channel
    - *Power, on average, will empty uniformly into the actual eigenmodes of the channel*
- If Alice and Bob use independent estimates
  - Emphasize different physical channels to create two random channels
    - *Alice pre-codes with right singular vectors that do not pair with the left singular vectors that Bob uses for decoding*



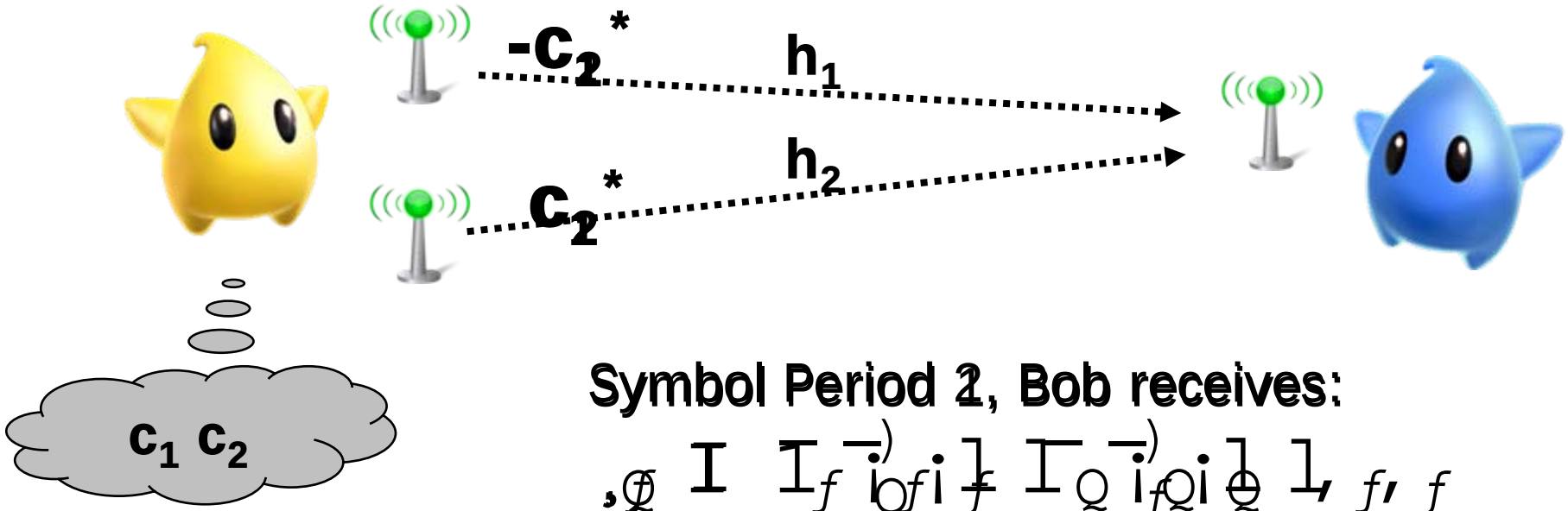


Another popular MIMO scheme is the Alamouti Space-Time Block Code (STBC).

- The Alamouti STBC is included in 802.11n, WiMax, and 3GPP
- Analyze the 2 by 1 STBC vulnerabilities
  - 2 transmit antennas
  - 1 receive antenna
- Extend results to 2 by 2 STBC and beyond

The Alamouti 2 by 1 STBC is essentially a spatial repeater with a decoding trick.

- Spatial repeater w/decoding trick
  - Alice has 2 transmit antennas
  - Bob has 1 receive antenna

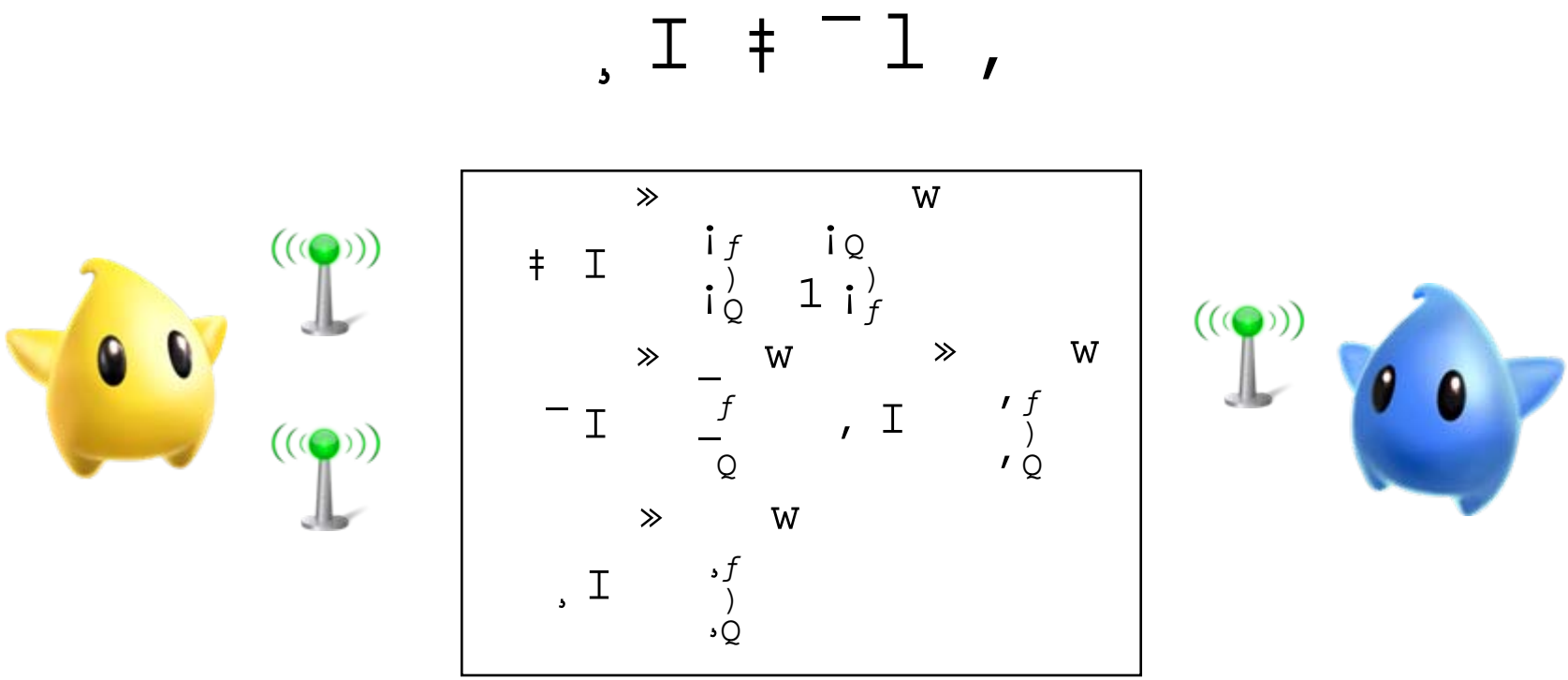


Symbol Period 2, Bob receives:

$$\text{[illegible]}$$

The Alamouti 2 by 1 STBC is essentially a spatial repeater with a decoding trick.

- Over <u>both</u> symbol periods, Bob receives:



The Alamouti 2 by 1 STBC is essentially a spatial repeater with a decoding trick.

- Bob decodes by selecting the symbol-tuple that minimizes the decoding metric:

Note:

We investigate the impact of jamming the channel estimate for the Alamouti 2 by 1 STBC.

- Eve jams: ‡ , ‡́
- Bob *now* selects the symbol-tuple that minimizes the jammed decoding metric:

i◦ I Ơ‡ ¸ 1 – Ơ

I Ơ‡ »‡ ¯ 1 , d1 – Ơ

I Ơ‡ »‡ ¯ 1 , 1 ‡ dƠ

I Ơ‡ »‡ ¯ 1 ‡ d1 ‡ , Ơ

Note: – I Ơi ƒ Ơ 1 Ơi Q Ơ

Eve's goal

Maximize d_J for the proper symbol-tuple, minimize it otherwise

Forcing minimization for the Alamouti 2 by 1 STBC can be done in multiple ways.

- Metric minimization occurs when »ǂ ¯1 ǂ´¯d[{ »ǂ´\ d
  - 2 interesting cases:

(1) ǂ´\ I H

(2) ǂ ¯1 ǂ´¯ I H

Not covert

decoding metric

i₀ I Oǂ´\ ,1 -¯O

I Oǂ´\ »ǂ ¯1 ,d1 -¯O

I Oǂ´\ »ǂ ¯1 , 1 ǂ´¯dO

I Oǂ´\ »ǂ ¯1 ǂ´¯dl ǂ´\ ,O

- Notable Attacks
  - Selective Symbol Jamming

    Force Bob to decode symbol-tuples Eve desires!
  - Oscillating Channel Inversion Attack

    Guaranteed jamming performance with no CSI!

With ample control, Eve can force Bob to decode the symbol-tuples that she desires.

- Selective Symbol Jamming
  - Eve chooses:
    where

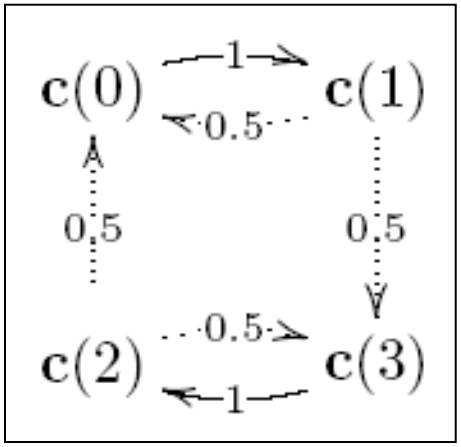
BPSK Example using h = [7 -8]

BPSK Symbol Tuples			
c(0)	c(1)	c(2)	c(3)
$\begin{bmatrix}-1\\-1\end{bmatrix}$	$\begin{bmatrix}-1\\1\end{bmatrix}$	$\begin{bmatrix}1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$

Eve's goal: Make Bob decode c(1) not c(0).

Transmitted c(0)	Decoded c(1)	$\hat{G}$	Metrics c(0)	c(1)	c(2)	c(3)
$\begin{bmatrix}-1\\-1\end{bmatrix}$	$\begin{bmatrix}-1\\1\end{bmatrix}$	$\begin{bmatrix}-0.5 & 0.5\\-7.5 & 7.5\end{bmatrix}$	160	0	320	160

But, jamming also affects the other transmitted symbol tuples.



With ample control, Eve can force Bob to decode the symbol-tuples that she desires.

- Selective Symbol Jamming
  - But, the format of G may be constrained:
  - Viable solutions still exist.

BPSK Example using h = [7 -8]

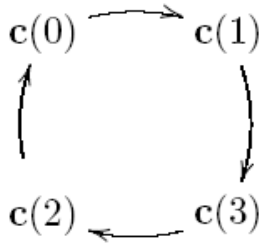
BPSK Symbol Tuples			
c(0)	c(1)	c(2)	c(3)
$\begin{bmatrix}-1\\-1\end{bmatrix}$	$\begin{bmatrix}-1\\1\end{bmatrix}$	$\begin{bmatrix}1\\-1\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$

Eve's goal: Make Bob decode c(1) not c(0).

Now use:

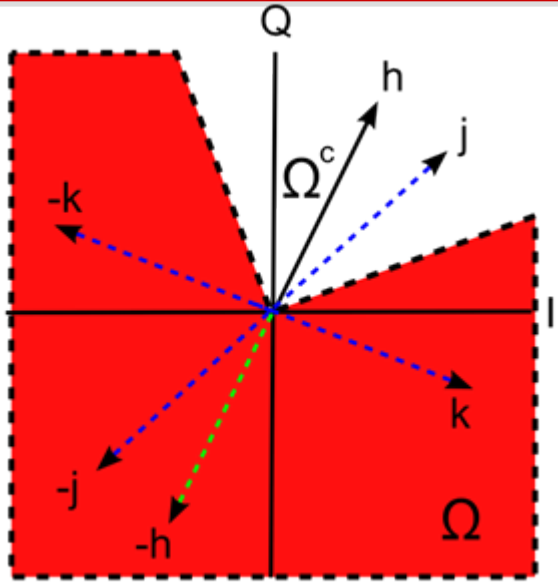
Jammed Metrics				
TX \ RX	c(0)	c(1)	c(2)	c(3)
c(0)	210	21	319	241
c(1)	319	210	241	21
c(2)	21	241	210	319
c(3)	241	319	21	210

Symbol-tuple Transitions



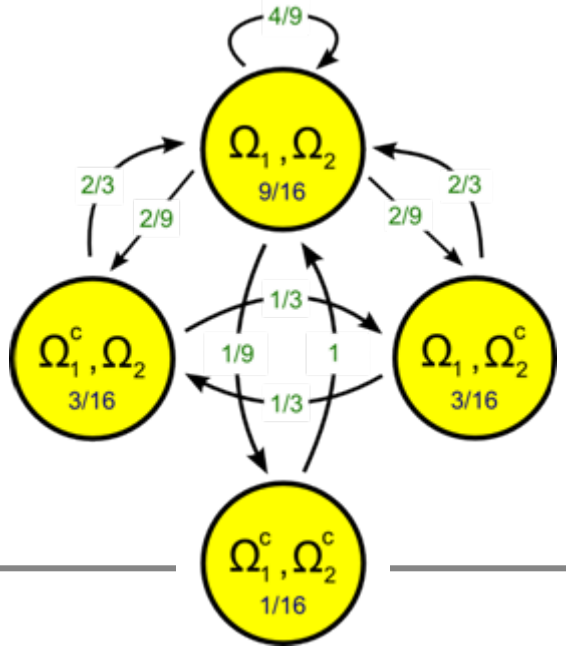
Without CSI or complete RF control, Eve can still effectively jam the Alamouti STBC.

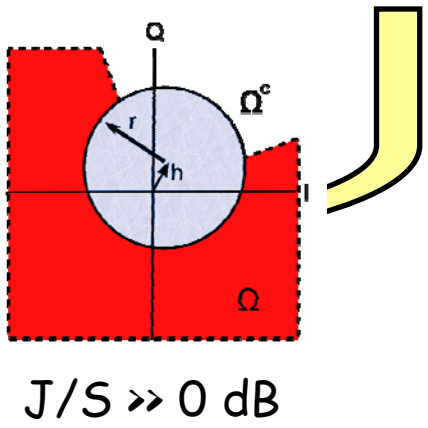
- Optimal Jamming Region is constellation specific
- Oscillating Channel Inversion Attack
  - For single antenna using QPSK, $P(\Omega) = \frac{3}{4}$ (when J/S >> 0 dB)
  - Oscillating by 180 guarantees jamming region penetration



Single Antenna Jamming Region

Dual Antenna Jamming Region FSM



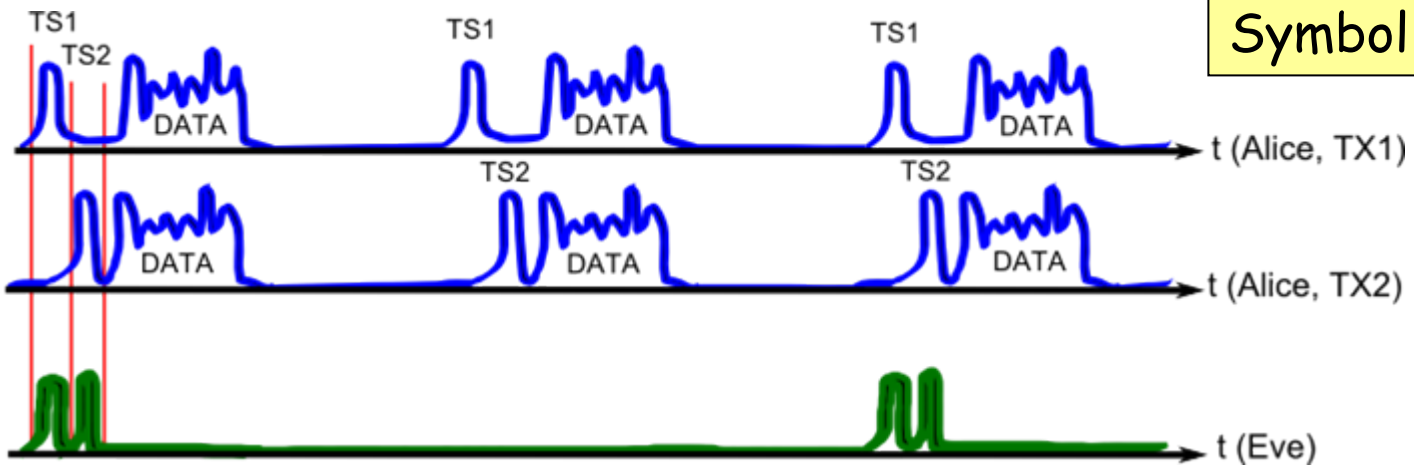


J/S >> 0 dB

The oscillating channel inversion attack was successful in a real-world experiment.

- GNU Radio/USRP
  - *Alamouti 2 by 1 STBC*
    - 1800 MHz
    - 12 QPSK symbols @12.5 kBd
- Arbitrary Waveform Generator
  - *Incremental 90 degrees per attack*

J/S ~ 10 dB
Symbol Error Rate 0.65



Attacking the CSI Procedure in MIMO Systems is viable, effective, and efficient.

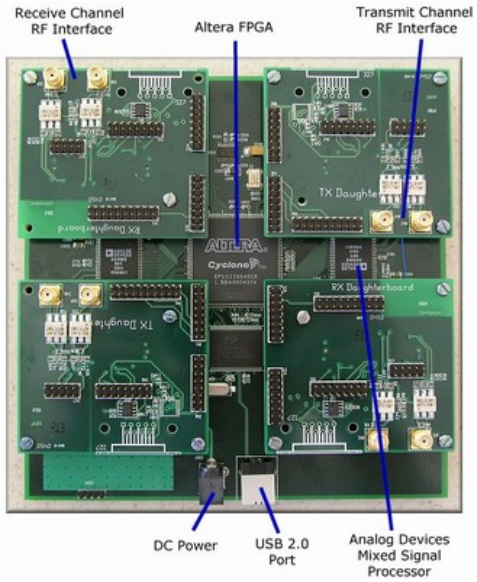
- CSI plays an important role in most MIMO systems.
- Jamming the CSI represents a powerful point of attack
  - SVD-based MIMO
  - Alamouti STBC
    - *Real world experimentation using 2 by 1 STBC*
    - *Extensions to higher order antenna constellations straightforward*

Questions & Comments?

Extra Slides Follow

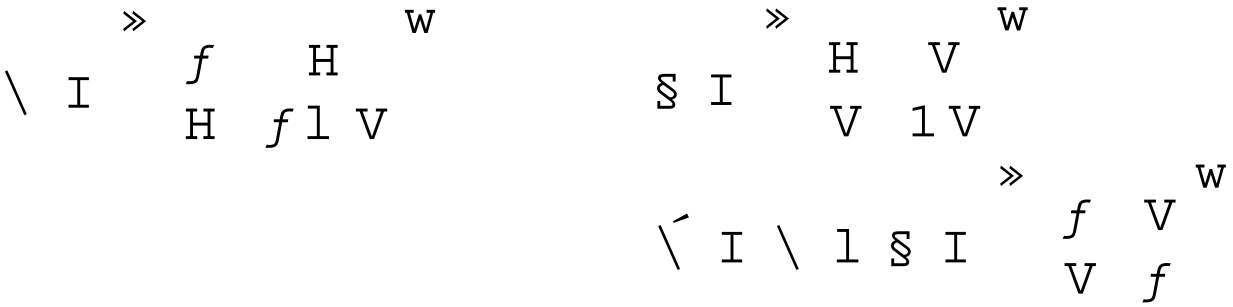
GNU Radio

the gnu software radio



Jamming SVD-based MIMO

- Unknown E can be a serious problem
  - SVD is non-continous function:



SVD

  - Only of concern for close singular values…

45° shift in eigenvector space!

Jamming SVD-based MIMO

- Close singular values in real-world channels?
- Consider a Rayleigh Fading MIMO channel
  - Uncorrelated Antenna elements
  - Singular values are roots of the eigenvalues of the central Wishart matrix: $g\ I \setminus \setminus$
  - Ordered eigenvalue distribution follows:

$$\breve{}\,\gg)_{f}5)_{Q}5\$\$\$5)_{,}dI\cdot\prod_{WI\,f}^{8'}\,"1\,)_{W})_{W}^{\gg e\ 1\ ,d}\,n\prod_{W\text{¥}\,\ll}^{8'}\gg)_{W}1\ )_{\ll}d^{Q}$$

,where $\cdot\ I\ \dfrac{D^{\gg,\gg,1\,fdd}}{3\gg e\ d3\gg,d}$ and $3_{,}\gg\%dI\ D^{\gg,\gg,1\,fd/Qd}\prod_{WI\,f}^{8'}\gg\%1\ W\text{Ð}=$

Jamming SVD-based MIMO

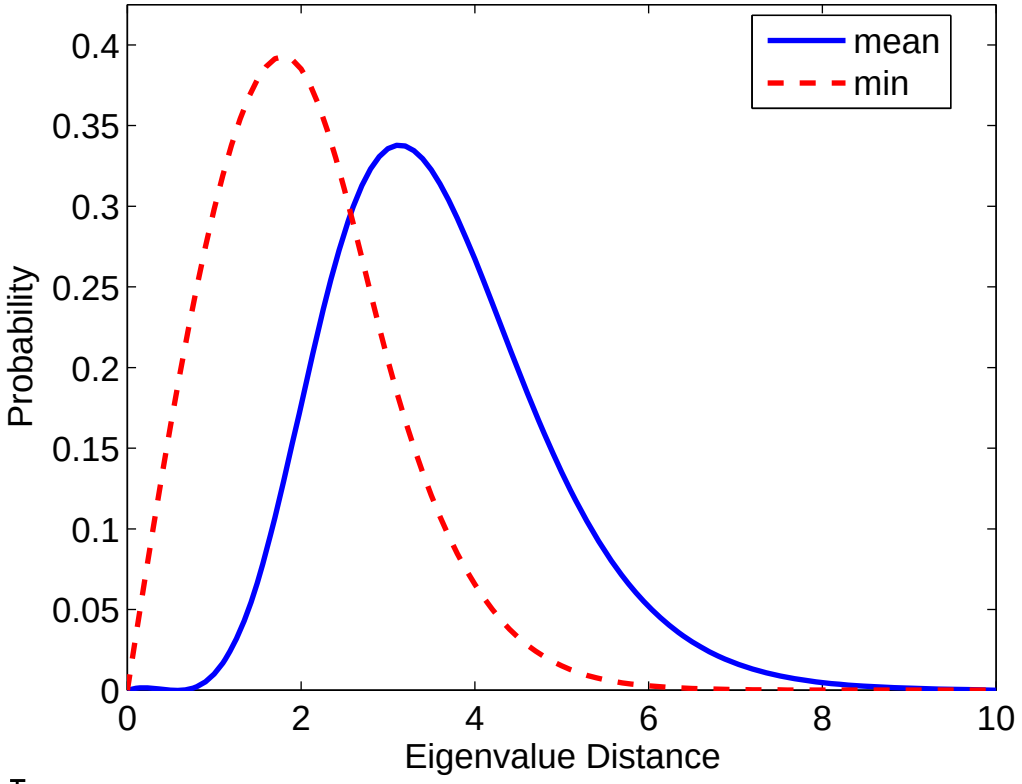
- Close singular values in real-world channels?
- Rayleigh 3x4

  3 Eigenvalues

- Not probable

  Reliable

  bounding:



S′

»5^»\ l § d1 5^»\ dd² . L§ L²ᵇ

^I ƒ

Ø5^»\ l § d1 5^»\ dØ. 5ƒ»§ dI L§ L²