Outer Bound for E-capacity - Equivocation Region of the Wiretap Channel

Mariam Haroutunian

Institute for Informatics and Automation Problems, National Academy of Sciences of Armenia
Yerevan, Armenia

e-mail: armar@ipia.sci.am

ABSTRACT

The basic wiretap channel model is considered. The aim is to maximize the rate of the reliable communication from the source to the legitimate receiver, while keeping the confidential information as secret as possible from the wiretapper (eavesdroper). The E-capacity - equivocation region, which is the generalization of the capacity - equivocation region, is investigated. The outer bound of this region is constructed.

Keywords

Information-theoretic security, wiretap channel, rate-reliability region, equivocation rate.

1. INTRODUCTION

Security is an important topic in communications. The information theoretical security is an approach, that demonstrates the possibility of transmitting confidential messages without using an encryption key. The main idea of the information theoretic security is to exploit the inherent noises and difference between the channels to a legitimate receiver and eavesdropper. In addition, the transmitter intentionally adds randomness to prevent eavesdroppers from accepting useful information while guaranteeing the legitimate receiver to obtain the information. Such an approach to guarantee secrecy has the advantage of eliminating the key management issue, resulting in lower complexity and savings in resources.
Such an approach was initiated by Wyner [1], who studied the most basic model called a wiretap channel. Later Csiszár and Körner [2] studied the broadcast channel with confidential messages, the special case of which is the more general model of wiretap channel from [1], when the channel to the eavesdropper is not necessarily degraded as assumed in [1]. In this paper we consider that general model of wiretap channel (see Fig. 1), which is defined as follows.
The source wishes to transmit a message m to a legitimate receiver while keeping it as secret as possible from an eavesdropper. The confidential message m is assumed to be randomly and uniformly distributed over a message set $\mathcal{M}$. The encoder f_N maps each message m to a codeword $\mathbf{x}(m) = (x_1, ..., x_N) \in \mathcal{X}^N$, where $\mathcal{X}$ is the input alphabet and N is the transmission length. The codeword $\mathbf{x}(m)$ is transmitted over a discrete memoryless channel (DMC) with transition probability $W(y, z|x)$. The noisy version $\mathbf{y} \in \mathcal{Y}^N$ is accepted by legitimate receiver and $\mathbf{z} \in \mathcal{Z}^N$ by eavesdropper, respectively. The decoder g_N at the receiver maps the received sequence $\mathbf{y}$ to an estimate $\hat{m}$ of the message.

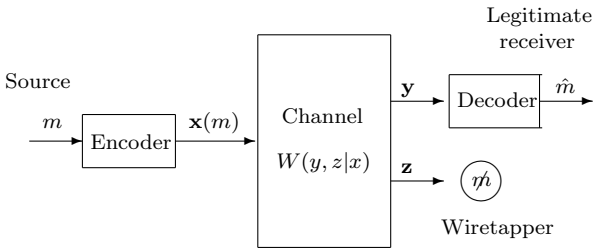

Fig. 1. Wiretap channel.

The capacity-equivocation region $\mathcal{C}$ of this model was obtained in [2]. Other models with secrecy constraints are surveyed in [3]. In this paper we investigate the E - capacity - equivocation region $\mathcal{C}(E)$, which is the closure of the set of all achievable rate - reliability - equivocation pairs $(R(E), R_e)$, where the function $R(E)$ presents optimal dependence of rate R from reliability (error probability exponent) E. It is the analogy of E - capacity (rate -reliabilty function) suggested by E. Haroutunian [4] and investigated for various channel models [5]. The inner (random coding) bound of E - capacity - equivocation region in another setting was investigated in [6]. Here the outer bound of this region is constructed. When E tends to zero, this bound coincides with the capacity-equivocation region obtained in [2].
The paper is organized as follows: In Section 2 the main definitions and the problem statement are presented. The formulation and the proof of the constructed bound is given in Section 3. In Section 4 along with the conclusion ideas for future work are discussed.

2. PROBLEM STATEMENT

The DMC $W(y, z|x)$ with finite input alphabet $\mathcal{X}$, finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ is memoryless

$$W^N(\mathbf{y}, \mathbf{z}|\mathbf{x}) = \prod_{n=1}^{N} W(y, z|x)$$

Let us denote

$$W_1(y|x) = \sum_z W(y, z|x),$$

$$W_2(z|x) = \sum_y W(y, z|x),$$

and

$$P_1W_1(y|u) = \sum_x P_1(x|u)W_1(y|x). \quad (1)$$

To formulate the problem consider auxiliary random variables U and Q with values in finite $\mathcal{U}$ and $\mathcal{Q}$, correspondingly, that satisfy the Markov chain relationship: $Q \to U \to X \to (Y, Z)$.

Let the probability distributions (PD) of random variable (RV) U be $P_0 = \{P_0(u), u \in \mathcal{U}\}$ and $P_1 = \{P_1(x|u), x \in \mathcal{X}, u \in \mathcal{U}\}$ be conditional PD of RV X for the given value u. Joint PD of RV U, X we denote by $P_{0,1} = \{P_{0,1}(u, x) = P_0(u)P_1(x|u), u \in \mathcal{U}, x \in \mathcal{X}\}$. and the marginal PD of X is $P = \sum_u P_{0,1}(u, x)$. We shall use also the following PD

$$V = \{V(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\},$$

$$P \circ V = \{P \circ V(x, y) = P(x)V_1(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$$

and

$$PV = \{PV(y) = \sum_x P(x)V(y|x), y \in \mathcal{Y}\}.$$

For N length code the code rate is (log and exp functions are taken to the base 2)

$$R = \frac{1}{N} \log |\mathcal{M}_N|$$

and the average error probability is

$$e_N = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} W_1^N\{\mathcal{Y}^N - g^{-1}(m)|\mathbf{x}(m)\},$$

where $g^{-1}(m) = \{\mathbf{y} : g(\mathbf{y}) = m\}$.

The secrecy level of confidential message m at the wiretapper is measured by the equivocation rate defined as

$$R_e^N = \frac{1}{N} H(M|Z^N),$$

where $H(X|Y)$ is the conditional entropy [7]. In other words, the equivocation rate indicates the eavesdroppers uncertainty about the message m given the channel outputs Z^N. Hence, the larger the equivocation rate, the higher the level of secrecy.

A rate equivocation pair (R, R_e) is **achievable** if there exists a sequence of message sets $\mathcal{M}_N$ with $|\mathcal{M}_N| = \exp NR$ and encoder decoder (f_N, g_N) such that the average error probability tends to zero as N goes to infinity, and the equivocation rate R_e satisfies

$$R_e \le \lim_{N \to \infty} \inf R_e^N.$$

The rate equivocation pair (R, R_e) indicates the confidential rate R achieved at certain secrecy level R_e.

The **capacity - equivocation region** $\mathcal{C}$ is defined to be the closure of the set that consists of all achievable rate equivocation pairs (R, R_e).

In this paper we investigate the E **- capacity - equivocation region** $\mathcal{C}(E)$, which is defined in the similar way with error probability satifying $e \le \exp\{-NE\}$.

The following result was obtained in [2].

Theorem 1. The capacity - equivocation region of wiretap channel is given by

$$\mathcal{C} = \bigcup_{P_{0,1}W} \left\{ \begin{array}{l} (R, R_e), \\ R \le I_{P_{0,1},W_1}(U; Y), \\ 0 \le R_e \le R, \\ R_e \le I_{P_{0,1},W_1}(U; Y|Q) - \\ -I_{P_{0,1},W_2}(U; Z|Q) \end{array} \right\} \quad (2)$$

where for generic random variables X and Y, $I(X; Y)$ denotes the mutual information between X and Y [7] . The auxiliary random variables Q and U are bounded in cardinality by $|Q| \le |X| + 3$ and $|U| \le |X|2 + 4|X| + 3$, respectively.

In this paper the following theorem is proved.

Theorem 2. The outer bound of E - capacity - equivocation region of wiretap channel is given by

$$\mathcal{R}_{sp}(E, W) = \bigcup_{P_{0,1}W} \left\{ \begin{array}{l} (R(E), R_e) : \\ R(E) \le \\ \le \min_{P_1V : D(P_1V||P_1W_1|P_0) \le E} I_{P_{0,1},V}(U; Y); \\ 0 \le R_e \le R(E); \\ R_e \le I_{P_{0,1},W_1}(U; Y|Q) - I_{P_{0,1},W_2}(U; Z|Q). \end{array} \right\} \quad (3)$$

Here $D(P_1V||P_1W_1|P_0)$ denotes the divergence between conditional distributions P_1V and P_1W_1 given PD P_0 [7]. The proof of Theorem 2 is given in the next section using the method of types [8]. The set of all $\mathbf{u} \in \mathcal{U}^N$ of the type P_0 is denoted by $\mathcal{T}_{P_0}^N(U)$ and $\mathcal{T}_P^N(X|\mathbf{u})$ is the set of all vectors $\mathbf{x} \in \mathcal{X}^N$ with conditional type $P_1(x|u)$ given $\mathbf{u} \in \mathcal{T}_{P_0}^N(U)$.

3. PROOF OF THE RESULT

Let E and δ be given such that $E > \delta > 0$. For given N let us consider the codes (f_N, g_N) with rate R error probabilities of which exponentially decrease with the given exponent E:

$$\frac{1}{|\mathcal{M}_N|} \sum_{m \in \mathcal{M}_N} W_1^N\{\mathcal{Y}^N - g^{-1}(m)|f(m)\} \le$$

$$\le \exp\{-N(E - \delta)\},$$

which can be rewritten as

$$\sum_{m:\mathbf{u},\mathbf{x}(m) \in f(\mathcal{M}_N)} P_1^N(\mathbf{x}|\mathbf{u})W_1^N\{\mathcal{Y}^N - g^{-1}(m)|\mathbf{u}, \mathbf{x}(m))\} \le$$

$$\le |\mathcal{M}_N| \exp\{-N(E - \delta)\}$$

Taking into account (1) we have

$$\sum_{m:\mathbf{u}(m) \in f(\mathcal{M}_N)} P_1W_1^N\{\mathcal{Y}^N - g^{-1}(m)|\mathbf{u}(m))\} \le$$

$$\le |\mathcal{M}_N| \exp\{-N(E - \delta)\}.$$

For any P_0 we can write

$$\sum_{m:\mathbf{u}(m) \in f(\mathcal{M}_N) \cap T_{P_0}^N(U)} P_1W_1^N\{\mathcal{Y}^N - g^{-1}(m)|\mathbf{u}(m)\} \le$$

$$\le |\mathcal{M}_N| \exp\{-N(E - \delta)\}.$$

The number of messages m can be presented as a sum of numbers of codewords of different types

$$|\mathcal{M}_N| = \sum_{P_0} |f(\mathcal{M}_N) \cap T^N_{P_0}(U)|;$$

and the number of all types P_0 is not greater than $(N+1)^{|\mathcal{U}|}$, then there exists a major type P_0^* such, that

$$|\mathcal{M}_N| \leq (N+1)^{|\mathcal{U}|} |f(\mathcal{M}_N) \cap T^N_{P_0^*}(U)|. \qquad (4)$$

Now we can write that for any type $P_1V(y|u)$

$$\sum_{m:\mathbf{u}(m)\in f(\mathcal{M}_N)\cap T^N_{P_0^*}(U)} P_1W_1^N\{T^N{}_{P_1,V}(Y|\mathbf{u}(m)) -$$

$$-g^{-1}(m)|\mathbf{u}(m)\} \leq |\mathcal{M}_N| \exp\{-N(E-\delta)\}$$

For fixed types the conditional probability $P_1W_1^N(\mathbf{y}|\mathbf{u})$ is constant [8]

$$P_1W_1^N(\mathbf{y}|\mathbf{u}) =$$

$$= \exp\{-N(H_{P^*_{0,1}V}(Y|U) + D(P_1V||P_1W_1|P_0^*))\}$$

and we can write

$$\sum_{m:\mathbf{u}(m)\in f(\mathcal{M}_N)\cap T^N_{P_0^*}(U)} \{|T^N{}_{P_1,V}(Y|\mathbf{u}(m))| -$$

$$-|T^N{}_{P_1,V}(Y|\mathbf{u}(m)) \cap g^{-1}(m)|\}P_1W_1^N(\mathbf{y}|\mathbf{u})\} \leq$$

$$\leq |\mathcal{M}_N| \exp\{-N(E-\delta)\}$$

or

$$\sum_{m:\mathbf{u}(m)\in f(\mathcal{M}_N)\cap T^N_{P_0^*}(U)} |T^N{}_{P_1,V}(Y|\mathbf{u}(m))| -$$

$$-\frac{|\mathcal{M}_N| \exp\{-N(E-\delta)\}}{\exp\{-N(H_{P^*_{0,1}V}(Y|U) + D(P_1V||P_1W_1|P_0^*))\}} \leq$$

$$\leq \sum_m |T^N{}_{P_1,V}(Y|\mathbf{u}(m)) \cap g^{-1}(m)|.$$

It follows from the definition of decoding function that the sets $g^{-1}(m)$ are disjoint and, hence, the right part of the last expression is not greater than $|T^N{}_{P^*_{0,1}V}(Y)|$. From the well known properties of types [8]

$$(N+1)^{-|\mathcal{Y}||\mathcal{U}|} \exp\{NH_{P^*_{0,1}}(Y|U)\} \leq$$

$$|T^N{}_{P_1,V}(Y|\mathbf{u}(m))| \leq \exp\{NH_{P^*_{0,1}}(Y|U)\}$$

we obtain

$$|f(\mathcal{M}_N) \cap T^N_{P_0^*}(U)|(N+1)^{-|\mathcal{Y}||\mathcal{U}|} \exp\{NH_{P^*_{0,1}}(Y|U)\} -$$

$$-|\mathcal{M}_N| \exp\{N(H_{P^*_{0,1},V}(Y|U) + D(P_1V||P_1W_1|P_0^*) -$$

$$-E+\delta)\} \leq \exp\{NH_{P^*_{0,1},V}(Y)\}.$$

Taking into account (4) we come at

$$|\mathcal{M}_N| \leq$$

$$\frac{\exp\{NI_{P^*_{0,1},V}(U;Y)\}}{(N+1)^{-|\mathcal{U}|(|\mathcal{Y}|+1)} - \exp\{D(P_1V||P_1W_1|P_0^*) - E + \delta)\}}.$$

The right part of this inequality can be minimized by the choice of conditional type P_1V, keeping the denominator positive, which takes place for large N when the following inequality holds

$$D(P_1V||P_1W_1|P_0^*) \leq E - \delta.$$

We ommit the proof of equivocation rate, as it is the same as in [3] page 384. Theorem 2 is proved.

Corollary. When $E \to 0$ the outer bound of E - capacity eequivocation region (3) coincides with capacity - equivocation region (2) obtained in [2].

4. CONCLUSION AND FUTURE WORK

The E- capacity - equivocation region of the wiretap channel is investigated, the outer bound of this region is derived. When $E \to 0$ this bound coincides with capacity -equivocation region (2) obtained in [2].

REFERENCES

[1] Wyner A. D., The wire-tap channel, *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 1387, 1975.

[2] Csiszár I. and Körner J., Broadcast channel with confidential messages, *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 339 348, 1978.

[3] Liang Y., Poor V., Shamai (Shitz) S., "Information theoretic security", *Foundations and Trends in Communications and Information Theory*, vol.5, nos. 4-5, pp. 355-580, 2008.

[4] Haroutunian E.,"for E-capacity of DMC", *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4210 - 4220, 2007.

[5] Haroutunian E., Haroutunian M., Harutyunyan A., "Reliability criteria in information theory and in statistical hypothesis testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, nos. 2 - 3, 2008.

[6] Haroutunian E., Haroutunian M., Afshar N., "Random coding bound for E-capacity region of the wiretap channel", *Proc. of int. conf. Comp. Science and Inf. Technologies*, Yerevan, pp. 121 - 124, 2011.

[7] Cover T. M. and Thomas J. A., Elements of Information Theory, 2nd edition, *A Wiley-Interscience Publication*, 2006.

[8] Csiszár I., Method of types, *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2505 2523, 1998.