SECRECY CAPACITY OF WIRETAP CHANNELS WITH ADDITIVE COLORED GAUSSIAN NOISE

Hachiro Fujita

Division of Information and Communications Systems
Tokyo Metropolitan University

ABSTRACT

Wyner has shown in his seminal paper on (discrete memoryless) wiretap channels that if the channel between the sender and an eavesdropper is a degraded version of the channel between the sender and the legitimate receiver, then the sender can reliably and securely transmit a message to the receiver, while the eavesdropper obtains absolutely no information about the message. Later, Leung-Yan-Cheong and Hellman extended Wyner's result to the case where the noise is white Gaussian. In this paper we extend the white Gaussian wiretap channel to the colored Gaussian case and show the finite block length secrecy capacity of colored Gaussian wiretap channels. We also show an asymptotic lower bound on the secrecy capacity of a specific colored Gaussian wiretap channel for which optimum power allocation can be found by water filling.

***Index Terms*—** Wiretap channel, colored Gaussian, secrecy capacity, water-filling, autoregressive process

1. INTRODUCTION

The wiretap channel was first introduced by Wyner [7]. He considered a degraded broadcast channel where a channel between the sender and the legitimate receiver is less noisy than the channel between the sender and an eavesdropper. The problem is as follows. The sender wants to reliably transmit a message to the legitimate receiver but wants to make a leakage to the eavesdropper as small as possible. The eavesdropper's uncertainty about the message is called a *message equivocation*. Wyner shows the optimum trade-off between the transmission rate and the message equivocation. The *secrecy capacity* of a wiretap channel is defined to be a maximum transmission rate at which the eavesdropper obtains absolutely no information about the message. Roughly speaking, the secrecy capacity is given by the mutual information between the sender and the receiver minus the mutual information between the sender and the eavesdropper. Wyner's result has been extended to a more general broadcast channel setting [3] and recently multiterminal settings have extensively been investigated. For an overview of wiretap channels see [6].

Leung-Yan-Cheong and Hellman [5] considered the same problem for the wiretap channel with additive white Gaussian noise (AWGN). In this case the secrecy capacity is given by the difference between the main channel capacity and the eavesdropper's channel capacity, that is,

$$\frac{1}{2}\log\left(1+\frac{P}{N_1}\right)-\frac{1}{2}\log\left(1+\frac{P}{N_2}\right) \tag{1}$$

where P is the average power constraint and N_1 (resp. N_2) is the noise power of the Gaussian channel between the sender and the legitimate receiver (resp. between the sender and the eavesdropper).

Images and speech signals are modeled by stationary Gaussian processes. Such signals could be used as wiretap channel noise as used in steganography. In this paper we extend the result of Leung-Yan-Cheong and Hellman to the case where the noise is *not white* but *colored* Gaussian. That is, we consider the wiretap channel with additive colored Gaussian noise (ACGN). We show the finite block length secrecy capacity of ACGN wiretap channels. Interestingly, contrary to the AWGN case, the asymptotic secrecy capacity of a general ACGN wiretap channel may not be equal to the difference between the main channel capacity and the eavesdropper's channel capacity.

The paper is organized as follows. In Section 2 we present the problem formulation for the ACGN wiretap channel and state the main result. In Section 3 we give the proofs of the main result. In Section 4 we show a lower bound on the secrecy capacity of a specific ACGN wiretap channel. We then provide numerical evaluations of the lower bound for an example of an ACGN wiretap channel. Section 5 concludes the paper with some remarks.

1.1. Notation

Capital italic letters such as X, Y and Z denote (usually continuous) random variables. For a positive integer N, X^N denotes a sequence of N random variables $(X_1,\ldots,\mathcal{X}_N)$. X^N can also be thought of as an N-dimensional column vector. We denote the covariance matrix of a random vector X^N by K_{X^N}, i.e., $K_{X^N}=\mathrm{E}[(X^N-\mathrm{E}[X^N])(X^N-\mathrm{E}[X^N])^T]$, and the differential entropy of X^N by $H(X^N)$ (instead of the

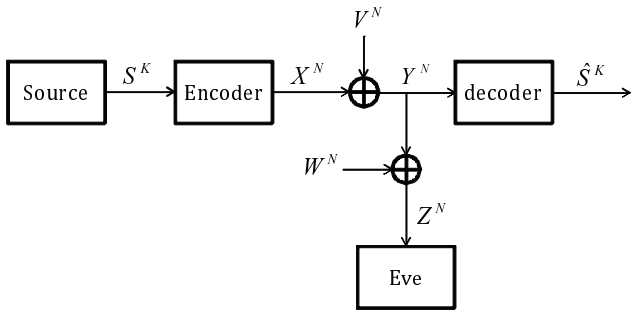

Fig. 1. The Gaussian wiretap channel.

usual notation $h(X^N)$). See standard textbooks on information theory (e.g., [2]) for the definition of differential entropy. We also denote the entropy of a discrete random variable X by $H(X)$. Throughout the paper logarithms are taken to the base 2. So the unit of entropy is a bit.

2. PROBLEM FORMULATION AND THE MAIN RESULT

We follow the problem formulation of [5]. Fig. 1 shows the Gaussian wiretap channel considered in this paper. For simplicity we assume that the source produces independent and identically distributed (i.i.d.) random variables, although the extension to the ergodic case is straightforward (see [5]). The source outputs are divided into blocks of length K and each block is input to the encoder. Let S^K be a block of K source outputs (i.e., K i.i.d. random variables). Alice encodes the block S^K into a codeword X^N of length N that satisfies the average power constraint

$$\mathrm{E}[\frac{1}{N}\sum_{i=1}^{N} X_i^2] \le P. \tag{2}$$

Alice transmits X^N to Bob. Bob receives a corrupted codeword $Y^N = X^N + V^N$ where the summation is taken component-wise and V^N is a Gaussian random vector with zero mean and covariance matrix K_{V^N}. Bob decodes Y^N to a codeword $\hat{X}^N$ from which he estimates the source outputs $\hat{S}^K$. We define the block error rate P_e and the transmission rate R to be respectively,

$$P_e = \Pr\left[S^K \neq \hat{S}^K\right] \quad \text{and} \quad R = H(S^K)/N. \tag{3}$$

On the other hand, Eve receives $Z^N = Y^N + W^N$, a degraded version of Y^N, where W^N is a Gaussian random vector with zero mean and covariance matrix K_{W^N}. We assume that V^N and W^N are statistically independent. We define the fractional equivocation of Eve to be

$$\Delta = H(S^K|Z^N)/H(S^K). \tag{4}$$

Remark 1. We assume that Alice and Bob and even Eve know the statistics of random vectors V^N and W^N, but Eve does not know the realizations of them. It will be shown that Eve's knowledge on the channel statistics does not help to decrease the equivocation.

Definition 1. The rate-equivocation pair (R^*, d^*) is *achievable* if and only if for any $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \ge R^* - \epsilon, \quad \Delta \ge d^* - \epsilon, \quad P_e \le \epsilon. \tag{5}$$

We denote the set of all achievable rate-equivocation pairs (R^*, d^*) by $\mathcal{R}$.

Definition 2. The *secrecy capacity* of a wiretap channel is defined to be

$$C_s = \max_{(R,1)\in\mathcal{R}} R. \tag{6}$$

Definitions 1 and 2 assume the asymptotic setting where N goes to infinity. We can also give similar definitions for the case where N is sufficiently large but fixed (in this case ϵ in Eqs. (5) depends on N.)

We are now ready to state the main result of the paper, i.e., the finite block length secrecy capacity of the ACGN wiretap channel.

Theorem 1. *The secrecy capacity of the N-block channel is given by*

$$C_s^{(N)} = \max_{K_{X^N}} \left[\frac{1}{2N}\log\frac{|K_{X^N}+K_{V^N}|}{|K_{V^N}|} - \frac{1}{2N}\log\frac{|K_{X^N}+K_{V^N}+K_{W^N}|}{|K_{V^N}+K_{W^N}|}\right] \tag{7}$$

where the maximization is over the set of positive semidefinite matrices K_{X^N} such that $\frac{1}{N}\mathrm{tr}(K_{X^N}) \le P$.

Remark 2. It is not hard to show that the difference in the brackets in Eq. (7) is nonnegative.

3. PROOFS

In this section we prove Theorem 1. We have to prove achievability and the converse.

3.1. Basic facts

Before giving the proofs, we give some basic facts as lemmas.

Lemma 1. *Let U^N and V^N be continuous random vectors and independent of each other, and let $W^N = U^N + V^N$.*

(a) $K_{W^N} = K_{U^N} + K_{V^N}$.

(b) If U^N and V^N are Gaussian, then W^N is also Gaussian.

(c) $H(W^N|U^N) = H(V^N)$.

Lemma 2. *Let U^N be a Gaussian random vector with any mean and covariance matrix K_{U^N}. Then*

$$H(U^N) = \frac{1}{2}\log[(2\pi e)^N |K_{U^N}|]. \tag{8}$$

3.2. Proof of achievability

We have to show that $(C_s^{(N)}, 1)$ is achievable, that is, for $\epsilon > 0$, there exists an encoder-decoder pair such that

$$R \geq C_s^{(N)} - \epsilon, \quad \Delta \geq 1 - \epsilon, \quad P_e \leq \epsilon. \tag{9}$$

The proof uses the finite block length coding theorem for ACGN channels [1]. Let Z^N be a Gaussian random vector with zero mean and covariance matrix K_{Z^N} and consider an N-block channel with additive noise Z^N: if X^N is the input to the channel, then the channel output is $Y^N = X^N + Z^N$, where the summation is taken component-wise. Define

$$C^{(N)} = \max_{K_{X^N}} \frac{1}{2N} \log \frac{|K_{X^N} + K_{Z^N}|}{|K_{Z^N}|} \tag{10}$$

where the maximization is over the set of positive semidefinite matrices K_{X^N} such that $\frac{1}{N}\mathrm{tr}(K_{X^N}) \leq P$.

Theorem 2. *[1] For $\epsilon > 0$ and for all sufficiently large integer N, there exists a $(2^{N(C^{(N)}-\epsilon)}, N)$ code with the probability of error approaching 0 as $N \to \infty$.*

The achievability proof of [5] is based on the random coding argument used in the proof of the (infinite block length) coding theorem for AWGN channels (see, e.g., [2]). The same argument using Theorem 2 applies. In fact, the achievability proof of [5] applies to our case if we replace the channel capacities C_M and C_{MW} of [5] by the Alice-Bob (finite block length) channel capacity $C_{AB}^{(N)}$ and the Alice-Eve (finite block length) channel capacity $C_{AE}^{(N)}$, respectively, where $C_{AB}^{(N)}$ and $C_{AE}^{(N)}$ are defined by respectively,

$$C_{AB}^{(N)} = \frac{1}{2N} \log \frac{|K_{X^N} + K_{V^N}|}{|K_{V^N}|} \quad \text{and} \tag{11}$$

$$C_{AE}^{(N)} = \frac{1}{2N} \log \frac{|K_{X^N} + K_{V^N+W^N}|}{|K_{V^N+W^N}|}, \tag{12}$$

and we take the covariance matrix K_{X^N} to be a maximizer of the right hand side of Eq. (7). From Lemma 1 (a) we have $K_{V^N+W^N} = K_{V^N} + K_{W^N}$, which completes the proof.

3.3. Proof of the converse

We will show that if (R, Δ) is an achievable pair, then we have

$$R(\Delta - \epsilon_N) \leq C_s^{(N)} \tag{13}$$

where $\epsilon_N \to 0$ as $N \to \infty$. If this is the case, taking $\Delta = 1$ we obtain $R \leq C_s^{(N)}/(1-\epsilon_N)$, which shows that $C_s^{(N)}/(1-\epsilon_N)$ is the maximum rate at which perfect secrecy is achieved. Note that in the finite block length case we cannot make ϵ_N zero, although $\epsilon_N \to 0$ as $N \to \infty$. The proof also follows the same line as the converse proof of [5].

Lemma 3. *[5, Lemma 6]*

$$R\left(\Delta - \frac{KP_e \log \nu + h(P_e)}{RN}\right) \leq \frac{I(X^N; Y^N|Z^N)}{N} \tag{14}$$

where ν is the size of the source alphabet and $h(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy function.

The following is a minor change of Lemma 7 of [5].

Lemma 4.

$$I(X^N; Y^N|Z^N) = \frac{1}{2}\log\frac{|K_{V^N} + K_{W^N}|}{|K_{V^N}|} - [H(Z^N) - H(Y^N)]. \tag{15}$$

Lemma 5. *$H(Z^N) - H(Y^N)$ is smallest if Y^N is Gaussian with zero mean.*

From the above lemma, to obtain an upper bound on $I(X^N; Y^N|Z^N)$ we may take Y^N to be Gaussian with zero mean. Then, from Lemma 1 (b) $Z^N = Y^N + W^N$ is also Gaussian with zero mean. Using Lemma 2 and Lemma 1 (a), Eq. (15) becomes

$$I(X^N; Y^N|Z^N) \leq \frac{1}{2}\log\frac{|K_{X^N} + K_{V^N}|}{|K_{V^N}|} - \frac{1}{2}\log\frac{|K_{X^N} + K_{V^N} + K_{W^N}|}{|K_{V^N} + K_{W^N}|}. \tag{16}$$

Taking the maximization of the right hand side of the above inequality with respect to K_{X^N} subject to $\frac{1}{N}\mathrm{tr}(K_{X^N}) \leq P$, we obtain

$$I(X^N; Y^N|Z^N)/N \leq C_s^{(N)}. \tag{17}$$

Using this and Lemma 3 we obtain

$$R\left(\Delta - \frac{KP_e \log \nu + h(P_e)}{RN}\right) \leq C_s^{(N)}. \tag{18}$$

Define $\epsilon_N = (KP_e \log \nu + h(P_e))/RN$. Since $P_e \to 0$ as $N \to \infty$, $\epsilon_N \to 0$ as $N \to \infty$, which completes the proof.

4. A LOWER BOUND ON THE SECRECY CAPACITY

In this section we give a lower bound on the secrecy capacity of a specific wiretap channel where $\{V_i\}_{i=1}^{\infty}$ is a stationary Gaussian process and $\{W_i\}_{i=1}^{\infty}$ is a sequence of i.i.d. Gaussian random variables of zero mean and variance σ_2^2. From the definition of the secrecy capacity $C_s^{(N)}$ we have that

$$C_s^{(N)} \geq \frac{1}{2N}\log\frac{|K_{X^N} + K_{V^N}|}{|K_{V^N}|} - \frac{1}{2N}\log\frac{|K_{X^N} + K_{V^N} + \sigma_2^2 I_N|}{|K_{V^N} + \sigma_2^2 I_N|} \tag{19}$$

for any input X^N whose covariance matrix K_{X^N} satisfies $\frac{1}{N}\mathrm{tr}(K_{X^N}) \le P$.

Let $N(f) = \sum_{k=-\infty}^{\infty} R_V(k) e^{-j2\pi kf}$ be the power spectral density of the noise process $\{V_i\}_{i=1}^{\infty}$, where $R_V(k) = \mathrm{E}[V_i V_{i+k}]$. Using a standard optimization technique and the Toeplitz distribution theorem we obtain a parametric expression for an asymptotic lower bound on the secrecy capacity

$$\liminf_{N\to\infty} C_s^{(N)} \ge \underline{C}_s(\theta) = \int_{-1/2}^{1/2} \frac{1}{2} \log\left(1 + \frac{[\theta - N(f)]^+}{N(f)}\right) df - \int_{-1/2}^{1/2} \frac{1}{2} \log\left(1 + \frac{[\theta - N(f)]^+}{N(f) + \sigma_2^2}\right) df \tag{20}$$

with the average power

$$P(\theta) = \int_{-1/2}^{1/2} [\theta - N(f)]^+ df. \tag{21}$$

The optimum power allocation for independent channel inputs is given by the so-called water-filling scheme.

4.1. An example

Speech signals are modeled by autoregressive (AR) processes. Suppose that V_i's in Fig. 1 are speech signals. In this case Bob's received signals are given by speech signals plus a codeword of a predetermined Gaussian random code (see Sec. 3.2). On the other hand, Eve's received signals are Bob's received signal plus white Gaussian noise. Below we compute the lower bound $\underline{C}_s(\theta)$ for the secrecy capacity of the ACGN wiretap channel where the noise is described by a first-order AR process.

Example 1. Let $\{V_i\}_{i=1}^{\infty}$ be an AR(1) process: $V_i = -\rho V_{i-1} + U_i$ where $-1 < \rho < 1$ and $\{U_i\}_{i=1}^{\infty}$ is a white Gaussian noise process with power spectral density σ_1^2. The power spectral density of $\{V_i\}_{i=1}^{\infty}$ is well-known and given by

$$N(f) = \frac{\sigma_1^2}{|1 + \rho e^{-j2\pi f}|^2}. \tag{22}$$

See, e.g., [4], for a derivation. Varying θ in Eqs. (20) and (21) we obtain numerical evaluations of the lower bound $\underline{C}_s(\theta)$ and average power $P(\theta)$ as shown in Fig. 2.

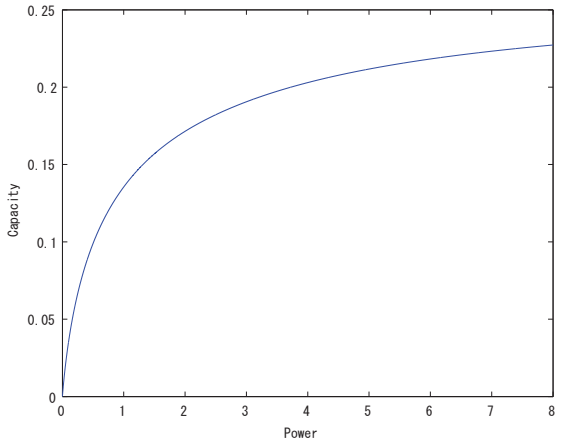

Fig. 2. Lower bound $\underline{C}_s(\theta)$ vs. average power $P(\theta)$ for the case $\rho = 0.5$ and $\sigma_1^2 = \sigma_2^2 = 1.0$.

5. CONCLUSION

In this paper we have presented the finite block length secrecy capacity of ACGN wiretap channels. We also derived an asymptotic lower bound on the secrecy capacity for the case where the Alice-Bob channel is an additive stationary Gaussian noise channel and Eve's channel is further disturbed by white Gaussian noise.

We conclude the paper with future research direction. Our proof is nonconstructive and does not give any practical code for the ACGN wiretap channel. So code construction is an important and interesting research problem. Recent development of LDPC codes for the AWGN wiretap channel may be suggestive (see [6] for a survey of this topic). It is also interesting to extend our result to the Gaussian waveform channel.

6. REFERENCES

[1] T. M. Cover and S. Pombra, "Gaussian feedback capacity," IEEE Trans. Inf. Theory, vol. 35, no. 1, pp. 37–43, 1989.

[2] T. M. Cover and J. A. Thomas, Elements of Information Theory, John Wiley & Sons, 1991.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, 1978.

[4] R. M. Gray and L. D. Davisson, An Introduction to Statistical Signal Processing, Cambridge University Press, London, 2005.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–456, 1978

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," Foundations and Trends in Communications and Information Theory, Vol. 5, Nos. 4–5, pp. 355–580, 2008.

[7] A. D. Wyner, "The wire-tap channel," Bell System Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.