Multiple Antenna Secret Broadcast over Wireless Networks

Ruoheng Liu and H. Vincent Poor

Princeton University

IAB – May, 2007

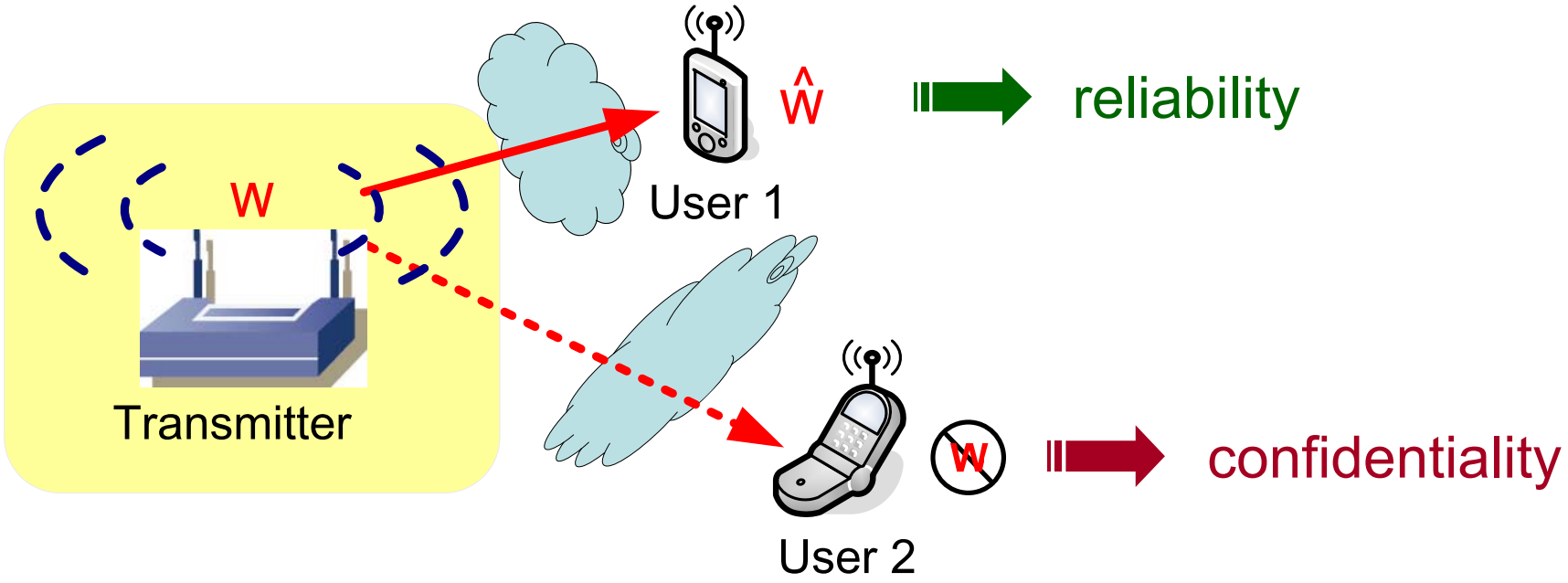
ACKNOWLEDGEMENTS

Ivana Marvic, Zang Li, Predrag Spasojevic, Roy Yates, and Wade Trappe

Outline of the Talk

- motivation
- physical-layer secret system
- secret broadcast over wireless networks

Reliable and Secret Communication over Wireless Network



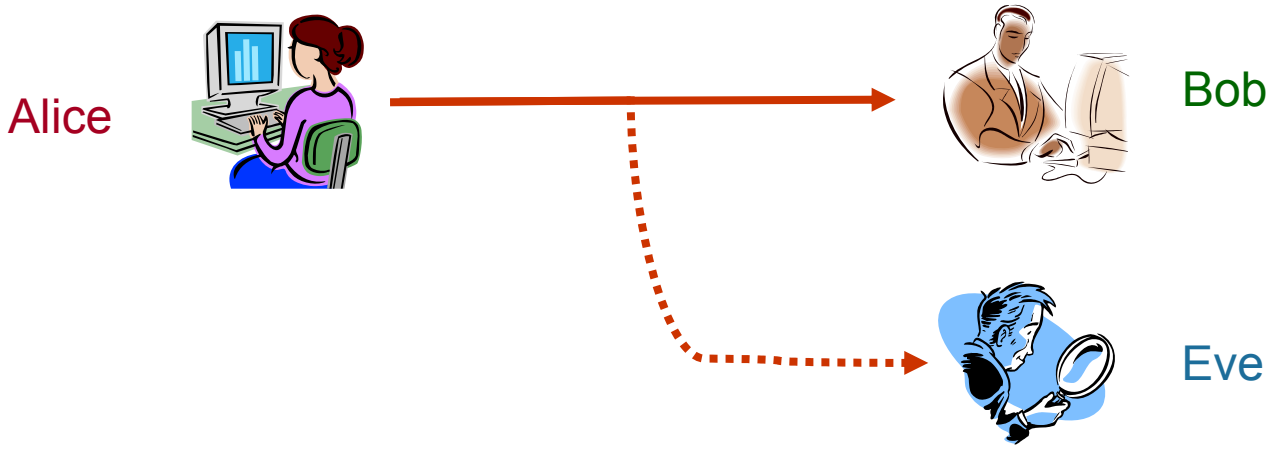
confidential message W

- can be successfully decoded by the desired receiver (user 1)
- cannot be understood by anyone else (e.g. user 2)

Secret Communication

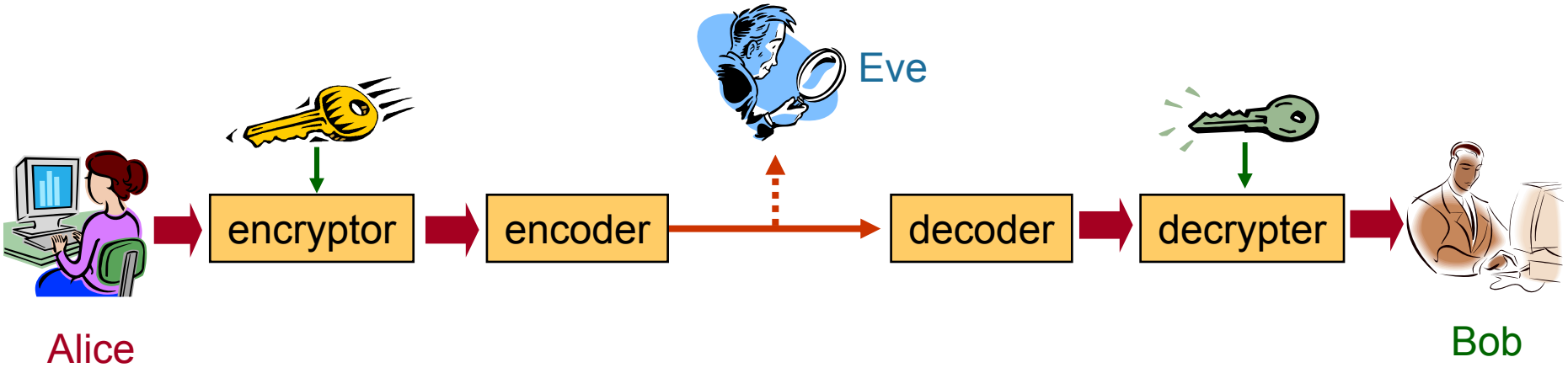
crypto-system
(secret key)

information-theoretic security
(physical-layer)



- Alice sends a message to Bob
- Eve accesses the channel and eavesdrops the information

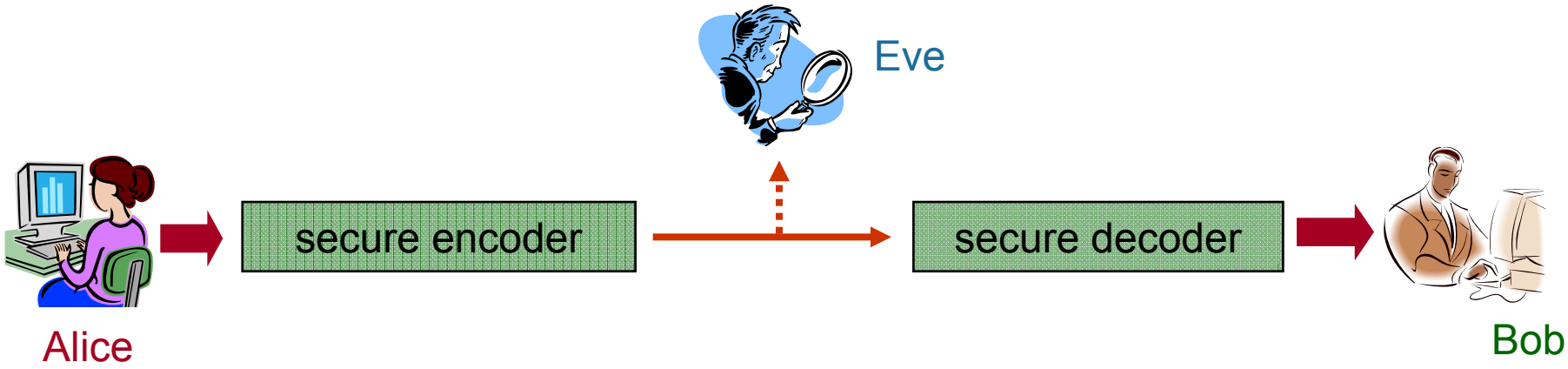
Traditional Crypto-System



disadvantage:

- it is very **difficult** to distribute **initial** key in a large wireless network
- Eve becomes smarter with time and lifetime of secret key is **shorter**

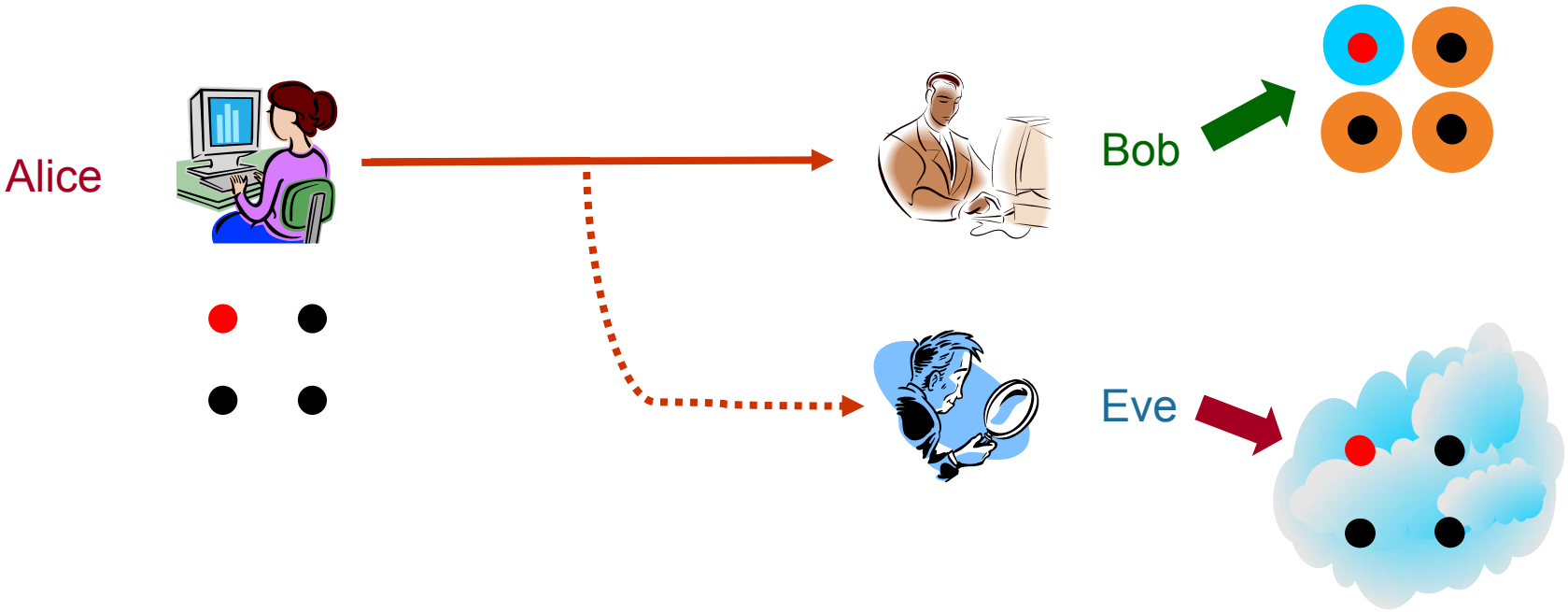
Physical-Layer Secret System



advantage:

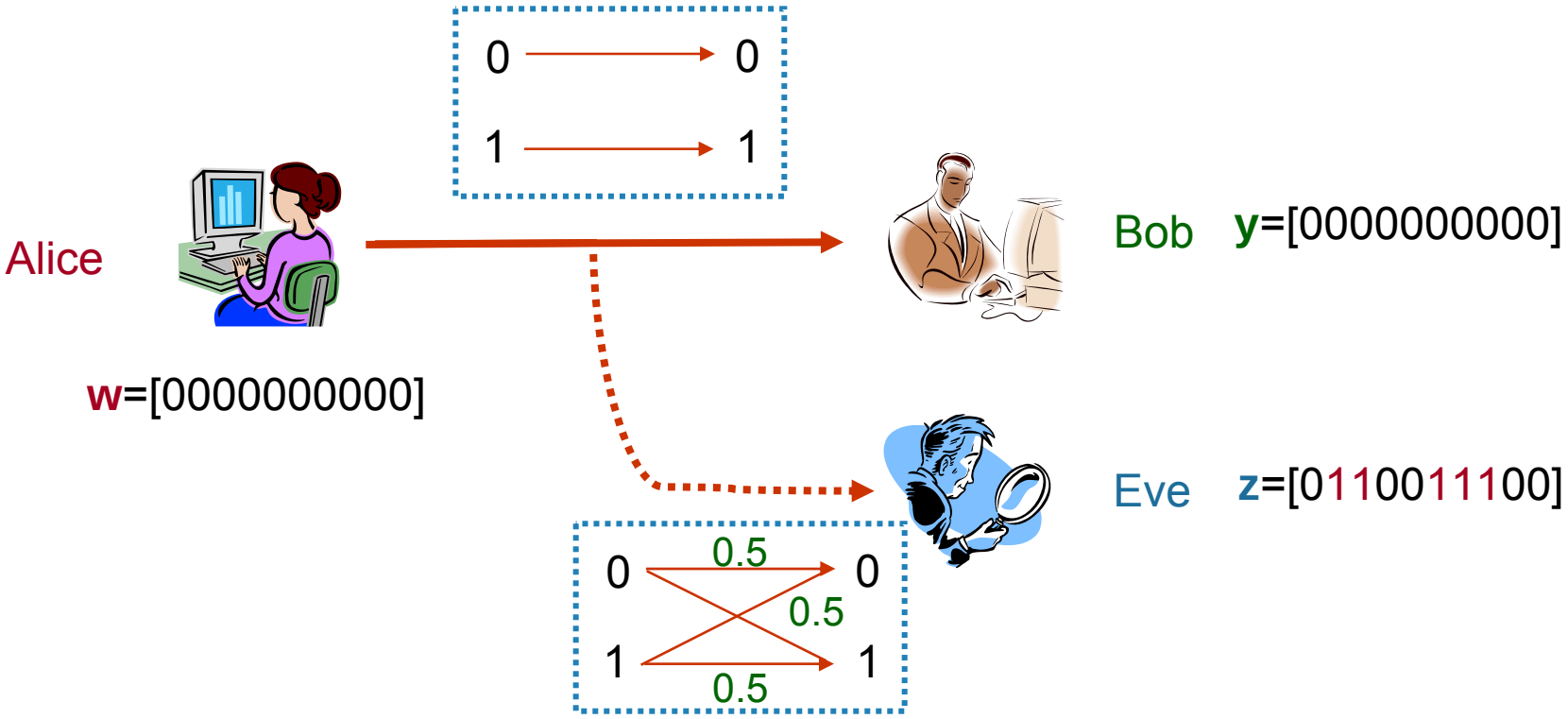
- secret communication can be achieved **without** a key
- **perfect** communication secrecy can be ensured

How Physical-Layer Secret System Works



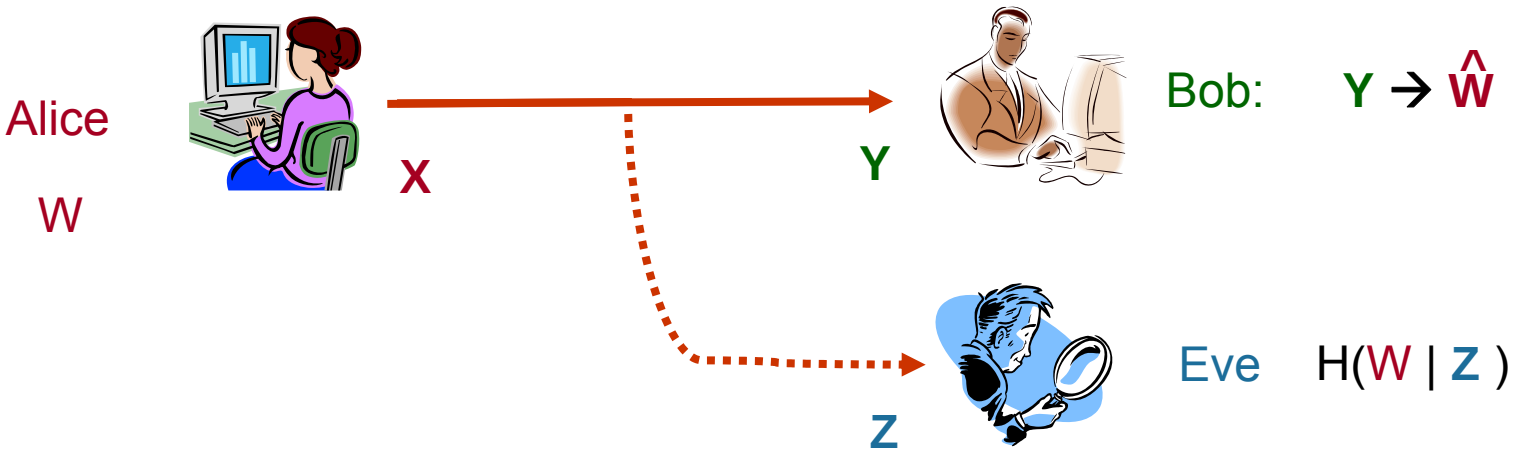
Bob has a **“better”** channel than Eve

How Physical-Layer Secret System Works



- Bob can get the message (**y**=**w**)
- Eve is kept ignorant with respect to the message (**w** and **z** are independent)

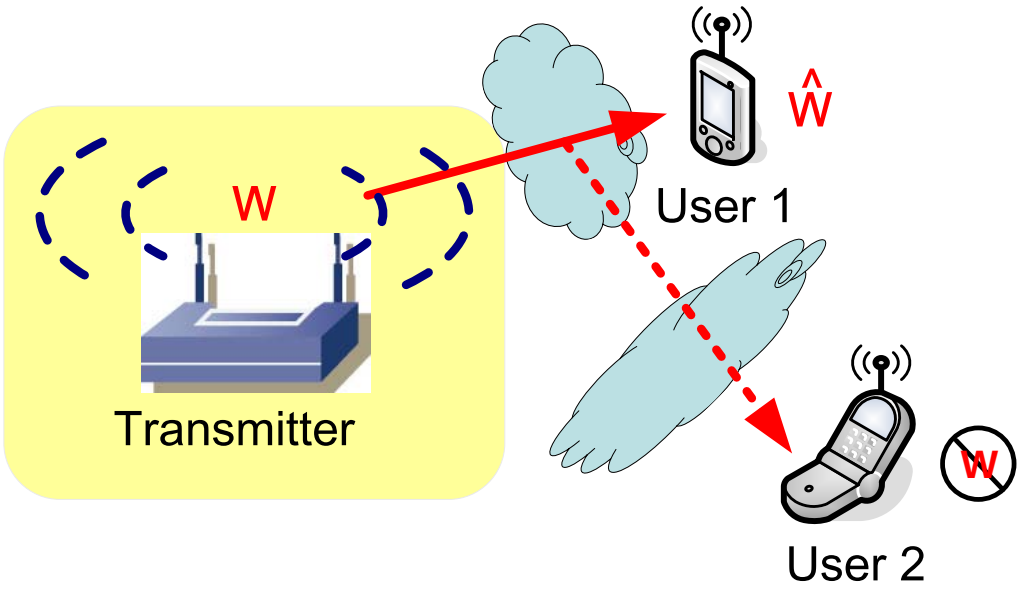
How to Measure Secrecy Level



physical-layer secret system can achieve: both reliability and confidentiality

- reliability is evaluated in terms of error probability
- secrecy level is measured by the equivocation rate: $H(W \mid Z)/n$
- **perfect** secrecy: $H(W \mid Z)/n \rightarrow H(W)/n$

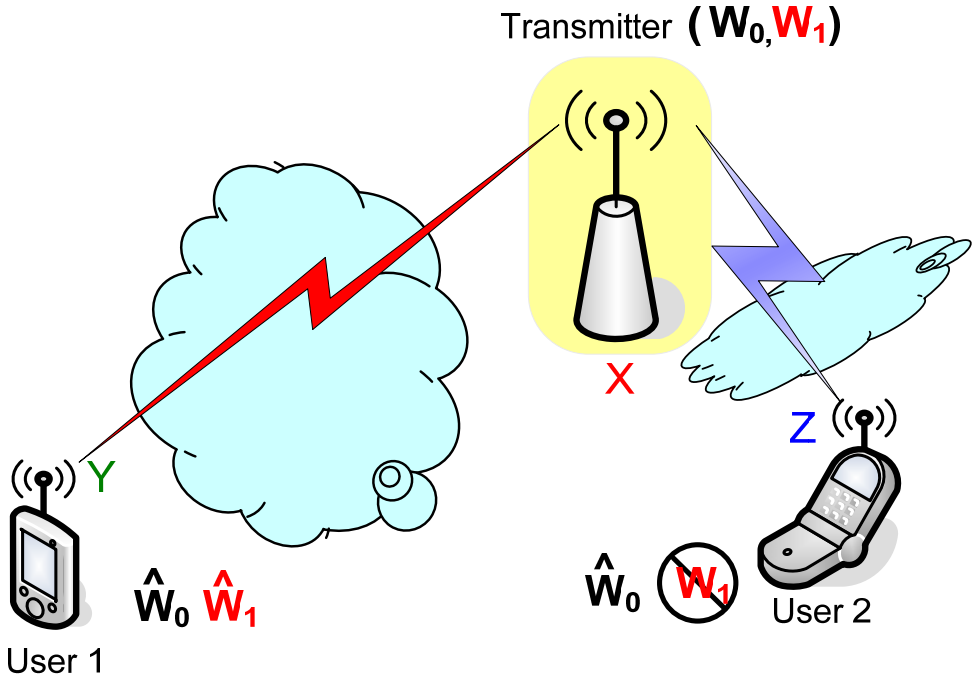
Wire-Tap Channel



[Wyner, 1975]

- user 1 is a desired receiver
- user 2 is an *eavesdropper*
- confidential message W to User 1
- degraded broadcast channel

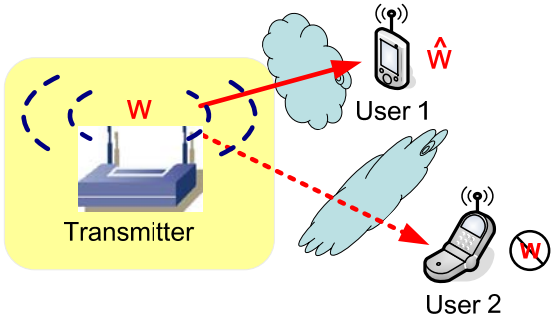
Broadcast Channel with Single CM Set



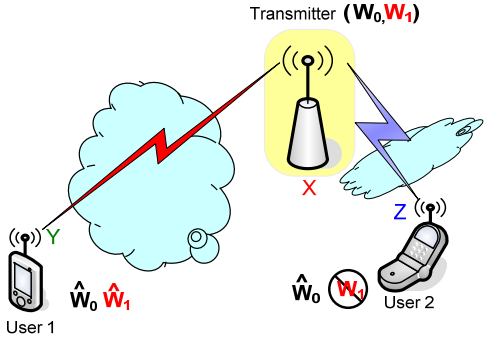
[Csiszár & Körner, 1978]

- W_1 is a confidential message to user 1
- W_0 is a common message to both users
- non-degraded broadcast channel

Communication of Confidential Messages



[Wyner, 1975]

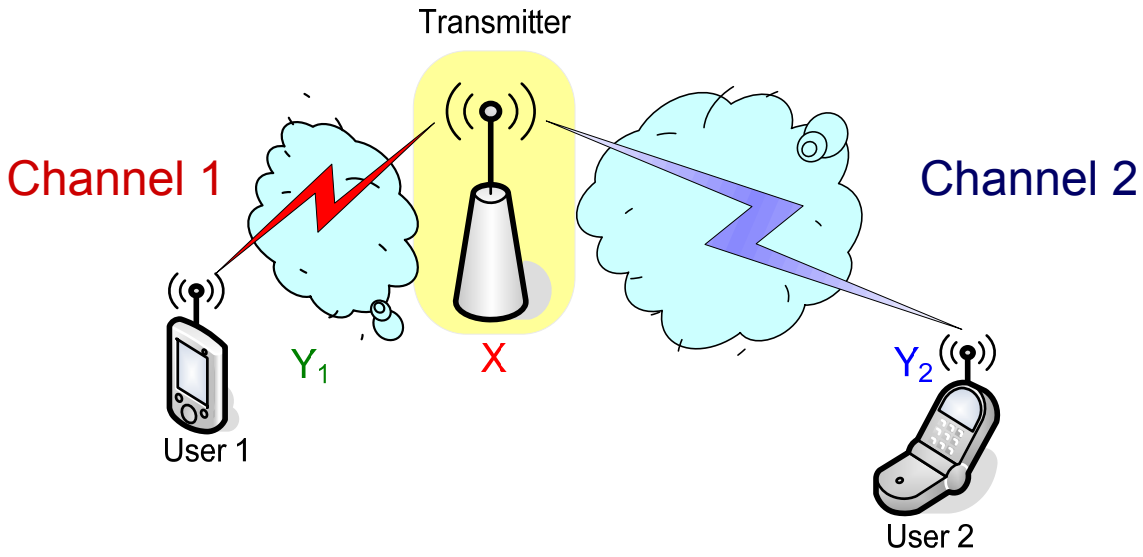


[Csiszár & Körner, 1978]

Can we send confidential messages to both users instantaneously?

?

Single Antenna Gaussian Broadcast Channel (GBC)

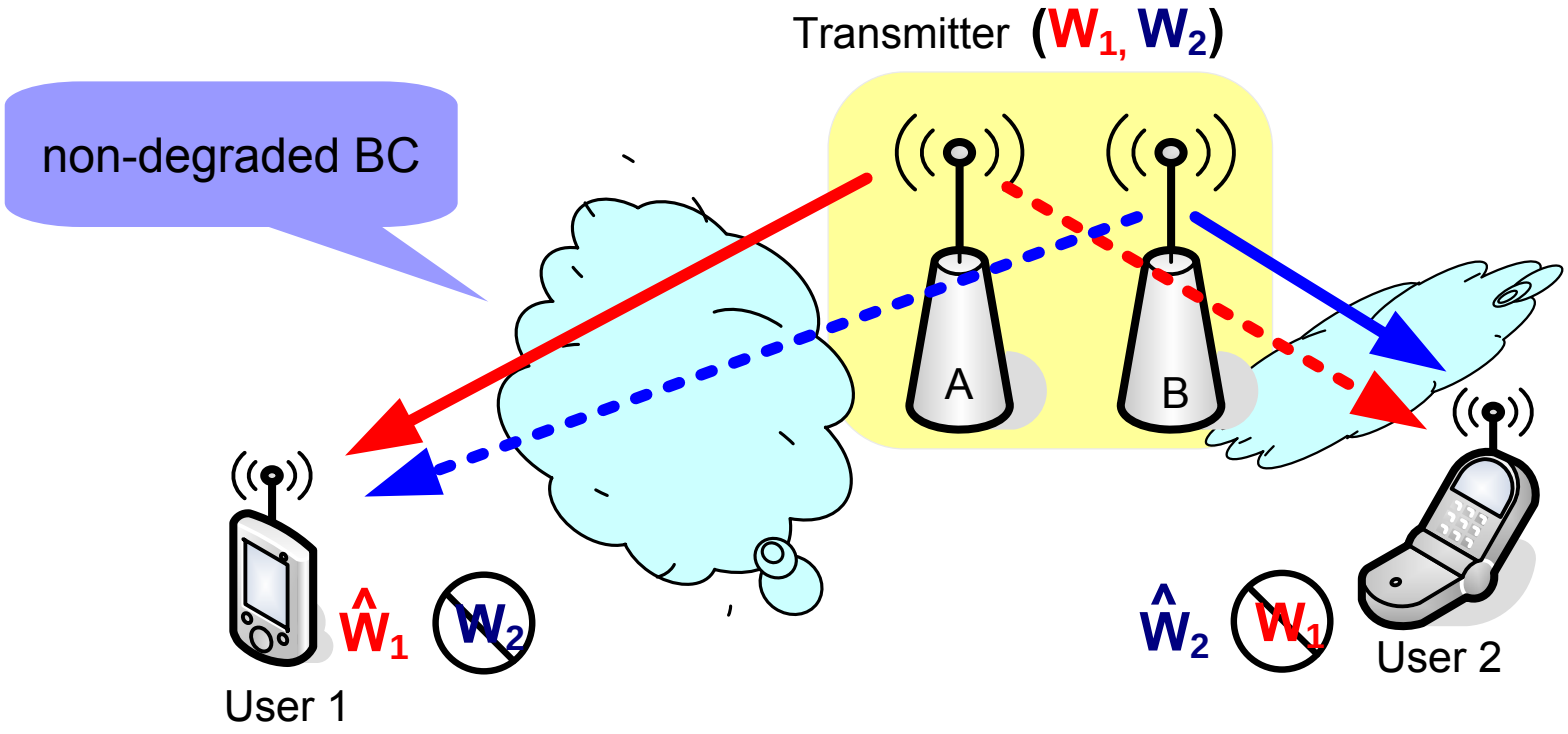


- Channel 1 is "better" than Channel 2 (degraded BC)
- this case reduces to Gaussian wire-tap channel

$$R_1 \le \max_{p(x)} [I(X;Y_1) - I(X;Y_2)]$$

$$R_2 = 0$$

Multi-Antenna Gaussian Broadcast Channel (MGBC)

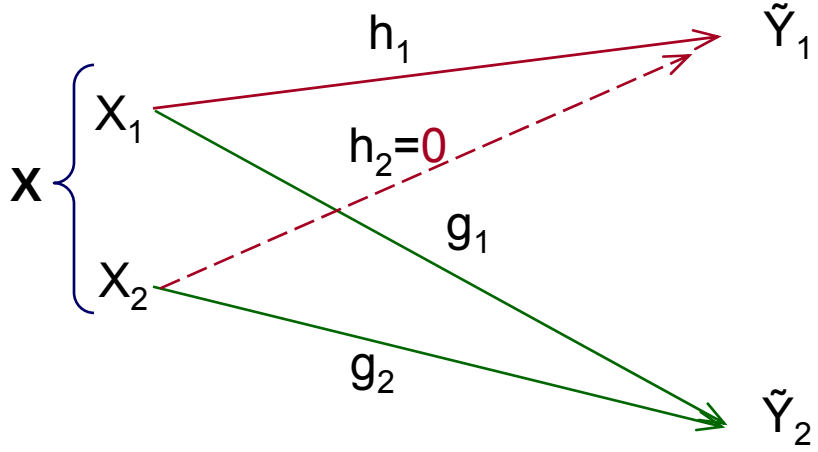


- (W_1, W_2): independent, confidential messages
- how to achieve reliable, secret communication over the MGBC-CM?
- what is the capacity region for the MGBC-CM?

A Computable Outer Bound for MGBC-CM

$$\mathcal{C}_{\mathrm{BCC}} \subseteq \bigcap_{p(\tilde{y}_1,\tilde{y}_2|\mathbf{x})} \bigcup_{p(\mathbf{x})} \left\{ \begin{array}{l} R_1 \le I(\mathbf{X};\tilde{Y}_1 \,|\, \tilde{Y}_2) \\ R_2 \le I(\mathbf{X};\tilde{Y}_2 \,|\, \tilde{Y}_1) \end{array} \right\}$$

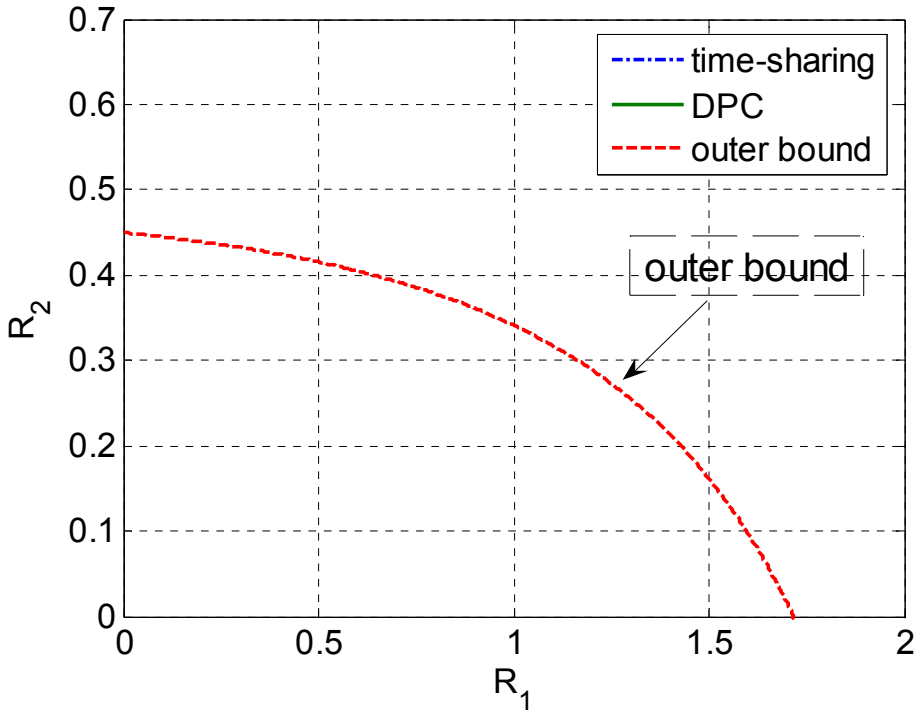
- basic ideas: decode the message in a cooperative manner
  evaluate the secrecy level in a individual manner
- for GBC, Gaussian input can optimize this outer bound
- MGBC can be transferred to an equivalent 2-dimension "Z-broadcast" channel model



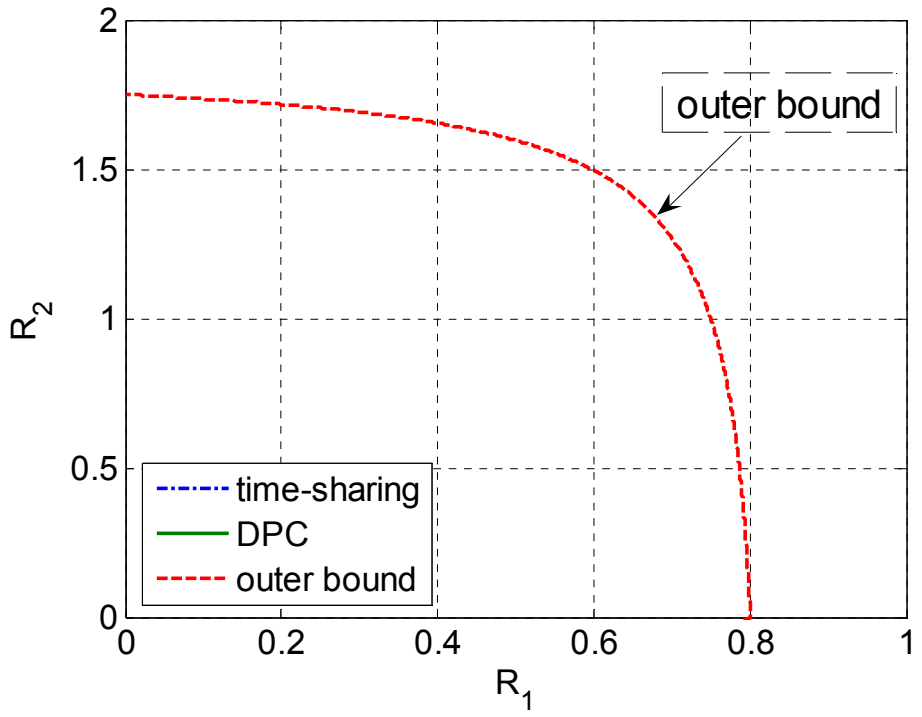
A Computable Outer Bound for MGBC-CM

$$\mathcal{C}_{\mathrm{BCC}} \subseteq \bigcap_{p(\tilde{y}_1,\tilde{y}_2|\mathbf{x})} \bigcup_{p(\mathbf{x})} \left\{ \begin{array}{l} R_1 \le I(\mathbf{X};\tilde{Y}_1 \,|\, \tilde{Y}_2) \\ R_2 \le I(\mathbf{X};\tilde{Y}_2 \,|\, \tilde{Y}_1) \end{array} \right\}$$

P=10, $\mathbf{h}=[1, 0]^T$, $\mathbf{g}=0.3\cdot[0.20, 0.98]^T$



P=10, $\mathbf{h}=[1, 0]^T$, $\mathbf{g}=2\cdot[0.90, 0.43]^T$



Transmission Strategy 1: Time Sharing

basic ideas:

- transmission period is divided into two slots of durations t_1 and t_2
- transmitter sends W_1 during time t_1 with power P_1,
- transmitter sends W_2 during time t_2 with power P_2,
- in each slot, the channel reduces to a Gaussian MISO wiretap channel

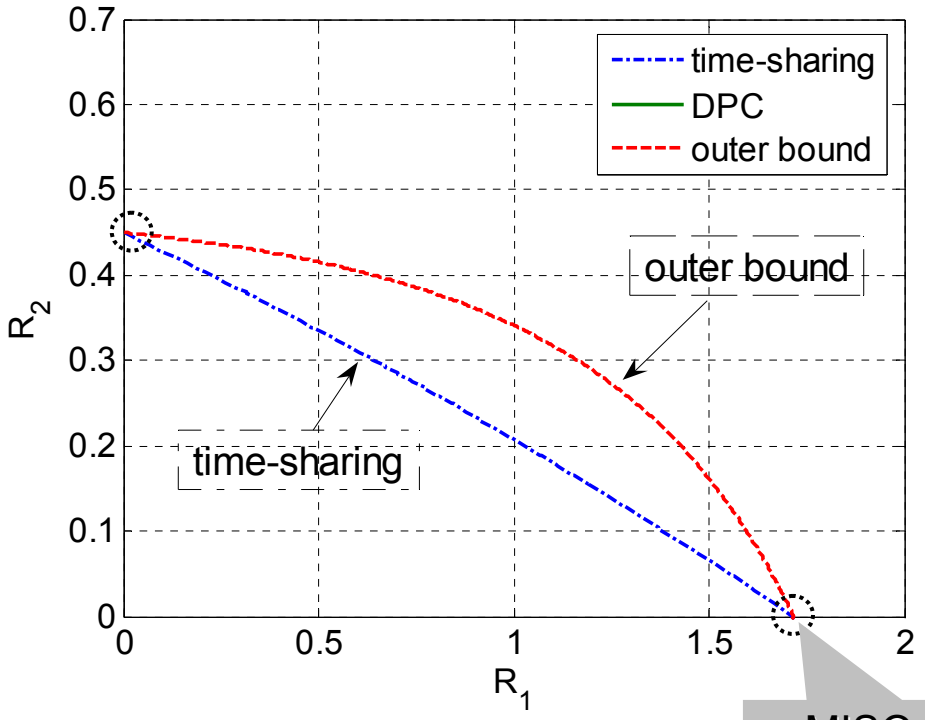
Transmission Strategy 1: Time Sharing

achievable region:

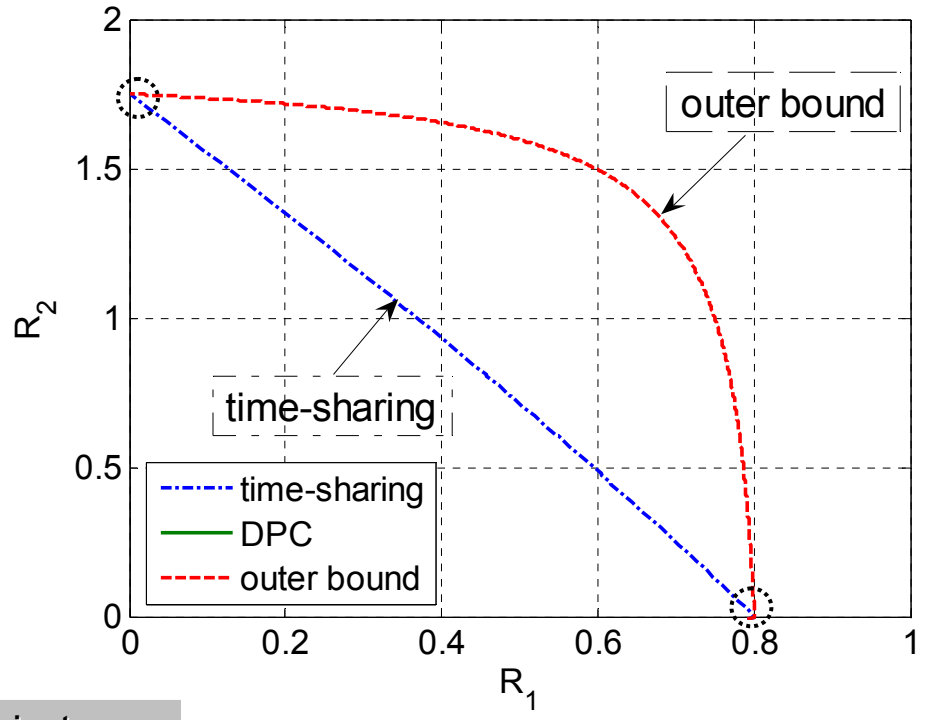
(R1, R2): $\{ t_1 C_{s,MISO}(P_1),\ t_2 C_{s,MISO}(P_2) \}$ for all $t_1P_1+t_2P_2=P$ $t_1+t_2=1$

$C_{s,MISO}$ is the secrecy capacity of Gaussian MISO wiretap channel [Li, *et. al.*, CISS 07]

P=10, $\mathbf{h}=[1, 0]^T$, $\mathbf{g}=0.3\cdot[0.20, 0.98]^T$



P=10, $\mathbf{h}=[1, 0]^T$, $\mathbf{g}=2\cdot[0.90, 0.43]^T$

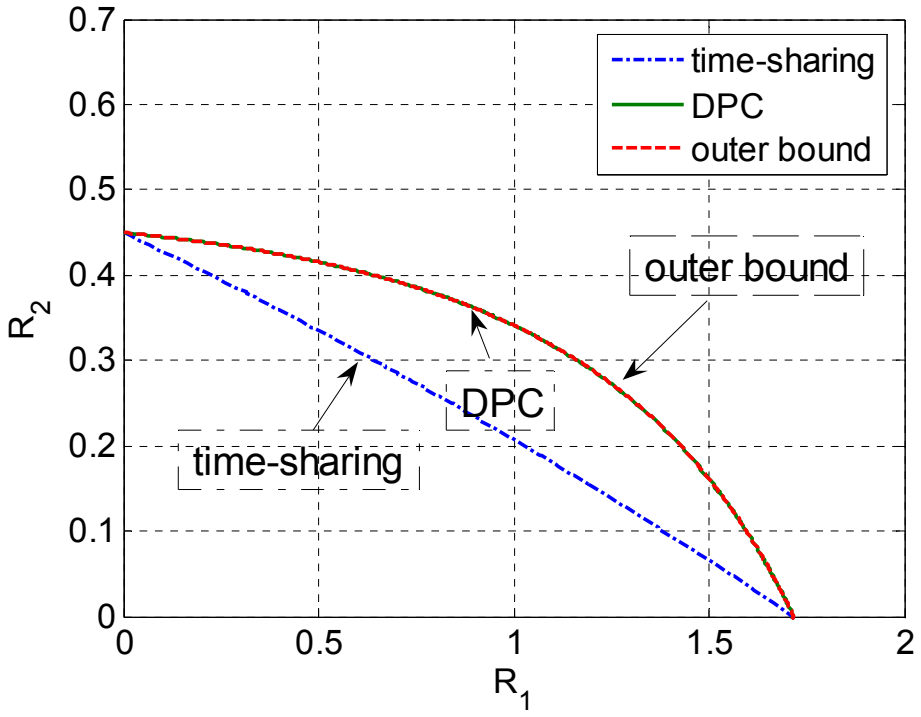


MISO wiretap

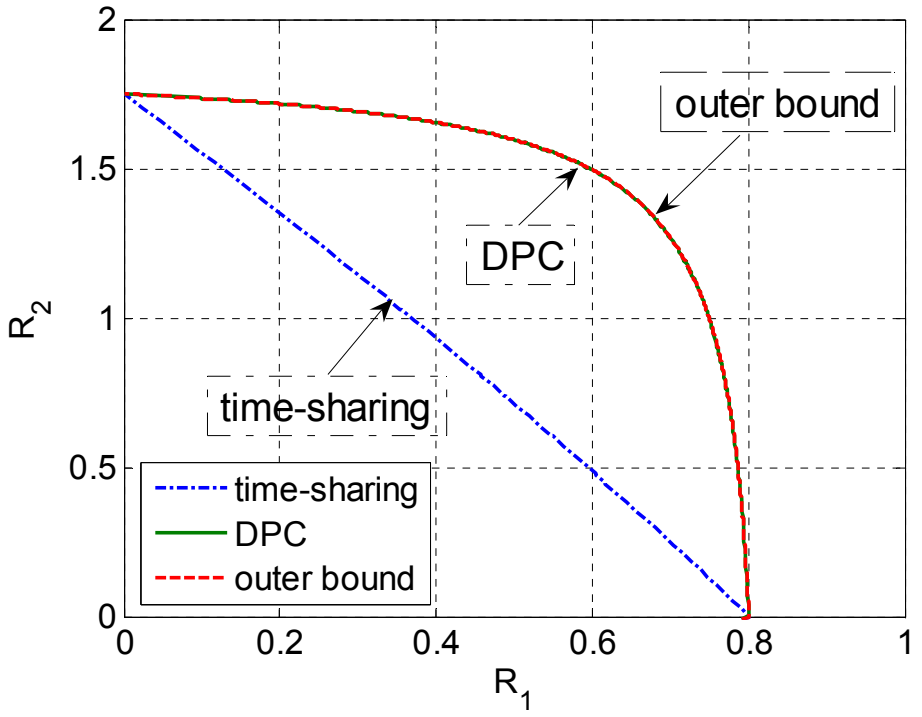
Transmission Strategy 2: Secret Dirty Paper Coding (DPC)

$$\mathcal{R}^{[DPC]} = \bigcup_{\mathrm{tr}(K_U+K_V)\le P} \left\{ \begin{array}{l} R_1 \le \log_2 \dfrac{1+\mathbf{h}^H(K_U+K_V)\mathbf{h}}{1+\mathbf{g}^H K_V \mathbf{g}} - \log_2 \dfrac{1+\mathbf{g}^H(K_U+K_V)\mathbf{g}}{1+\mathbf{h}^H K_V \mathbf{h}} \\ R_2 \le \log_2 \dfrac{1+\mathbf{g}^H K_V \mathbf{g}}{1+\mathbf{h}^H K_V \mathbf{h}} \end{array} \right\}$$

P=10, $\mathbf{h}=[1, 0]^T$, $\mathbf{g}=0.3\cdot[0.20, 0.98]^T$

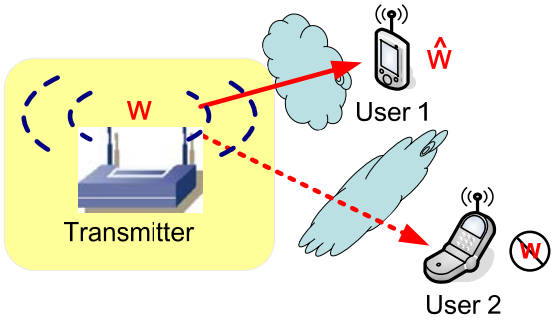


P=10, $\mathbf{h}=[1, 0]^T$, $\mathbf{g}=2\cdot[0.90, 0.43]^T$

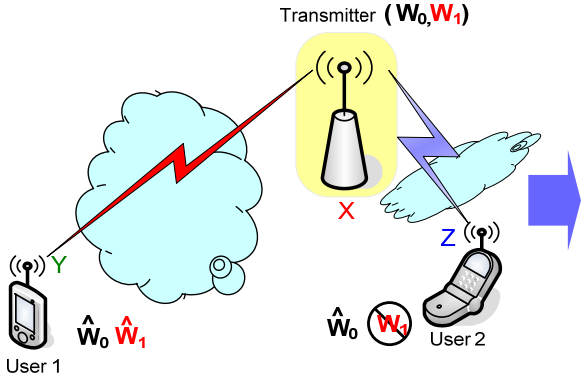


Communication of Confidential Messages

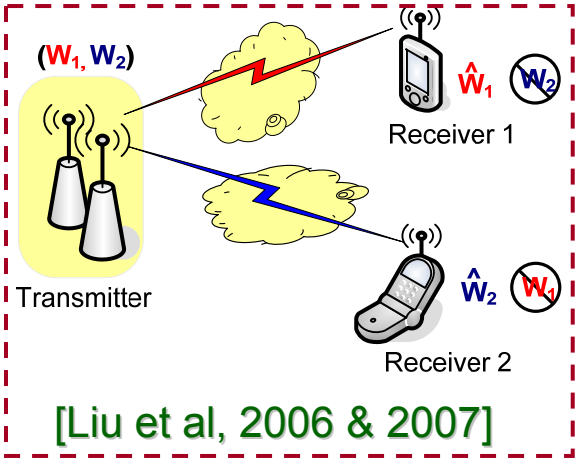
downlink scenario



[Wyner, 1975]



[Csiszár & Körner, 1978]



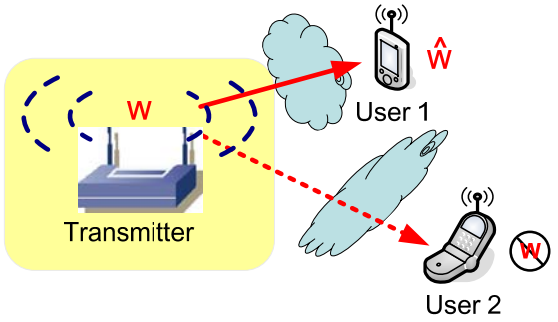
[Liu et al, 2006 & 2007]

uplink scenario

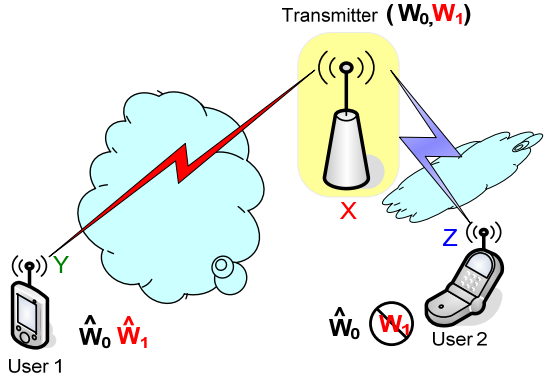
?

Communication of Confidential Messages

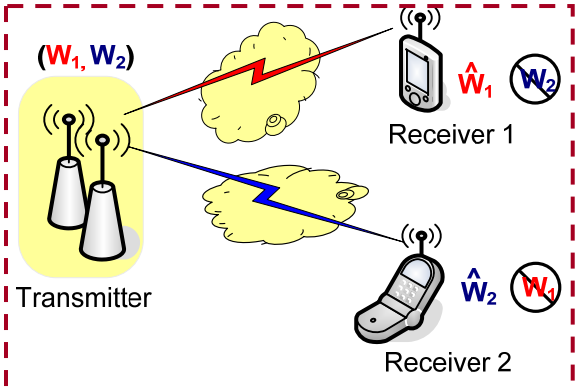
downlink scenario



[Wyner, 1975]

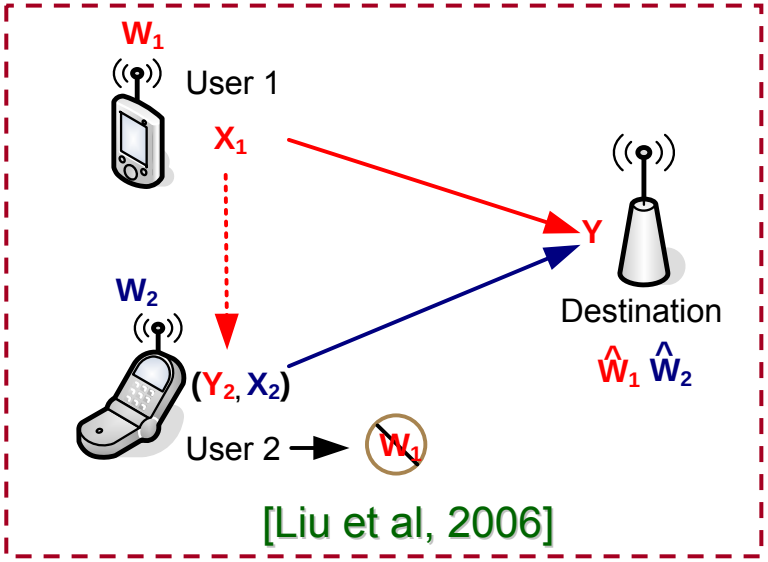


[Csiszár & Körner, 1978]



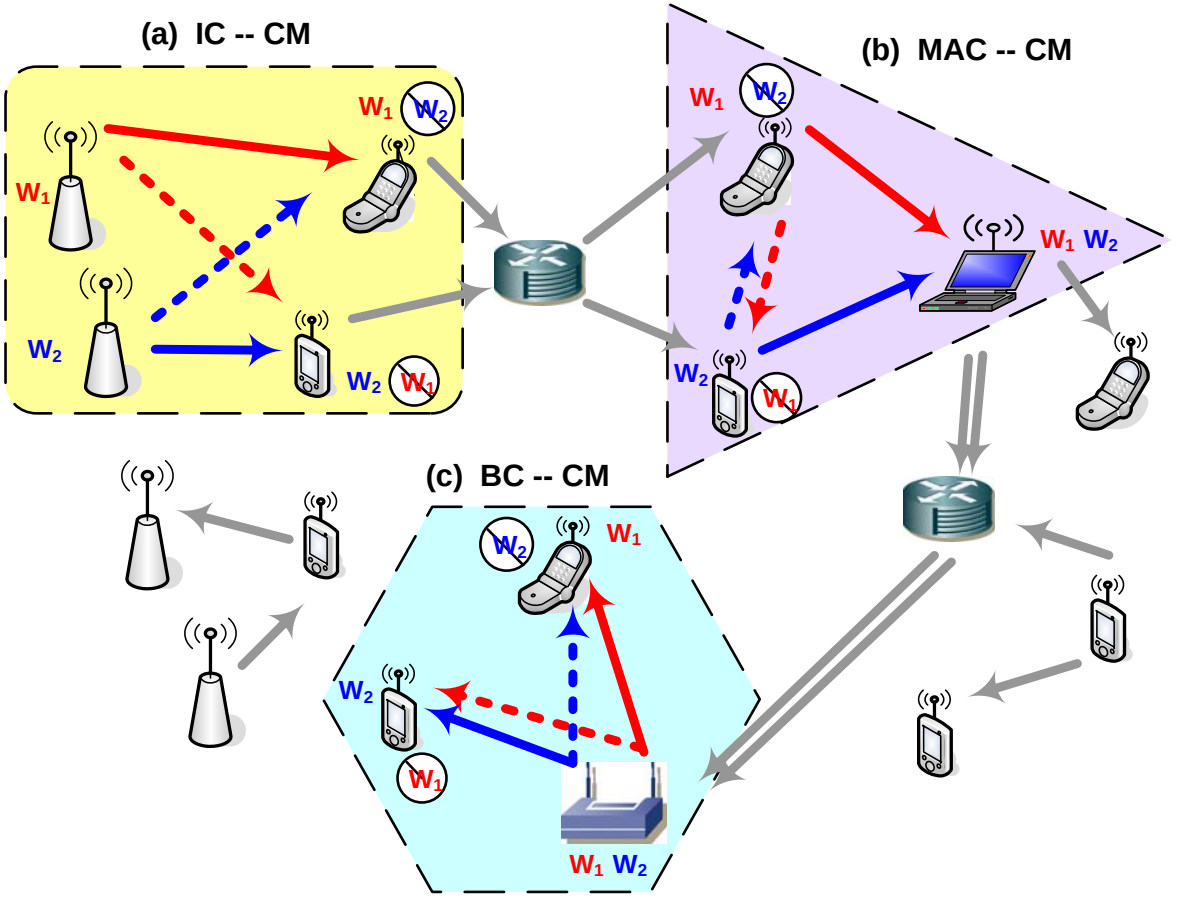
[Liu et al, 2006 & 2007]

uplink scenario



[Liu et al, 2006]

Challenge and Opportunity



(a) Interference Channel with Confidential Messages (IC-CM)

(b) Multiple Access Channel with Confidential Messages (MAC-CM)

(c) Broadcast Channel with Confidential Messages (BC-CM)

A Computable Outer Bound for MGBC-CM

$$\mathcal{C}_{\mathrm{BCC}} \subseteq \bigcap_{p(\tilde{y}_1,\tilde{y}_2|\mathbf{x})} \bigcup_{p(\mathbf{x})} \left\{ \begin{array}{l} R_1 \le I(\mathbf{X};\tilde{Y}_1 \,|\, \tilde{Y}_2) \\ R_2 \le I(\mathbf{X};\tilde{Y}_2 \,|\, \tilde{Y}_1) \end{array} \right\}$$

- basic ideas: decode the message in a cooperative manner
  evaluate the secrecy level in a individual manner
- for GBC, Gaussian input can optimize this outer bound
- MGBC can be transferred to an equivalent 2-dimension "Z-broadcast" channel model