The Individual Secrecy Capacity of Degraded Multi-Receiver Wiretap Broadcast Channels

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

* Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

† Department of Electrical Engineering
Princeton University, USA

June 9, 2015

Outline

Outline

Information Theoretic Security

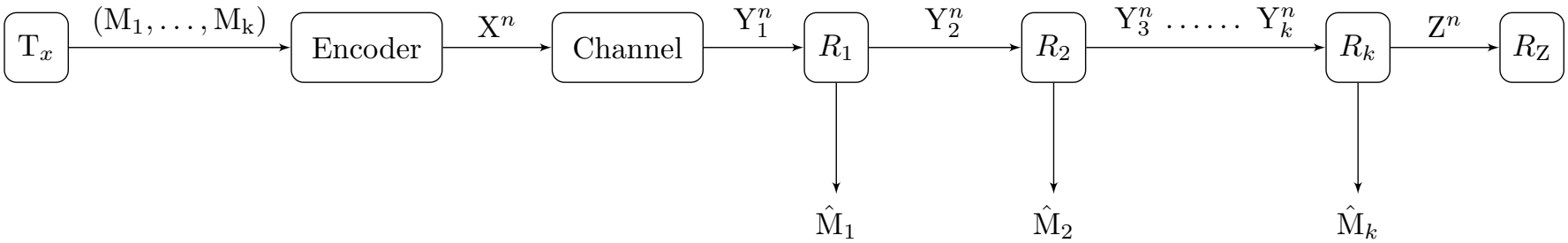
- Secret Key encoding [Shannon '49]
  - $\Rightarrow$ $\mathrm{M}_{\otimes} = \mathrm{M} \otimes \mathrm{K}$, Secrecy Requirement: $\mathbb{I}(\mathrm{M}; \mathrm{Z}^n) = 0$.
  - $\Rightarrow$ Transmit $x^n(m_{\otimes}) \rightarrow \mathbb{H}(\mathrm{M}) \leq \mathbb{H}(\mathrm{K})$
- Wiretap Random Coding [Csiszár/Körner '78]
  - $\Rightarrow$ Randomization message m_r to confuse the eavesdropper.
  - $\Rightarrow$ Secrecy Requirement: $\lim_{n\to\infty} \mathbb{I}(\mathrm{M}; \mathrm{Z}^n) = 0$.
  - $\Rightarrow$ Transmit $x^n(m, m_r) \rightarrow R_r \geq \mathbb{I}(\mathrm{X}; \mathrm{Z})$.
- Random Coding + Secret Key encoding [Kang/Liu '10]
  - $\Rightarrow$ $m_{\otimes}$ plays a role in confusing the eavesdropper.
  - $\Rightarrow$ Secrecy Requirement: $\lim_{n\to\infty} \mathbb{I}(\mathrm{M}; \mathrm{Z}^n) = 0$.
  - $\Rightarrow$ Transmit $x^n(m, m_{\otimes}, m_r) \rightarrow R_r + R_{\otimes} \geq \mathbb{I}(\mathrm{X}; \mathrm{Z})$.

C. Shannon, "Communication theory of secrecy systems," vol. 28, pp. 656–715, Oct. 1949

I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978

W. Kang and N. Liu, "Wiretap channel with shared key," Dublin, Ireland, Sep. 2010, pp. 1–5

Degraded Multi-Receiver Wiretap BC



- Important Feature: $\mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$
- Reliability Requirement:

$$P_e(\mathcal{C}_n) \triangleq \mathbb{P}\left[\hat{\mathrm{M}}_1 \neq \mathrm{M}_1 \text{ or } \ldots \text{ or } \hat{\mathrm{M}}_k \neq \mathrm{M}_k\right].$$

$$R_j \leq \frac{1}{n}\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n) + \tilde{\gamma}_j(\epsilon_n)$$

- Secrecy Requirement:
  - Joint Secrecy:

$$\Rightarrow \mathbb{I}(\mathrm{M}_1,\ldots,\mathrm{M}_k;\mathrm{Z}^n) \leq \tau_n$$

  - Individual Secrecy:

$$\Rightarrow \sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n) \leq \tau_n$$

- Properties?, Which one? and Why???

Joint Secrecy Vs Individual Secrecy

1. *Joint Secrecy:* $\mathbb{I}(\mathrm{M}_1,\ldots,\mathrm{M}_k;\mathrm{Z}^n) \leq \tau_n$
   - Focus of most previous works.
   - Receivers do not trust each other.
   - Conservative and immune against compromised receivers.
   - Vanishing capacity for eavesdropper with statistical advantage.

2. *Individual Secrecy:* $\sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n) \leq \tau_n$
   - BC with message cognition. [Mansour/Schaefer/Boche '15]
   - Mutual trust and Receiver cooperation.
   - less conservative, secrecy might fails.
   - Higher throughput is expected.
   - How to encode? Use messages as secret keys.

A. S. Mansour, R. F. Schaefer, and H. Boche, "Capacity regions for broadcast channels with degraded message sets and message cognition under different secrecy constraints," *CoRR*, vol. abs/1501.04490, January 2015, [Online]

Outline

Joint Secrecy: Achievability and Converse

Theorem 1: Capacity Region [Ekrem/Ulukus/ '09]

The joint secrecy capacity region of the degraded multi-receiver wiretap BC is given by all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j; \mathrm{Z}|\mathrm{U}_{j+1})$$

where $\mathrm{U}_1 = \mathrm{X}$, $\mathrm{U}_{k+1} = \emptyset$ and the union is taken over all random variables such that, $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$.

- Achievability: Superposition encoding with Random binning.
- Converse: Standard Techniques + Prop. of Markov chain.
- For a two-receiver wiretap BC:

$$R_2 \leq \mathbb{I}(\mathrm{U}; \mathrm{Y}_2) - \mathbb{I}(\mathrm{U}; \mathrm{Z})$$
$$R_1 \leq \mathbb{I}(\mathrm{X}; \mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X}; \mathrm{Z}|\mathrm{U})$$

E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, pp. 1–29, March 2009

Outline

Individual Secrecy: Achievability

Theorem 2: Degraded Two-Receiver Wiretap BC

The individual secrecy capacity region of the degraded two-receiver wiretap BC is given by the union of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy

$$\begin{aligned} R_2 &\leq \mathbb{I}(\mathrm{U};\mathrm{Y}_2) - \mathbb{I}(\mathrm{U};\mathrm{Z}) \\ R_1 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) + \mathbb{I}(\mathrm{U};\mathrm{Z}) \\ R_1 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) + R_2 \end{aligned}$$

where the union is taken over all random variables (U, X), such that $\mathrm{U} - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \mathrm{Z}$ forms a Markov chain.

- Achievability: Random coding + Secret Key encoding.
- Y_1 can decode m_2: Prop. of degraded BC.
  $\Rightarrow$ m_2 is used a secret key for Y_1.

Individual Secrecy: Multi-Receiver Wiretap BC

Theorem 3: Capacity Region

The individual secrecy capacity region of the degraded multi-receiver wiretap BC is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j; \mathrm{Z}|\mathrm{U}_{j+1}) + \sum_{l=j+1}^{k} R_l$$

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j|\mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_{j+1}; \mathrm{Z})$$

$$\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k} \mathbb{I}(\mathrm{U}_l; \mathrm{Y}_l|\mathrm{U}_{l+1})$$

where $\mathrm{U}_1 = \mathrm{X}$, $\mathrm{U}_{k+1} = \emptyset$ and the union runs over all random variables such that, $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$.

Bounds Implication and Converse

1. $R_j \leq \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1}) + \sum_{l=j+1}^{k} R_l$.
   - $\Rightarrow$ Total Rate = Random Coded + Secret Key Encoded.
   - $\Rightarrow$ Adapting the Joint converse by $\sum_{l=j+1}^{k} R_l$.
2. $R_j \leq \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_{j+1};\mathrm{Z})$
   - $\Rightarrow$ A User's Rate = Information in his own layer + Randomization Indcies of Lower Layers.
   - $\Rightarrow$ $R_j \leq \frac{1}{n}\left[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1}) + \mathbb{I}(\ddot{\mathrm{M}}_{j+1};\mathrm{Z}^n)\right] + \tilde{\gamma}_j(\epsilon_n)$
3. $\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k} \mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1})$
   - $\Rightarrow$ A Randomization index can be used only once.
   - $\Rightarrow$ Reliability Bound as in Degraded BC without secrecy.

Outline

Gaussian Two-Receiver Wiretap BC

Theorem 4: Capacity Region: Joint Vs Individual

Consider a two-receiver Gaussian wiretap BC, the joint secrecy capacity region is given by

$$R_2 \leq f\left(1+\frac{\bar{\alpha}P}{\alpha P+\sigma_2^2}\right)-f\left(1+\frac{\bar{\alpha}P}{\alpha P+\sigma_Z^2}\right)$$
$$R_1 \leq f\left(1+\frac{\alpha P}{\sigma_1^2}\right)-f\left(1+\frac{\alpha P}{\sigma_Z^2}\right),$$

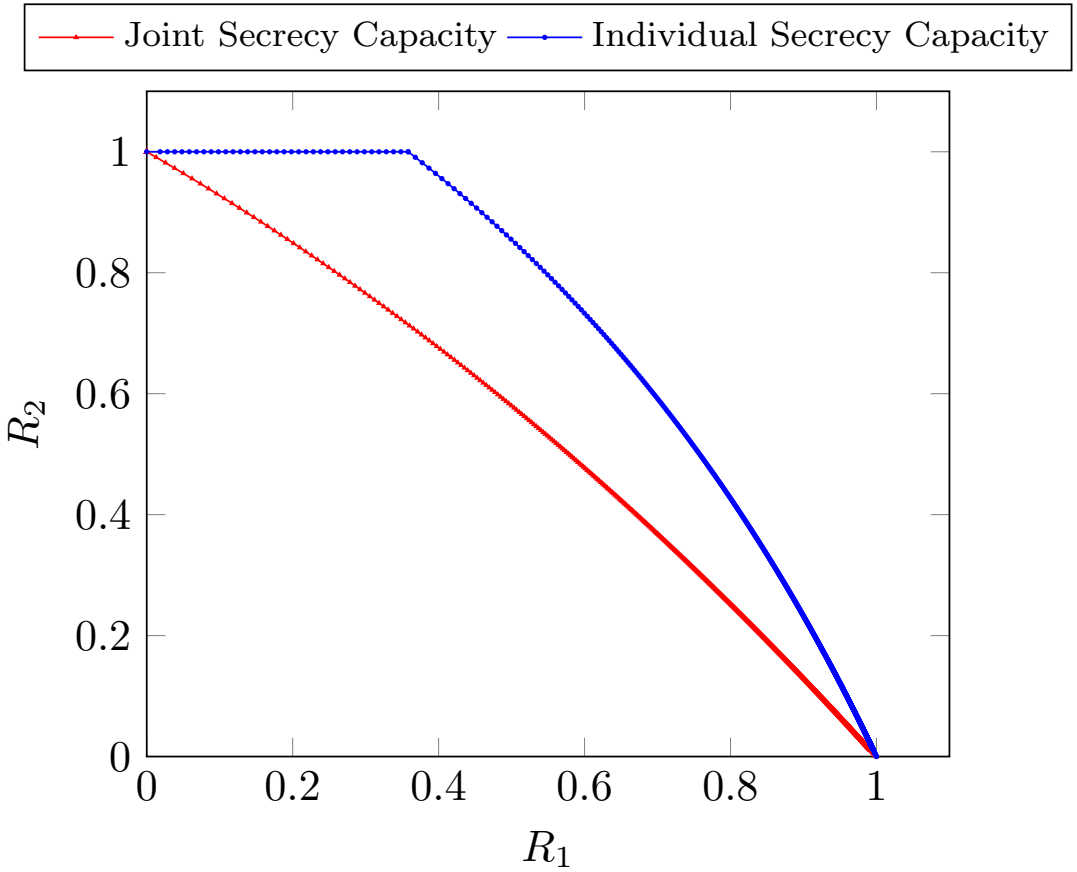
while the individual secrecy capacity region is given by

$$R_2 \leq f\left(1+\frac{\bar{\alpha}P}{\alpha P+\sigma_2^2}\right)-f\left(1+\frac{\bar{\alpha}P}{\alpha P+\sigma_Z^2}\right)$$
$$R_1 \leq f\left(1+\frac{\alpha P}{\sigma_1^2}\right)+f\left(1+\frac{\bar{\alpha}P}{\alpha P+\sigma_Z^2}\right)$$
$$R_1 \leq f\left(1+\frac{\alpha P}{\sigma_1^2}\right)-f\left(1+\frac{\alpha P}{\sigma_Z^2}\right)+R_2,$$

where $f(x)=\frac{1}{2}\log(x)$ and $\bar{\alpha}=1-\alpha$.

Example

- Sweep over α.
  $\Rightarrow$ $\sigma_1^2 = 0.05$,
  $\sigma_2^2 = 0.1$,
  $\sigma_Z^2 = 0.15$.
- Higher throughput for Individual Secrecy
- $R_1 > 0$, although $\alpha = 0$.



Outline

Conclusion & Future Work

- Conclusion
  - $\Rightarrow$ Investigated secrecy in degraded multi-receiver wiretap BC.
  - $\Rightarrow$ Established the individual secrecy capacity region.
  - $\Rightarrow$ Bigger capacity region as compared to the joint one.
- Extensions and Future work
  - $\Rightarrow$ Extension to the Gaussian BC. (Done)
  - $\Rightarrow$ Extension to the MIMO Gaussian BC. (In Progress)
  - $\Rightarrow$ Investigation of the less noisy wiretap BC. (In Progress)

References I


C. Shannon, "Communication theory of secrecy systems," vol. 28, pp. 656–715, Oct. 1949.


I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.


W. Kang and N. Liu, "Wiretap channel with shared key," Dublin, Ireland, Sep. 2010, pp. 1–5.


A. S. Mansour, R. F. Schaefer, and H. Boche, "Capacity regions for broadcast channels with degraded message sets and message cognition under different secrecy constraints," *CoRR*, vol. abs/1501.04490, January 2015, [Online].


E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, pp. 1–29, March 2009.

Thank YOU!

Thank You