Super-Activation as a Unique Feature of Arbitrarily Varying Wiretap Channels

Rafael Schaefer

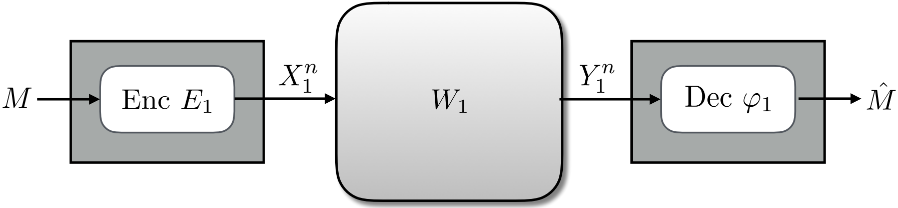
TU BERLIN

joint work with Holger Boche (TU München)
and H. Vincent Poor (Princeton University)

2016 IEEE International Symposium on Information Theory

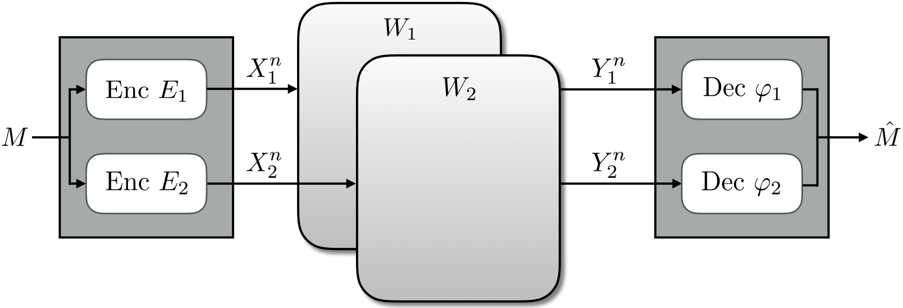
July 15, 2016

Capacity of DMC



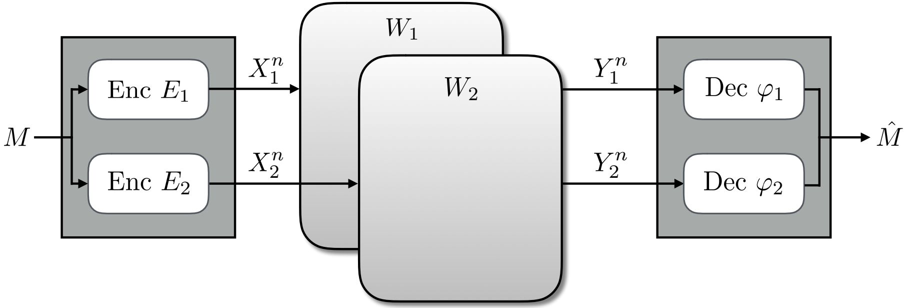
- Capacity: $C(W_1)$

Capacity of Orthogonal DMCs



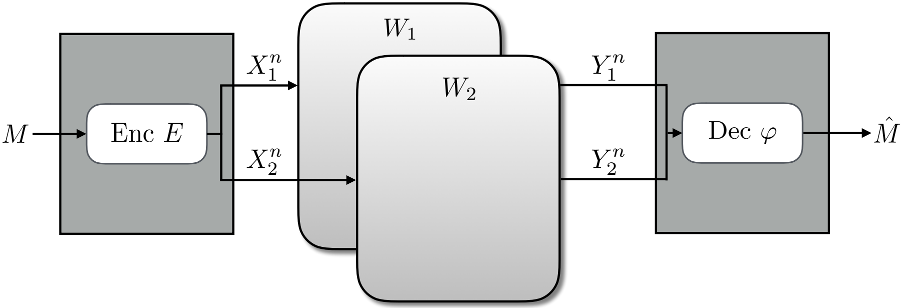
- Independent encoding/decoding: $C(W_1) + C(W_2)$

Capacity of Orthogonal DMCs



- Independent encoding/decoding: $C(W_1) + C(W_2)$

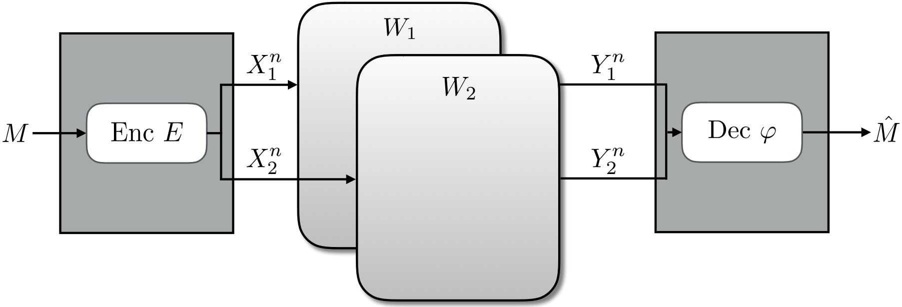
Capacity of Orthogonal DMCs



- Independent encoding/decoding: $C(W_1) + C(W_2)$
- Joint encoding/decoding: $C(W_1 \otimes W_2)$

$$C(W_1 \otimes W_2) = C(W_1) + C(W_2)$$

Capacity of Orthogonal DMCs



- Independent encoding/decoding: $C(W_1) + C(W_2)$
- Joint encoding/decoding: $C(W_1 \otimes W_2)$

$$C(W_1 \otimes W_2) = C(W_1) + C(W_2)$$

Zero Error Capacity

- Shannon conjectured the zero-error capacity to be additive:

$$C_0(W_1 \otimes W_2) \stackrel{?}{=} C_0(W_1) + C_0(W_2)$$

Theorem 4, of course, is analogous to known results for ordinary capacity C, where the product channel has the sum of the ordinary capacities and the sum channel has an equivalent number of letters equal to the sum of the equivalent numbers of letters for the individual channels. We conjecture but have not been able to prove that the equalities in Theorem 4 hold in general, not just under the conditions given.

C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956

Zero Error Capacity and AVCs

- Later disproved constructing explicit counter-examples with:

$$C_0(W_1 \otimes W_2) > C_0(W_1) + C_0(W_2)$$

- However, complete characterization is still an open problem

W. Haemers, "On Some Problems of Lovász Concerning the Shannon Capacity of a Graph," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 231–232, Mar. 1979

N. Alon, "The Shannon Capacity of a Union," *Combinatorica*, vol. 18, no. 3, pp. 301–310, Mar. 1998

- Zero error capacity and arbitrarily varying channels (AVCs) are related

R. Ahlswede, "A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity," *Ann. Math. Stat.*, vol. 41, no. 3, pp. 1027–1033, 1970

Worth to study this additivity problem in the context of AVCs!

Zero Error Capacity and AVCs

- Later disproved constructing explicit counter-examples with:

$$C_0(W_1 \otimes W_2) > C_0(W_1) + C_0(W_2)$$

- However, complete characterization is still an open problem

W. Haemers, "On Some Problems of Lovász Concerning the Shannon Capacity of a Graph," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 231–232, Mar. 1979

N. Alon, "The Shannon Capacity of a Union," *Combinatorica*, vol. 18, no. 3, pp. 301–310, Mar. 1998

- Zero error capacity and arbitrarily varying channels (AVCs) are related

R. Ahlswede, "A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity," *Ann. Math. Stat.*, vol. 41, no. 3, pp. 1027–1033, 1970

Worth to study this additivity problem in the context of AVCs!

Zero Error Capacity and AVCs

- Later disproved constructing explicit counter-examples with:

$$C_0(W_1 \otimes W_2) > C_0(W_1) + C_0(W_2)$$

- However, complete characterization is still an open problem

W. Haemers, "On Some Problems of Lovász Concerning the Shannon Capacity of a Graph," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 231–232, Mar. 1979

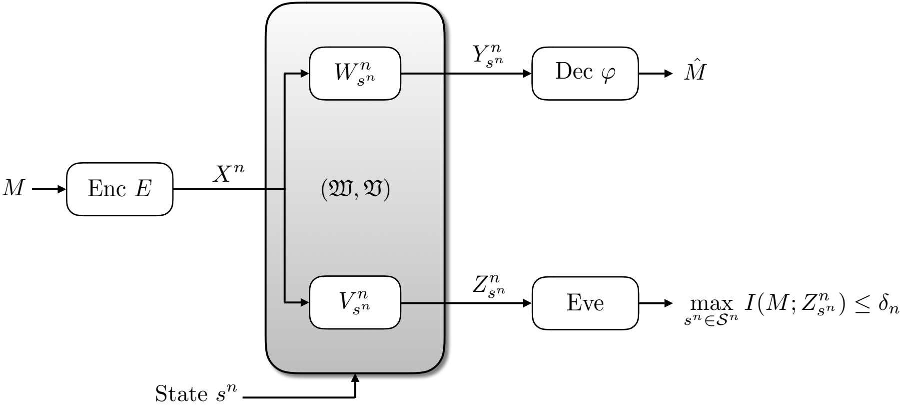
N. Alon, "The Shannon Capacity of a Union," *Combinatorica*, vol. 18, no. 3, pp. 301–310, Mar. 1998

- Zero error capacity and arbitrarily varying channels (AVCs) are related

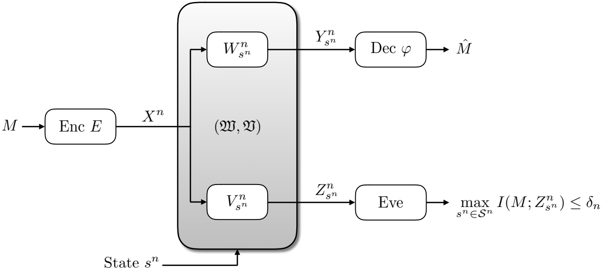
R. Ahlswede, "A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity," *Ann. Math. Stat.*, vol. 41, no. 3, pp. 1027–1033, 1970

➠ **Worth to study this additivity problem in the context of AVCs!**

Arbitrarily Varying Wiretap Channel



Arbitrarily Varying Wiretap Channel

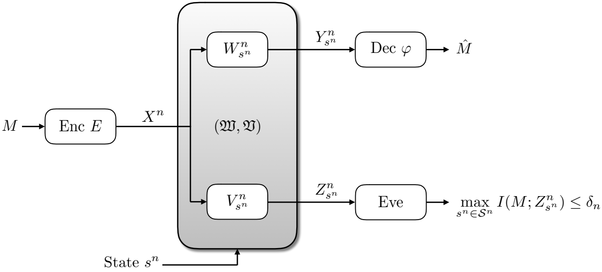


- **Uncertainty set $\mathcal{S}$**
  - actual state sequence $s^n \in \mathcal{S}^n$ unknown to Alice and Bob
  - channel may vary in an unknown and arbitrary manner

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

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

Arbitrarily Varying Wiretap Channel



➠ We want universal codes which work for **all possible state sequences simultaneously** (not depending on specific $s^n \in \mathcal{S}^n$)!

- Traditional code $\mathcal{C}$ (pre-determined):
  - Stochastic encoder $E : \mathcal{M}_n \to \mathcal{P}(\mathcal{X}^n)$
  - Deterministic decoder: $\varphi : \mathcal{Y}^n \to \mathcal{M}_n$

Symmetrizability

- For symmetrizable AVCs it turns out that traditional codes $\mathcal{C}$ are not sufficient...

***Definition:* Symmetrizability**

An AVC is symmetrizable if for some channel $\sigma : \mathcal{X} \to \mathcal{P}(\mathcal{S})$

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

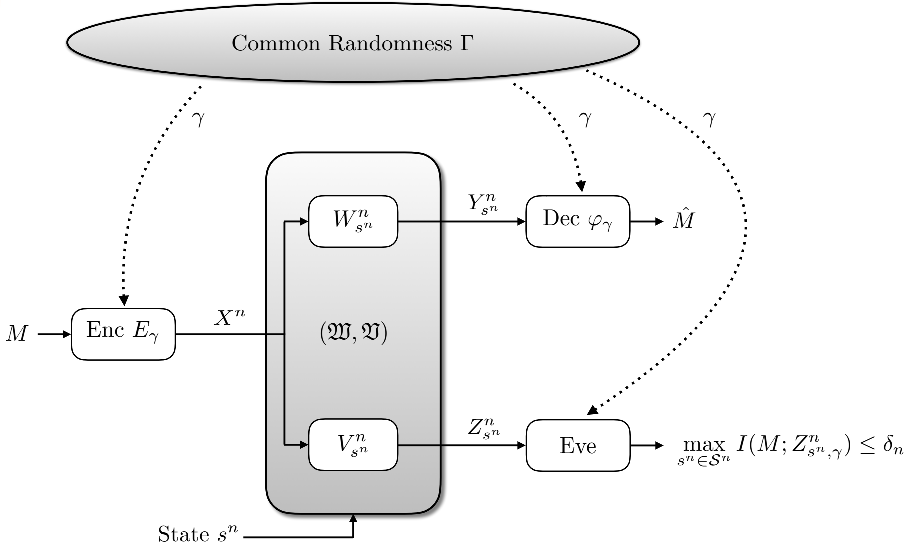
holds for every $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$.

- This means $\widetilde{W}(y|x,x') = \sum_{s\in\mathcal{S}} W(y|x,s)\sigma(s|x')$ is symmetric in x, x'!
  - ➠ State sequence can emulate a valid channel input

➠ **Capacity is zero although entropic quantities are non-zero!**

➠ Need of more **sophisticated** coding strategies!

Common Randomness



CR-Assisted Secrecy Capacity

Theorem: CR-Assisted Secrecy Capacity

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

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

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

M. Wiese, J. Nötzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack–correlated random coding capacities under strong secrecy criteria," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3844–3862, Jul. 2016

Unassisted Secrecy Capacity

Theorem: Unassisted Secrecy Capacity

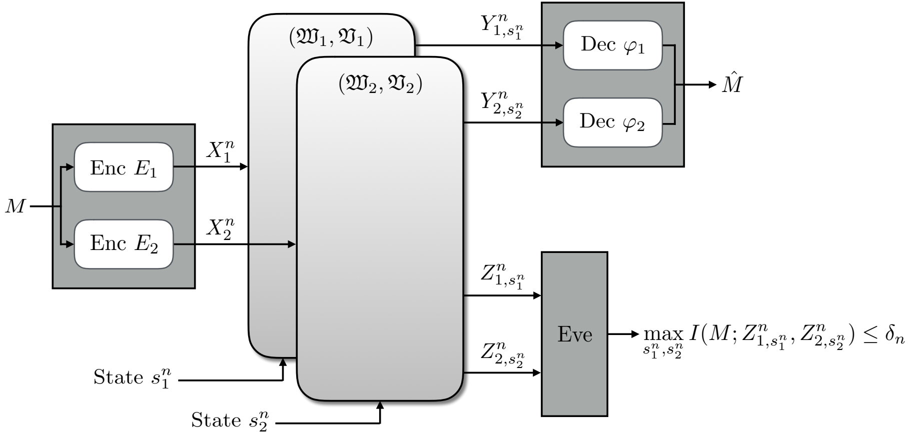
The unassisted secrecy capacity $C_S(\mathfrak{W}, \mathfrak{V})$ of the AVWC $(\mathfrak{W}, \mathfrak{V})$ possesses the following symmetrizability properties:

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

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

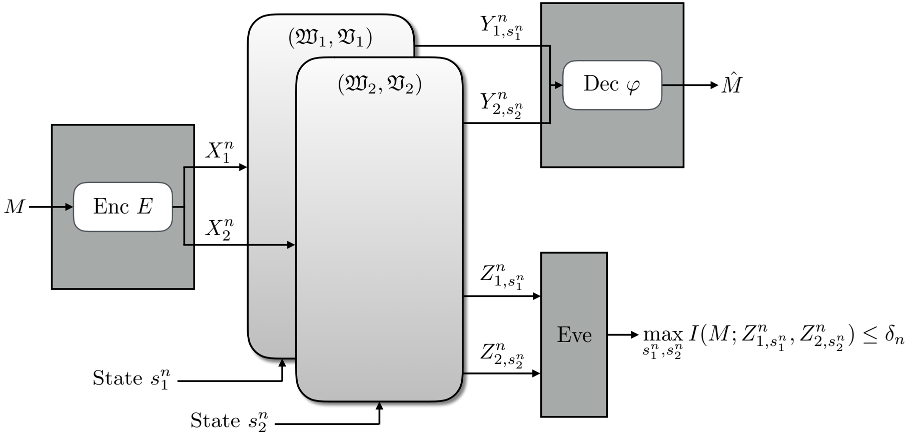
J. Nötzel, M. Wiese, and H. Boche, "The Arbitrarily Varying Wiretap Channel–Secret Randomness, Stability and Super-Activation," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, Jun. 2016

Parallel Use of AVWCs



➠ Independent encoders and decoders for each AVWC

Joint Use of AVWCs



Do we benefit from joint encoding and decoding?

Super-Activation

Theorem: Super-Activation

Let $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ be two orthogonal AVWCs. We have:

1. If $C_S(\mathfrak{W}_1, \mathfrak{V}_1) = C_S(\mathfrak{W}_2, \mathfrak{V}_2) = 0$, then

$$C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$$

   if and only if $\mathfrak{W}_1 \otimes \mathfrak{W}_2$ is non-symmetrizable and $C_{S,\text{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) > 0$. If $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$ can be super-activated it holds

$$\boldsymbol{C_S(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2) = C_{S,\text{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2, \mathfrak{V}_1 \otimes \mathfrak{V}_2)}.$$

2. If $C_{S,\text{CR}}$ shows no super-activation for $(\mathfrak{W}_1, \mathfrak{V}_1)$ and $(\mathfrak{W}_2, \mathfrak{V}_2)$, then super-activation of C_S can only happen if $\mathfrak{W}_1$ is non-symmetrizable and $\mathfrak{W}_2$ is symmetrizable and $C_{S,\text{CR}}(\mathfrak{W}_1, \mathfrak{V}_1) = 0$ and $C_{S,\text{CR}}(\mathfrak{W}_2, \mathfrak{V}_2) > 0$.

H. Boche and R. F. Schaefer, "Capacity Results and Super-Activation for Wiretap Channels with Active Wiretappers," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1482–1496, Sep. 2013

J. Nötzel, M. Wiese, and H. Boche, "The Arbitrarily Varying Wiretap Channel–Secret Randomness, Stability and Super-Activation," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, Jun. 2016

Properties

- Further properties:
  1. Robust - whenever two AVWCs can be super-activated, this is possible for all channels that are sufficiently close
  2. Super-activation depends only on the legitimate AVC and not on the eavesdropper AVC

➠ Details are in the paper

R. F. Schaefer, H. Boche, and H. V. Poor, "Super-Activation as a Unique Feature of Arbitrarily Varying Wiretap Channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, Jul. 2016

——, "Super-Activation as a Unique Feature of Secure Communication in Malicious Environments," *Information - Special Issue "Physical Layer Security in Wireless Networks"*, vol. 7, no. 2, p. 24, May 2016, invited

Is this also possible for public (non-secure) communication over AVCs?

Properties

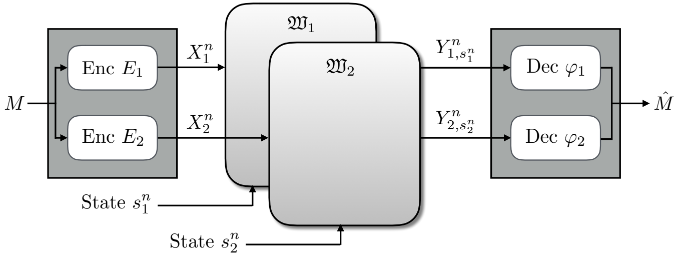
- Further properties:
  1. Robust - whenever two AVWCs can be super-activated, this is possible for all channels that are sufficiently close
  2. Super-activation depends only on the legitimate AVC and not on the eavesdropper AVC

➠ Details are in the paper

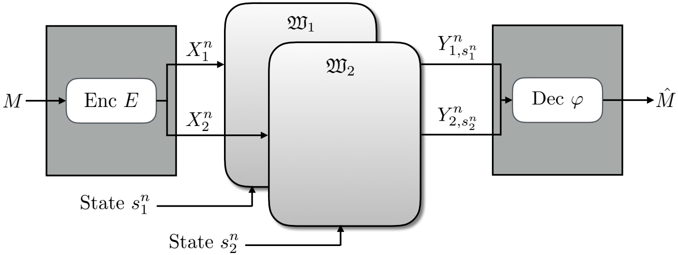
- R. F. Schaefer, H. Boche, and H. V. Poor, "Super-Activation as a Unique Feature of Arbitrarily Varying Wiretap Channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, Jul. 2016
- ——, "Super-Activation as a Unique Feature of Secure Communication in Malicious Environments," *Information - Special Issue "Physical Layer Security in Wireless Networks"*, vol. 7, no. 2, p. 24, May 2016, invited

Is this also possible for public (non-secure) communication over AVCs?

Arbitrarily Varying Channel



vs



Additivity of CR-Assisted Capacity

Theorem: CR-Assisted Capacity

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. Then the CR-assisted capacity is additive, i.e.,

$$C_{\mathsf{CR}}(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C_{\mathsf{CR}}(\mathfrak{W}_1) + C_{\mathsf{CR}}(\mathfrak{W}_2)$$

- CR-assisted capacity additive, i.e., no gain in capacity by joint encoding and decoding

Unassisted Capacity

Proposition: Additivity

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) > 0$ and $C(\mathfrak{W}_2) > 0$, then the unassisted capacity is additive, i.e.,

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C(\mathfrak{W}_1) + C(\mathfrak{W}_2)$$

Proposition: Additivity

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) = C(\mathfrak{W}_2) = 0$, then the unassisted capacity is additive, i.e.,

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C(\mathfrak{W}_1) + C(\mathfrak{W}_2)$$

➠ **Super-activation not possible!**

Unassisted Capacity

Proposition: Additivity

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) > 0$ and $C(\mathfrak{W}_2) > 0$, then the unassisted capacity is additive, i.e.,

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C(\mathfrak{W}_1) + C(\mathfrak{W}_2)$$

Proposition: Additivity

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. If the unassisted capacities satisfy $C(\mathfrak{W}_1) = C(\mathfrak{W}_2) = 0$, then the unassisted capacity is additive, i.e.,

$$C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) = C(\mathfrak{W}_1) + C(\mathfrak{W}_2)$$

➠ **Super-activation not possible!**

Unassisted Capacity (2)

***Theorem:* Super-Additivity**

Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two orthogonal AVCs. The unassisted capacity $C(\mathfrak{W}_1 \otimes \mathfrak{W}_2)$ is super-additive, i.e.,

$$\boldsymbol{C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) > C(\mathfrak{W}_1) + C(\mathfrak{W}_2)}$$

if and only if either of **$\mathfrak{W}_1$ or $\mathfrak{W}_2$ is symmetrizable** and has a positive CR-assisted capacity.

Without loss of generality, let $\mathfrak{W}_1$ be symmetrizable; then

$$\begin{aligned} C(\mathfrak{W}_1 \otimes \mathfrak{W}_2) &= C_{CR}(\mathfrak{W}_1) + C(\mathfrak{W}_2) \\ &> C(\mathfrak{W}_1) + C(\mathfrak{W}_2) = C(\mathfrak{W}_2). \end{aligned}$$

Conclusions

Studied the question of additivity of capacity

➠ Non-trivial in general

Arbitrarily varying channel (AVC)

- CR-assisted capacity is additive
- Unassisted capacity is **super-additive**
- Provided complete characterization

Arbitrarily varying wiretap channel (AVWC)

- Unassisted secrecy capacity is non-additive

➠ **Super-activation is possible, i.e., "$0 + 0 > 0$"**

Thank you for your attention!

Conclusions

Studied the question of additivity of capacity

➠ Non-trivial in general

Arbitrarily varying channel (AVC)

- CR-assisted capacity is additive
- Unassisted capacity is **super-additive**
- Provided complete characterization

Arbitrarily varying wiretap channel (AVWC)

- Unassisted secrecy capacity is non-additive

➠ **Super-activation is possible, i.e., "$0+0>0$"**

Thank you for your attention!

Conclusions

Studied the question of additivity of capacity

➠ Non-trivial in general

Arbitrarily varying channel (AVC)

- CR-assisted capacity is additive
- Unassisted capacity is **super-additive**
- Provided complete characterization

Arbitrarily varying wiretap channel (AVWC)

- Unassisted secrecy capacity is non-additive

➠ **Super-activation is possible, i.e.,** "$0 + 0 > 0$"

Thank you for your attention!

Conclusions

Studied the question of additivity of capacity

➠ Non-trivial in general

Arbitrarily varying channel (AVC)

- CR-assisted capacity is additive
- Unassisted capacity is **super-additive**
- Provided complete characterization

Arbitrarily varying wiretap channel (AVWC)

- Unassisted secrecy capacity is non-additive

➠ **Super-activation is possible, i.e., "$0 + 0 > 0$"**

Thank you for your attention!

References I

- C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.
- W. Haemers, "On Some Problems of Lovász Concerning the Shannon Capacity of a Graph," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 231–232, Mar. 1979.
- N. Alon, "The Shannon Capacity of a Union," *Combinatorica*, vol. 18, no. 3, pp. 301–310, Mar. 1998.
- R. Ahlswede, "A Note on the Existence of the Weak Capacity for Channels with Arbitrarily Varying Channel Probability Functions and Its Relation to Shannon's Zero Error Capacity," *Ann. Math. Stat.*, vol. 41, no. 3, pp. 1027–1033, 1970.
- M. Wiese, J. Nötzel, and H. Boche, "A channel under simultaneous jamming and eavesdropping attack–correlated random coding capacities under strong secrecy criteria," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3844–3862, Jul. 2016.
- 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," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3504–3531, Jun. 2016.
- H. Boche and R. F. Schaefer, "Capacity Results and Super-Activation for Wiretap Channels with Active Wiretappers," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1482–1496, Sep. 2013.
- R. F. Schaefer, H. Boche, and H. V. Poor, "Super-Activation as a Unique Feature of Arbitrarily Varying Wiretap Channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, Jul. 2016.
- ——, "Super-Activation as a Unique Feature of Secure Communication in Malicious Environments," *Information - Special Issue "Physical Layer Security in Wireless Networks*", vol. 7, no. 2, p. 24, May 2016, invited.