The impact of finite-alphabet input on the secrecy-achievable rates for broadcast channel with confidential message

Zeina Mheich, Florence Alberge, Pierre Duhamel

▶ **To cite this version:**

Zeina Mheich, Florence Alberge, Pierre Duhamel. The impact of finite-alphabet input on the secrecy-achievable rates for broadcast channel with confidential message. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014), May 2014, Florence, Italy. hal-01849649

HAL Id: hal-01849649
https://hal.science/hal-01849649

Submitted on 26 Jul 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THE IMPACT OF FINITE-ALPHABET INPUT ON THE SECRECY-ACHIEVABLE RATES FOR BROADCAST CHANNEL WITH CONFIDENTIAL MESSAGE

Zeina Mheich, Florence Alberge, and Pierre Duhamel

LSS (Supelec–Univ Paris-Sud–CNRS), 3 rue Joliot-Curie, 91192 Gif-sur-Yvette cedex, France, e-mail: {zeina.mheich, alberge, pierre.duhamel}@lss.supelec.fr

Motivations and Objectives

The broadcast channel with confidential message (BCCM):

- In theory: the secrecy-capacity region of Gaussian BCCM is achieved using **Gaussian codebook**
- In practice: symbols belong to **finite size constellations** (M-PAM,..) and are used with **equal probability**

Objectives

- Computation of secrecy-achievable rate region using finite input alphabet for various broadcast strategies
- Is using practical broadcast strategies sufficient to achieve good rates? or it leads to significant losses?

System Model

A broadcast channel with 2 receivers and a sender attempting to send 2 messages

1. A ***common message*** w_0 for both receivers
2. A ***confidential message*** w_1 for receiver 1

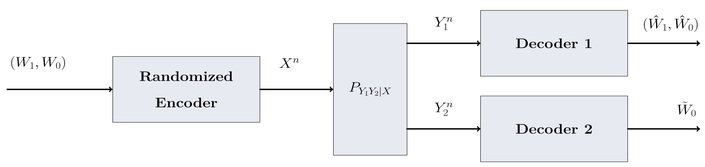

Figure 1: The broadcast channel with confidential message (BCCM)

The *secrecy capacity region* for the degraded BCCM $X \leftrightarrow Y_1 \leftrightarrow Y_2$ is the set that includes all (R_0, R_1) such that:

$$\begin{aligned} R_1 &\leq I(X;Y_1|U) - I(X;Y_2|U) \\ R_0 &\leq I(U;Y_2) \end{aligned}$$

for some $P_{UX} \cdot P_{Y_1|X} \cdot P_{Y_2|X}$.

- **U** is an auxiliary random variable carrying the ***common information***.
- The cardinality of $\mathcal{U}$ can be limited to $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$
- The secrecy-capacity region of the power constrained **Gaussian** BCCM is achievable using **Gaussian** input.

Broadcast Transmission Strategies

Strategies for transmitting both messages w_0 and w_1 separately in time (time sharing) or simultaneously (superposition modulation, superposition coding).

Broadcast Strategies

In ascending order in complexity of implementation:

1. Time Sharing (TS)
2. Superposition Modulation (SM)
3. Superposition Coding (SC)

Time Sharing

- The messages w_0 and w_1 are transmitted in *different time slots*.
- Simple implementation: in each slot the system is equivalent to a classical point-to-point communication system.

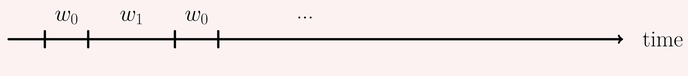

Figure 2: Time sharing

Superposition Modulation

- The messages w_0 and w_1 are transmitted *simultaneously*.
  $X = U + X_1 \qquad \left(|\mathcal{X}| = |\mathcal{U}| \cdot |\mathcal{X}_1|\right)$
- Practical example: *Hierarchical Modulation*

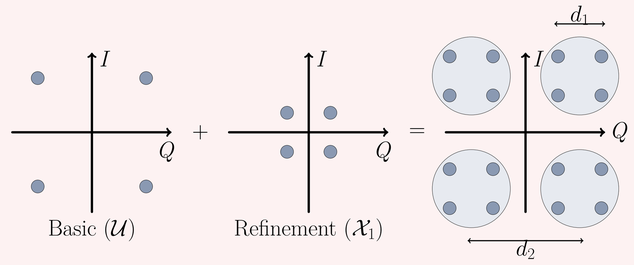

Figure 3: Hierarchical Modulation

Transmitted codeword $X^n(W_0, W_1) = U^n(W_0) + X_1^n(W_1)$

Superposition Coding

- The joint distribution P_{UX} takes the most general form: $|\mathcal{U}| = |\mathcal{X}|$.
- Example for $|\mathcal{X}| = 4$:

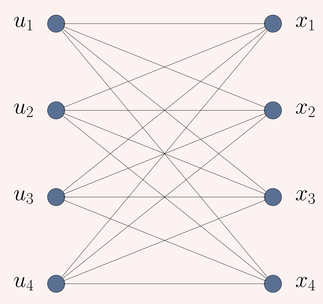

Figure 4: P_{UX} for $|\mathcal{X}| = 4$

- *Labeling* does not allow to distinguish between common and secret information as in hierarchical modulation.
- The encoding of both messages is done jointly using P_{UX} and the decoding is based on large block typicality.

Secrecy-Achievable Rates With M-PAM

Hypotheses:

- Gaussian BCCM with signal power constraint P.
- The channel input belongs to a finite set $\mathcal{X} = \{x_1, .., x_M\} \subset \mathbb{R}$.
- To determine the secrecy-achievable rates region when using a certain broadcast strategy:

Problem Formulation

$$\max_{P_{UX}, \mathcal{X}} \quad f(P_{UX}, \mathcal{X}) = \theta \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U) \Big] + (1-\theta) \cdot I(U;Y_2)$$

$$s.t. \quad \begin{cases} p_{ij} \geq 0 \quad \forall (i,j) \in \mathcal{I} \times \mathcal{J} \\ \sum_{ij} p_{ij} \cdot x_j^2 \leq P \\ \sum_{ij} p_{ij} = 1 \end{cases} \qquad (1)$$

where $\theta \in [0,1]$, $p_{ij} = \Pr\{U = u_i, X = x_j\}$, $\mathcal{J} = \{1, .., M\}$, $\mathcal{I} = \{1, .., |\mathcal{U}|\}$.

Numerical Solution:

First form the Lagrangian L of (1) :

$$L(\mathcal{X}, P_{UX}, s) = f(\mathcal{X}, P_{UX}) + s \cdot \left(P - \sum_{ij} p_{ij} \cdot x_j^2 \right) \qquad (2)$$

1. For a given value of s, the maximization of L with respect to P_{UX} and to $\mathcal{X}$ is done iteratively until convergence:
   - $P_{UX}^{(\ell)} = \arg \max_{P_{UX} \in \mathcal{C}} L(\mathcal{X}^{(\ell-1)}, P_{UX}, s)$
     - We observe in experiments that $L(\mathcal{X}, P_{UX}^{(\ell)}, s)$ is a concave function if $\mathcal{X} \in \mathcal{D}$ where $\mathcal{D} = \{\mathcal{X} \in \mathbb{R}^M : |x_i - x_j| > d \ \ \forall i, j \in \{0, .., M-1\} \text{ and } i \neq j\}$ and d depends on the size of the constellation and on the *SNR*.
     - A simplex method can be used with initialization in $\mathcal{D}$.
   - $\mathcal{X}^{(\ell)} = \arg \max_{\mathcal{X}} L(\mathcal{X}, P_{UX}^{(\ell)}, s)$
     - A Blahut-Arimoto-type algorithm is used. This algorithm converges if the initial guess lies in the domain where $L(\mathcal{X}, P_{UX}^{(\ell)}, s)$ is concave in P_{UX}.
2. To update the value of s, a gradient search method is used.

Experimental Results

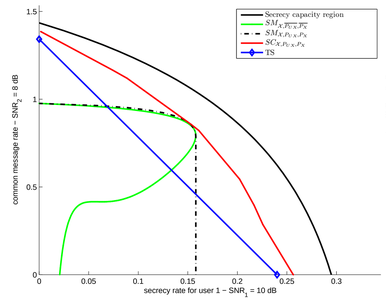

Figure 5: M=4, $(SNR_1, SNR_2) = (10, 8)$ dB

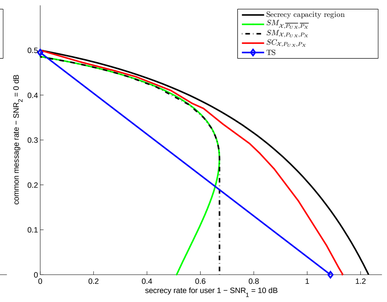

Figure 6: M=4, $(SNR_1, SNR_2) = (10, 0)$ dB

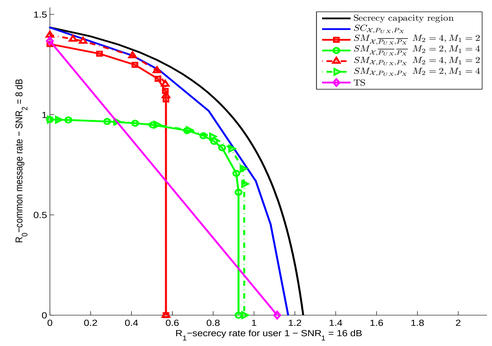

Figure 7: M=8, $(SNR_1, SNR_2) = (16, 8)$ dB

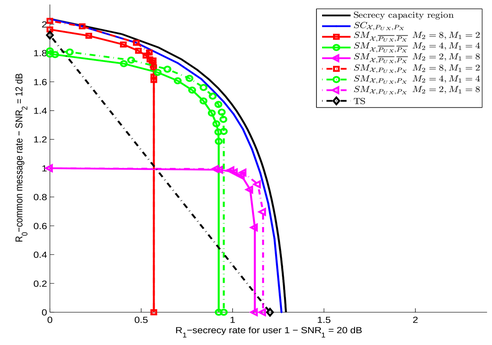

Figure 8: M=16, $(SNR_1, SNR_2) = (20, 12)$ dB

Remark: $\overline{P_{UX}} \equiv$ "P_{UX} is uniform" and $\overline{\mathcal{X}} \equiv$ "$\mathcal{X}$ is a standard constellation"

- The maximal achievable secrecy rate for SM is not necessarily obtained when the total transmission power is dedicated to the secrecy information.

General Conclusion

The general case of superposition coding can provide significant gains comparing to practical schemes (Time Sharing and Superposition Modulation). However in other cases, using practical schemes is sufficient to achieve good rates and provides a *compromise between complexity of implementation and efficiency.*