Comparison of Different Attack Classes in Arbitrarily Varying Wiretap Channels

Holger Boche and Rafael Wyrembelski

Technische Universität München
Lehrstuhl für Theoretische Informationstechnik

WIFS 2012
Oral Session 5: Secure Communications
December 5, 2012

Motivation

- In wireless systems, a transmitted signal is received by its intended users but can also easily be eavesdropped
  - Current systems usually apply cryptographic techniques to keep information secret
  - Becomes more and more insecure due to increasing computational power or improved algorithms

➠ **Information theoretic security** solely uses the physical properties of the wireless channel to establish a higher level of security

- Another problem in practical systems is the uncertainty in channel state information due to
  - the nature of the wireless medium
  - implementational issues
  - attacks of wiretappers

- Establish security under channel uncertainty and attacks

  ➠ In this work: **Arbitrarily varying wiretap channel (AVWC)**

Motivation

- In wireless systems, a transmitted signal is received by its intended users but can also easily be eavesdropped
  - Current systems usually apply cryptographic techniques to keep information secret
  - Becomes more and more insecure due to increasing computational power or improved algorithms

➠ **Information theoretic security** solely uses the physical properties of the wireless channel to establish a higher level of security

- Another problem in practical systems is the uncertainty in channel state information due to
  - the nature of the wireless medium
  - implementational issues
  - attacks of wiretappers

- Establish security under channel uncertainty and attacks

  ➠ In this work: **Arbitrarily varying wiretap channel (AVWC)**

Motivation

- In wireless systems, a transmitted signal is received by its intended users but can also easily be eavesdropped
  - Current systems usually apply cryptographic techniques to keep information secret
  - Becomes more and more insecure due to increasing computational power or improved algorithms

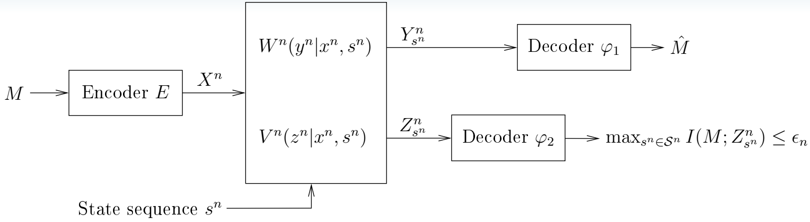
➠ **Information theoretic security** solely uses the physical properties of the wireless channel to establish a higher level of security

- Another problem in practical systems is the uncertainty in channel state information due to
  - the nature of the wireless medium
  - implementational issues
  - attacks of wiretappers

- Establish security under channel uncertainty and attacks

  ➠ In this work: **Arbitrarily varying wiretap channel (AVWC)**

Arbitrarily Varying Wiretap Channel



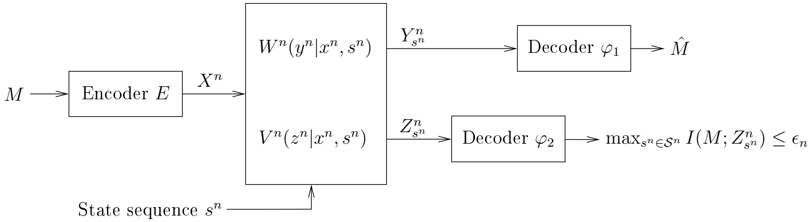
For **fixed state sequence** $s^n \in \mathcal{S}^n$ the channels are

$$W^n(y^n|x^n, s^n) = \prod_{i=1}^n W(y_i|x_i, s_i) \quad \text{and} \quad V^n(z^n|x^n, s^n) = \prod_{i=1}^n V(z_i|x_i, s_i)$$

The **arbitrarily varying channels (AVCs)** to the legitimate receiver and wiretapper are the collections

$$\mathcal{W} = \{W^n(\cdot|\cdot, s^n) : s^n \in \mathcal{S}^n\} \quad \text{and} \quad \mathcal{V} = \{V^n(\cdot|\cdot, s^n) : s^n \in \mathcal{S}^n\}$$

Arbitrarily Varying Wiretap Channel (2)

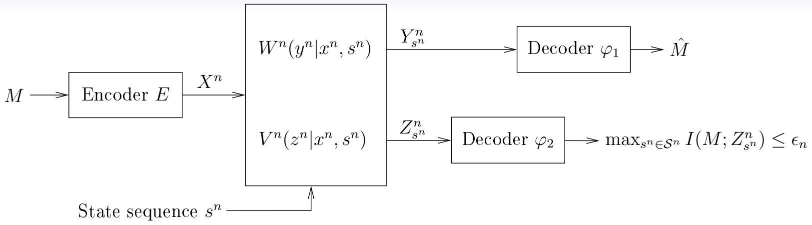


The **arbitrarily varying wiretap channel (AVWC)** is given by

$$\mathfrak{W} = \Big\{ \big(W^n(\cdot|\cdot, s^n), V^n(\cdot|\cdot, s^n) \big) : s^n \in \mathcal{S}^n \Big\}$$

Task: Establish reliable communication to the legitimate receiver in the presence of unknown varying channel conditions and, at the same time, keeping the information secret from the wiretapper.

Strong Secrecy Criterion

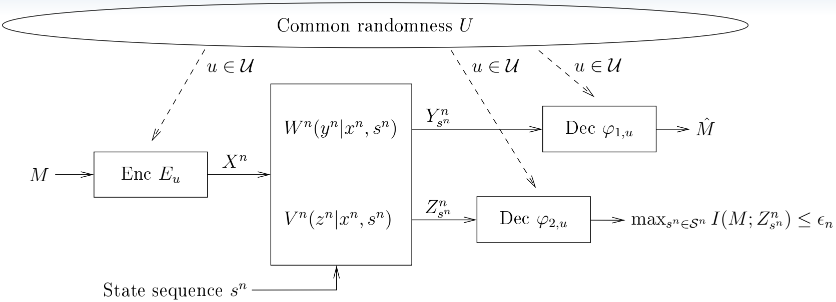


- Total amount of information leaked to receiver 2 has to be small for all $s^n \in \mathcal{S}^n$ simultaneously
  - **Strong secrecy** requirement on M, i.e.,

$$\max_{s^n \in \mathcal{S}^n} I(M; Z^n_{s^n}) \leq \epsilon_n$$

- Strong secrecy can be given an operational meaning:
  - **Average decoding error** at wiretapper goes to 1!

Role of Common Randomness

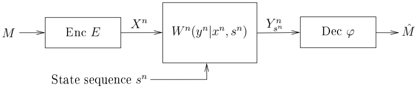


- Assume all parties (legitimate users AND wiretapper) have access to common randomness (CR)
  - ➠ Can be realized over a public channel open to everyone

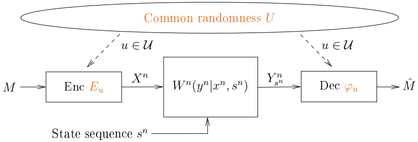
- (If wiretapper would have no access, CR can be used to create a secret key keeping wiretapper completely ignorant)

Ordinary AVCs

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



deterministic capacity $C_{\text{det}}(\mathcal{W}) = 0$



random capacity $C_{\text{ran}}(\mathcal{W}) > 0$!

- 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 $y \in \mathcal{Y}$.

Ordinary AVCs (2)

Random code capacity

$$C_{\text{ran}}(\mathcal{W}) = \max_{p \in \mathcal{P}(\mathcal{X})} \min_{q \in \mathcal{P}(\mathcal{S})} I(p, W_q)$$

with $W_q(y|x) = \sum_{s \in \mathcal{S}} W(y|x,s)q(s)$.

Deterministic code capacity (*Ahlswede's dichotomy*)

$$C_{\text{det}}(\mathcal{W}) = \begin{cases} C_{\text{ran}}(\mathcal{W}) & \text{if } \mathcal{W} \text{ is non-symmetrizable} \\ 0 & \text{if } \mathcal{W} \text{ is symmetrizable} \end{cases}$$

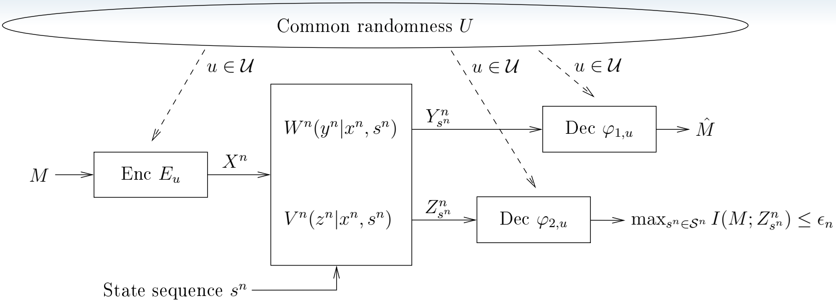
➡ **Common randomness** is an important resource to establish reliable communication over arbitrarily varying channels

- R. Ahlswede, ''Elimination of Correlation in Random Codes for Arbitrarily Varying Channels,'' *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978
- I. Csiszár and P. Narayan, ''The Capacity of the Arbitrarily Varying Channel Revisited: Positivity, Constraints,'' *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988

Question

What is the impact of common randomness on the behavior and the strategies of potential wiretappers?

Passive Wiretappers



- **Passive wiretapper**
  - Does **not** exploit CR
  - Does **not** influence the channel conditions

  ➡ State sequence only reflects the influence of channel uncertainty and, in particular, does **not** depend on CR!

➡ Strategy: Simply tries to eavesdrop the communication

- $C_{S,\mathrm{ran}}(\mathfrak{W})$ is CR assisted secrecy capacity of the AVWC $\mathfrak{W}$

Passive Secrecy Capacity

- If CR is available, legitimate users can coordinate their choice of encoder and decoder based on CR

Theorem: CR assisted secrecy capacity

Under the assumption of a best channel to the wiretapper, for the CR assisted secrecy capacity $C_{S,\text{ran}}(\mathfrak{W})$ of the AVWC $\mathfrak{W}$ with passive wiretapper it holds

$$C_{S,\text{ran}}(\mathfrak{W}) \geq \max_{p\in\mathcal{P}(\mathcal{X})} \Big(\min_{q\in\mathcal{P}(\mathcal{S})} I(p, W_q) - \max_{q\in\mathcal{P}(\mathcal{S})} I(p, V_q) \Big)$$

with $W_q(y|x) = \sum_{s\in\mathcal{S}} W(y|x,s)q(s)$ and $V_q(z|x) = \sum_{s\in\mathcal{S}} V(z|x,s)q(s)$.

- I. Bjelaković, H. Boche, and J. Sommerfeld, ''Strong Secrecy in Arbitrarily Varying Wiretap Channels,'' in *Proc. IEEE Inf. Theory Workshop*, Lausanne, Switzerland, Sep. 2012
- ——, ''Capacity Results for Arbitrarily Varying Wiretap Channels,'' will be published in Springer LNCS in Memory of Rudolf Ahlswede

Passive Secrecy Capacity (2)

- If CR is not available, deterministic codes are needed

Theorem: Deterministic secrecy capacity

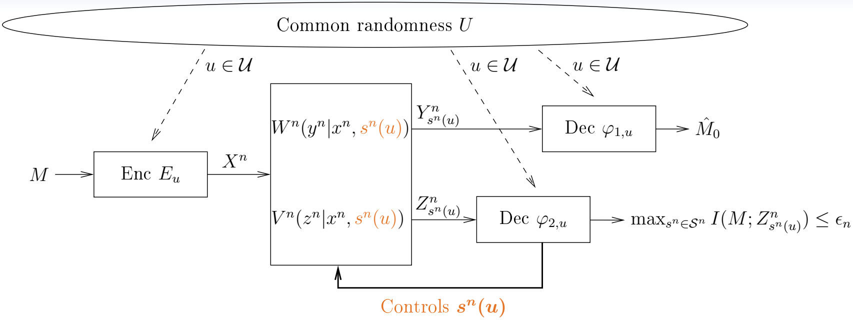
If $C_{S,\mathrm{ran}}(\mathfrak{W}) > 0$, then the deterministic code secrecy capacity is given by

$$C_S(\mathfrak{W}) = C_{S,\mathrm{ran}}(\mathfrak{W})$$

if and only if the AVC $\mathcal{W}$ is non-symmetrizable.

If AVC $\mathcal{W}$ is symmetrizable, then $C_S(\mathfrak{W}) = 0$.
If $C_S(\mathfrak{W}) = 0$ and $C_{S,\mathrm{ran}}(\mathfrak{W}) > 0$, then AVC $\mathcal{W}$ is symmetrizable.

Active Wiretappers

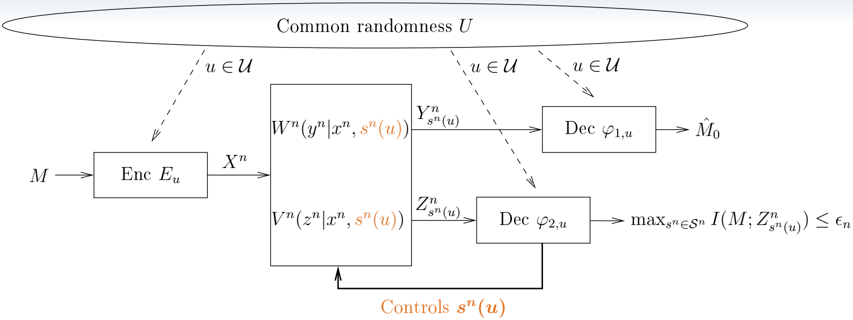


- **Active wiretapper**
  - **Exploits CR** to influence the channel conditions

  ➡ State sequence depends on CR!

➡ Includes jamming models where the wiretapper acts as a jammer!

Active Wiretappers (2)



Different strategies possible:

- try to maximize information leaked to him
- try to disturb the communication between legitimate users
- (and anything in between)

- $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ is CR assisted secrecy capacity of the AVWC $\mathfrak{W}$ with active wiretapper

Positive Active Secrecy Capacity

Theorem: Positive Active Secrecy Capacity

If $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) > 0$, then

$$C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = C_{S,\text{ran}}(\mathfrak{W})$$

Proof idea: Inspired by *random code reduction* and *elimination of correlation* techniques for ordinary AVCs

- Use (for a negligible part of transmission) a passive code to indicate which active code is used in the following!

- If active secrecy capacity is positive, an active wiretapper is as effective as a passive wiretapper
- Strategy must be to **destroy communication of legitimate users**, i.e., $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$!

Zero Active Secrecy Capacity (2)

- Study the case $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$ in the following

Theorem:

Let $C_{S,\text{ran}}(\mathfrak{W}) > 0$. We have $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W}) = 0$ if and only if AVC $\mathcal{W}$ is symmetrizable.

- Active secrecy capacity $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ displays a dichotomy behavior:

➡ It either equals the passive secrecy capacity $C_{S,\text{ran}}(\mathfrak{W})$ or else is zero!

➡ Can be completely characterized in terms of symmetrizability

➡ Depends only on the legitimate users' channel $\mathcal{W}$!

Conclusion

- Studied **arbitrarily varying wiretap channels (AVWCs)**
  - Passive wiretappers
  - Active wiretappers who exploit CR to control the state sequence

- For active wiretappers, CR is **useless**

  ➡ $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ displays dichotomy behavior similarly as for deterministic codes!

- For passive wiretappers, CR is **useful**

  ➡ Can lead to significant gains compared to deterministic codes!

Thank you for your attention!

Conclusion

- Studied **arbitrarily varying wiretap channels (AVWCs)**
  - Passive wiretappers
  - Active wiretappers who exploit CR to control the state sequence

- For active wiretappers, CR is **useless**
  - ➠ $C_{S,\mathrm{ran}}^{\mathrm{active}}(\mathfrak{W})$ displays dichotomy behavior similarly as for deterministic codes!

- For passive wiretappers, CR is **useful**
  - ➠ Can lead to significant gains compared to deterministic codes!

Thank you for your attention!

Conclusion

- Studied **arbitrarily varying wiretap channels (AVWCs)**
  - Passive wiretappers
  - Active wiretappers who exploit CR to control the state sequence

- For active wiretappers, CR is **useless**

  ➡ $C_{S,\text{ran}}^{\text{active}}(\mathfrak{W})$ displays dichotomy behavior similarly as for deterministic codes!

- For passive wiretappers, CR is **useful**

  ➡ Can lead to significant gains compared to deterministic codes!

Thank you for your attention!

References I

- R. Ahlswede, ‘‘Elimination of Correlation in Random Codes for Arbitrarily Varying Channels,’’ *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978.
- I. Csiszár and P. Narayan, ‘‘The Capacity of the Arbitrarily Varying Channel Revisited: Positivity, Constraints,’’ *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.
- I. Bjelaković, H. Boche, and J. Sommerfeld, ‘‘Strong Secrecy in Arbitrarily Varying Wiretap Channels,’’ in *Proc. IEEE Inf. Theory Workshop*, Lausanne, Switzerland, Sep. 2012.
- ——, ‘‘Capacity Results for Arbitrarily Varying Wiretap Channels,’’ will be published in Springer LNCS in Memory of Rudolf Ahlswede.