Joint and Individual Secrecy in Broadcast Channels with Receiver Side Information

Ahmed S. Mansour*, Rafael F. Schaefer†, and Holger Boche*

* Technische Universität München, Lehrstuhl für Theoretische Informationstechnik

† Princeton University, Department of Electrical Engineering

Introduction

- The open nature of BC allows transmitted signals to be received not only by legitimate users but eavesdroppers as well.

⇒ Shared secret key

⇒ Wiretap random encoding

⇒ Combination of the two techniques

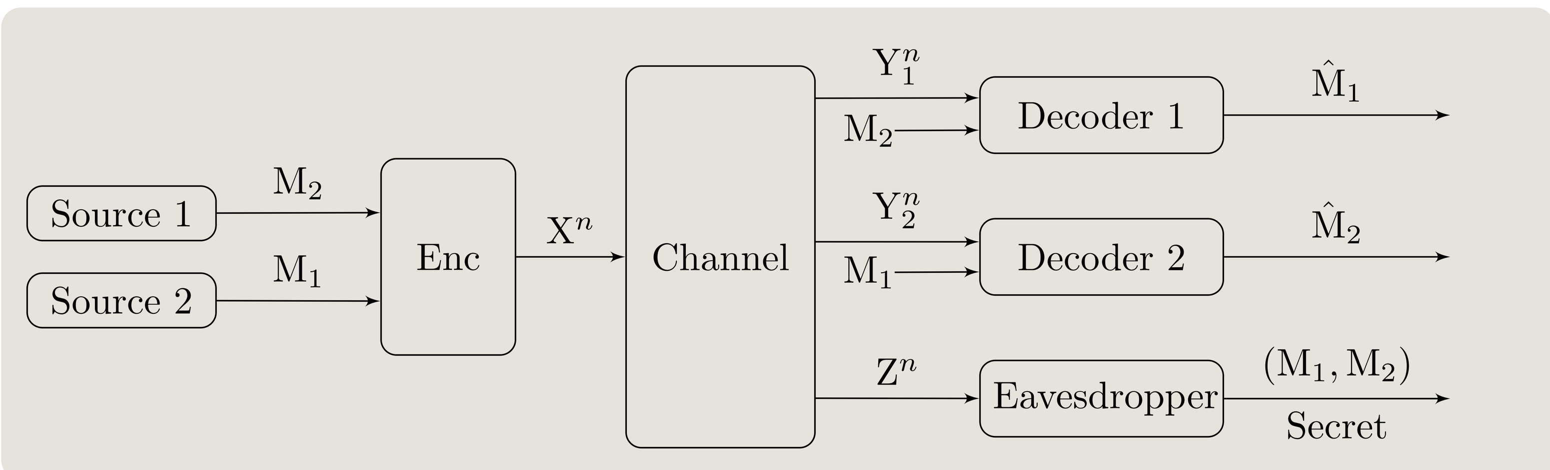
- Although the problem of secure communication in BC with one receiver and one eavesdropper is solved, the extension to BC with two or more legitimate receivers remains an open topic.

- Problem is motivated by the BC phase of **secure bidirectional relaying** in a three-node network.

MAC phase **BC phase**

BC With Receiver Side Information

- System Model



- The average probability of error is defined as:

$$P_e(\mathcal{C}_n) \triangleq \mathbb{P}\left[\hat{M}_1 \neq M_1 \text{ or } \hat{M}_2 \neq M_2\right] \leq \epsilon_n$$

Secrecy Criteria

- *Joint Secrecy:* This criterion requires the joint leakage of M_1 and M_2 to the eavesdropper to be small

$$L_J(\mathcal{C}_n) \triangleq \mathbb{I}(M_1M_2;Z^n) \leq \tau_n$$

- *Individual Secrecy:* This criterion requires the sum of the individual leakages of M_1 and M_2 to the eavesdropper to be small

$$L_I(\mathcal{C}_n) \triangleq \mathbb{I}(M_1;Z^n) + \mathbb{I}(M_2;Z^n) \leq \tau_n$$

⇒ The joint secrecy criterion is stronger than the individual one

⇒ Any code that satisfies the joint criterion also satisfies the individual one.

⇒ The individual secrecy criterion has a higher secrecy capacity compared to the joint one.

The Joint Secrecy Capacity Region

Achievable Rate Region

Lemma: *An achievable joint secrecy rate region for the BC with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_j \leq \mathbb{I}(V;Y_j) - \mathbb{I}(V;Z), \quad j = 1,2$$

for random variables with joint probability distribution $Q_V(v)\ Q_{X|V}(x|v)\ Q_{Y_1Y_2Z|X}(y_1,y_2,z|x)$.

- The proof combines the technique of random coding with product structure along with the usage of resolvability to achieve secrecy.

Multi-Letter Upper Bound

Proposition: *The joint secrecy capacity region of the BC with receiver side information is upper bounded as follows*

$$R_j \leq \lim_{n\to\infty} \frac{1}{n}\left[\mathbb{I}(V;Y_j^n) - \mathbb{I}(V;Z^n)\right], \quad j = 1,2$$

for random variables satisfying the Markov chain $V - X^n - (Y_1^n, Y_2^n, Z^n)$.

⇒ Since the multi-letter upper bound matches the achievable rate region applied to the n-fold product of the BC, this establishes a multi-letter description for the capacity region.

More Capable Channels

Defination: *The two legitimate receivers are said to be more capable than the eavesdropper in a wiretapper BC with receiver side information, if*

$$\mathbb{I}(X;Y_j) \geq \mathbb{I}(X;Z), \quad j = 1,2$$

for every input distribution on X.

⇒ The class of more capable channels contains physically and stochastically degraded channels as well as less noisy channels.

Proposition: *Let $Q(y,z|x)$ be a discrete memoryless BC and assume that Y is more capable than Z. Consider U and V to be any two random variables, such that $U - V - X - (Y,Z)$ forms a Markov chain. Then the following holds*

$$\begin{aligned}\mathbb{I}(V;Y|U) - \mathbb{I}(V;Z|U) &= \mathbb{E}\left[\mathbb{I}(V;Y|U=u) - \mathbb{I}(V;Z|U=u)\right]\\ &\leq \mathbb{I}(V^*;Y) - \mathbb{I}(V^*;Z)\\ &\leq \mathbb{I}(X;Y) - \mathbb{I}(X;Z)\end{aligned}$$

where V^* is distributed as $Q_{V|U=u^*}$ and u^* is the value of U that maximizes the difference.

Joint Secrecy for More Capable Channels

Theorem: *The joint secrecy capacity region of the more capable BC with receiver side information is the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_j \leq \mathbb{I}(X;Y_j) - \mathbb{I}(X;Z), \quad j = 1,2$$

for random variables with joint probability distribution $Q_X(x)\ Q_{Y_1Y_2Z|X}(y_1,y_2,z|x)$.

⇒ The achievability follows as in the previous lemma, while the converse follows by applying the previous proposition to standard outer bounds:

$$R_j \leq \mathbb{I}(V_j;Y_j|U_j) - \mathbb{I}(V_j;Z|U_j), \quad j = 1,2$$

The Individual Secrecy Capacity Region

Achievable Rate Region

Lemma: *An achievable individual secrecy rate region for the BC with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_1 \leq \min\left[\mathbb{I}(V;Y_1) - \mathbb{I}(V;Z) + R_2\ ,\ \mathbb{I}(V;Y_1)\right]$$
$$R_2 \leq \min\left[\mathbb{I}(V;Y_2) - \mathbb{I}(V;Z) + R_1\ ,\ \mathbb{I}(V;Y_2)\right]$$

for random variables with joint probability distribution $Q_V(v)\ Q_{X|V}(x|v)\ Q_{Y_1Y_2Z|X}(y_1,y_2,z|x)$, such that $\mathbb{I}(V;Y_1)$ and $\mathbb{I}(V;Y_2)$ are greater than $\mathbb{I}(V;Z)$.

- The proof combines the techniques of wiretap random encoding along with secret key encoding, where one message is used as a secret key for the other one and the resultant ciphered message is used as a part of the random index for wiretap encoding.
- The leakage analysis is carried out as follows:

$$\mathbb{I}(M_1;Z^n) = \mathbb{I}(M_{1W};Z^n) + \mathbb{I}(M_{1K};Z^n|M_{1W}).$$

where M_{1W} is the part of the message protected by wiretap encoding and M_{1K} is the part protected by secret key encoding.

Individual Secrecy for More Capable Channels

Theorem: *The individual secrecy capacity region of the more capable BC with receiver side information is the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_1 \leq \min\left[\mathbb{I}(X;Y_1) - \mathbb{I}(X;Z) + R_2\ ,\ \mathbb{I}(X;Y_1)\right]$$
$$R_2 \leq \min\left[\mathbb{I}(X;Y_2) - \mathbb{I}(X;Z) + R_1\ ,\ \mathbb{I}(X;Y_2)\right]$$

for random variables with joint probability distribution $Q_X(x)\ Q_{Y_1Y_2Z|X}(y_1,y_2,z|x)$.

⇒ The achievability follows as in the previous lemma, while the converse follows as in the joint secrecy case and the fact that the difference between the joint and individual secrecy constraints for each user is upper bounded by the rate of the other user.

SPAWC 2014 - Special Session IV: Wireless Cellular Systems

SPAWC 2014

Toronto - June 22-25, 2014