情報セキュリティ研究センター
Research Center for Information Security
Joint Work with :
B. Hassibi, **CalTech**
F. Oggier

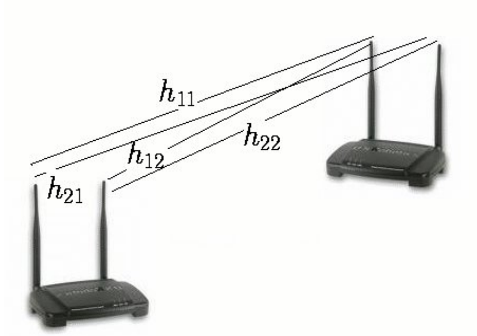
Information theoretic security for multiple antenna communication

Channel model:

We consider a MIMO (multiple input multiple output) channel

$$Y = H X + W, \quad H, W \text{ complex Gaussian.}$$

Alice sends a message to Bob using a MIMO channel, while Eve tries to eavesdrop. We thus have a MIMO broadcast channel.



Security scenario:

We are interested in information theoretic confidentiality: the amount of information an eavesdropper can get is measured by mutual information

$$I (W ; Z) .$$

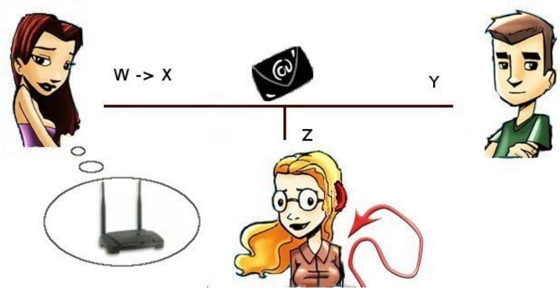
There is no computational assumption. This is called a wiretap channel (introduced by Wyner in 1975 for Discrete Memoryless Channels (DMC)).

Secrecy capacity:

We are interested in the perfect secrecy capacity, that is, the maximum rate at which Alice can communicate with Bob ensuring Eve gets a negligible amount of information.
For DMC channels, Wyner proved that the secrecy capacity C_S is given by

$$C_S=C_B-C_E$$

where C_B and C_E denote the classical channel capacity.



A short history:

- ❖ Leung and Hellman (1978) for Gaussian channels.
- ❖ El Gamal et al. (2006) for Rayleigh fading channels.
- ❖ Barros et al, Liang et al, Li et al, Shafiee et al, Wornell et al (2007)

Our result:

We proved (F.O.-Hassibi) the secrecy capacity for the MIMO wiretap channel (independent proof by Khisti-Wornell).
The proof involves computing an achievable rate and a converse.
Key ideas of the proof:

- ❖ The achievability shows that the transmitter does not transmit in the directions favourable to the eavesdropper.
- ❖ The converse is done through a Sato bound, and a closed form solution of a Ricatti equation.

Applications and future work:

- ❖ This result gives the limit of communication in the presence of an eavesdropper.
- ❖ What are the strategies to actually reach this limit?
- ❖ How to exploit the physical properties of the wireless medium?