On the Continuity of the Secrecy Capacity of Wiretap Channels Under Channel Uncertainty

Holger Boche*, **Rafael Schaefer**†, and H. Vincent Poor†

* Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

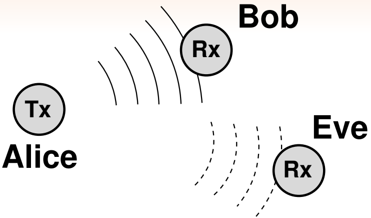
† Department of Electrical Engineering
Princeton University, United States

ICC 2015
CTS-04: Physical-Layer Security

June 9, 2015

Motivation

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

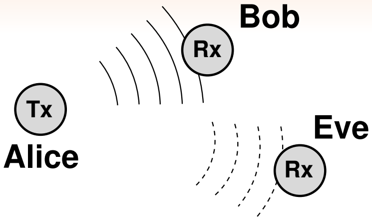


- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers
  - ➠ **Use of information theoretic secrecy concepts**

- 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**



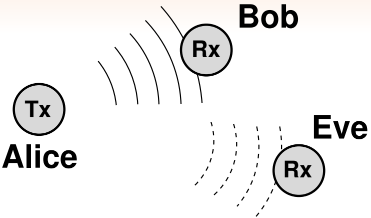
- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers
  - ➠ **Use of information theoretic secrecy concepts**

- 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**



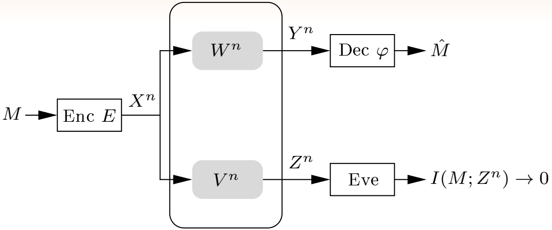
- Security on higher layers is usually based on the assumption of insufficient computational capabilities of non-legitimate receivers

  ➠ **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



- Discrete memoryless **wiretap channel** with
  - $W(y|x)$ the legitimate channel (Bob)
  - $V(z|x)$ the eavesdropper channel (Eve)

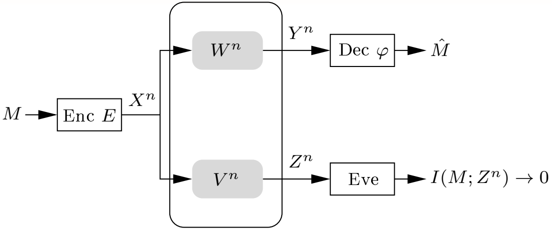
- Confidential message M to be reliably decoded by Bob

$$\Pr\{\hat{M} \neq M\} \to 0$$

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

$$\boldsymbol{I(M; Z^n) \to 0}$$

Wiretap Channel (2)



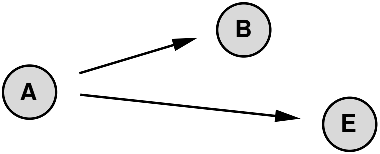
Secrecy Capacity [Wyner '75, Csiszár/Körner '78]

The *secrecy capacity* C_S of the wiretap channel is

$$C_S = \max_{U-X-(Y,Z)} \big(I(U;Y) - I(U;Z)\big).$$

- 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

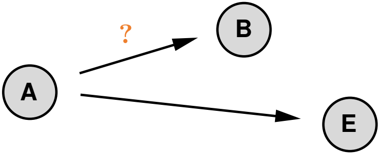
Channel Uncertainty



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

Perfect CSI of the legitimate channel is a challenging task

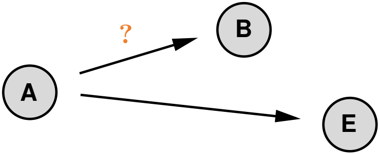
Channel Uncertainty



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

➠ Perfect CSI of the legitimate channel is a challenging task

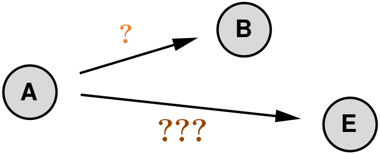
Channel Uncertainty



- Eve will **not** share its channel information with Alice to make eavesdropping harder

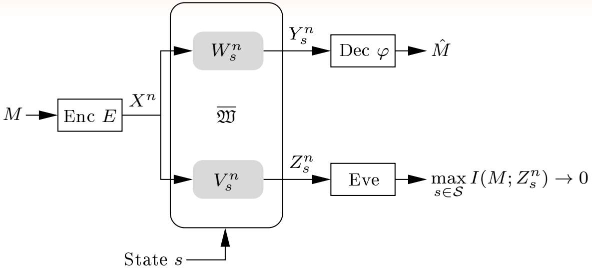
  ➠ Perfect eavesdropper CSI is **more than questionable**

Channel Uncertainty



- Eve will **not** share its channel information with Alice to make eavesdropping harder
  - ➠ Perfect eavesdropper CSI is **more than questionable**

Compound Wiretap Channel



- **Uncertainty set $\mathcal{S}$**
  - actual realization $s \in \mathcal{S}$ unknown to Alice and Bob
  - remains constant during the entire transmission

The **compound wiretap channel** $\overline{\mathfrak{W}}$ is given by the family

$$\overline{\mathfrak{W}} = \Big\{ \{W_s\}_{s \in \mathcal{S}}, \{V_s\}_{s \in \mathcal{S}} \Big\}$$

Compound Wiretap Channel (2)

- Single-letter secrecy capacity is only known for special cases (degraded channels, CSIT, certain MIMO configurations, ...)
- For general case only multi-letter characterization is known:

Theorem: Secrecy Capacity [BBS '13]

The secrecy capacity $C_S(\overline{\mathfrak{W}})$ of the compound wiretap channel $\overline{\mathfrak{W}}$ is

$$C_S(\overline{\mathfrak{W}}) = \lim_{n\to\infty} \frac{1}{n} \max_{U - X^n - (Y_s^n, Z_s^n)} \Big(\inf_{s\in\mathcal{S}} I(U; Y_s^n) - \sup_{s\in\mathcal{S}} I(U; Z_s^n) \Big)$$

for random variables $U - X^n - (Y_s^n, Z_s^n)$ forming a Markov chain.

I. Bjelaković, H. Boche, and J. Sommerfeld, ''Secrecy Results for Compound Wiretap Channels,'' *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013

- Obviously, the secrecy capacity depends on the uncertainty set

How does the secrecy capacity change if there are (small) variations in the uncertainty set?

- Desired behavior: **CONTINUITY**
  - ➠ Small variations in the uncertainty set should result in small variations in the secrecy capacity only!

➠ Robust approaches

- In particular relevant in the context of active adversaries who might influence the system parameters in a malicious way

- Obviously, the secrecy capacity depends on the uncertainty set

How does the secrecy capacity change
if there are (small) variations in the uncertainty set?

- Desired behavior: **CONTINUITY**
  - ➠ Small variations in the uncertainty set should result in small variations in the secrecy capacity only!

➠ Robust approaches

- In particular relevant in the context of active adversaries who might influence the system parameters in a malicious way

Distance

- We need a concept to measure the distance between two channels:

- The distance between two channels W_1 and W_2 is defined based on the total variation distance as

$$d(W_1, W_2) = \max_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \left| W_1(y|x) - W_2(y|x) \right|$$

➠ The distance $D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2)$ between two compound wiretap channels $\overline{\mathfrak{W}}_1$ and $\overline{\mathfrak{W}}_2$ is given by the largest distance for all possible realizations for the legitimate and eavesdropper channel

- Note that other norms will work as well to define the distance

➠ Will only lead to slightly different constants

Continuity

Theorem: Continuity of Compound Secrecy Capacity

Let $\overline{\mathfrak{W}}_1$ and $\overline{\mathfrak{W}}_2$ be two compound wiretap channels. If the distance satisfies

$$D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2) < \epsilon,$$

then it holds that

$$\boldsymbol{\big|C_S(\overline{\mathfrak{W}}_1) - C_S(\overline{\mathfrak{W}}_2)\big| \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)}$$

with $\delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) = 4\epsilon \log |\mathcal{Y}||\mathcal{Z}| + 8H_2(\epsilon)$ a constant depending on the distance ϵ and the output alphabet sizes $|\mathcal{Y}|$ and $|\mathcal{Z}|$.

- C_S is a **continuous function** of $\overline{\mathfrak{W}}$
  - Small variations in $\overline{\mathfrak{W}} \Rightarrow$ small variations in C_S
- $\delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)$ quantifies how much the secrecy capacities differ
- multi-letter description makes it non-trivial to show

Continuity

Theorem: Continuity of Compound Secrecy Capacity

Let $\overline{\mathfrak{W}}_1$ and $\overline{\mathfrak{W}}_2$ be two compound wiretap channels. If the distance satisfies

$$D(\overline{\mathfrak{W}}_1, \overline{\mathfrak{W}}_2) < \epsilon,$$

then it holds that

$$\big|C_S(\overline{\mathfrak{W}}_1) - C_S(\overline{\mathfrak{W}}_2)\big| \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)$$

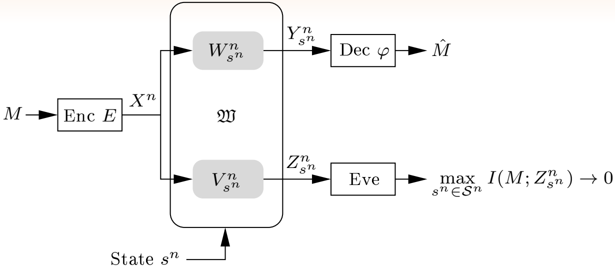
with $\delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) = 4\epsilon \log |\mathcal{Y}||\mathcal{Z}| + 8H_2(\epsilon)$ a constant depending on the distance ϵ and the output alphabet sizes $|\mathcal{Y}|$ and $|\mathcal{Z}|$.

- C_S is a **continuous function** of $\overline{\mathfrak{W}}$
  - Small variations in $\overline{\mathfrak{W}} \Rightarrow$ small variations in C_S
- $\delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)$ quantifies how much the secrecy capacities differ
- multi-letter description makes it non-trivial to show

- Secrecy capacity of compound wiretap channel is continuous

Is this still true for other / more involved uncertainty models?

Arbitrarily Varying Wiretap Channel



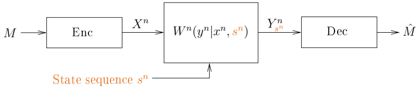
- **Uncertainty set $\mathcal{S}$**
  - actual state sequence $s^n \in \mathcal{S}^n$ unknown to Alice and Bob
  - channel may vary in an unknown and arbitrary manner from channel use to channel use

The **arbitrarily varying wiretap channel (AVWC)** $\mathfrak{W}$ is given by the family

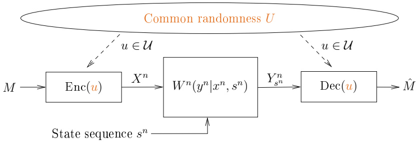
$$\mathfrak{W} = \Big\{\mathcal{W}, \mathcal{V}\Big\} = \Big\{\{W^n_{s^n}\}_{s^n \in \mathcal{S}^n}, \{V^n_{s^n}\}_{s^n \in \mathcal{S}^n}\Big\}$$

Ordinary AVCs

- For ordinary AVCs $\mathcal{W}$ (without any wiretappers) we know that for symmetrizable channels



unassisted capacity $C(\mathcal{W}) = 0$



CR-assisted capacity $C_{\mathrm{CR}}(\mathcal{W}) > 0$!

- An AVC $\mathcal{W}$ is called *symmetrizable* if there exists a stochastic matrix $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$ such that

$$\sum_{s\in\mathcal{S}} W(y|x,s)\sigma(s|x') = \sum_{s\in\mathcal{S}} W(y|x',s)\sigma(s|x)$$

holds for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$.

Secrecy Capacity

Theorem: CR-Assisted Secrecy Capacity [WNB '15]

A multi-letter description of the CR-assisted secrecy capacity $C_{S,\mathsf{CR}}(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ is

$$C_{S,\mathsf{CR}}(\mathfrak{W}) = \lim_{n\to\infty} \frac{1}{n} \max_{U-X^n-(\overline{Y}_q^n, Z_{s^n}^n)} \Big(\min_{q\in\mathcal{P}(\mathcal{S}^n)} I(U;\overline{Y}_q^n) - \max_{s^n\in\mathcal{S}^n} I(U;Z_{s^n}^n) \Big)$$

with $\overline{Y}_q^n$ the random variable associated with the output of the averaged channel $\overline{W}_q^n = \sum_{s^n\in\mathcal{S}^n} q(s^n) W_{s^n}$, $q\in\mathcal{P}(\mathcal{S}^n)$.

M. Wiese, J. Nötzel, and H. Boche, ''The Arbitrarily Varying Wiretap Channel – Communication under Uncoordinated Attacks,'' in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015, extended version available at http://arxiv.org/abs/1410.8078

Secrecy Capacity (2)

***Theorem:* Unassisted Capacity** [BBS '13], [NWB '15]

The unassisted secrecy capacity $C_S(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ possesses the following symmetrizability properties:

1. If $\mathcal{W}$ is symmetrizable, then $C_S(\mathfrak{W}) = 0$.
2. If $\mathcal{W}$ is non-symmetrizable, then $C_S(\mathfrak{W}) = C_{S,\text{CR}}(\mathfrak{W})$.

I. Bjelaković, H. Boche, and J. Sommerfeld, *Information Theory, Combinatorics, and Search Theory*. Springer, 2013, ch. Capacity Results for Arbitrarily Varying Wiretap Channels, pp. 123–144

J. Nötzel, M. Wiese, and H. Boche, ''The Arbitrarily Varying Wiretap Channel - Secret Randomness, Stability and Super-Activation,'' in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015, extended version available at http://arxiv.org/abs/1501.07439

Is the secrecy capacity of the AVWC continuous or discontinuous?

Discontinuity

- One can define an AVWC $\mathfrak{W}(\lambda)$ for which the following holds:

Theorem: Discontinuity Point

1. The CR-assisted secrecy capacity $C_{S,\text{CR}}(\mathfrak{W}(\lambda))$ is continuous in λ for all $\lambda \in [0,1]$ and it holds that

$$\min_{\lambda\in[0,1]} C_{S,\text{CR}}(\mathfrak{W}(\lambda)) > 0.$$

2. The unassisted secrecy capacity $C_S(\mathfrak{W}(\lambda))$ is continuous in λ for all $\lambda \in (0,1]$. It holds that $\boldsymbol{C_S(\mathfrak{W}(0)) = 0}$ and further that

$$\lim_{\lambda\searrow 0} \boldsymbol{C_S(\mathfrak{W}(\lambda)) > 0},$$

i.e., $\lambda = 0$ is a **discontinuous point** of $C_S(\cdot)$.

➠ For $\lambda = 0$ the AVWC $\mathfrak{W}(0)$ is symmetrizable $\Rightarrow$ zero capacity!

Conclusions

- System performance should depend continuously on its parameters
  - ➠ Small changes in the parameters result in small changes of the performance only

- **Compound wiretap channel**
  - ➠ Capacity is continuous in the uncertainty set!

- **Arbitrarily varying wiretap channel**
  - ➠ Unassisted capacity is **discontinuous** in the uncertainty set!

➠ Continuity is not only a property of secrecy capacity, but extends to actual code designs as well (ongoing work)

Thank you for your attention!

H. Boche, R. F. Schaefer, and H. V. Poor, "On the Continuity of the Secrecy Capacity of Compound and Arbitrarily Varying Wiretap Channels," *under submission, revised Mar. 2015*, available online at http://arxiv.org/abs/1409.4752

Conclusions

- System performance should depend continuously on its parameters
  - ➠ Small changes in the parameters result in small changes of the performance only

- **Compound wiretap channel**
  - ➠ Capacity is continuous in the uncertainty set!

- **Arbitrarily varying wiretap channel**
  - ➠ Unassisted capacity is **discontinuous** in the uncertainty set!

➠ Continuity is not only a property of secrecy capacity, but extends to actual code designs as well (ongoing work)

Thank you for your attention!

H. Boche, R. F. Schaefer, and H. V. Poor, ‘‘On the Continuity of the Secrecy Capacity of Compound and Arbitrarily Varying Wiretap Channels,’’ *under submission, revised Mar. 2015*, available online at http://arxiv.org/abs/1409.4752

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.

I. Bjelaković, H. Boche, and J. Sommerfeld, ''Secrecy Results for Compound Wiretap Channels,'' *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

M. Wiese, J. Nötzel, and H. Boche, ''The Arbitrarily Varying Wiretap Channel – Communication under Uncoordinated Attacks,'' in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015, extended version available at http://arxiv.org/abs/1410.8078.

I. Bjelaković, H. Boche, and J. Sommerfeld, *Information Theory, Combinatorics, and Search Theory*. Springer, 2013, ch. Capacity Results for Arbitrarily Varying Wiretap Channels, pp. 123–144.

References II

J. Nötzel, M. Wiese, and H. Boche, ''The Arbitrarily Varying Wiretap Channel - Secret Randomness, Stability and Super-Activation,'' in *Proc. IEEE Int. Symp. Inf. Theory*, Hong Kong, China, Jun. 2015, extended version available at http://arxiv.org/abs/1501.07439.

H. Boche, R. F. Schaefer, and H. V. Poor, ''On the Continuity of the Secrecy Capacity of Compound and Arbitrarily Varying Wiretap Channels,'' *under submission, revised Mar. 2015*, available online at http://arxiv.org/abs/1409.4752.