Strong Secrecy and Decoding Performance Analysis for Robust Broadcasting under Channel Uncertainty

Rafael Schaefer

PRINCETON UNIVERSITY

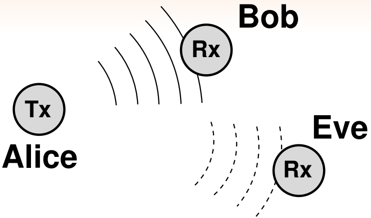
joint work with
Holger Boche (Technische Universität München)

IFS-L1: Secret Communications, Fingerprinting, and Security

May 8, 2014

Motivation

- Signal is received by legitimate users but also eavesdropped by **non-legitimate users**
  - ➠ Need of **secure communication systems**

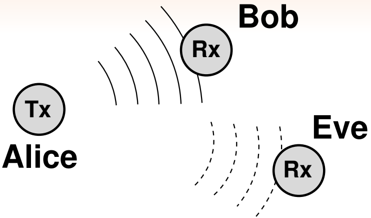


- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers
  - ➠ **Use of information theoretic secrecy concepts**

- Imperfect channel estimation, limited feedback schemes, etc.
- Eve will **not** share its channel information with Alice to make eavesdropping harder
  - ➠ **Uncertainty in channel state information**

Motivation

- Signal is received by legitimate users but also eavesdropped by **non-legitimate users**
  - ➠ Need of **secure communication systems**

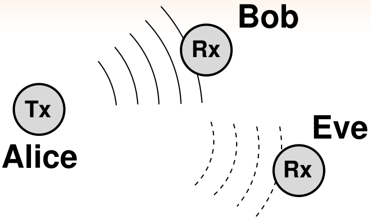


- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers
  - ➠ **Use of information theoretic secrecy concepts**

- Imperfect channel estimation, limited feedback schemes, etc.
- Eve will **not** share its channel information with Alice to make eavesdropping harder
  - ➠ **Uncertainty in channel state information**

Motivation

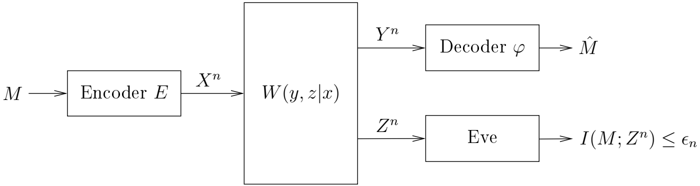
- Signal is received by legitimate users but also eavesdropped by **non-legitimate users**
  - ➠ Need of **secure communication systems**



- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers
  - ➠ **Use of information theoretic secrecy concepts**

- Imperfect channel estimation, limited feedback schemes, etc.
- Eve will **not** share its channel information with Alice to make eavesdropping harder
  - ➠ **Uncertainty in channel state information**

Wiretap Channel



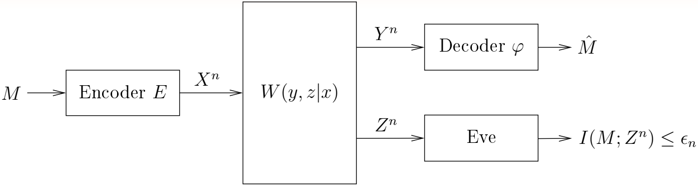
- Consider discrete memoryless **wiretap channel** with
    - confidential message M with rate R for receiver 1 (Bob)

- Total amount of information leaked to receiver 2 (Eve) has to be small

  ➠ **Strong secrecy** requirement on M, i.e.,

$$I(M;Z^n) \leq \epsilon_n$$

Secrecy Capacity of Wiretap Channel



Secrecy Capacity [Wyner '75, Csiszár/Körner '78]

The strong secrecy capacity of the wiretap channel is

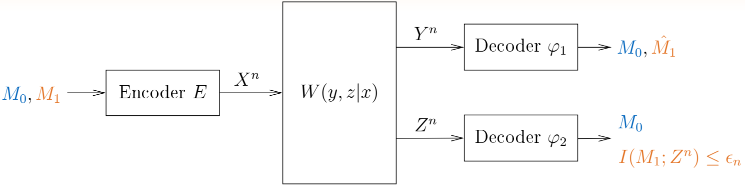
$$C = \max_{P_{VX}} \big(I(V;Y) - I(V;Z) \big)$$

for random variables $V - X - (Y, Z)$.

A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975

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

Broadcast Channel with Confidential Messages



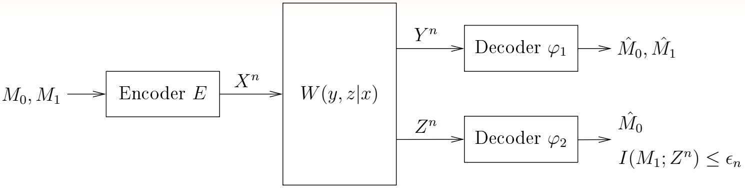
- Consider discrete memoryless **broadcast channel with common and confidential messages (BCC)** with
  - common message M_0 with rate R_0 for both receivers
  - confidential message M_1 with rate R_1 for receiver 1

- Total amount of information leaked to receiver 2 has to be small

➠ **Strong secrecy** requirement on M_1, i.e.,

$$I(M_1; Z^n) \leq \epsilon_n$$

Secrecy Capacity Region of BCC



Secrecy Capacity Region [Csiszár/Körner '78 and '11]

The strong secrecy capacity region of the BCC is the set of all rate pairs $(R_1, R_0) \in \mathbb{R}_+^2$ that satisfy

$$R_1 \leq I(V;Y|U) - I(V;Z|U)$$
$$R_0 \leq \min\{I(U;Y), I(U;Z)\}$$

for random variables $U - V - X - (Y, Z)$.

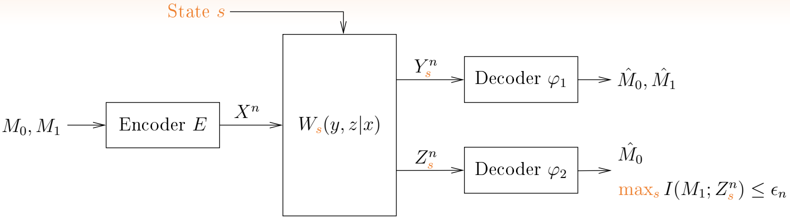
I. Csiszár and J. Körner, ''Broadcast Channels with Confidential Messages,'' *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978

Channel Uncertainty

- Practical systems always suffer from uncertainty in CSI due to
  - nature of the wireless channel
  - estimation/feedback inaccuracy
  - ...

➠ **Perfect CSI is a challenging task**

Compound BCC



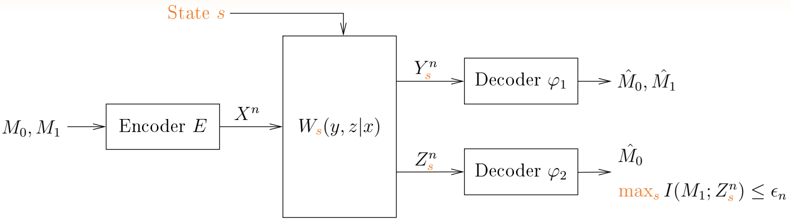
- In this work we additionally consider **channel uncertainty**
- State set $\mathcal{S} := \{1, ..., S\}$
  - actual channel realization $s \in \mathcal{S}$ unknown to sender and receiver
  - remains constant during whole transmission

The discrete memoryless **compound BCC** $\mathfrak{W}$ is given by the family

$$\mathfrak{W} := \{W_s(y,z|x) : s \in \mathcal{S}\}$$

➠ Need strategy that works for all $s \in \mathcal{S}$ simultaneously!

Achievable Secrecy Rate Region



Theorem 1: Achievable Secrecy Rate Region

An achievable strong secrecy rate region for the compound BBC $\mathfrak{W}$ is given by all rate pairs $(R_1, R_0) \in \mathbb{R}_+^2$ that satisfy

$$R_1 \leq \min_{s\in\mathcal{S}} I(V;Y_s|U) - \max_{s\in\mathcal{S}} I(V;Z_s|U)$$

$$R_0 \leq \min_{s\in\mathcal{S}} \min\{I(U;Y_s), I(U;Z_s)\}$$

for random variables $U - V - X - (Y_s, Z_s)$.

Achievable Secrecy Rate Region

Theorem 1: Achievable Secrecy Rate Region

An achievable strong secrecy rate region for the compound BBC $\mathfrak{W}$ is given by all rate pairs $(R_1, R_0) \in \mathbb{R}_+^2$ that satisfy

$$R_1 \leq \min_{s \in \mathcal{S}} I(V; Y_s | U) - \max_{s \in \mathcal{S}} I(V; Z_s | U)$$

$$R_0 \leq \min_{s \in \mathcal{S}} \min\{I(U; Y_s), I(U; Z_s)\}$$

for random variables $U - V - X - (Y_s, Z_s)$.

- Node 2 is legitimate receiver for M_0 and, at the same time, non-legitimate receiver for M_1

  ➠ Different assumptions on its channel:
  - best channel for confidential M_1
  - worst channel for common M_0

Questions

- Theorem 1 gives an achievable rate region at which rates can be communicated reliably and securely simultaneously
  - ➠ Several questions arise

- Theorem 1 is proved using random coding arguments
  - ➠ What can we say about properties of such strategies?
- Secrecy criterion is

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n$$

  - ➠ Common message M_0 is available at receiver 2. Should **M_0 be taken into account**?
  - ➠ What is the **operational meaning** of this? What are the **implications** for the non-legitimate receiver?

Vanishing Output Variation

- Investigating proof of Theorem 1 reveals the following property

Definition: Vanishing Output Variation

A code has exponentially fast *vanishing output variation* if there exists for each $s \in \mathcal{S}$ and $m_0 \in \mathcal{M}_0$ a non-negative measure ϑ_{s,m_0} on $\mathcal{Z}^n$ such that for all $m_1 \in \mathcal{M}_1$ it holds

$$\sum_{z^n \in \mathcal{Z}^n} \left| \overline{W}^n_{\mathcal{Z},s}(z^n | m_0, m_1) - \vartheta_{s,m_0}(z^n) \right| \leq 2^{-n\beta} \tag{1}$$

for some $\beta > 0$. Instead of (1) we also write $\|\overline{W}^n_{\mathcal{Z},s}(\cdot|m_0,m_1) - \vartheta_{s,m_0}\| \leq 2^{-n\beta}$ interchangeably.

➠ For each channel realization $s \in \mathcal{S}$ and each common $m_0 \in \mathcal{M}_0$:

  ➠ Channel output at receiver 2 "is the same" **for all $m_1 \in \mathcal{M}_1$**

Strong Secrecy

- Receiver is supposed to decode the common message $m_0 \in \mathcal{M}_0$
  - ➠ Secrecy criterion should reflect this fact:

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n | M_0) \leq \epsilon_n$$

Proposition: Strong Secrecy

If a code for the compound BCC has the vanishing output variation property, then the strong secrecy criterion satisfies

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n$$

and

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n | M_0) \leq \epsilon_n$$

with $\epsilon_n \to 0$ exponentially fast as $n \to \infty$.

Decoding Performance of Non-Legitimate Reciever

What are the implications for the non-legitimate receiver?

- Assume worst case: Receiver 2 knows
  - channel state $s \in \mathcal{S}$
  - common message $m_0 \in \mathcal{M}_0$ (supposed to decode it anyway)

➠ Receiver 2 can choose arbitrary decoding sets $\mathcal{D}_{s,m_0}(m_1)$, $m_1 \in \mathcal{M}_1$, for each $s \in \mathcal{S}$, $m_0 \in \mathcal{M}_0$

Proposition: Average Decoding Error

If the code has vanishing output variation, then the average probability of decoding error satisfies

$$\min_{s\in\mathcal{S}} \bar{e}'_{2,n}(s) \geq 1 - \frac{1}{|\mathcal{M}_1|} - \lambda_n$$

with $\frac{1}{|\mathcal{M}_1|} \to 0$ and $\lambda_n \to 0$ exponentially fast as $n \to \infty$.

Implications

Theorem: Implications

If a code for the compound BCC has the vanishing output variation property, then secrecy is guaranteed in the *information theoretic sense* of

$$\max_{s\in\mathcal{S}} \max\left\{I(M_1;Z_s^n), I(M_1;Z_s^n|M_0)\right\} \leq \epsilon_n$$

but also in the *signal processing sense* of

$$\min_{s\in\mathcal{S}} \bar{e}'_{2,n}(s) \geq 1 - \frac{1}{|\mathcal{M}_1|} - \lambda_n$$

with $\frac{1}{|\mathcal{M}_1|} \to 0$, $\epsilon_n \to 0$, and $\lambda_n \to 0$ exponentially fast as $n \to \infty$.

- Holds for any decoding strategy of receiver 2 (no restrictions on the complexity or computational resources)

➠ Universal results which hold for any applied post-processing strategy of the non-legitimate receiver.

Conclusions

- Studied **compound BC with confidential messages**
  - Incorporates public **and** confidential communication
  - Reliable communication and, especially, secrecy must be established under channel uncertainty

- Established achievable strong secrecy rate region

- Identified desirable code property of **vanishing output variation**
  - ➠ Implies strong secrecy in the information theoretic sense
  - ➠ Implies strong secrecy in terms of average decoding error
  - ➠ Gives strong secrecy an operational meaning/interpretation

Thank you for your attention!

Conclusions

- Studied **compound BC with confidential messages**
  - Incorporates public **and** confidential communication
  - Reliable communication and, especially, secrecy must be established under channel uncertainty

- Established achievable strong secrecy rate region

- Identified desirable code property of **vanishing output variation**

  ➠ Implies strong secrecy in the information theoretic sense
  ➠ Implies strong secrecy in terms of average decoding error
  ➠ Gives strong secrecy an operational meaning/interpretation

Thank you for your attention!

References I

- A. D. Wyner, ''The Wire-Tap Channel,'' *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- I. Csiszár and J. Körner, ''Broadcast Channels with Confidential Messages,'' *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.