# Secret Communication via Multi-antenna Systems

Zang Li
Wade Trappe
Roy Yates

WINLAB, Rutgers University

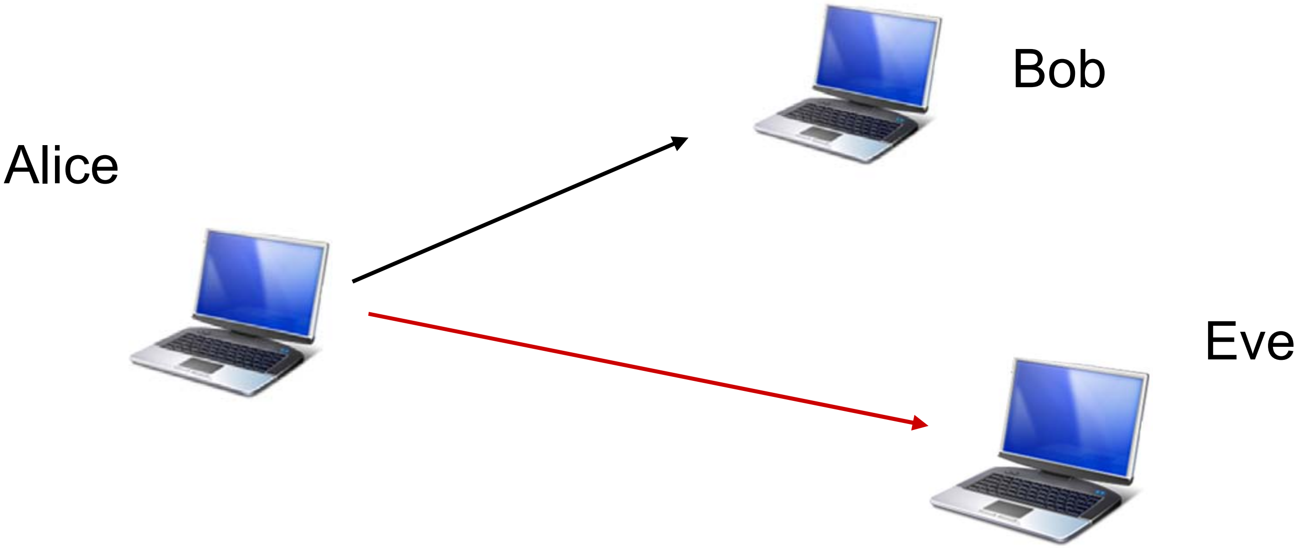
# Outline

- Information theory background on information security
- Problem formulation for multiple antenna system
- Solution for a multiple-input-single-output (MISO) system
- Numerical evaluation
- Conclusion

# Introduction

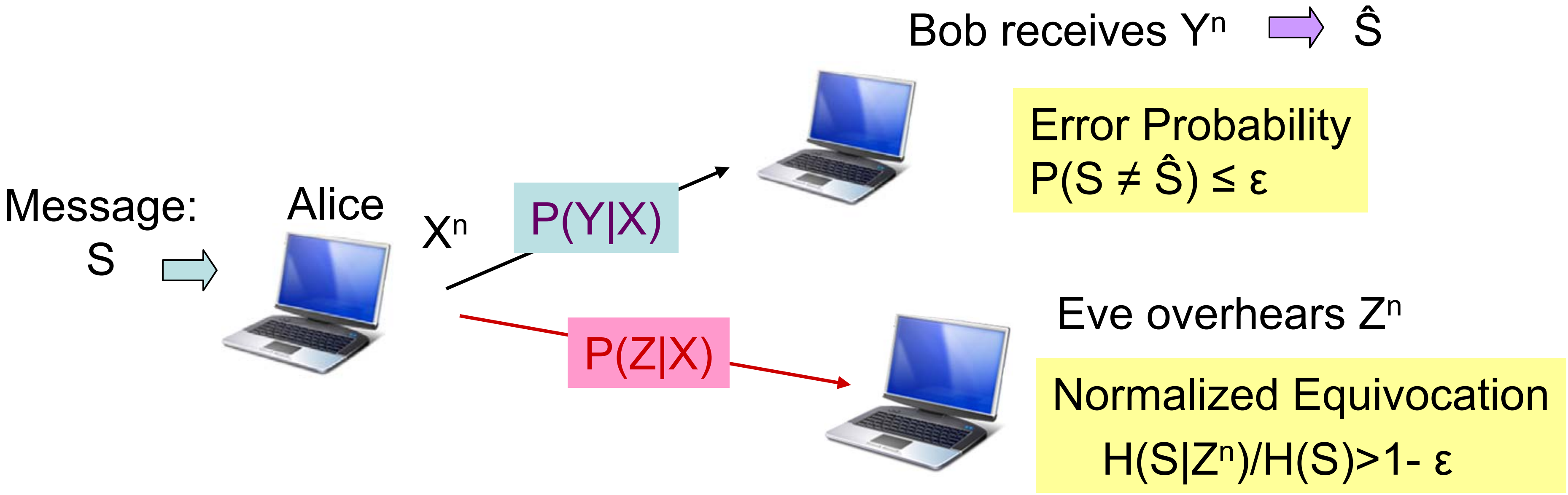
- Information theoretic secret communication over wireless medium in presence of a passive eavesdropper
  - Eavesdropper is no better than random guessing the secret message
- The noisy nature of the wireless medium can be exploited to achieve information theoretic communication
- Multi-antenna system: the extra degrees of freedom facilitates secret communication

# Scenario



- Wireless broadcast channel
- Passive eavesdropper
- Can Alice talk to Bob secretly? If yes, what is the secrecy rate?

# Information Secure Secret Communication



Message: S

Alice

$X^n$

$P(Y|X)$

Bob receives $Y^n$ ⇨ $\hat{S}$

Error Probability
$P(S \neq \hat{S}) \leq \varepsilon$

$P(Z|X)$

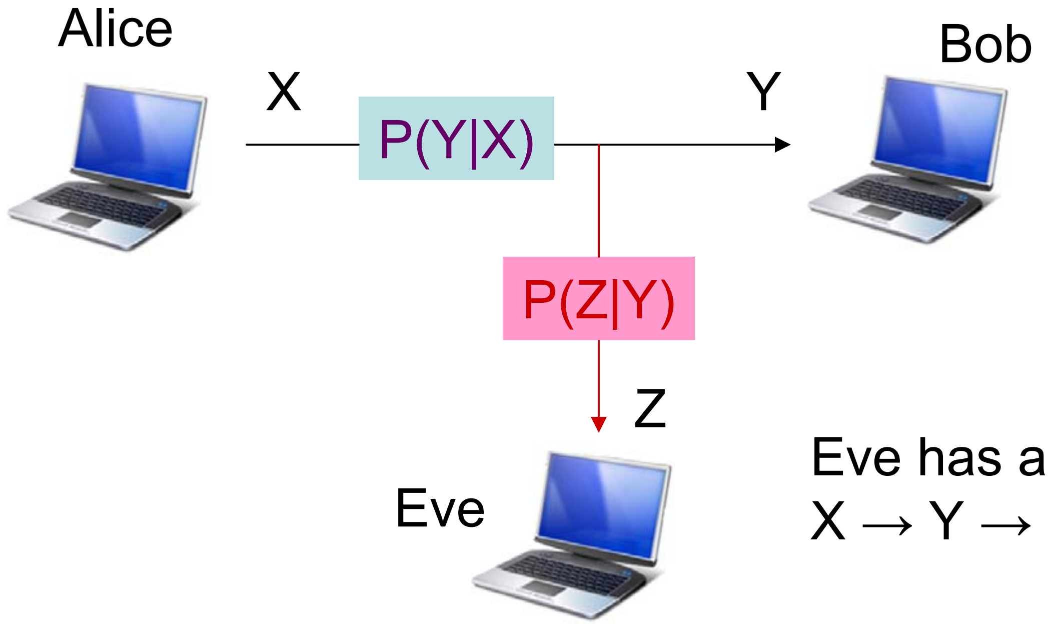
Eve overhears $Z^n$

Normalized Equivocation
$H(S|Z^n)/H(S) > 1 - \varepsilon$

- Reliable transmission requirement
- Perfect secrecy requirement
- **Secrecy capacity:** maximum reliable rate with perfect secrecy
  - This rate might be very small, but we only need it to setup the key for subsequent communication

# Wiretap Channel

- Wiretap channel (Wyner75)

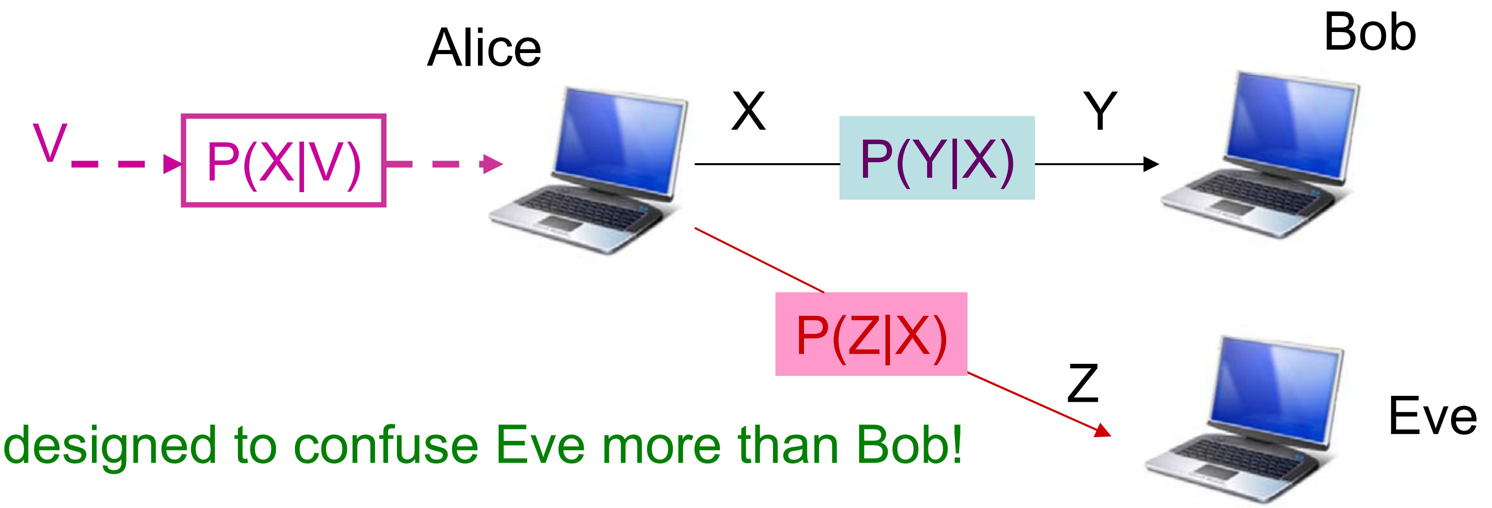


Eve has a degraded channel
X → Y → Z

$$C_{\text{sec}} = \max_{P(x)} I(X;Y) - I(X;Z)$$

# Broadcast Channel

- Broadcast channel (Csiszar & Korner 78)



V is designed to confuse Eve more than Bob!

$$\boxed{C_{sec} = \max_{V \to X \to YZ} \left( I(V;Y) - I(V;Z) \right)}$$

?

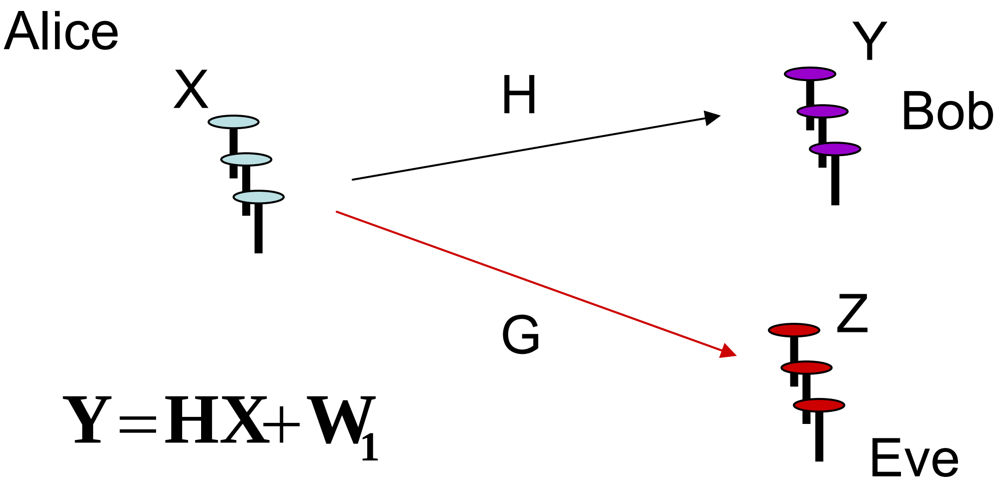
# When does V = X?

- More capable condition (Csiszar & Korner 78) :
  - $I(X; Y) - I(X; Z) \geq 0$ for all input x
- Bob’s channel is more capable $\Rightarrow$ V = X
  - Wiretap channel satisfies the more capable condition
  - Gaussian broadcast channel (when Bob’s SNR > Eve’s SNR)
    - Leung-Yan-Cheong &Hellman 1978
- Still a mystery in many other scenarios

# Recent Work on Wireless PHY Secrecy

- Mitrpant, Vinck, Luo [ISIT 06] Wiretap with noncausal CSI
- Barros & Rodrigues [ISIT 06] Outage in Rayleigh Fading
- Liang & Poor [Allerton 06] Ergodic Secrecy Capacity in Flat Fading
- Li, Yates, Trappe [Allerton 06] Parallel Channels
- Gopala, Lai, H. El Gamal [ITA 07] Slow Fading
- Khisti, Tchamkerten and Wornell [IT] Secure broadcasting
- Relay channel, multiple access channel, interference channel…
- Multi-antenna system: Hero 03, Negi et. al. 03, Xiaohua Li et. al. 03, Parada & Blahut 05 …

# Problem Formulation



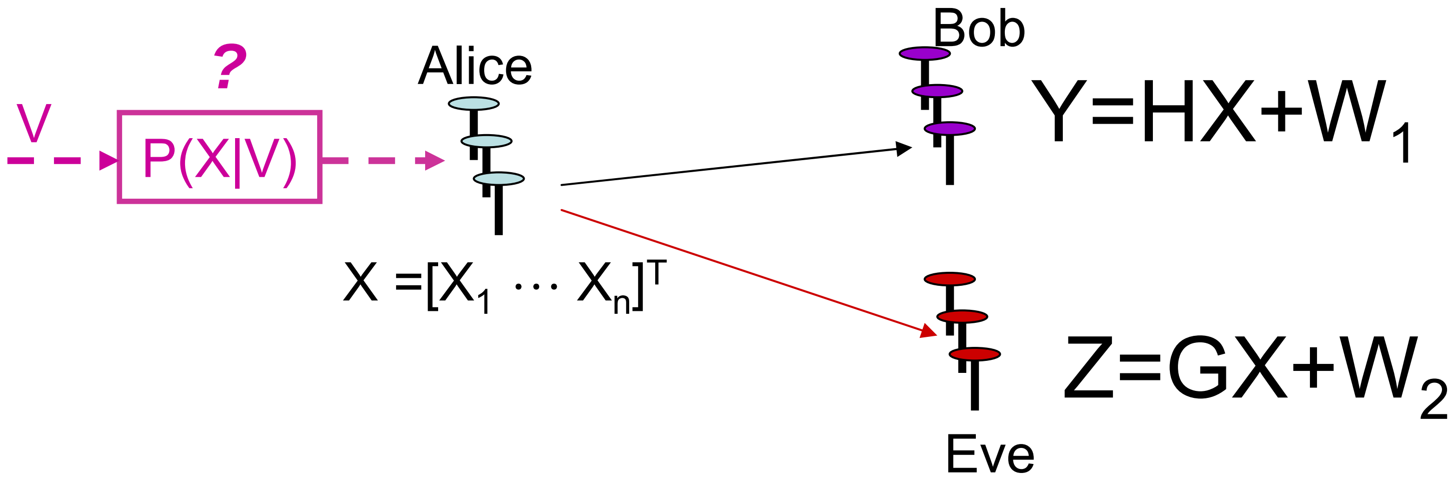
$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{W}_1$$

$$\mathbf{Z} = \mathbf{G}\mathbf{X} + \mathbf{W}_2$$

Multi-antenna system provides gains in both communication rate and error performance. Can multiple antennas facilitate secret communication?

*What is the secrecy capacity for this system?*

# Why is the Problem Hard?



?

V

P(X|V)

Alice

$X = [X_1 \cdots X_n]^T$

Bob

$Y = HX + W_1$

$Z = GX + W_2$

Eve

Capacity $C_{\text{sec}} = \max_{V \to X \to YZ} I(V;Y) - I(V;Z)$

Issues:

Preprocessing V→X ?

Optimal Input V ?

More capable condition is not satisfied!

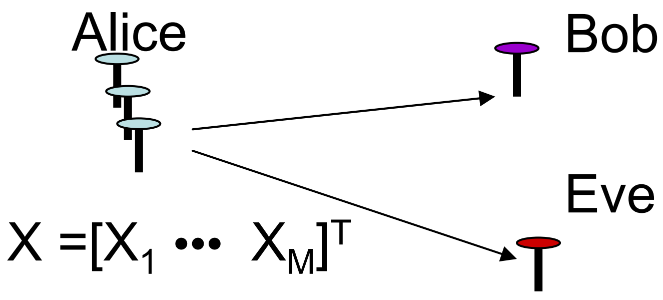
# Simplification: Achievable Secrecy Rate

- Take V=X to obtain a secrecy rate lower bound
  - Achievable Rate: $R = \max_X I(X;Y) - I(X;Z)$
- Assume H & G are known to all parties
- How to maximize the rate over the distribution of X?
  - Gaussian input characterized by covariance matrix Q

$$\begin{array}{ll} \max & \log\det(I_r + HQH^\dagger) - \log\det(I_r + GQG^\dagger) \\ \text{s.t.} & \text{tr}(Q) \le P, \;\; Q \succeq 0, \; Q = Q^\dagger, \end{array}$$

Difference of concave functions ☹

# Gaussian MISO:
## M TX antennas, 1 RX antenna/user



$$Y = h^T X + W_1 \qquad h = [h_1 \cdots h_M]^T$$

$$Z = g^T X + W_2 \qquad g = [g_1 \cdots g_M]^T$$

Now the outputs are scalars!

Coordinate rotation can simplify the expressions without changing the system properties

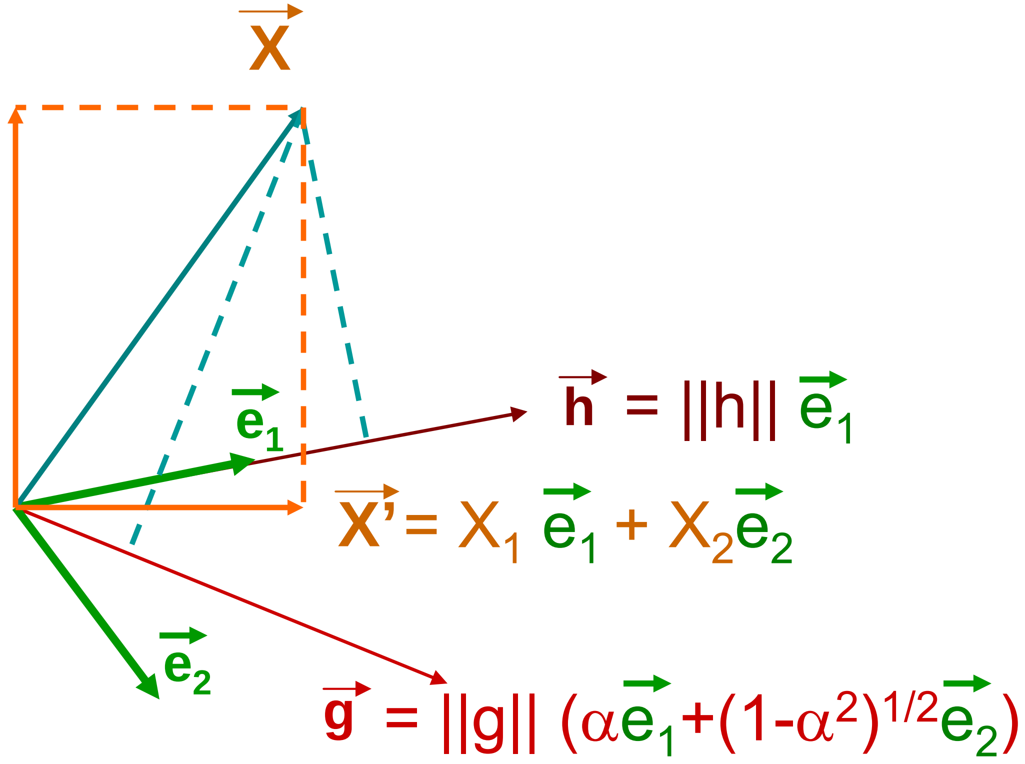
# Coordinate Transform

$Y = h^T X + W_1$

$Z = g^T X + W_2$

Useless to put power in the space orthogonal to h & g

$$\alpha = \frac{g^T h}{\| g \| \cdot \| h \|}$$

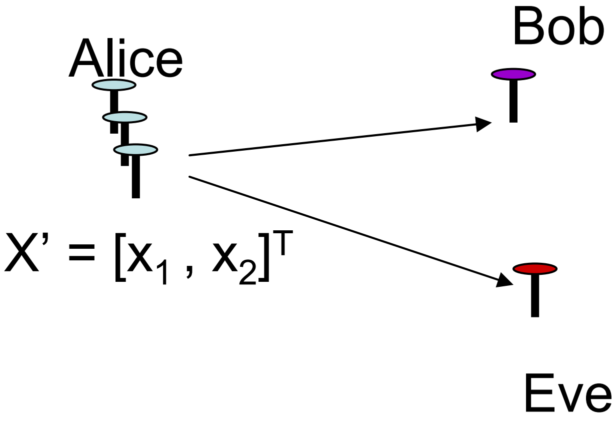


$\vec{h} = \|h\| \, \vec{e}_1$

$\vec{X}' = X_1 \, \vec{e}_1 + X_2 \vec{e}_2$

$\vec{g} = \|g\| \, (\alpha \vec{e}_1 + (1-\alpha^2)^{1/2} \vec{e}_2)$

# Jamming View of the MISO Problem



$$Y = \|h\| X_1 + W_1$$

$$Z = \|g\| \alpha X_1 + \|g\| \sqrt{1-\alpha^2} X_2 + W_2$$

- $X_1$ is signal for Bob, with power $P_1$
- $X_2$ is jamming signal to annoy Eve, with power $P_2$
- Similar to correlated jamming [Medard 97], [Shafiee+Ulukus 05]
  - except $X_1$ and $X_2$ are designed and transmitted by TX,
  - $P_1 + P_2 \leq P$
- **Questions:**
  - **How to signal?**
  - **How to allocate power between $X_1$ and $X_2$?**

# Gaussian MISO with Gaussian Input

$$Y = \| h \| X_1 + W_1$$

$$Z = \| g \| \alpha X_1 + \| g \| \sqrt{1-\alpha^2} X_2 + W_2$$

- $X_2$ should be linear to $X_1$ for cancellation at Eve
- When $P_1$ is small, we should zero force Eve
  - Choose $$\boxed{X_2 = \frac{-\alpha}{\sqrt{1-\alpha^2}} X_1}$$
  - Eve receives $Z = W_2 \Rightarrow$ pure noise
  - $R_{ZF} = I(X; Y) = \log(1+\|h\|^2 P_1)$
- For zero-forcing to be possible, $P_1 \cdot P^* = (1- \alpha^2)P$

# Gaussian MISO with Gaussian Input

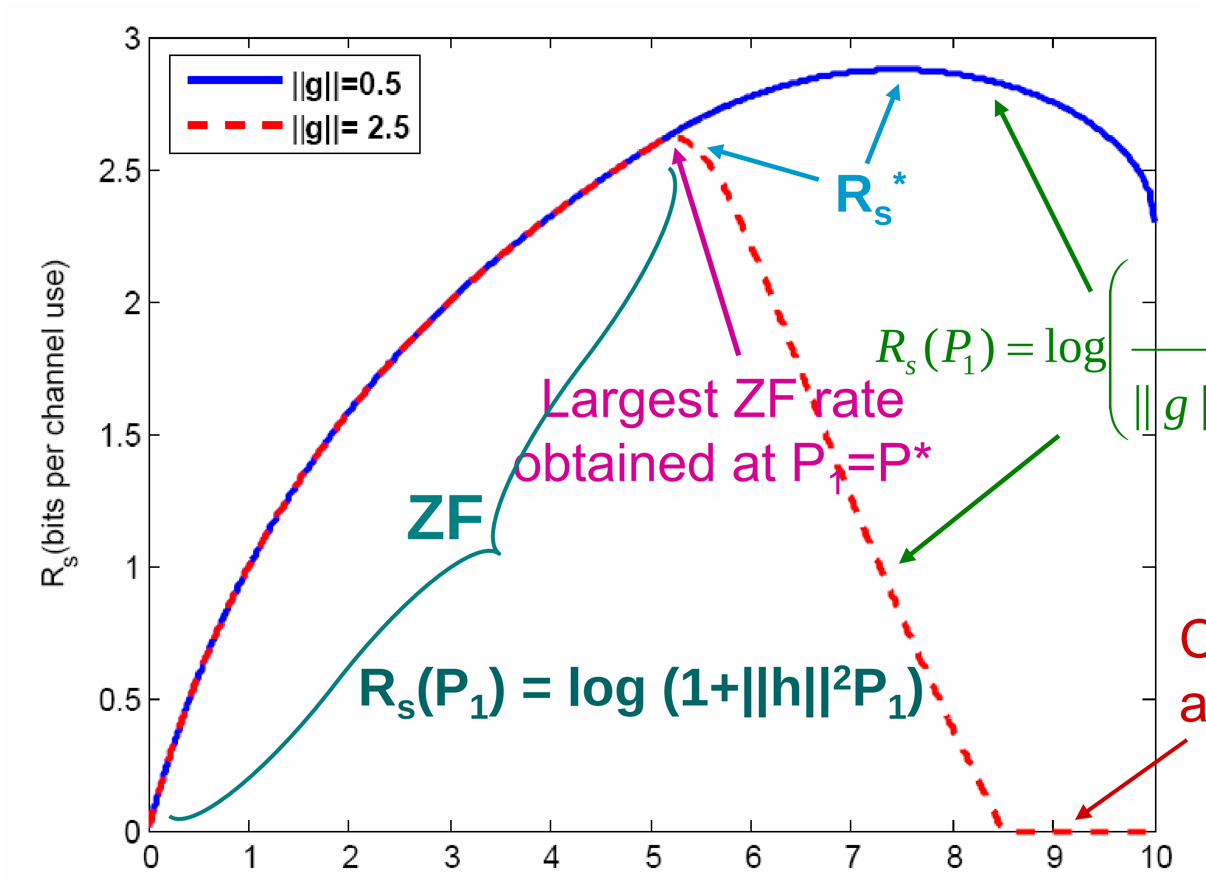
$$Y = \| h \| X_1 + W_1$$

$$Z = \| g \| \alpha X_1 + \| g \| \sqrt{1-\alpha^2} X_2 + W_2$$

- Largest rate obtained by zero-forcing:
  - $R_{ZF}^{*} = \log(1 + \|h\|^2 P^{*})$
- But this is not optimal!
  - Very conservative, same rate regardless of Eve's channel gain
- For $P_1 > P^*$, choose $X_2 = -c\alpha X_1$ and $P_2 = P - P_1$ to cancel $X_1$ as much as possible
  - $Rs(P_1) = I(X;Y) - I(X;Z) = \log\left( \frac{\| h \|^2 P_1 + 1}{\| g \|^2 \left( \sqrt{\alpha^2 P_1} - \sqrt{(1-\alpha^2)(P-P_1)} \right)^2 + 1} \right)$

# Secrecy Rate $R_S(P_1)$

## $\alpha = 0.7$, $P = 10$, $||\boldsymbol{h}|| = 1$.



$R_s^*$

Largest ZF rate obtained at $P_1$=P*

ZF

$R_s(P_1)$ = log $(1+||h||^2P_1)$

$$R_s(P_1) = \log\left(\frac{\|h\|^2\, P_1 + 1}{\|g\|^2\left(\sqrt{\alpha^2 P_1} - \sqrt{(1-\alpha^2)(P-P_1)}\right)^2 + 1}\right)$$

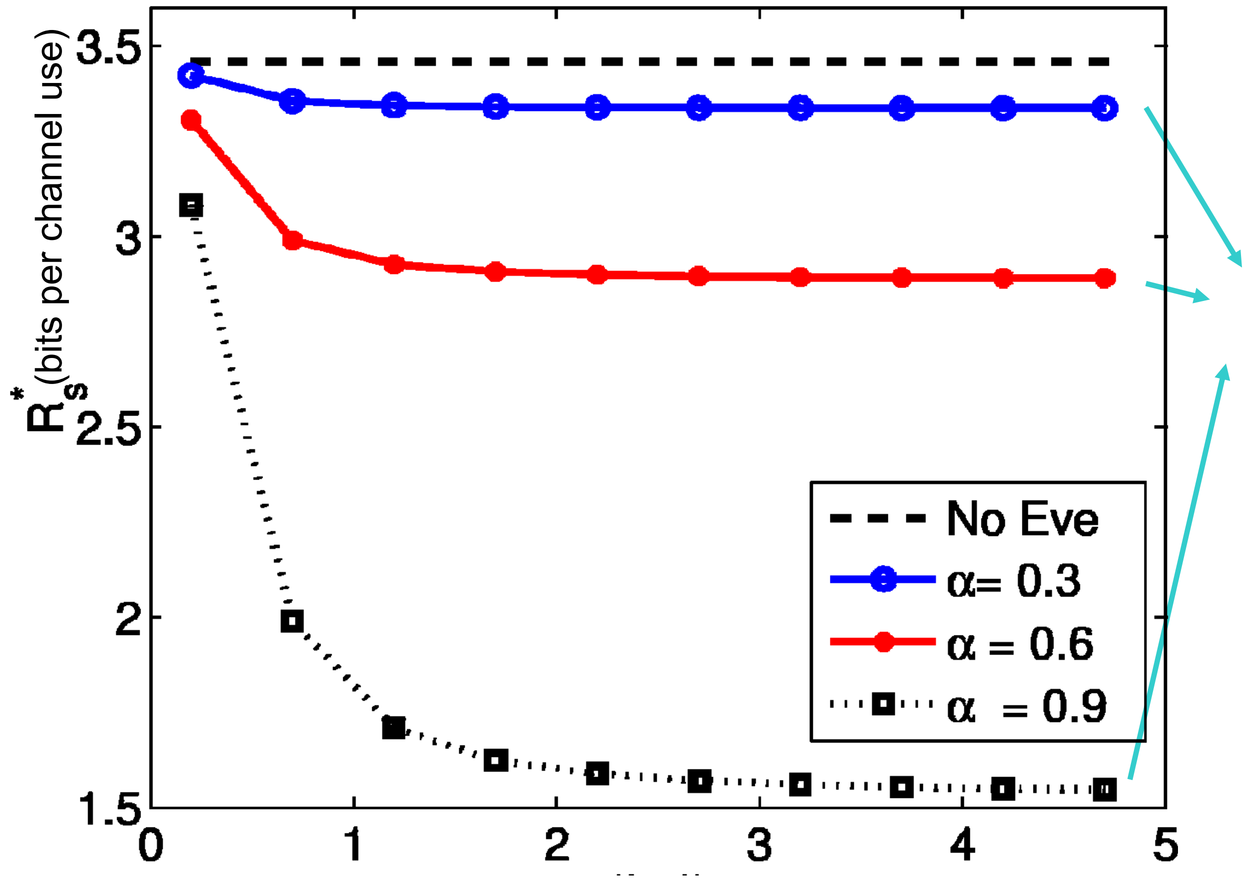
Cancellation is not enough and Eve has a better channel

$$R_s^* = \max_{P^* \le P_1 \le P} \log\left(\frac{\|h\|^2\, P_1 + 1}{\|g\|^2\left(\sqrt{\alpha^2 P_1} - \sqrt{(1-\alpha^2)(P-P_1)}\right)^2 + 1}\right)$$

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

# Optimal Secrecy Rate $R_s^*$

P =10, ||h|| = 1



Eavesdropper Link Gain ||g||

**Converge to ZF rate**

$R_{ZF}$=log $(1+||h||^2P^*)$

$P^* = (1-\alpha^2)P$

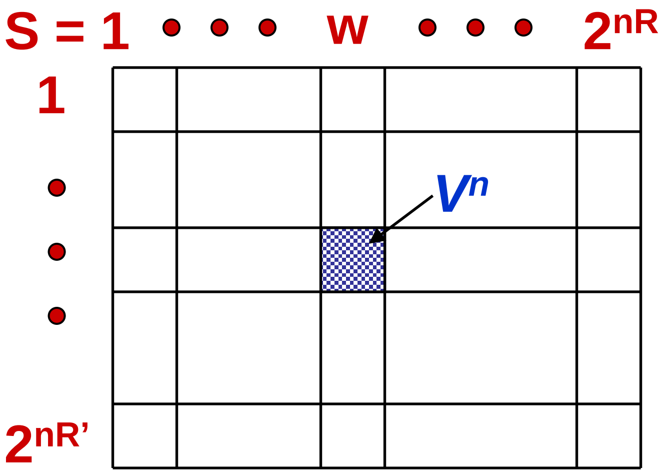
# Conclusions

- The extra dimensions provided by multi-antenna system can enhance the secrecy rate
- Derived the secrecy rate for MISO Gaussian broadcast channel
  - Coordinate transform
  - Partial cancellation at Eve
  - This rate was shown to be the capacity recently (Khisti et al ISIT2007)

# Thanks! Any Questions?

# Coding Procedure

- Stochastic encoding, joint typical decoding (Csiszar&Korner 78)



$$X^n = f(V^n)$$

To ensure correct decoding at Bob

(Bob finds only one typical sequence in the whole table.)

$$R + R' < I(V;Y)$$

To ensure full equivocation at Eve

(Eve finds at least one typical sequence in every column.)

$$R' > I(V;Z)$$

$$\Rightarrow \quad R < I(V;Y) - I(V;Z)$$