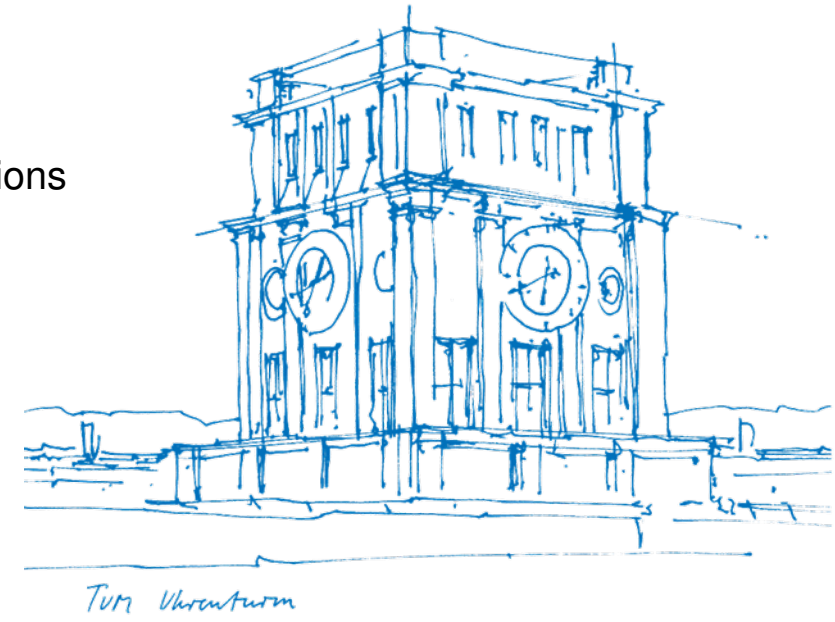
Secure Identification Under Jamming Attacks

Holger Boche[1] and Christian Deppe[2]
Technische Universität München
Department of Electrical and Computer Engineering
[1] Chair of Theoretical Information Technology
[2] Institute for Communications Engineering

IEEE International Workshop on
Signal Processing Advances in Wireless Communications
SPAWC 2018
25-28 June
Kalamata, Greece

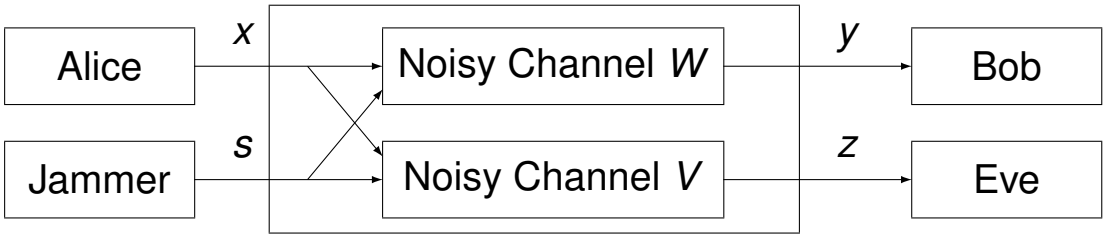


Contents

- Jamming Attacks in Communication Systems
- Basic Communication and Identification
- Basic Secure Communication and Secure Identification
- Impact of Jamming
- Conclusions and Discussions

Jamming Attacks in Communication Systems

- General picture for different communication tasks



- 4 parties with different goals
- Alice and Bob: legimate sender and legimate receiver
  $\Longrightarrow$ They want to solve a communication task.
- Eve: non legimate receiver – wiretapper
  (passive attacks) $\Longrightarrow$ adversarial behavior
- Jammer: chooses jamming sequence as input for channels W and V
  to prevent communication from Alice to Bob.
  support of Eve $\Longrightarrow$ adversarial behavior

The Communication and Identification Task without Jammer

The Classical Communication (Shannon Picture)

- Classical Communication is implemented according to Shannon's 1948 approach
  - Alice has to transmit a message $m \in \mathscr{M} = \{1, 2, \ldots, M\}$ to Bob
  - Alice uses a block code $\mathscr{X}^n = \{0, 1, \ldots, q-1\}^n$
  - $W = \{W(y|x) : x \in \mathscr{X}, y \in \mathscr{Y}\}$ is a stochastic matrix.
  - The probability for a sequence $y \in \mathscr{Y}^n$ to be received if $x^n \in \mathscr{X}^n$:

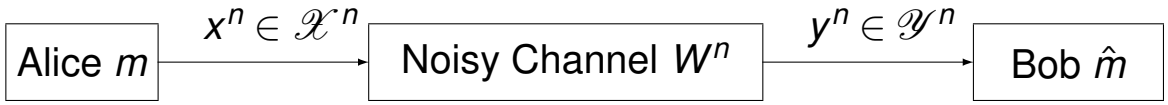
$$W^n(y^n|x^n) = \prod_{t=1}^{n} W(y_t|x_t)$$

  - Bob receives a word in $\mathscr{Y}^n$. For simplification we assume $\mathscr{X} = \mathscr{Y} = \{0, 1\}$.

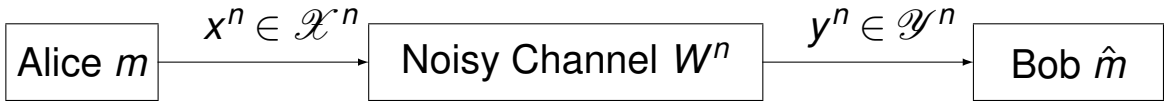
Goal:

Bob has to decode the correct message with a small decoding error
$\Longrightarrow$ Finding the correct answer to: **"What was Alice's message?"**

The Classical Communication (Shannon Picture)



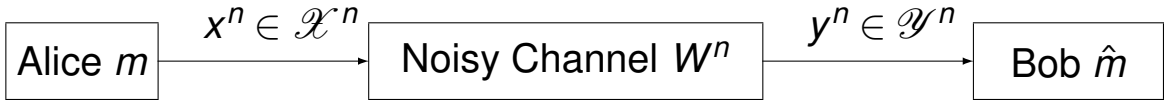
The Classical Communication (Shannon Picture)



Practical Question: What is the largest rate ($R = \frac{\log M}{n}$) of (almost) error free communication from Alice to Bob?

$\Longrightarrow$ Message transmission capacity C

The Classical Communication (Shannon Picture)



Practical Question: What is the largest rate ($R = \frac{\log M}{n}$) of (almost) error free communication from Alice to Bob?

$\Longrightarrow$ Message transmission capacity $C = \max(I(P;W))$

$\Longrightarrow$ Size of message set $|M| = 2^{Cn}$

$$I(X \wedge Y) := H(Y) - H(Y|X)$$

If P is a probability distribution on $\mathscr{X}$ and $W = \{W(y|x) : x \in \mathscr{X}, y \in \mathscr{Y}\}$ a stochastical matrix, we define

$$I(P;W) := I(X \wedge Y)$$

where X is a RV with distribution P and Y has conditional distribution $W(\cdot|x)$ given $X = x$.

Deterministic vs. Random

A (deterministic) (n, M, λ) code for W is a set of pairs $\{(u_i, \mathscr{D}_i) : i \in \mathscr{M}\}$

$$u_i \in \mathscr{X}^n, \mathscr{D}_i \subset \mathscr{Y}^n \quad \text{for all } i \in \mathscr{M} \tag{1}$$

$$\mathscr{D}_i \cap \mathscr{D}_j = \emptyset \text{ for all } 1 \leq i, j \leq n, i \neq j \tag{2}$$

$$W^n(\mathscr{D}_i | u_i) \geq 1 - \lambda \text{ for all } i \in \mathscr{M} \tag{3}$$

A randomized (n, M, λ) code for W is a set of pairs $\{(Q(\cdot|i), \mathscr{D}_i) \mid \text{for all } i \in \mathscr{M}\}$

$$Q(\cdot|i) \in \mathscr{P}(\mathscr{X}^n), \quad \mathscr{D}_i \subset \mathscr{Y}^n \text{ for all } i \in \mathscr{M} \tag{4}$$

$$\mathscr{D}_i \cap \mathscr{D}_j = \emptyset \text{ for all } 1 \leq i, j \leq n, i \neq j \tag{5}$$

$$\sum_{x^n \in \mathscr{X}^n} Q(x^n|i)\, W^n(\mathscr{D}_i | x^n) \geq 1 - \lambda \text{ for all } i \in \mathscr{M} \tag{6}$$

Shannon's Coding Theorem

Theorem (Channel Coding Theorem)

Let $\lambda \in (0,1)$ be fixed. Then

$$\lim_{n\to\infty} \frac{\log M(n,\lambda)}{n} = \max_{P\in\mathscr{P}(\mathscr{X})} I(P,W) \triangleq C \tag{7}$$

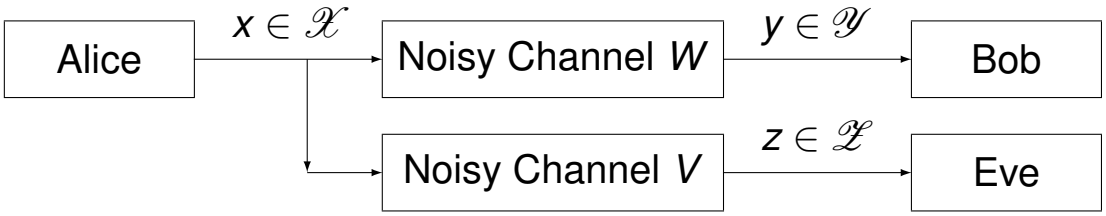
Lemma

Let W be a DMC, $\lambda < 1/2$. A deterministic (n,M,λ) transmission code for W exists if and only if a randomized (n,M,λ) transmission code exists.

Physical Layer Security

- Classical approach to support security in communication systems $\Rightarrow$ separation of communication and encryption $\Rightarrow$ in general no provable security
- New approach: embedded security with information theoretic approach

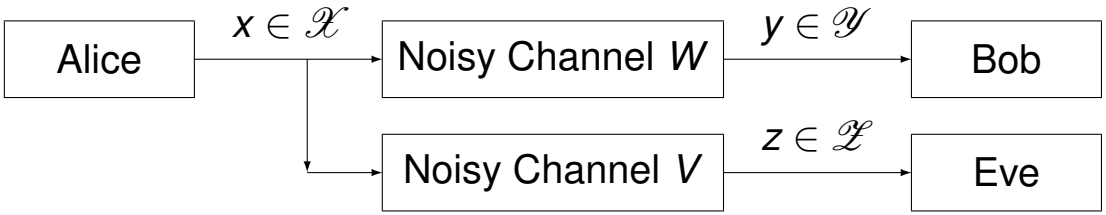
  Goal:
  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob has to decode the correct message with small decoding error
  - Non legitimate receiver Eve is not able to decode the message



Physical Layer Security

- Classical approach to support security in communication systems $\Rightarrow$ separation of communication and encryption $\Rightarrow$ in general no provable security
- New approach: embedded security with information theoretic approach

  Goal:
  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob has to decode the correct message with small decoding error
  - Non legitimate receiver Eve is not able to decode the message



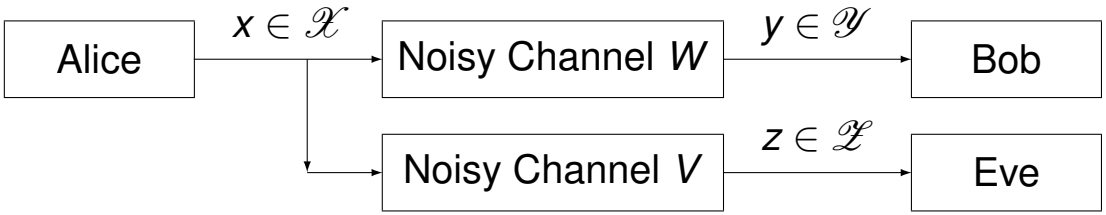
What is the largest rate of (almost) error free secure communication from Alice to Bob?

$\Longrightarrow$ Secure message transmission capacity C_S

Physical Layer Security

- Classical approach to support security in communication systems $\Rightarrow$ separation of communication and encryption $\Rightarrow$ in general no provable security
- New approach: embedded security with information theoretic approach

  Goal:
  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob has to decode the correct message with small decoding error
  - Non legitimate receiver Eve is not able to decode the message



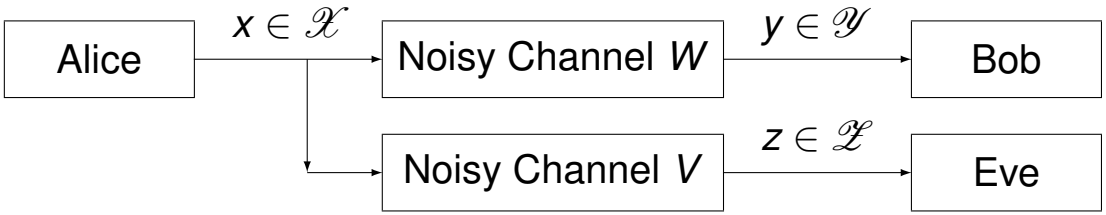
What is the largest rate of (almost) error free secure communication from Alice to Bob?

$\Longrightarrow$ Secure message transmission capacity $C_S = \max(I(U \wedge Y) - I(U \wedge Z))$

Physical Layer Security

- Classical approach to support security in communication systems $\Rightarrow$ separation of communication and encryption $\Rightarrow$ in general no provable security
- New approach: embedded security with information theoretic approach

  Goal:
  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob has to decode the correct message with small decoding error
  - Non legitimate receiver Eve is not able to decode the message



What is the largest rate of (almost) error free secure communication from Alice to Bob?

$\Longrightarrow$ Secure message transmission capacity $C_S = \max(I(U \wedge Y) - I(U \wedge Z))$

Message size $|M| = 2^{C_S n}$ with provable security.

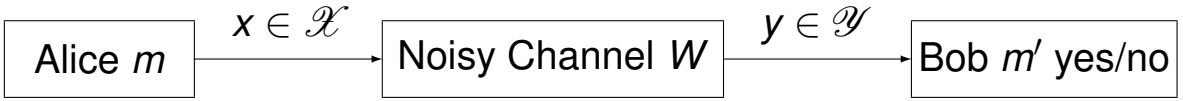
Here a randomized encoding is necessary! The local randomness is absolutely important.

A New Communication Paradigm

- New applications are event-driven, e.g. Industry 4.0, V2X, V2V, ... $\Longrightarrow$ Identification task

  Goal:
  - Alice has to transmit a message $m \in \mathcal{M}$ to Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'

    $\Longrightarrow$ Bob's question: "Is the message m'?"

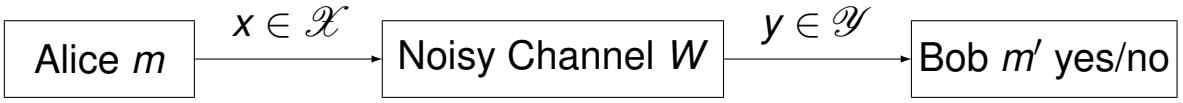


A New Communication Paradigm

- New applications are event-driven, e.g. Industry 4.0, V2X, V2V, ... $\Longrightarrow$ Identification task

  Goal:
  - Alice has to transmit a message $m \in \mathcal{M}$ to Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'

    $\Longrightarrow$ Bob's question: "Is the message m'?"



Practical Question: What is the largest rate of (almost) error free identification?

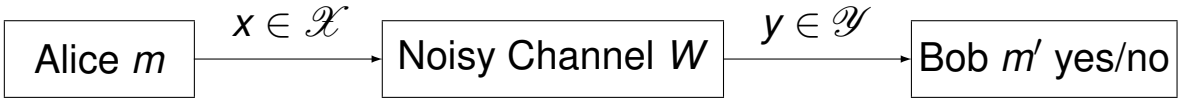
$\Longrightarrow$ Identification capacity C_{ID}

A New Communication Paradigm

- New applications are event-driven, e.g. Industry 4.0, V2X, V2V, ... $\Longrightarrow$ Identification task

  Goal:
  - Alice has to transmit a message $m \in \mathcal{M}$ to Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'

    $\Longrightarrow$ Bob's question: "Is the message m'?"



Practical Question: What is the largest rate of (almost) error free identification?

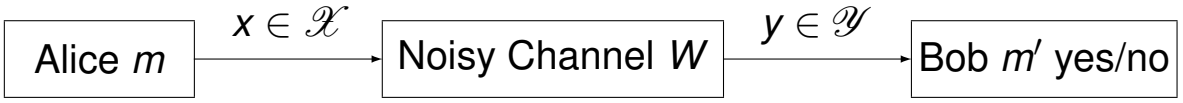
$\Longrightarrow$ Identification capacity $C_{ID} = C = \max(I(X \wedge Y))$

A New Communication Paradigm

- New applications are event-driven, e.g. Industry 4.0, V2X, V2V, ... $\Longrightarrow$ Identification task

  Goal:
  - Alice has to transmit a message $m \in \mathcal{N}$ to Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'

    $\Longrightarrow$ Bob's question: "Is the message m'?"



Practical Question: What is the largest rate of (almost) error free identification?

$\Longrightarrow$ Identification capacity $C_{ID} = C = \max(I(X \wedge Y))$

However: Message size $|N| = 2^{2^{Cn}}$ $\Longrightarrow$ double exponential increase

Here again randomized encoding is necessary! The local randomness is absolutely important. Otherwise $|N| = 2^{Cn}$.

A New Communication Paradigm

A randomized $(n, N, \lambda_1, \lambda_2)$ identification code is a set of pairs $\{(Q_i, \mathscr{D}_i)\,|i = 1, \ldots, N\}$ with

$$Q_i \in \mathscr{P}\left(\mathscr{X}^n\right), \quad \mathscr{D}_i \subset \mathscr{Y}^n \text{ for all } i = 1, \ldots, N$$

and with errors of first resp. second kind bounded by

$$\sum_{x \in \mathscr{X}^n} Q_i\left(x^n\right) W^n\left(\mathscr{D}_i | x^n\right) \geq 1 - \lambda_1 \text{ for all } i = 1, \ldots, N \tag{8}$$

and

$$\sum_{x \in \mathscr{X}^n} Q_j\left(x^n\right) W^n\left(\mathscr{D}_i | x^n\right) \leq \lambda_2 \text{ for all } i, j = 1, \ldots, N, \quad i \neq j \tag{9}$$

The receiver who is interested in message i will decide that his message was transmitted iff the received channel output is in $\mathscr{D}_i$, otherwise he will deny that message i was sent.

A New Communication Paradigm

Theorem (Ahlswede, Dueck, Han, Verdú)

Let $N(n,\lambda)$ be the max. number, such that an $(n,N,\lambda_1,\lambda_2)$ ID code exists with $\lambda_1,\lambda_2 \leq \lambda$. Then

$$\lim_{n\to\infty} \frac{\log\log N(n,\lambda)}{n} = C \text{ for all } \lambda \in (0,1/2) \tag{10}$$

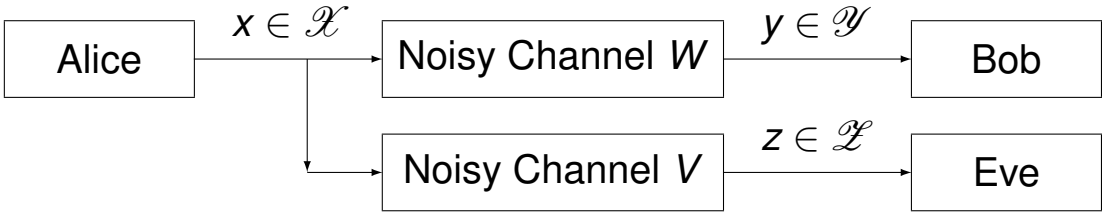
where the constant C denotes the Shannon's channel capacity.

Physical Layer Security and Identification

- New approach: embedded security and identification

  Goal:

  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'
  - Non legitimate receiver Eve is not able to identify any message

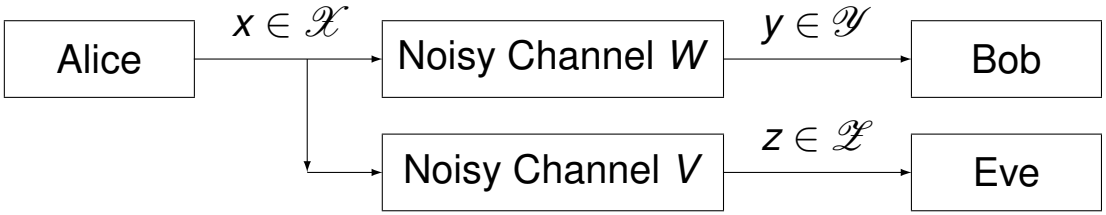


Physical Layer Security and Identification

- New approach: embedded security and identification

  Goal:

  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'
  - Non legitimate receiver Eve is not able to identify any message



What is the largest rate of (almost) error free secure identification from Alice to Bob?

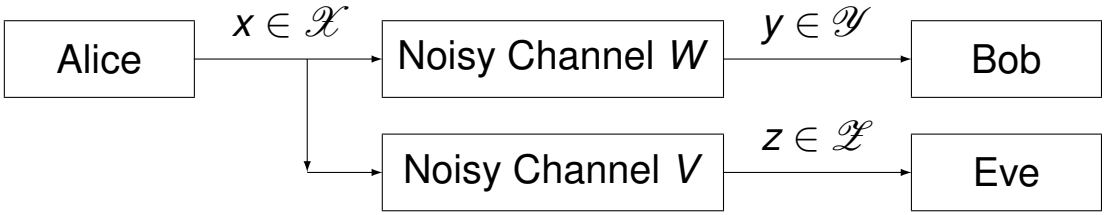
$\Longrightarrow$ Secure message transmission capacity C_{SID}

Physical Layer Security and Identification

- New approach: embedded security and identification

  Goal:

  - Alice has to transmit a message to the legitimate receiver Bob
  - Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  - Alice has no knowledge about m'
  - Non legitimate receiver Eve is not able to identify any message



What is the largest rate of (almost) error free secure identification from Alice to Bob?

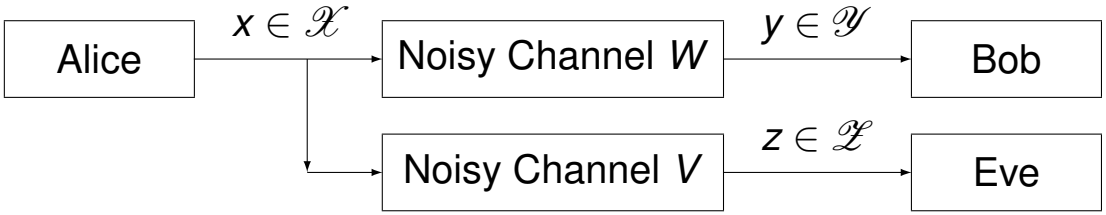
$$\Longrightarrow \text{Secure message transmission capacity } C_{SID} = \begin{cases} 0 & \text{if } C_S > 0 \\ C_{ID} & \text{otherwise.} \end{cases}$$

Physical Layer Security and Identification

- New approach: embedded security and identification

  Goal:

  – Alice has to transmit a message to the legitimate receiver Bob
  – Bob is interested in message m', and he has to decide "m' is transmitted or not ?"
  – Alice has no knowledge about m'
  – Non legitimate receiver Eve is not able to identify any message



What is the largest rate of (almost) error free secure identification from Alice to Bob?

$$\Longrightarrow \text{Secure message transmission capacity } C_{SID} = \begin{cases} 0 & \text{if } C_S > 0 \\ C_{ID} & \text{otherwise.} \end{cases}$$

Message size $|N| = 2^{2^{Cn}}$ with provable security if $C_S > 0$.

Here a randomized encoding is necessary! The local randomness is absolutely important.

Physical Layer Security and Identification

A randomized (n, N, λ) identification code of a wiretap-channel is a family of pairs $\{(Q_i, \mathscr{D}_i) \,|\, i \in \{1, \ldots, N\}\}$ with

$$Q_i \in \P(\mathscr{X}^n), \quad \mathscr{D}_i \subset \mathscr{Y}^n, \ \forall\, i \in \{1, \ldots, N\}$$

such that $\forall\, i, j \in \{1, \ldots, N\}, \quad i \neq j$

$$\sum_{x^n \in \mathscr{X}^n} Q_i(x^n)\, W^n(\mathscr{D}_i | x^n) \geq 1 - \lambda, \tag{11}$$

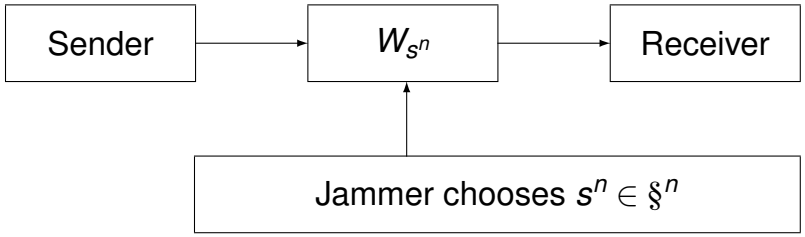
$$\sum_{x^n \in \mathscr{X}^n} Q_j(x^n)\, W^n(\mathscr{D}_i | x^n) \leq \lambda, \tag{12}$$

$$\sum_{x^n \in \mathscr{X}^n} Q_j(x^n)\, V^n(\mathscr{E} | x^n) + \sum_{x^n \in \mathscr{X}^n} Q_i(x^n)\, V^n(\mathscr{E}^c | x^n) \geq 1 - \lambda \tag{13}$$

for any pair (i, j) with $i \neq j$ and any $\mathscr{E} \subset \mathscr{Z}^n$.

Communication and Identification Task with Jammer

A Channel Model with a Jammer



- This setting is modeled by a given set of channels.
- The communication participants are aware of the state set but not of the actual realization determining the probabilistic channel law.
- So they do not know the jamming strategy of the jammer.
- In every time step the state of the channel can be changed by the jammer.
- The channel is called an Arbitrarily Varying Channel (AVC).
- In the calculation, a new effect occurs: symmetrizability.
- The intuitive meaning of this is that the jammer can choose the state of the channel such that any two codewords, x and x', may be confused by the receiver. In this situation, the decoder will be unable to tell if the transmitted codeword was x or x'. When a channel is symmetrizable, it is not possible to transmit or identify a message.

A Channel Model with a Jammer

Definition

An AVC $\mathscr{W}$ is symmetrizable if there exists a channel $U : \mathscr{X} \to \P(\mathscr{S})$, such that

$$\sum_s U(s|x')W(y|x,s) = \sum_s U(s|x)W(y|x',s) \tag{14}$$
$$\text{for all } x, x' \in \mathscr{X} \text{ and for all } y \in \mathscr{Y}.$$

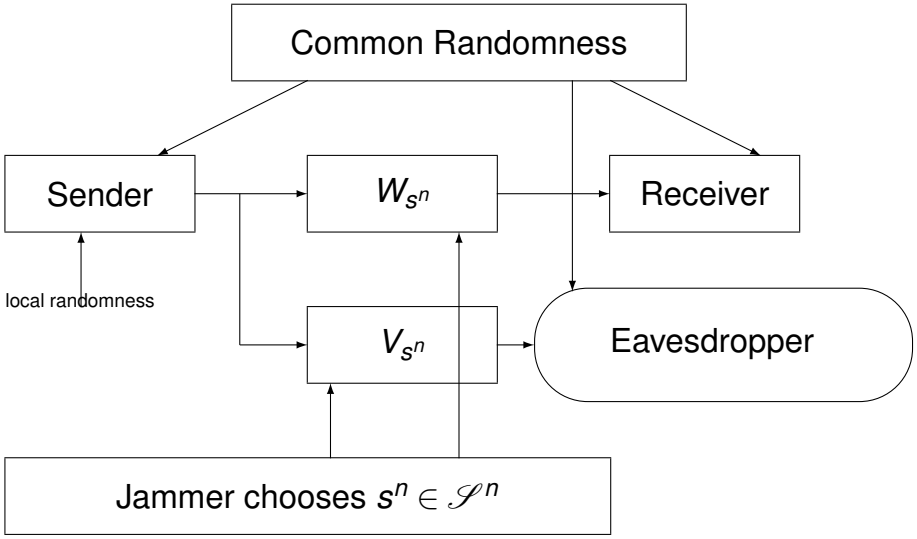
Csiszár and Narayan provided the following expression.

Theorem (Csiszár, Narayan, 1988)

$$C = \begin{cases} 0 & \text{if } \mathscr{W} \text{ is symmetrizable} \\ \max_P \min_{W \in \overline{\mathscr{W}}} I(P;W) & \text{otherwise,} \end{cases}$$

where $\overline{\mathscr{W}} = \{\sum_s P(s)W(\cdot|\cdot,s) : P \in \P(\mathscr{S})\}$.

A Channel Model with a Jammer and a Wiretapper



- The additional aspect of security is modeled by a wiretap channel.
- There is no single-letter formula for the capacity.

A Channel Model with a Jammer and a Wiretapper

Theorem (Nötzel, Wiese, B., 2016)

For the AVWC $(\mathscr{W}, \mathscr{V})$*, we have*

$$C_{S,ran}(\mathscr{W}, \mathscr{V}) = \lim_{n\to\infty} \frac{1}{n} \sup_{\{\bar{U}, \bar{X}^n, \bar{Y}_q^n, \bar{Z}_{s^n}^n\}} \left(\min_{q\in\mathscr{P}(\mathscr{S})} I(\bar{U} \wedge \bar{Y}_q^n) - \max_{s^n\in\mathscr{S}^n} I(\bar{U} \wedge \bar{Z}_{s^n}^n) \right),$$

where the supremum is over the set of families of RVs

$$\{\bar{U}, \bar{X}^n, \bar{Y}_q^n, \bar{Z}_{s^n}^n : q \in \mathscr{P}(\mathscr{S}), s^n \in \mathscr{S}^n\}. \tag{15}$$

$\bar{U}$ *assumes values in some finite subset of the integers. The values of* $\bar{X}^n$ *lie in* $\mathscr{A}^n$*, those of* $\bar{Y}_q^n$ *in* $\mathscr{B}^n$*, those of* $\bar{Z}_{s^n}^n$ *in* $\mathscr{C}^n$*, and such that for every* $q \in \mathscr{P}(\mathscr{S})$ *and* $s^n \in \mathscr{S}^n$*,*

$$P_{\bar{U}\bar{X}^n\bar{Y}_q^n\bar{Z}_{s^n}^n}(u, x^n, y^n, z^n) = P_{\bar{U}}(u) P_{\bar{X}^n|\bar{U}}(x^n|u) \left(\prod_{i=1}^n \left[\sum_{s\in\mathscr{S}} q(s) W_s(y_i|x_i) \right] \right) V^n(z^n|x^n, s^n). \tag{16}$$

$P_{\bar{U}}$ *and* $P_{\bar{X}^n|\bar{U}}$ *may be arbitrary probability distributions and stochastic matrices, respectively.*

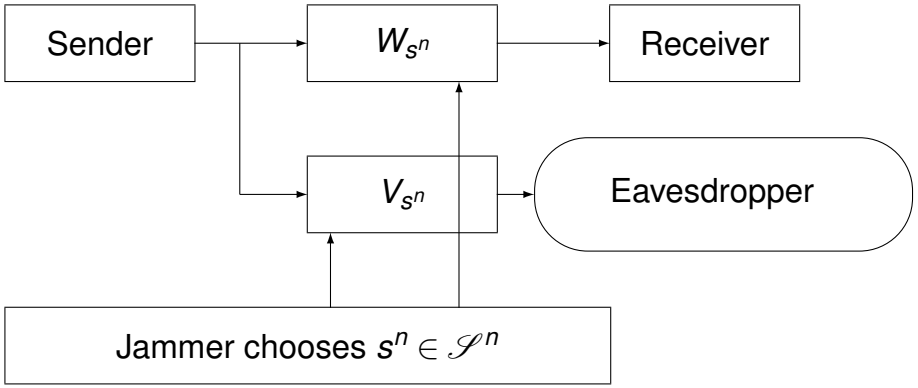
A Channel Model with a Jammer and a Wiretapper

Using the capacity for random codes and Ahlswede's elimination technique the following result was obtained.

Theorem (Bjelakovic, B., Sommerfeld, 2012)

$$C_S(\mathscr{W},\mathscr{V}) = \begin{cases} 0 & \text{if } C_S(\mathscr{W},\mathscr{V}) = 0 \text{ or} \\ & \mathscr{W} \text{ symmetrizable} \\ C_{S,ran}(\mathscr{W},\mathscr{V}) & \text{otherwise.} \end{cases}$$

Identification with a Jammer and a Wiretapper



Same model like before for robust transmission, new goal: Identification.

Theorem (B., Deppe, 2018)

Let $C_{\mathrm{ran}}(\mathcal{W})$ be the random coding capacity of the AVC $\mathcal{W}$ and let $C_{\mathrm{SID}}(\mathcal{W},\mathcal{V})$ be the random coding secrecy capacity of the AVWC $(\mathcal{W},\mathcal{V})$. Then,

1. $C_{\mathrm{SID}}(\mathcal{W},\mathcal{V}) = C_{\mathrm{ran}}(\mathcal{W})$, *if* $C_{\mathrm{S,ran}}(\mathcal{W},\mathcal{V}) > 0$ *and* $\mathcal{W}$ *is not symmetrizable.*
2. $C_{\mathrm{SID}}(\mathcal{W},\mathcal{V}) = 0$, *otherwise.*

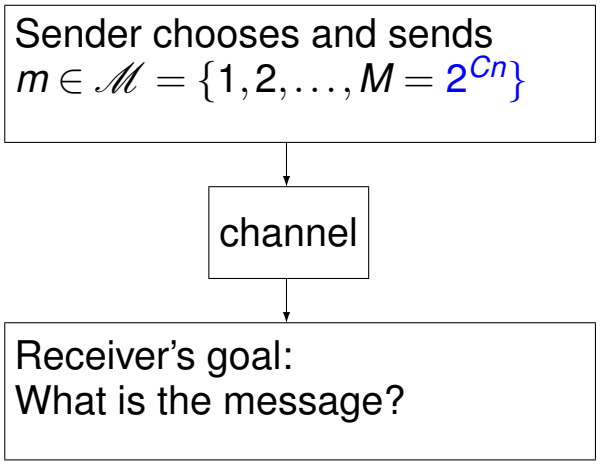
Identification with a Jammer and a Wiretapper

Remarks

1. The formula for secure identification with a jammer is a single-letter formula. The condition for positivity is unfortunately a multi-letter formula.
2. C_{SID} is generally a discontinuous function depending on $(\mathscr{W}, \mathscr{V})$.
3. We investigated the discontinuity behavior and the superactivation in detail.
4. For future applications with secure communication, it is important that the implemented coding methods are efficient and provable. This proof is provided by the certification and standardization. This proof must be effective in the future, i.e. by an algorithm. In this case, it is necessary to understand exactly the analyzed properties of the corresponding capacity as a function of channels.
5. Here we have presented the theory of classical channels. For quantum channels, the theory was developed by Boche, Deppe, and Winter.

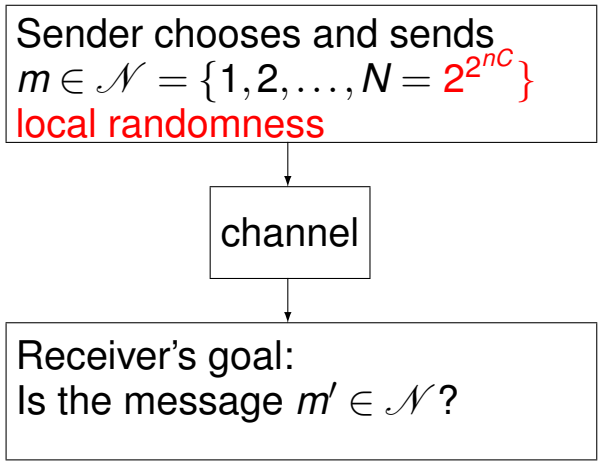
Conclusions: A New Communication Paradigm

Transmission - Shannon Picture



Shannon 1948

Identification - New Communication Task



Ahlswede/Dueck 1989

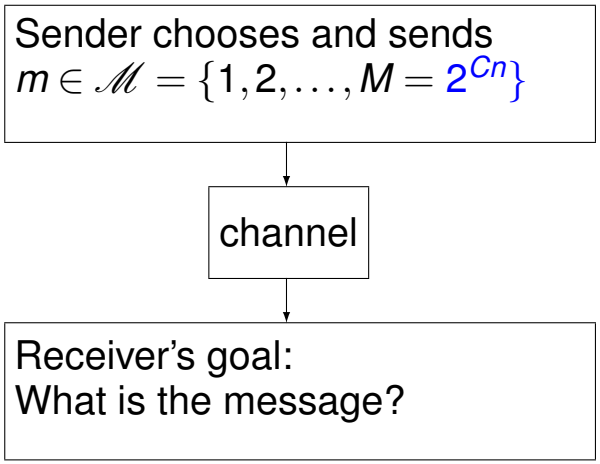
First Robust Optimal Protocol; H.B., C. Deppe;

ISIT 2017, IEEETIFS 2018

$\Rightarrow$ Extension to Quantum Systems; H.B., C. Deppe, A. Winter

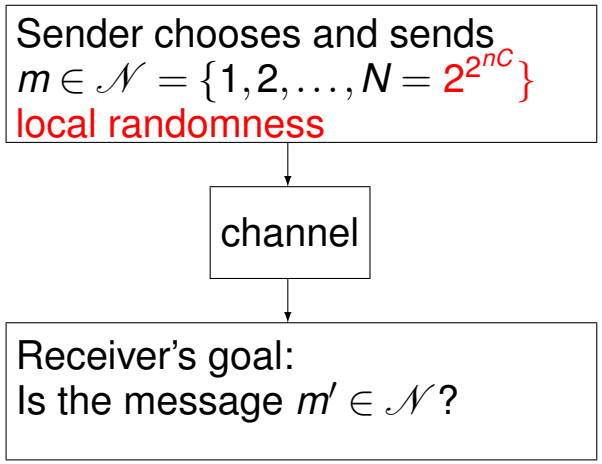
Conclusions: A New Communication Paradigm

Transmission - Shannon Picture



Shannon 1948

Identification - New Communication Task



Ahlswede/Dueck 1989

First Robust Optimal Protocol; H.B., C. Deppe;

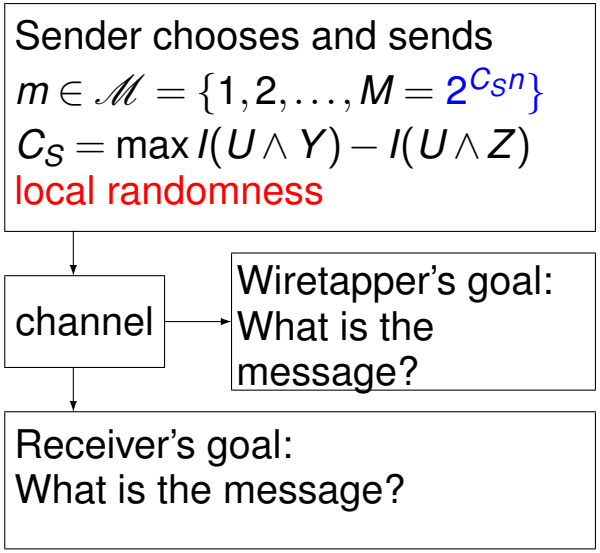
ISIT 2017, IEEETIFS 2018

$\Rightarrow$ Extension to Quantum Systems; H.B., C. Deppe, A. Winter

$\Rightarrow$ **exponential performance increase**

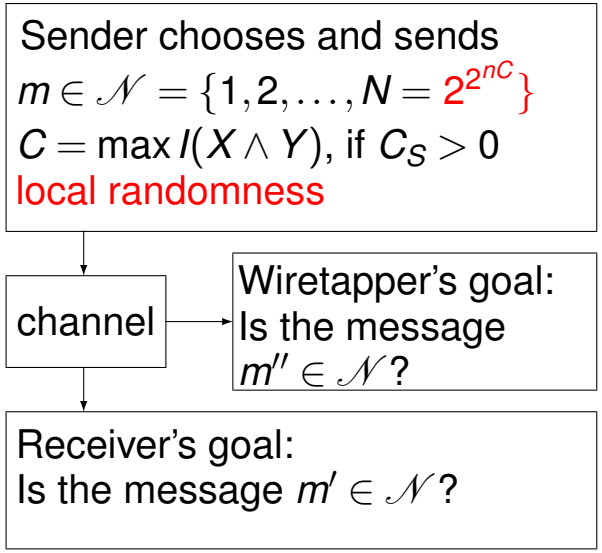
Conclusions: Security - New Quality

Transmission - Shannon Picture



Wyner 1978

Identification - New Communication Task

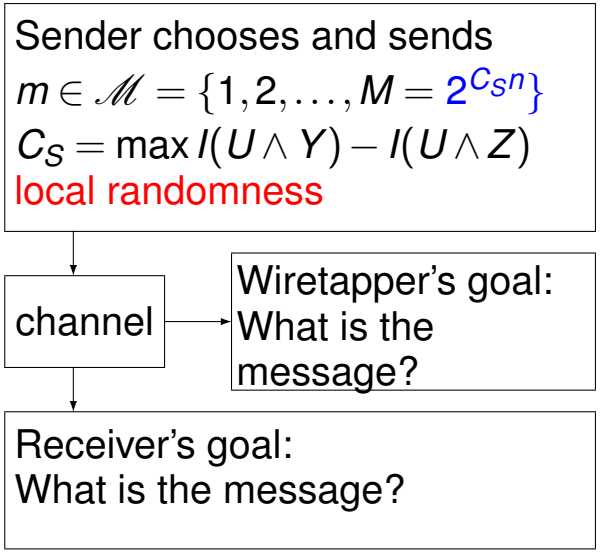


First Secure Robust Optimal Protocol; H.B., C. Deppe; ISIT 2017

$\Rightarrow$ Extension to Quantum Systems; H.B., C. Deppe, A. Winter ISIT 2018

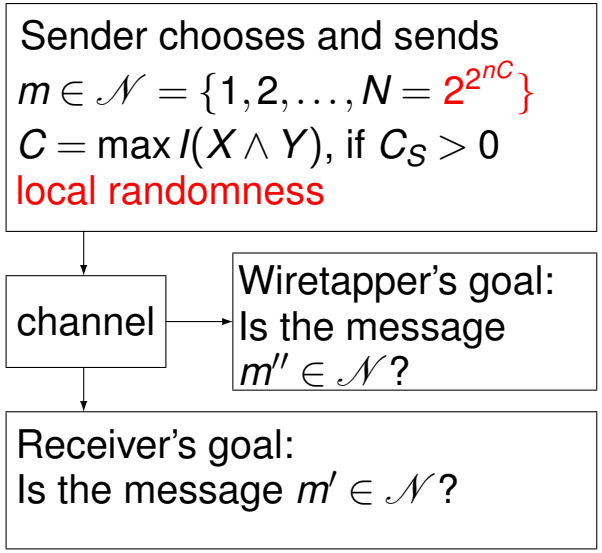
Conclusions: Security - New Quality

Transmission - Shannon Picture



Wyner 1978

Identification - New Communication Task



First Secure Robust Optimal Protocol; H.B., C. Deppe; ISIT 2017

$\Rightarrow$ Extension to Quantum Systems; H.B., C. Deppe, A. Winter ISIT 2018

$\Rightarrow$ **exponential performance increase and we pay no price for Security**

Conclusions: Extensions for New Approaches

- Other communication/signal processing tasks for communication systems
- Secure data storage on public data base with double exponential growth
  $\Rightarrow$ “Big Data” is not a problem, ...
- Quantum Identification ... even new identification tasks according Quantum Physics
- Communication tasks for Quantum Computing
- Quantum Information
  - Entanglement-Generation / Distributions
  - Strong Subspace
  - Private Keys ...
- Authentication via PUFs (Physical Unclonable Functions)
- Computations over channels

- H. Boche and C. Deppe, Secure identification under passive eavesdroppers and active jamming attacks, IEEE Transactions on Information Forensics and Security, accepted.
- H. Boche and C. Deppe, Identification, wiretap channel, robustness, super-additivity, continuity, IEEE Transactions on Information Forensics and Security 13, 7, 2018.
- H. Boche and C. Deppe, Secure identification under jamming attacks, IEEE Workshop on Information Forensics and Security (WIFS), 2017.
- H. Boche and C. Deppe, Robust and secure identification, IEEE International Symposium on Information Theory (ISIT), 2017.
- H. Boche, C. Deppe, and A. Winter, Secure and robust identification via classical-quantum channels, IEEE International Symposium on Information Theory (ISIT), 2018. (arXiv:1801.09967)
- H. Boche, R.F. Schaefer, and H.V. Poor, On the continuity of the secrecy capacity of compound and AVW channels, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 12, 2531-2546, 2015.
- R.F. Schaefer, H. Boche, A. Khisti, and H.V. Poor, Information Theoretic Security and Privacy of Information Systems, Cambridge University Press, 2017.