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

Zeina Mheich, Florence Alberge, Pierre Duhamel

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

Zeina Mheich *Florence Alberge* *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

ABSTRACT

This paper investigates the maximization of the secrecy-achievable rate region for the Gaussian broadcast channel with confidential message (BCCM) using finite input constellations. The maximization is done jointly over symbol positions and their joint probabilities. The secrecy-achievable rate regions are given for various broadcast strategies which differ in their complexity of implementation. We compare these strategies in terms of improvement in achievable rates and we study the impact of finite input alphabet on the secrecy-achievable rates. It is shown that finite alphabet constraints may change well known results holding in the Gaussian case.

Index Terms— Secrecy-achievable rate region, information-theoretic security, finite-input alphabet.

1. INTRODUCTION

Securing data communication over wireless networks has become an important concern. Compared to wired networks, the broadcast nature of wireless communications makes the data more susceptible to eavesdropping. Traditionally, security is implemented in communication systems by using cryptographic techniques at higher layers of the protocol stack. Recently, information theoretic security at the physical layer, which makes use of totally different concepts (exploiting the randomness of wireless channels) has become a topic of wide interest. E.g. Wyner [1] introduced the wiretap channel where the signal received by the eavesdropper is a degraded version of the signal received by the legitimate receiver. The secrecy capacity is the maximal achievable rate to communicate reliably with the destination while the wiretapper is not able to obtain any information from the observed signal. In [2] the secrecy capacity was given for the Gaussian wiretap channel. Csiszar and Korner studied in [3] a more general model called broadcast channel with confidential messages (BCCM) where the channels do not obey necessarily any degradation relationship. In this model, there is a common message for two receivers in addition to the confidential message for one receiver. More recently, fading was also considered [4],[5].

The secrecy capacity for the BCCM is achieved using random Gaussian codebook. However, in practical systems, the transmitted symbols belong to finite constellations *e.g.* M-PAM, M-QAM constellations, and are classically used with equal probability. These practical constraints reduce the secrecy rate. In [6] and [7], the authors consider the secrecy rate achievable in this context. It is shown that the secrecy rate curves for a finite constellation plotted against the SNR and for a fixed noise variance of the eavesdropper's channel have a global maximum at an internal point. This comes in contrast to the case of Gaussian codebook input where secrecy capacity is a bounded, monotonically increasing function of SNR. Ref. [8] investigates the secrecy rate of the Gaussian wiretap channel with standard M-PAM inputs. The authors provide necessary conditions for the M-PAM input power and the M-PAM input distribution to maximize the secrecy rate. Ref. [9] studies the effect of discrete-constellation on the achievable secrecy rate of multi-antenna wiretap channels.

This paper studies the achievable rates for the Gaussian BCCM using M-PAM constellations. We determine the maximal secrecy-achievable rate region for Gaussian BCCM by optimizing over both symbol positions and the joint distribution of probability. The symbol positions in our work are allowed to take arbitrary values and are not necessarily proportional to standard constellation as in [8]. This leads to the determination of the upper bound of the secrecy rate of any constellation with M symbols. The secrecy achievable rate regions are also given for various transmission strategies which differ in their complexity of implementation. The corresponding trade-off between complexity and efficiency is discussed. The goal is to know whether using practical schemes is sufficient to achieve good rates or it leads to significant losses. This is a first step towards a practical implementation of secure communication at the physical layer.

2. PRELIMINARIES AND SYSTEM DESCRIPTION

The BCCM is a broadcast channel with two receivers for which a sender attempts to send two messages simultaneously: a common message w_0 for both receivers and a secret

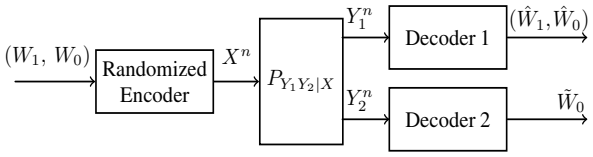

Fig. 1. The broadcast channel with confidential message

message w_1 for receiver 1 [3]. A BCCM consists of an input alphabet $\mathcal{X}$, two output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$ and transition probability $P_{Y_1Y_2|X}$ (Fig.1). In this work, we focus on the case in which *perfect secrecy* is achieved [3]. 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 [4]:

$$R_1 \leq I(X;Y_1|U) - I(X;Y_2|U) \quad (1)$$
$$R_0 \leq I(U;Y_2) \quad (2)$$

for some $P_{UX} \cdot P_{Y_1|X} \cdot P_{Y_2|X}$. U is an auxiliary random variable (RV) which carries the common information. The cardinality of the alphabet $\mathcal{U}$ is bounded by $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\}$. Throughout this work, we consider the (degraded) Gaussian BCCM, thus $|\mathcal{U}| \leq |\mathcal{X}|$. The channel outputs are $Y_i = X + Z_i$, where $i \in \{1, 2\}$ and $Z_i \sim \mathcal{N}(0, N_i)$ and the input is power constrained. The secrecy capacity region of the Gaussian BCCM with input power constraint P is given in [4], and the achievability of the secrecy-capacity region follows with the following choice of RVs: $U \sim \mathcal{N}(0, (1-\beta) \cdot P)$, $X = U + X'$ with $X' \sim \mathcal{N}(0, \beta \cdot P)$ where $\beta \in [0, 1]$.

3. BROADCAST TRANSMISSION STRATEGIES

The common rate R_0 and the secrecy rate R_1 are achieved using superposition coding (SC) to transmit simultaneously both messages. A random binning scheme (stochastic encoding) [3], [10] is used to ensure security. This section presents various broadcast transmission strategies which differ in their complexity of implementation. The simple schemes can be understood as adding constraints to the most general case. A detailed description of these strategies applied to the two-user broadcast channel (without security) can be found in [11].

3.1. Time Sharing (TS)

In TS, messages w_0 and w_1 are transmitted in different timeslots. TS is widely used due to its simple implementation since in each slot the system is equivalent to a classical point-to-point communication. Here, we consider the cases where the transmitted symbols belong to a standard M-PAM constellation with equal probability.

3.2. Superposition Modulation (SM)

In SM, the M symbols are obtained by adding two random variables X_1 and X_2 of cardinalities M_1 and M_2 respectively, *i.e.* $M = M_1 M_2$. In this case the labeling is separable. This work first considers the scheme denoted as $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ where symbols are equiprobable but their position in the constellation is optimized. In this case, the encoding for both common and secret information can be done separately and the codewords added before transmission. Then, the constraint of equiprobable symbols is relaxed and we consider the strategy $SM_{\mathcal{X},P_{UX},P_X}$ in which both the symbol positions and the joint probability distribution P_{UX} are optimized. This increases the implementation complexity but provides better performance.

3.3. Superposition Coding (SC)

In SC, the joint distribution of probability P_{UX} takes the most general form, *i.e.* when $|\mathcal{U}| = |\mathcal{X}|$. Indeed, the auxiliary variable U serves as a cloud center for the information. Thus, labeling does not allow to distinguish between the common and the secret information. This makes this scheme more complex. The encoding of both messages is done jointly using the joint distribution of probability P_{UX} and the decoding is based on large block typicality [12]. In this work, we consider superposition coding scheme denoted by $SC_{\mathcal{X},P_{UX},P_X}$ when symbol position and the joint distribution P_{UX} are optimized.

4. ACHIEVABLE RATES WITH M-PAM

4.1. Problem formulation

Consider a memoryless Gaussian BCCM with signal power constraint P. The transmitter wants to convey a secret message to receiver 1 in the presence of the eavesdropper (receiver 2) and a common message to both receivers. The channel input belongs to a finite set $\mathcal{X} = \{x_0, .., x_{M-1}\} \subset \mathbb{R}$ represented by an M-PAM constellation. The signal-to-noise ratio for each receiver $k \in \{1, 2\}$ is defined by $SNR_k = \frac{P}{N_k}$. Assume that $SNR_2 < SNR_1$, otherwise there is no possibility to achieve a positive secrecy rate. To determine the secrecy-achievable rates region when using a certain broadcast strategy, we should solve the following weighted sum rate maximization problem:

$$\begin{aligned} \max_{P_{UX},\mathcal{X}} \quad & f(\mathcal{X}, P_{UX}) = \theta \cdot \Big[I(X;Y_1|U) - I(X;Y_2|U)\Big] \\ & +(1-\theta) \cdot I(U;Y_2) \\ s.t. \quad & \begin{cases} p_{ij} \geq 0 \quad \forall (i,j) \in \mathcal{I} \times \mathcal{J} \\ \sum_{ij} p_{ij} \cdot x_j^2 \leq P \\ \sum_{ij} p_{ij} = 1 \end{cases} \end{aligned} \quad (3)$$

where $\theta \in [0, 1]$, $p_{ij} = \Pr\{U = u_i, X = x_j\}$, $j \in \mathcal{J} = \{0, .., M-1\}$ and $i \in \mathcal{I} = \{0, .., |\mathcal{U}|-1\}$. The expression of the mutual information $I(X;Y_k|U)$, $k \in \{1, 2\}$, and $I(U;Y_2)$

can be found in [11]. The AWGN channel for each user k is characterized by the classical conditional pdf of variance N_k.

4.2. Numerical solution

In this section, we present an alternative maximization algorithm to solve (3), similar to that in [11] without security constraint. First form the Lagrangian L of (3) :

$$L(\mathcal{X}, P_{UX}, s) = f(\mathcal{X}, P_{UX}) + s \cdot \Big(P - \sum_{ij} p_{ij} \cdot x_j^2\Big) \quad (4)$$

For a given value of s, the maximization of L with respect to P_{UX} and to $\mathcal{X}$ is done iteratively until convergence:

$$P_{UX}^{(\ell)} = \arg \max_{P_{UX} \in \mathcal{C}} L(\mathcal{X}^{(\ell-1)}, P_{UX}, s) \quad (5)$$

$$\mathcal{X}^{(\ell)} = \arg \max_{\mathcal{X}} L(\mathcal{X}, P_{UX}^{(\ell)}, s) \quad (6)$$

where ℓ is the iteration index and $\mathcal{C}$ denotes the set of constraints on P_{UX} and can be defined either as $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_{i,j} p_{i,j} = 1\}$ or as $\mathcal{C} = \{P_{UX} : p_{ij} \geq 0, \sum_i p_{i,j} = \frac{1}{M}\}$ if symbols are used with equal probability.

To solve the optimization in (6), we observed in our experiments that $L(\mathcal{X}, P_{UX}^{(\ell)}, s)$ is a concave function if $\mathcal{X} \in \mathcal{D}$ where $\mathcal{D} = \{\mathcal{X} \in \mathbb{R}^M : |x_i - x_j| > d \ \ \forall i, j \in \{0, .., M-1\}$ and $i \neq j\}$ and d depends on the size of the constellation and on the SNR. Then a simplex method can be used to solve (6) where the symbol positions are initialized in $\mathcal{D}$.

In order to solve the optimization problem in (5) with constraint set $\mathcal{C}$ for the BCCM, we used a Blahut-Arimoto type algorithm which is a generalization of that proposed in [13] for the wiretap channel. However since (5) is not convex in P_{UX}, the Blahut-Arimoto type algorithm converges when some conditions hold [14]. Indeed, if the solution of (5), $P_{UX}^{*(l)}(s)$, lies in a set $T_{k,\theta}(\tilde{P}_{UX})$ and the function $L(\mathcal{X}^{(\ell-1)}, P_{UX}, s)$ is concave in $T_{k,\theta}(\tilde{P}_{UX})$ and the initial guess $P_{UX}^{(0)(l)}(s) \in T_{k,\theta}(\tilde{P}_{UX})$, the Blahut-Arimoto type algorithm is shown to converge to the optimal value. $T_{k,\theta}(\tilde{P}_{UX})$ is defined in [14] as the set of all the points $P_{UX} \in S_{k,\theta} \triangleq \{P_{UX} | L(\mathcal{X}^{(\ell-1)}, P_{UX}, s) \geq k\}$ such that P_{UX} is reachable from $\tilde{P}_{UX} \in S_{k,\theta}$ by a continuous path.

In the experiments, we observe that the region $T_{k,\theta}(\tilde{P}_{UX})$ where the objective function in (5) is concave in P_{UX} is larger when θ increases. This is because the weight for the concave part of the function *i.e.* $I(X;Y_1|U) - I(X;Y_2|U)$ increases with θ. Thus we have more chance that the algorithm converges from initial guess in this case. The initial guesses to be avoided are the uniform distribution of P_{UX} because in this case we observed that the algorithm converges to the same distribution, and also when there is some similarities in the initial matrix P_{UX}. The initial guesses are chosen randomly in the experiments and the Blahut-Arimoto type algorithm is shown to converge.

Clearly, each iteration of the alternative maximization method increases the objective function. In the experiments, we have observed that this method converges at least to a local maximum (denoted $p_{i,j}^*(s)$, $x_j^*(s)$, $j \in \mathcal{J}, i \in \mathcal{I}$). Finally, in order to update the value of s, we use a gradient search method as follows, where $[.]^+ = \max(., 0)$:

$$s^{(k+1)} = \Big[s^{(k)} - \gamma\Big(P - \sum_{i,j} p_{ij}^*(s^{(k)}) \cdot (x_j^*(s^{(k)}))^2\Big)\Big]^+ \quad (7)$$

5. RESULTS AND DISCUSSION

This section provides an evaluation of the secrecy achievable rate regions for Gaussian BCCM using various transmission strategies, namely time sharing, superposition modulation and superposition coding. The effect of constellation shaping is evaluated by analyzing the secrecy-achievable rate region curves obtained for an M-PAM constellation (M=4, 8, 16) and for several pairs (SNR_1, SNR_2). The comparisons of secrecy-achievable rates are conducted in terms of SNR savings for target achievable rates (Maximum Shaping Gain).

5.1. Superposition modulation using M-PAM

First consider $M = 4$. In this case, the symbols carrying both the common and the secrecy message belong to a BPSK modulation. Let αP be the power used for the constellation symbols of the secret information with $0 \leq \alpha \leq 1$. Fig. 2 and 3 depict the secrecy-achievable rate regions for various transmission strategies using 4-PAM when SNR_1= 10 dB and $SNR_2 \in \{0, 8\}$ dB. We observe that for superposition modulation schemes, the maximal achievable secrecy rate is not necessarily obtained when $\alpha = 1$, *i.e.* when the total transmission power is dedicated to the secrecy information, unlike the case of a broadcast channel with two messages without security constraint [15][16]. This shows that the secrecy rate does not necessarily increase with the user SNRs.

Regions of secrecy achievable rate (Fig 2 to 5) show the improvement obtained by optimizing symbol positions and the joint probabilities ($SM_{\mathcal{X},P_{UX},P_X}$ (full optimization)) compared to $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$(optim. of $\mathcal{X}$ only). One can observe that the maximum shaping gain increases with the constellation size. Thus, constellation shaping for SM strategy seems more useful for high values of M. Moreover, we observe that independently of M, the maximum shaping gain is very small when the gap between the user SNRs (δ_{SNR}) increases. The analysis of the optimal matrix P_{UX} (results not reported) leads to the conclusion that X_1 and X_2 are not independent in general when using finite-size constellations.

5.2. comparison of classical schemes (SM vs TS)

Time sharing with standard constellations and superposition modulation with equally probable symbols are classically

used as broadcast transmission strategies for simplicity. It can be observed from Fig. 2 to 5 that the secrecy achievable rate region can be split into two parts where $SM_{\mathcal{X},\overline{P_{UX}},\overline{P_X}}$ is better than TS and vice versa. The achievable rate region that can be achieved by time sharing is larger when the users SNRs are close to each other. It can also be observed that the best improvement happens when δ_{SNR} increases for all $M \in \{4, 8, 16\}$. Thus superposition modulation should be preferred to TS when users have very different SNRs.

5.3. Superposition coding

The results obtained for the general case of superposition coding $SC_{\mathcal{X},P_{UX},P_X}$ lead to the same conclusions as for a broadcast channel model without security constraints [11]. In the model with security constraint, $SC_{\mathcal{X},P_{UX},P_X}$ can achieve also better rates than superposition modulation which means that SM is not the optimal broadcast strategy as in the Gaussian alphabet case. It can be observed from the curves that the maximum gain is proportionally greater for small values of M. This is due to the fact that when M increases, we have more configurations to obtain an M-PAM by superposing two constellations. Asymptotically, we know that when $M \to \infty$, $SM_{\mathcal{X},P_{UX},P_X}$ is the optimal superposition coding scheme because it achieves the capacity region for two-user Gaussian broadcast channel using Gaussian alphabets. Note that in the curves of secrecy achievable rate regions using the general case of SC, the maximum achievable secrecy rate is achieved when the maximal power is used to transmit the confidential message. This is due to the fact that the user SNRs in Fig. 2 to 5 are chosen in the region where the secrecy rate is increasing with the user SNRs using M-PAM.

6. CONCLUSION

This work considers the problem of maximizing the secrecy-achievable rate region for the Gaussian BCCM using finite input constellations. The maximization of the secrecy achievable rate regions is done for superposition modulation and the general case of superposition coding. For superposition modulation, it is seen that the maximal achievable secrecy rate is not necessarily obtained when all the power is allocated for transmitting the secret message. In addition, the full maximization of secrecy-achievable rate region for superposition modulation provides more significant improvements when the cardinality of the input alphabet increases compared to the case where we optimize only symbol positions. In the case of finite input alphabet, superposition modulation is not the optimal strategy like in the Gaussian alphabet case. The general case of superposition coding can provide significant gains comparing to practical schemes. However in other cases, using practical schemes is sufficient to achieve good rates and provides a compromise between complexity of implementation and efficiency.

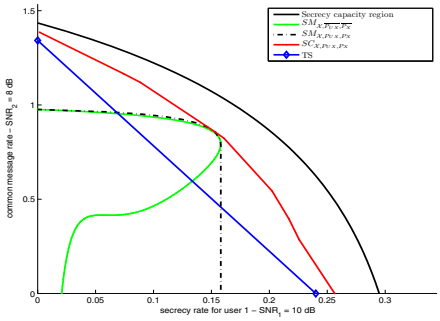

Fig. 2. Secrecy achievable rate regions with $M = 4$ and $(SNR_1, SNR_2) = (10, 8)$ dB

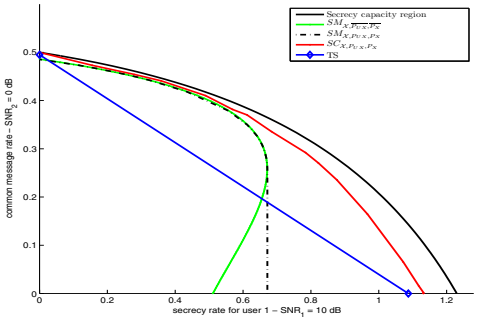

Fig. 3. Secrecy achievable rate regions with $M = 4$ and $(SNR_1, SNR_2) = (10, 0)$ dB

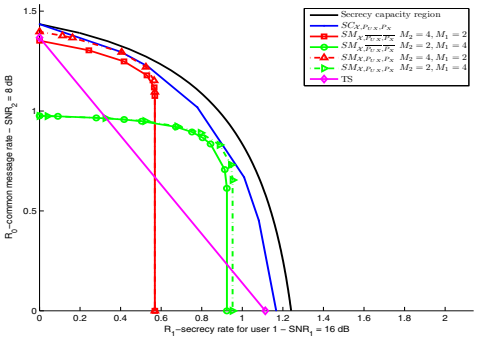

Fig. 4. Secrecy achievable rate regions with $M = 8$ and $(SNR_1, SNR_2) = (16, 8)$ dB

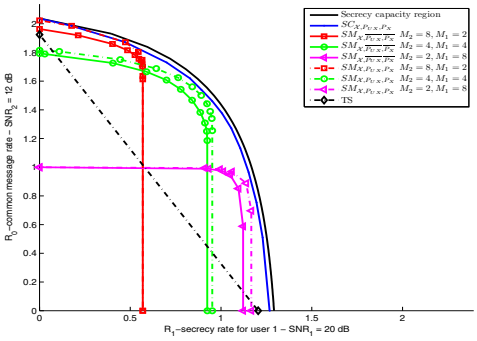

Fig. 5. Secrecy achievable rate regions with $M = 16$ and $(SNR_1, SNR_2) = (20, 12)$ dB

7. REFERENCES

[1] A. D. Wyner, "The wiretap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[5] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[6] G. D. Raghava and B. S. Rajan, "Secrecy capacity of the gaussian wiretap channel with finite complex constellation input," `[online].Available:http://arxiv.org/abs/1010.1163`, 2010.

[7] F. Renna, N. Laurenti, and H. V. Poor, "Achievable secrecy rates for wiretap OFDM with QAM constellations," in *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools, VALUETOOLS '11*, Paris, France, 2011.

[8] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On gaussian wiretap channels with M-PAM inputs," in *2010 European Wireless Conference (EW)*, 2010, pp. 774–781.

[9] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. on communications*, vol. 60, no. 12, pp. 3816–3825, dec. 2012.

[10] M. Bloch and J. Barros, *Physical layer security: from information theory to security engineering*, Cambridge University Press, 2011.

[11] Z. Mheich, F. Alberge, and P. Duhamel, "Achievable rates optimization for broadcast channels using finite size constellations under transmission constraints," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 254, 2013.

[12] T. M. Cover, "Comments on broadcast channels," *IEEE Trans. on Inform. Theory*, vol. 44, no. 6, october 1998.

[13] K. Yasui, T. Suko, and T. Matsushima, "An algorithm for computing the secrecy capacity of broadcast channels with confidential messages," in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pp. 936–940.

[14] K. Yasui and T. Matsushima, "Toward computing the capacity region of degraded broadcast channel," in *2010 IEEE International Symposium on Information Theory Proceedings (ISIT)*, June 2010, pp. 570–574.

[15] Z. Mheich, P. Duhamel, L. Szczecinski, and M-L. Alberi-Morel, "Constellation shaping for broadcast channels in practical situations," in *Proc. of the 19th European Signal Processing Conference*, Barcelona, Spain, Aug. 2011.

[16] C. Huppert and M. Bossert, "On achievable rates in the two user AWGN broadcast channel with finite input alphabets," in *IEEE International Symposium on Information Theory, 2007 (ISIT 2007)*, Nice, France, June 2007.