The Role of Feedback in Two-way Secure Communication

Xiang He, Aylin Yener
xxh119@psu.edu, yener@ee.psu.edu

Industrial Day, October 2009

Wireless Communications & Networking Laboratory
WCAN@PSU

Two-way Secure Communication

•IT Secrecy: Secrecy measured with mutual information. (Shannon).

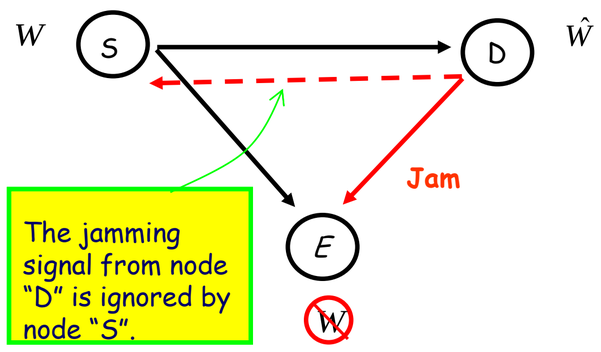
(1) The adversary is not computational power limited

(2) The adversary's observation of the crypted text contains uncertainty.

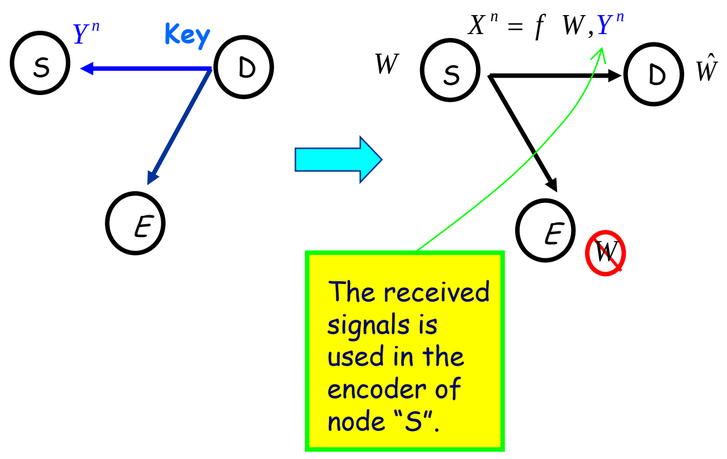
•Most practical communication system is *two-way.*

•There are *two* schemes for secure communication when the communication is two-way.

Scheme 1: Cooperative Jamming (CJ)



Scheme 2: Using a Secret Key



What is the *Optimal* Scheme?

•Two Models are considered:

(1) Two-way Wire-tap Channel

(2)Two-way Relay Channel with untrusted Relay Node

• For each Model

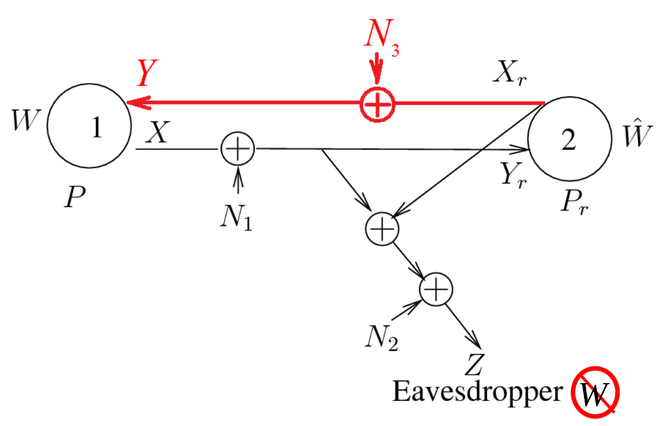
(1) *Both* schemes are useful in achieving secrecy rate

(2) Question: What is the *optimal* scheme?

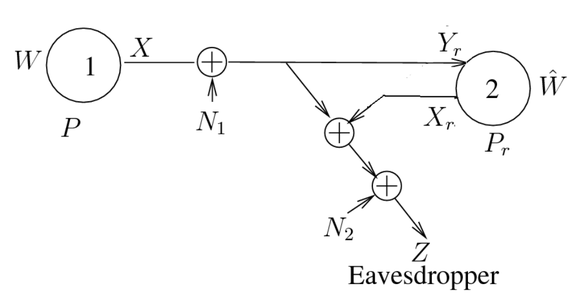
Scheme 1? Scheme 2?

Scheme 1+Scheme 2?

Model One

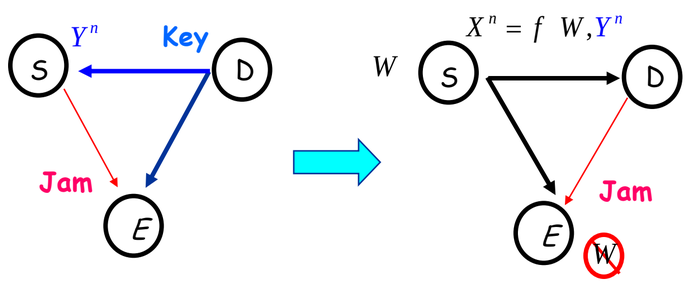


If only Scheme 1 is used:



Upper Bound for Scheme 1: $R_e \le \min\ C\ P\ , C\ P_r + \sigma_2^2$

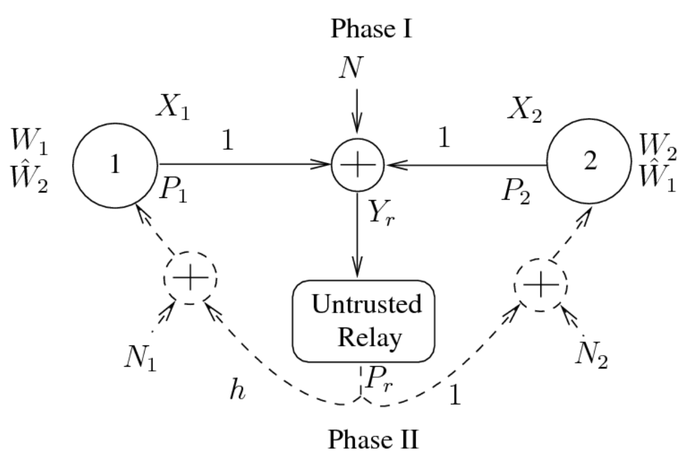
If Scheme 1+Scheme 2 is used:



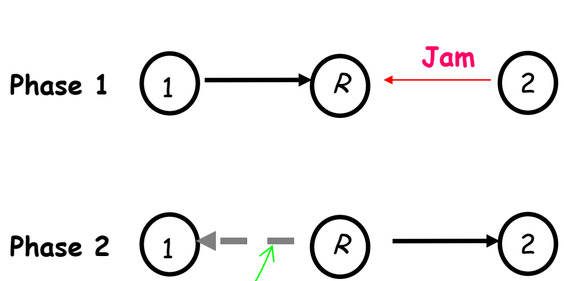
The achieved secrecy rate can be bigger than The upper bound for Scheme 1.

For Model one, feedback is *useful.*

Model Two



If Only Scheme 1 is used



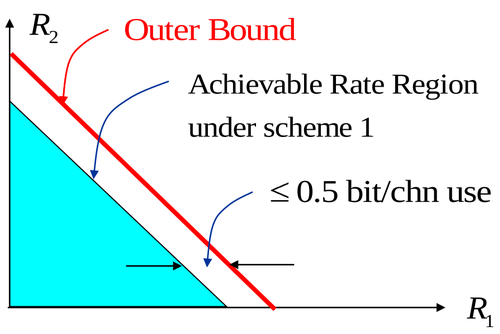
Outer Bound

$$\bigcup_{0\le\alpha\le 1} \mathrm{A}\cap\mathrm{B}$$

$$\text{where A}=\left\{\begin{array}{l} R_1, R_2 \\ R_1+R_2\le \alpha \min\ C\ \ \bar{P}_1/\alpha\ \ , C\ \ \bar{P}_2/\alpha \\ R_1\ge 0, R_2\ge 0 \end{array}\right\}$$

$$\text{B}=\left\{\begin{array}{l} 0\le R_1\le \bar{\alpha}C\ \ \bar{P}_r/\bar{\alpha} \\ 0\le R_2\le \bar{\alpha}C\ \ h^2\bar{P}_r/\bar{\alpha} \end{array}\right\}, \bar{\alpha}=1-\alpha$$

When relay power is large, scheme 1 is close to optimality



When relay power is large, feedback can be ignored.

Conclusion

•The role of feedback in enhancing secrecy was examined.

•Ignoring feedback can lead to simple system design, but may incur loss in achieved secrecy rate.

•Two models were considered:

- •Model 1 (Two-Way Wire-tap Channel):
  - Feedback is useful
- •Model 2(Two Way Relay Channel with Untrusted Relay):
  - Feedback is not very useful when relay power is abundant.