Gaussian Wiretap Channel with Collaborative Wiretappers

Svyatoslav Voloshynovskiy, Taras Holotyak, Ivan Prudyus

***Abstract*—In this paper, we consider the compound wiretap channel with collaborative wiretappers. Contrarily to [1], where the wiretappers act independently, we analyze the setup when the wiretappers form a coalition, which shares the observed data within the coalition. The goal of coalition consists in learning the secret message communicated to the legitimate user by sharing their observations to produce the best possible estimate thus benefiting from available redundancy. We analyze the secrecy capacity for the Gaussian data and correlated observations. As the result, we provide the estimate of the impact of coalition of wiretappers on reduction of secrecy capacity.**

***Index Terms*—Wiretap channel, secrecy capacity, collaborative wiretappers.**

I. Introduction

The wiretap channel model of Wyner appeared as a noisy counterpart of noiseless secure information transmission problem of Shannon [2]. In Wyner wiretap model [3], essentially linked to the secure extension of broadcast channel [4], the advantage of legitimate information receiver in the level of noise in data is exploited over the opponent who observes the same transmission in more noisy environment. Several cases of discrete memoryless channels (DMC) including Gaussian one were studied in [5] and it was demonstrated that the secrecy capacity is equal to the difference between the capacity of the main channel connecting the sender and the legitimate user and the wiretap channel. Csiszar and Korner in [6] extended this model and characterized the capacity of DMC under security constraints. Liang et al [1] further extended these results to compound channel where both legitimate and wiretap channels might take a number of states. The most related considered case is based on the semi deterministic compound wiretap channel where the secrecy capacity is found. This case includes the legitimate receiver and the the group of wiretappers that observe independently the transmission. The secrecy capacity is determined by the worst channel among the group of wiretappers. It is important to underline that the wiretappers do not form any sort of coalition to benefit from their joint knowledge that makes this strategy restrictive in sense of largest expected harm.

At the same time, in the number of applications such as ongoing payment systems based on near-field communication (NFC) [7], [8], the wiretappers can form the coalitions and share among them the results of their individual observations. Such a form of collaborative coalition is able to benefit from the redundant noisy observations and can produce better estimate of the secret message in comparison to the individual estimates analyzed in [1]. If the number of wiretappers in the coalition is sufficient, the coalition can disclose the secret message. It also means that the secrecy rate approaches zero and no secure transmission is possible anymore. At the same time, the distortions in the wiretapper channels might be correlated and it is important to establish the theoretical limits of this coalition. Therefore, the goal of this paper is to establish the secrecy rate under collaborative coalition of wiretappers and to investigate the impact of dependent observations for the Gaussian and binary observation models.

S. Voloshynovskiy and T. Holotyak are with the Department of Computer Sciences, University of Geneva, Switzerland. E-mails: {svolos, Taras.Holotyak}@unige.ch

I. Prudyus is with the Institute of Telecommunications, Radioelectronics and Electronic Engineering, Lviv Polytechnic National University, Ukraine. E-mail: iprudyus@lp.edu.ua

II. Problem formulation

We consider the following wiretap channel model.

Definition 1 (*degraded wiretap channel*): The degraded wiretap channel consists of input alphabet $\mathcal{X}^N$, the output alphabet of legitimate user $\mathcal{Y}^N$, J channel outputs of wiretappers $\mathcal{V}^N$ and the corresponding transition probabilities for the legitimate user, assumed to be memoryless, $p(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^N p(y_i|x_i)$ and the wiretappers $p(\mathbf{v}_j|\mathbf{y}) = \prod_{i=1}^N p(v_{ij}|y_i)$, where $\mathbf{x} \in \mathcal{X}^N$ is the channel input generated by the encoder, $\mathbf{y} \in \mathcal{Y}^N$ is the channel output available for the legitimate user, $\mathbf{v}_j \in \mathcal{V}_j^N$ is the wiretap channel output available for the j wiretapper.

Definition 2 (*code construction*): The $(2^{NR}, N)$ code for the wiretap channel consists of:

- a *message set* $\mathcal{W} = \{1, 2, \cdots, 2^{NR}\}$ with the message M uniformly distributed over $\mathcal{W}$;
- an *encoder* ϕ: $\mathcal{W} \mapsto \mathcal{X}^N$;
- a *decoder* g: $\mathcal{Y}^N \mapsto \mathcal{W}$.

The wiretap observation model $V_j = X + Z + W_j = X + W_j'$, $1 \le j \le J$ and $W_j' = Z + W_j$ denotes the equivalent noise in the jth wiretap channel.

The secrecy capacity with the collaborative wiretappers is:

$$C_s = \max_{p(x)} \left[I(X;Y) - I(X;V_1, V_2, \cdots, V_J) \right]. \qquad (1)$$

The first term represents the capacity for the legitimate channel that under the Gaussian assumptions yields:

$$C_L = I(X;Y) = \frac{1}{2} \log_2 \left(1 + \frac{\sigma_X^2}{\sigma_Z^2} \right). \qquad (2)$$

The second term corresponds to the capacity of collaborative wiretapper channel:

$$\begin{aligned} C_W=&I(X;V_1,V_2,\cdots,V_J)\\ =&h(V_1,V_2,\cdots,V_J)-h(V_1,V_2,\cdots,V_J|X)\\ =&h(V_1,V_2,\cdots,V_J)-h(W_1',W_2',\cdots,W_J'). \end{aligned} \quad (3)$$

The vector $(V_1,V_2,\cdots,V_J)$ is distributed according to the Gaussian distribution $\mathcal{N}(\mathbf{0},\mathbb{K}_{V_1,V_2,\cdots,V_J})$ with the covariance matrix:

$$\mathbb{K}_{V_1,V_2,\cdots,V_J}=\begin{bmatrix} E[V_1V_1]\,E[V_1V_2]\cdots E[V_1V_J]\\ E[V_1V_2]\,E[V_2V_2]\cdots E[V_2V_J]\\ \cdots\\ E[V_1V_J]E[V_2V_J]\cdots E[V_JV_J] \end{bmatrix} \quad (4)$$

with the diagonal elements $E[V_jV_j]=\sigma_X^2+\sigma_Z^2+\sigma_W^2$, $1\leq j\leq J$ and off-diagonal elements $E[V_iV_j]=\sigma_X^2+\sigma_Z^2+\rho\sigma_W^2$, $i\neq j$. The entropy of this vector is defined as [4]:

$$h(V_1,V_2,\cdots,V_J)=\frac{1}{2}\log_2(2\pi e)^J|\mathbb{K}_{V_1,V_2,\cdots,V_J}|, \quad (5)$$

that for the above case yields:

$$\begin{aligned} h(V_1,V_2,\cdots,V_J)=&\frac{1}{2}\log_2((2\pi e)^J((1-\rho)\sigma_W^2)^{J-1}\times\\ &\times(J(\sigma_X^2+\sigma_Z^2)+\sigma_W^2(1+(J-1)\rho))). \end{aligned} \quad (6)$$

The second term in (3) corresponds to the entropy of equivalent noise vector W_j', $1\leq j\leq J$ in wiretap channels that is considered to be correlated over wiretap channels and distributed according to $\mathcal{N}(\mathbf{0},\mathbb{K}_{W_1',W_2',\cdots,W_J'})$. The noise in each wiretap channel consists of the regular part Z that is the same for all channels and the correlated component W_j. The covariance matrix $\mathbb{K}_{W_1',W_2',\cdots,W_J'}$ is the Toeplitz matrix with the diagonal elements $E[W_j'W_j']=\sigma_Z^2+\sigma_W^2$, $1\leq j\leq J$ and off-diagonal elements $E[W_i'W_j']=\sigma_Z^2+\rho\sigma_W^2$, $i\neq j$. The entropy of this terms is:

$$h(W_1',W_2',\cdots,W_J')=\frac{1}{2}\log_2(2\pi e)^J|\mathbb{K}_{W_1',W_2',\cdots,W_J'}|. \quad (7)$$

One can easily find the determinant $|\mathbb{K}_{W_1',W_2',\cdots,W_J'}|=((1-\rho)\sigma_W^2)^{J-1}(J\sigma_Z^2+\sigma_W^2(1+(J-1)\rho))$ and the entropy:

$$\begin{aligned} h(Z_1,Z_2,\cdots,Z_J)=&\frac{1}{2}\log_2((2\pi e)^J((1-\rho)\sigma_W^2)^{J-1}\times\\ &\times(J\sigma_Z^2+\sigma_W^2(1+(J-1)\rho))). \end{aligned} \quad (8)$$

Combining (6) and (8), the capacity of J wiretap channels (3) yields:

$$C_W=\frac{1}{2}\log_2\left(1+\frac{\sigma_X^2}{\sigma_Z^2+\frac{(1+(J-1)\rho)}{J}\sigma_W^2}\right). \quad (9)$$

For the case $J=2$ and assumption of stationary component Z for both channels, the obtained result coincides with the well-known exercise for the two-look channel from [4]:

$$I(X;V_1,V_2)=\frac{1}{2}\log_2\left(1+\frac{\sigma_X^2}{\sigma_Z^2+\frac{(1+\rho)}{2}\sigma_W^2}\right). \quad (10)$$

The resulting secrecy capacity (1) is then defined by:

$$\begin{aligned} &C_s=\\ &\tfrac{1}{2}\log_2\left(1+\tfrac{\sigma_X^2}{\sigma_Z^2}\right)-\tfrac{1}{2}\log_2\left(1+\tfrac{\sigma_X^2}{\sigma_Z^2+\frac{(1+(J-1)\rho)}{J}\sigma_W^2}\right). \end{aligned} \quad (11)$$

The goal of the coalition of wiretappers consists in the disclose of secret message sent to the legitimate user or equivalently in the minimization of secrecy capacity C_s using the multiple observations.

In the case when there is only one member of coalition, i.e., when $J=1$, the secrecy capacity simply reduces to the classical case:

$$C_s=\frac{1}{2}\log_2\left(1+\frac{\sigma_X^2}{\sigma_Z^2}\right)-\frac{1}{2}\log_2\left(1+\frac{\sigma_X^2}{\sigma_Z^2+\sigma_W^2}\right). \quad (12)$$

It is important to note that the coalition can only benefit in the situation when the noise in each channel is independent. Indeed, if the observations are correlated with $\rho=1$, there is no any gain from the multiple observations since the term $\frac{(1+(J-1)\rho)}{J}=1$ is non-decreasing with J. In this case, the legitimate user channel is always less noisy with respect to the wiretap channel.

Therefore, the only situation of interest is when the noise in the wiretap channels is uncorrelated. The extreme case corresponds to the situation when $\rho=0$, i.e., all observations are also independent in the considered Gaussian case. Under this assumption, the coalition of wiretappers can minimize the noise up to the factor $\frac{1}{J}\sigma_W^2$. Therefore, increasing the size of coalition J the secrecy capacity tends to 0.

III. Conclusions

In this paper, we addressed the problem of impact of collaborative wiretappers on the capacity of wiretap channels. It is demonstrated that increasing the number of wiretappers, the coalition can asymptotically reduce the secrecy capacity and disclose secure communications. The impact of correlation between the noise realizations in each channel is also demonstrated.

References

[1] Yingbin Liang, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai, "Compound wiretap channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 5:1–5:12, March 2009.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal, Vol 28, pp. 656715*, October 1949.

[3] Aaron D. Wyner, "The wiretap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[4] T. Cover and J. Thomas, *Elements of information theory*, Wiley, 1991.

[5] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451 – 456, jul 1978.

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339 – 348, may 1978.

[7] Brad Molen, "Engadget primed: What is nfc, and why do we care?," Jun 2011, http://www.engadget.com/2011/06/10/engadget-primed-what-is-nfc-and-why-do-we-care/.

[8] Nick Pelly and Jeff Hamilton, "How to nfc," May 2011, http://www.google.com/events/io/2011/sessions/how-to-nfc.html.