The Arbitrarily Varying Wiretap Channel – Communication under Uncoordinated Attacks

Moritz Wiese, Janis Nötzel, Holger Boche

Royal Institute of Technology (KTH)/Technische Universität München

ISIT 2015, Hong Kong – June 18

Work supported by German Research Foundation project
DFG Bo 1734/20-1

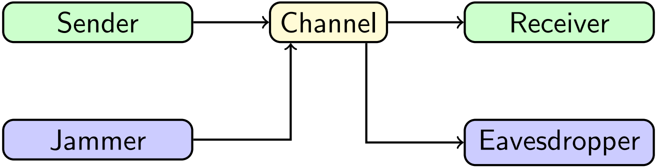
Outline

Two kinds of attacks are the most investigated in information theoretic security:

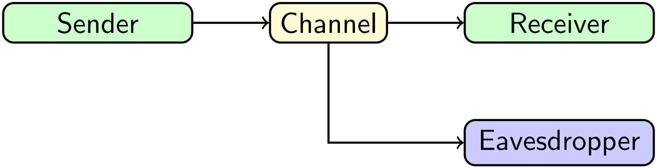
- **passive:** an eavesdropper overhears communication $\rightsquigarrow$ wiretap channel,
- **active:** a jammer tries to destroy communication (DoS) $\rightsquigarrow$ arbitrarily varying channel (AVC).

Question: What if both happen simultaneously?

Arbitrarily varying wiretap channel (AVWC)

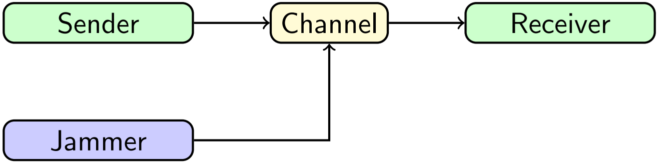


Discrete memoryless wiretap channel



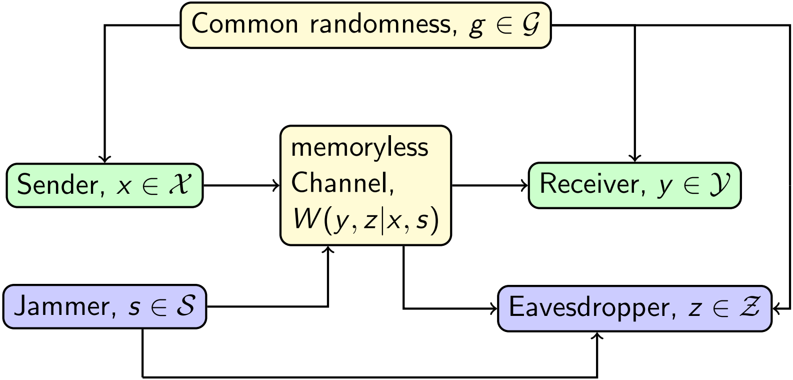
- various secrecy criteria possible
  - mutual information based
  - total variation distance based
  - ...
- stochastic encoding allowed
- common randomness shared by sender and receiver does not bring any advantage

Arbitrarily varying channel



- the jammer does not know the message to be sent nor channel input or output
- sender and receiver do not know the jammer's channel input
- capacity without common randomness shared by sender and receiver equals
  - either common randomness assisted capacity
  - or zero

  (Ahlswede dichotomy, 1978).



- The arrows from CR and jammer to eavesdropper increase the secrecy requirements!
- Jammer and eavesdropper know channel and code, but not the realizations of message nor stochastic encoding.

A code with blocklength n and rate R consists of

- **common randomness (CR):**

  a set $\mathcal{G}$ and a probability distribution μ on $\mathcal{G}$

- **message** M uniformly distributed on $\mathcal{M} = \{1, \ldots, \lfloor 2^{nR} \rfloor\}$,
- the **encoder**: a stochastic matrix

$$E(x^n|m, g) \qquad (x^n \in \mathcal{X}^n, m \in \mathcal{M}, g \in \mathcal{G})$$

- the **decoding function**

$$\varphi : \mathcal{Y}^n \times \mathcal{G} \longrightarrow \mathcal{M}.$$

Secrecy criterion 1:

$$\max_{s^n \in \mathcal{S}^n} \max_{g \in \mathcal{G}} I(M \wedge Z_{s^n,g}) \quad \text{vanish asymptotically}$$

Secrecy criterion 2:

$$\max_{s^n \in \mathcal{S}^n} I(M \wedge Z_{s^n,G} | G) \quad \text{vanish asymptotically}$$

Secrecy criterion 3:

$$\max_{s^n \in \mathcal{S}^n} \max_{g \in \mathcal{G}} \| P_{MZ_{s^n,g}} - P_M P_{Z_{s^n,g}} \| \quad \text{vanish asymptotically}$$

$P_{MZ_{s^n,g}}$ the joint distribution of message and eavesdropper's output induced by the code given jammer's input s^n and CR realization g.

Theorem: Under the average error criterion for reliable transmission, the capacity of the AVWC under all three above secrecy criteria equals

$$\lim_{n\to\infty}\frac{1}{n}\max_{\mathcal{I}}\Big(\min_{q\in\mathcal{P}(\mathcal{S})} I(U\wedge Y_q^n)-\max_{s^n\in\mathcal{S}^n} I(U\wedge Z_{s^n}^n)\Big).$$

Here

$$\mathcal{I}:=\{U-X^n-Y_q^nZ_{S^n}^n : q\in\mathcal{P}(\mathcal{S}), s^n\in\mathcal{S}^n, U \text{ finite},$$
$$P_{Y_q^n|X^n}(y^n|x^n)=W_q^n(y^n|x^n),\quad P_{Z^n|X^n}(y^n|x^n)=W^n(z^n|x^n,s^n).\}$$

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

Simplest method of getting tight AVC results **(non-secret)**:

Ahlswede's "robustification technique". Let (E,φ) be a code without CR and assume

$$\max_{q\in\mathcal{P}(\mathcal{S})}\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{x^n\in\mathcal{X}^n}E(x^n|m)W_q^n(\varphi(m)^{-1}|x^n)\geq 1-\varepsilon.$$

Then

$$\max_{s^n\in\mathcal{S}^n}\frac{1}{n!|\mathcal{M}|}\sum_{\pi}\sum_{\substack{m\in\mathcal{M},\\ x^n\in\mathcal{X}^n}}E(\pi x^n|m)W^n(\pi\varphi(m)^{-1}|\pi x^n,s^n)\geq 1-\varepsilon'.$$

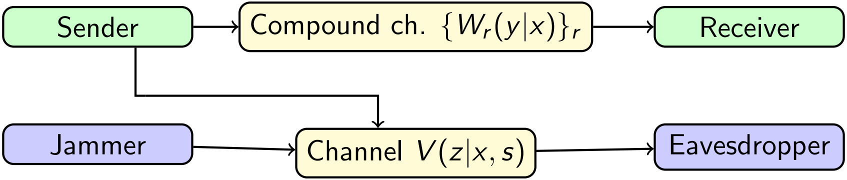
ε' is polynomially in n larger than ε.

For the AVWC, robustification cannot be done naively:

- The secrecy criteria cannot in general be controlled this way.
- Previous approaches to special cases by [Bjelaković et al., 2013] and [MolavianJazi et al., 2009].

Solution: introduce new channel **CAVWC**:

- Compound from sender to receiver,
- AVC from sender to eavesdropper.



Secrecy results for the CAVWC can be "robustified".

Theorem: The secrecy capacity of the CAVWC without CR under the average error criterion equals

$$\lim_{n\to\infty} \frac{1}{n} \max_{\mathcal{I}} \Big(\min_{r\in\mathcal{R}} I(U \wedge Y_r^n) - \max_{s^n\in\mathcal{S}^n} I(U \wedge Z_{s^n}^n) \Big).$$

The average error tends to zero at exponential speed (important for robustification).

Achievability, reliable transmission: Random coding for a code with message set $\mathcal{M} \times \mathcal{L}$.

$$\frac{1}{n}\log|\mathcal{M}| = \min_{r\in\mathcal{R}} I(X \wedge Y_r) - \max_{q\in\mathcal{P}(\mathcal{S})} I(X \wedge Z_q) - \varepsilon_1,$$
$$\frac{1}{n}\log|\mathcal{L}| = \max_{q\in\mathcal{P}(\mathcal{S})} I(X \wedge Z_q) + \varepsilon_2.$$

Approximation argument because $|\mathcal{R}| = \infty$, [Blackwell et al., 1959].

Achievability, secrecy: How does one ensure secrecy for all possible $|\mathcal{S}|^n$ states?

Encoder

$$E^{\{X_{ml}\}_{m,l}}(x^n|m) = \frac{1}{|\mathcal{L}|}\sum_{l\in\mathcal{L}} 1\{X_{ml} = x^n\}.$$

Using a simple Chernoff bound twice, one shows that

$$\mathbb{P}\left[\|P_{Z_{s^n,\pi}|M}(z^n|m) - P_{Z_{s^n,\pi}}(z^n)\| > 2^{-\alpha n}\right] \longrightarrow 0$$

doubly exponentially for every $m \in \mathcal{M}, s^n \in \mathcal{S}^n$ and permutation π. Therefore

$$\mathbb{P}\left[\bigcup_{m,s^n,\pi} \|P_{Z_{s^n,\pi}|M}(z^n|m) - P_{Z_{s^n,\pi}}(z^n)\| > 2^{-\alpha n}\right] \longrightarrow 0.$$

Thus all three secrecy criteria can be satisfied with probability tending to 1.

Proof idea due to [Devetak, 2005].

- With a natural metric on the set of AVWCs, the CR assisted AVWC capacity discussed here is continuous in the channel.
- What is the AVWC capacity without CR? Is it still continuous?
- What happens if the eavesdropper does not share the CR?