ISIT'2013 1569716585

Joint Source-Channel Coding for Multiple-Access Wiretap Channels

Sadaf Salehkalaibar and Mohammad Reza Aref
Information Systems and Security Lab (ISSL),
Department of Electrical Engineering,
Sharif University of Technology, Tehran, Iran
E-mails: s_saleh@ee.sharif.edu, aref@sharif.edu

***Abstract*—In this paper, we consider lossy source transmission over a Multiple Access WireTap Channel (MAC-WT). In this model, there are two correlated sources, each of them is available at the corresponding encoder. The receiver tries to reconstruct both sources with desired distortions. The sources should be kept secret from an eavesdropper. We propose a joint source-channel scheme for the MAC-WT. In this scheme, each source sequence is mapped to common and private codewords. The common codeword can be decoded by the eavesdropper. The private codeword needs to be kept secret from the eavesdropper by using Wyner's wiretap coding. We also discuss some special cases of the proposed scheme.**

I. Introduction

The problem of transmitting correlated sources over multi-user channels has received considerable attention, recently. It has been shown that in multi-user discrete memoryless channels, the separation scheme is not generally optimal [1]. Designing joint source-channel codes has been considered in some works [2]-[6] to provide a general scheme for the transmission of sources over networks. In [3]-[4], both joint and separate schemes have been studied for a class of multi-user channels. In [5], a joint source-channel coding scheme has been proposed where the encoder maps the observed sequence and the corresponding compressed codeword to the channel input. The decoder reconstructs the source sequence by a mapping of the channel output and the decoded codeword. In [6], secure transmission of correlated sources with side information at the receivers has been investigated.

In this paper, we consider lossy transmission of correlated sources over a Multiple Access WireTap Channel (MAC-WT). Consider a MAC-WT where there are two correlated sources, each of them at the corresponding encoder. The legitimate receiver tries to reconstruct the sources with desired distortions. The sources should be kept secret from the eavesdropper. In this work, a joint scheme based on hybrid coding of [5] is proposed to find sufficient conditions for the lossy communication of sources over MAC-WT. In this scheme, each source sequence is mapped to two codewords. The first codeword denotes the common part of the source sequence which can be decoded by the eavesdropper. The second codeword denotes the private part of the source sequence that needs to be kept secret from the eavesdropper using Wyner's coding scheme [7]. The encoder maps the source sequence and the corresponding codewords to the channel input. We discuss some special cases of the proposed inner bound. The case of uncoded transmission as a special case of our scheme is also studied. It is shown that the correlation of sources helps the eavesdropper to obtain some information about the sources.

The paper is organized as follows. In Section II, we present a mathematical framework for the work. In Section III, we propose a joint scheme for the lossy communication of sources over MAC-WT. In Section IV, some special cases are studied. Conclusions are provided in Section V.

II. Preliminaries and Definitions

We denote discrete random variables with capital letters, e.g., X, Y, and their realizations with lower case letters x, y. X_i^j indicates a sequence of random variables $(X_i, ..., X_j)$. We use $H(.)$ to denote the entropy of a discrete random variable and $I(.;.)$ to denote the mutual information between two discrete random variables. We denote by $A_\varepsilon^n(X,Y)$ the set of ε-strongly jointly typical sequences of length n, on $p(x,y)$. A random variable X takes values in a set $\mathcal{X}$. Finally, we denote the probability density function of X over $\mathcal{X}$ with $p(x)$ and the conditional probability density function of X given Y by $p(x|y)$.

Consider the problem of transmission of correlated discrete memoryless sources (S_1, S_2) over a discrete memoryless Multiple-Access WireTap Channel (MAC-WT) $(\mathcal{X}_1 \times \mathcal{X}_2, p(y,z|x_1,x_2), \mathcal{Y} \times \mathcal{Z})$ as depicted in Fig. 1. Each sender tries to send its source to the legitimate receiver so that both sources are reconstructed with desired distortions. The sources must be kept secret from the eavesdropper.

Let $d_1 : \mathcal{S}_1 \times \mathcal{S}_1 \to [0, d_{\max}]$ and $d_2 : \mathcal{S}_2 \times \mathcal{S}_2 \to [0, d_{\max}]$ be two finite distortion measures such that $0 \leq d_{\max} < \infty$.

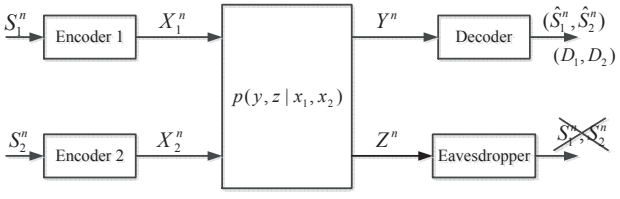

Fig. 1. Lossy source transmission over MAC-WT

The average per-letter distortion for each $s_j^n, \hat{s}_j^n \in \mathcal{S}_j^n$, $j = 1:2$, is defined as $d(s_j^n, \hat{s}_j^n) = \frac{1}{n}\sum_{i=1}^n d(s_{j,i}, \hat{s}_{j,i})$.

Definition 1: An (n, n)-code for source-channel coding is defined by

- two stochastic encoding functions at senders: $f_1 : \mathcal{S}_1^n \to \mathcal{X}_1^n$ and $f_2 : \mathcal{S}_2^n \to \mathcal{X}_2^n$,
- a decoding function at the receiver: $g : \mathcal{Y}^n \to \mathcal{S}_1^n \times \mathcal{S}_2^n$.

Definition 2: A tuple $(D_1, D_2, R_{e1}, R_{e2}, R_{e12})$ is said to be achievable if there exists an (n, n)-code such that

$$E[d_1(S_1^n, \hat{S}_1^n)] \le D_1, \tag{1}$$
$$E[d_2(S_2^n, \hat{S}_2^n)] \le D_2, \tag{2}$$
$$\frac{1}{n}H(S_1^n|Z^n) \ge R_{e1} \tag{3}$$
$$\frac{1}{n}H(S_2^n|Z^n) \ge R_{e2} \tag{4}$$
$$\frac{1}{n}H(S_1^n, S_2^n|Z^n) \ge R_{e12}. \tag{5}$$

The set of all achievable tuples is denoted by $\mathcal{R}^*$ and is referred to as the rate-distortion-equivocation region.

III. Main Result

In this section, we first review hybrid coding for a point-to-point channel which was first introduced in [5]. Then, we propose an achievable region for the MAC-WT. Suppose that a source $S \sim p(s)$ is to be sent over the discrete memoryless channel $(\mathcal{X}, p(y|x), \mathcal{Y})$, see Fig. 2. The decoder reconstructs the sequence S by $\hat{S}$. The average distortion must satisfy $E[d(S, \hat{S})] \le D$, where d is a distortion measure. In the hybrid scheme of [5] (see Fig. 3), 2^{nR} sequences $u^n(T), T \in [1 : 2^{nR}]$ are generated. The source sequence S^n is mapped to one of 2^{nR} sequences $U^n(T)$. The sequence $U^n(T)$ is then mapped to X^n. The decoder finds $U^n(T)$ and reconstructs $\hat{S}^n$ from $U^n(T)$. In this scheme, a single codeword $U^n(T)$ depends on both source and channel codebooks, so it depends on the entire codebooks. Just as mentioned in [5], averaging over all codebooks is not the same as the coventional random coding proof. Let P_e be the probability of the event that there exists $\tilde{T} \ne T$ such that $(U^n(\tilde{T}), Y^m) \in A_\epsilon^n$. Then, we have the following lemma.

Lemma 1 ([5]): The probability P_e is upper bounded as

$$P_e < 4.2^{n(R - I(U;Y) + \epsilon)} \tag{6}$$

for $\epsilon > 0$.

Now, we are ready to find an achievable region for the MAC-WT using hybrid scheme.

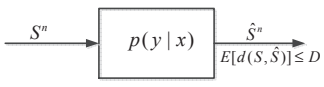

Fig. 2. Lossy communication over a point-to-point channel

Theorem 1: A tuple $(D_1, D_2, R_{e1}, R_{e2}, R_{e12})$ is achievable for MAC-WT if

$$\left\{\begin{array}{l} I(W_1;S_1) < I_1, I(W_2;S_2) < I_2, \\ I(W_1;S_1) + I(W_2;S_2) < I_3, \\ I(V_1;S_1) < I_4, I(V_2;S_2) < I_5, \\ I(V_1;S_1|W_1) < I_6, I(V_2;S_2|W_2) < I_7, \\ I(V_1;S_1) + I(V_2;S_2) < I_8, \\ I(V_1;S_1|W_1) + I(V_2;S_2|W_2) < I_9, \\ I(V_1;S_1) + I(V_2;S_2|W_2) < I_{10}, \\ I(V_1;S_1|W_1) + I(V_2;S_2) < I_{11}, \\ R_{e1} < H(S_1|W_1) - I(X_1;Z|W_1) + \\ \quad \min\{I_{12} - I(V_1;S_1|W_1), \\ \quad I_6 - I(V_1;S_1|W_1), I_4 - I(V_1;S_1)\}, \\ R_{e2} < H(S_2|W_2) - I(X_2;Z|W_2) + \\ \quad \min\{I_{13} - I(V_2;S_2|W_2), \\ \quad I_7 - I(V_2;S_2|W_2), I_5 - I(V_2;S_2)\}, \\ R_{e12} < H(S_1,S_2|W_1,W_2) - I(X_1,X_2;Z|W_1,W_2) + \\ \quad \min\{I_{14} - I(V_1;S_1|W_1) - I(V_2;S_2|W_2), \\ \quad I_8 - I(V_1;S_1) - I(V_2;S_2), \\ \quad I_9 - I(V_1;S_1|W_1) - I(V_2;S_2|W_2), \\ \quad I_{10} - I(V_1;S_1) - I(V_2;S_2|W_2), \\ \quad I_{11} - I(V_1;S_1|W_1) - I(V_2;S_2)\} \end{array}\right\} \tag{7}$$

for some $p(s_1, s_2)p(x_1, v_1, w_1|s_1)p(x_2, v_2, w_2|s_2)$ and functions $\hat{s}_1(v_1, w_1, v_2, w_2, y)$ and $\hat{s}_2(v_1, w_1, v_2, w_2, y)$ such that $E[d_j(S_j, \hat{S}_j)] \le D_j$, $j = 1:2$, where $I_i (i = 1:14)$ are shown in (8) at the top of next page.

Proof: Each source sequence S_j^n, $j = 1:2$, is mapped to one of $2^{nR_j^o}$ sequences $W_j^n(r_j^o)$ (see Fig. 4). The pair $(S_j^n, W_j^n(r_j^o))$ is then mapped to one of $2^{n(R_j^p + R_j^r)}$ sequences $V_j^n(r_j^o, r_j^p, r_j^r)$. The sequence $W_j^n(r_j^o)$ denotes the common information that can be decoded by the eavesdropper. The sequence $V_j^n(r_j^o, r_j^p, r_j^r)$ denotes the private information that should be kept secret from the eavesdropper by using randomness. Then, the source and the codewords corresponding to the indices (r_j^o, r_j^p, r_j^r) are mapped to the sequence X_j^n. In this scheme, the codewords $W_j^n(r_j^o)$ and $V_j^n(r_j^o, r_j^p, r_j^r)$ depend on the entire source sequences. Therefore, the analysis of the probability of error is not the same as the conventional random coding proof.

A. Codebook Generation

Fix a conditional pmf $p(v_1, w_1|s_1)p(v_2, w_2|s_2)$, encoding functions $x_1(w_1, v_1, s_1)$ and $x_2(w_2, v_2, s_2)$, and reconstruction functions $\hat{s}_1(v_1, w_1, v_2, w_2, y)$ and $\hat{s}_2(v_1, w_1, v_2, w_2, y)$ such that $E[d_j(S_j, \hat{S}_j)] \le D_j/(1+\epsilon)$, $j = 1:2$. For $j = 1:2$,

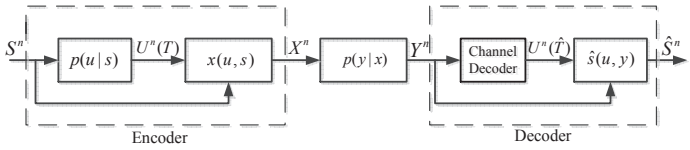

Fig. 3. Hybrid scheme for a point-to-point channel

$$
\begin{aligned}
&I_1 = I(W_1; Z|W_2), I_2 = I(W_2; Z|W_1), I_3 = I(W_1, W_2; Z) + I(W_1; W_2)\\
&I_4 = I(W_1, V_1; W_2, V_2, Y),\\
&I_5 = I(W_2, V_2; W_1, V_1, Y),\\
&I_6 = I(V_1; W_2, V_2, Y|W_1),\\
&I_7 = I(V_2; W_1, V_1, Y|W_2)\\
&I_8 = I(W_1, V_1, W_2, V_2; Y) + I(W_1, V_1; W_2, V_2),\\
&I_9 = I(V_1, V_2; Y|W_1, W_2) + I(W_1, V_1; W_2, V_2) - I(W_1; W_2)\\
&I_{10} = I(W_1, V_1, V_2; Y|W_2) + I(W_1, V_1; W_2, V_2),\\
&I_{11} = I(V_1, W_2, V_2; Y|W_1) + I(W_1, V_1; W_2, V_2)\\
&I_{12} = I(V_1; S_1, Z|W_1),\\
&I_{13} = I(V_2; S_2, Z|W_2),\\
&I_{14} = I(V_1, V_2; S_1, S_2, Z|W_1, W_2)
\end{aligned} \tag{8}
$$

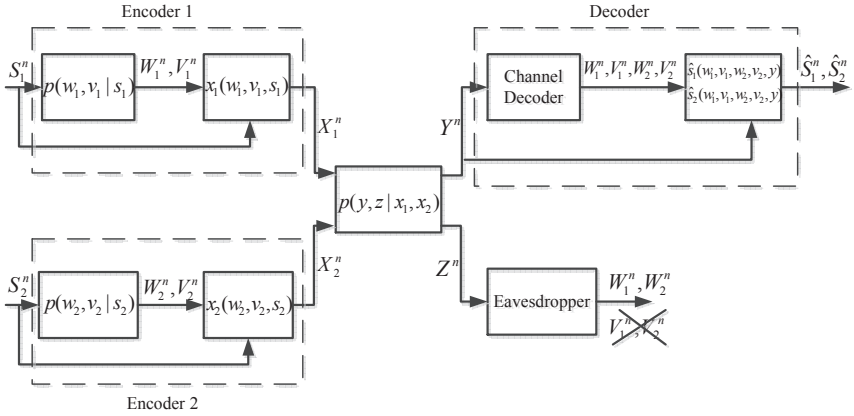

Fig. 4. Hybrid scheme for MAC-WT

randomly and independently generate $2^{nR_j^o}$ sequences $w_j^n(r_j^o)$, $r_j^o \in [1 : 2^{nR_j^o}]$ each according to $\prod_{i=1}^n p(w_{ji})$. For each $w_j^n(r_j^o)$, randomly and independently generate $2^{n(R_j^p+R_j^r)}$ sequences $v_j^n(r_j^o, r_j^p, r_j^r)$, $r_j^p \in [1 : 2^{nR_j^p}]$, $r_j^r \in [1 : 2^{nR_j^r}]$, each according to $\prod_{i=1}^n p(v_{ji}|w_{ji}(r_j^o))$. See Fig. 5.

B. Encoding

Assume that the random index r_j^r, $j = 1 : 2$, is provided to encoder j. Transmitter j first finds codewords $w_j^n(r_j^o)$ and $v_j^n(r_j^o, r_j^p, r_j^r)$ such that $(w_j^n(r_j^o), v_j^n(r_j^o, r_j^p, r_j^r), s_j^n) \in A_\epsilon^n(W_j, V_j, S_j)$. This can be done with an arbitrarily small probability of error if

$$R_j^o \geq I(W_j; S_j) \tag{9}$$

$$R_j^p \geq I(V_j; S_j|W_j). \tag{10}$$

Sender j then transmits $x_{ji} = x_j(w_{ji}(r_j^o), v_{ji}(r_j^o, r_j^p, r_j^r), s_{ji})$ at time $i = 1, ..., n$.

C. Decoding

The receiver looks for unique indices r_j^o, r_j^p and r_j^r, $j = 1 : 2$, such that $(\{w_j^n(r_j^o), v_j^n(r_j^o, r_j^p, r_j^r)|\ j = 1 : 2\}, y^n) \in A_\epsilon^n(W_1, W_2, V_1, V_2, Y)$. It then finds s_{ji}, $j = 1 : 2$, for $i = 1 : n$ as the following

$$s_{ji} = \hat{s}_j(v_{1i}(r_1^o, r_1^p, r_1^r), w_{1i}(r_1^o), v_{2i}(r_2^o, r_2^p, r_2^r), w_{2i}(r_2^o), y_i).$$

The eavesdropper also finds the indices r_j^o, $j = 1 : 2$, such that $(\{w_j^n(r_j^o)|j = 1 : 2\}, z^n) \in A_\epsilon^n(W_1, W_2, Z)$.

D. Analysis of Probability of Error

We outline the analysis of probability of error in the following. We declare an error if one of the following events occurs

$$
\begin{aligned}
\mathcal{E}_1 =&\{(S_1^n, S_2^n, W_1^n(r_1^o), W_2^n(r_2^o), V_1^n(r_1^o, r_1^p, r_1^r),\\
&V_2^n(r_2^o, r_2^p, r_2^r), Y^n) \notin A_\epsilon^n\},\\
\mathcal{E}_2 =&\{(S_1^n, S_2^n, W_1^n(\tilde{r}_1^o), W_2^n(\tilde{r}_2^o), V_1^n(\tilde{r}_1^o, \tilde{r}_1^p, \tilde{r}_1^r),\\
&V_2^n(\tilde{r}_2^o, \tilde{r}_2^p, \tilde{r}_2^r), Y^n) \in A_\epsilon^n \ \ for\ \ some\\
&(\tilde{r}_1^o, \tilde{r}_1^p, \tilde{r}_1^r, \tilde{r}_2^o, \tilde{r}_2^p, \tilde{r}_2^r) \neq (r_1^o, r_1^p, r_1^r, r_2^o, r_2^p, r_2^r)\},\\
\mathcal{E}_3 =&\{(W_1^n(r_1^o), W_2^n(r_2^o), Z^n) \notin A_\epsilon^n\},\\
\mathcal{E}_4 =&\{(W_1^n(\tilde{r}_1^o), W_2^n(\tilde{r}_2^o), Z^n) \in A_\epsilon^n \ \ for\ \ some\\
&(\tilde{r}_1^o, \tilde{r}_2^o) \neq (r_1^o, r_2^o)\}.
\end{aligned}
$$

From the Markov lemma [8, Lecture Note 13], $P(\mathcal{E}_1)$ and $P(\mathcal{E}_3)$ tend to zero as $n \to \infty$. The event $\mathcal{E}_2$ occurs in one of the following cases (see Lemma 1 for the analysis of the probability of error)

1) $\tilde{r}_1^o \neq r_1^o$, $\tilde{r}_2^o \neq r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) \neq (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) \neq$

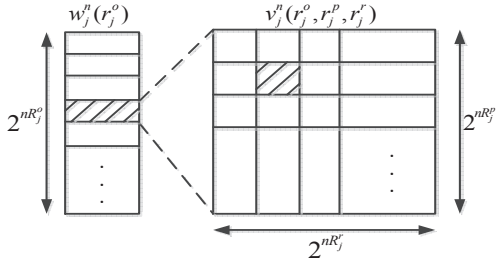

Fig. 5. Codebook of hybrid scheme

(r_2^p, r_2^r): The probability of this event goes to zero as $n \to \infty$ if

$$R_1^o + R_1^p + R_1^r + R_2^o + R_2^p + R_2^r < I(W_1, V_1, W_2, V_2; Y) + I(W_1, V_1; W_2, V_2) \tag{11}$$

2) $\tilde{r}_1^o = r_1^o$, $\tilde{r}_2^o \neq r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) \neq (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) \neq (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^p + R_1^r + R_2^o + R_2^p + R_2^r < I(V_1, W_2, V_2; Y|W_1) + I(W_1, V_1; W_2, V_2) \tag{12}$$

3) $\tilde{r}_1^o \neq r_1^o$, $\tilde{r}_2^o = r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) \neq (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) \neq (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^o + R_1^p + R_1^r + R_2^p + R_2^r < I(W_1, V_1, V_2; Y|W_2) + I(W_1, V_1; W_2, V_2) \tag{13}$$

4) $\tilde{r}_1^o = r_1^o$, $\tilde{r}_2^o = r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) \neq (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) \neq (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^p + R_1^r + R_2^p + R_2^r < I(V_1, V_2; Y|W_1, W_2) + I(W_1, V_1; W_2, V_2) - I(W_1; W_2) \tag{14}$$

5) $\tilde{r}_1^o = r_1^o$, $\tilde{r}_2^o \neq r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) = (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) \neq (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_2^o + R_2^p + R_2^r < I(W_2, V_2; Y, W_1, V_1) \tag{15}$$

6) $\tilde{r}_1^o = r_1^o$, $\tilde{r}_2^o = r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) = (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) \neq (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_2^p + R_2^r < I(V_2; Y, W_1, V_1|W_2) \tag{16}$$

7) $\tilde{r}_1^o \neq r_1^o$, $\tilde{r}_2^o = r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) \neq (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) = (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^o + R_1^p + R_1^r < I(W_1, V_1; Y, W_2, V_2) \tag{17}$$

8) $\tilde{r}_1^o = r_1^o$, $\tilde{r}_2^o = r_2^o$, $(\tilde{r}_1^p, \tilde{r}_1^r) \neq (r_1^p, r_1^r)$ and $(\tilde{r}_2^p, \tilde{r}_2^r) = (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^p + R_1^r < I(V_1; Y, W_2, V_2|W_1). \tag{18}$$

Therefore, $P(\mathcal{E}_2)$ tends to zero as $n \to \infty$ if the inequalities for all cases are satisfied. The event $\mathcal{E}_4$ occurs in one of the following cases (see Lemma 1 for the analysis of the probability of error)

1) $\tilde{r}_1^o \neq r_1^o$ and $\tilde{r}_2^o \neq r_2^o$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^o + R_2^o < I(W_1, W_2; Z) + I(W_1; W_2) \tag{19}$$

2) $\tilde{r}_1^o \neq r_1^o$ and $\tilde{r}_2^o = r_2^o$: The probability of this event goes to zero as $n \to \infty$ if

$$R_1^o < I(W_1; Z|W_2) \tag{20}$$

3) $\tilde{r}_1^o = r_1^o$ and $\tilde{r}_2^o \neq r_2^o$: The probability of this event goes to zero as $n \to \infty$ if

$$R_2^o < I(W_2; Z|W_1). \tag{21}$$

Therefore, $P(\mathcal{E}_4)$ tends to zero as $n \to \infty$ if the inequalities for all cases are satisfied.

E. Secrecy Analysis

Consider the following equivocation rate

$$\begin{aligned}
&H(S_1^n|Z^n) \\
&= H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) - H(r_1^o, r_1^p, r_1^r, X_1^n|S_1^n, Z^n) \\
&\overset{(a)}{=} H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) - H(r_1^o, r_1^p, r_1^r|S_1^n, Z^n) \\
&\overset{(b)}{=} H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) - H(r_1^p, r_1^r|r_1^o, S_1^n, Z^n)
\end{aligned} \tag{22}$$

where (a) follows because X_1^n is a deterministic function of $(r_1^o, r_1^p, r_1^r, S_1^n)$, (b) follows because r_1^o is a deterministic function of S_1^n. Now, consider the first term of (22)

$$\begin{aligned}
&H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) \\
&\geq H(r_1^p, r_1^r, S_1^n, X_1^n|r_1^o, Z^n) \\
&= H(r_1^p, r_1^r, S_1^n, X_1^n|r_1^o) - I(r_1^p, r_1^r, S_1^n, X_1^n; Z^n|r_1^o) \\
&= H(r_1^p, r_1^r, S_1^n, X_1^n|r_1^o) - H(Z^n|r_1^o) \\
&+ H(Z^n|r_1^p, r_1^r, S_1^n, X_1^n, r_1^o) \\
&\overset{(a)}{=} H(r_1^r, S_1^n|r_1^o) - H(Z^n|r_1^o) + H(Z^n|r_1^p, r_1^r, S_1^n, X_1^n, r_1^o) \\
&\overset{(b)}{=} H(r_1^r, S_1^n|r_1^o) - H(Z^n|r_1^o) + H(Z^n|X_1^n) \\
&\overset{(c)}{=} H(S_1^n|r_1^o) + H(r_1^r) - H(Z^n|r_1^o) + H(Z^n|X_1^n) \\
&\overset{(d)}{\geq} n(H(S_1|W_1) - \epsilon) + nR_1^r - n(H(Z|W_1) + \epsilon) \\
&+ n(H(Z|X_1) - \epsilon) \\
&= n[H(S_1|W_1) - H(Z|W_1) + H(Z|X_1) + R_1^r] - 3n\epsilon \\
&= n[H(S_1|W_1) - I(X_1; Z|W_1) + R_1^r] - 3n\epsilon
\end{aligned}$$

where (a) follows because X_1^n (resp. r_1^p) is a deterministic function of $(r_1^o, r_1^p, r_1^r, S_1^n)$ (resp. S_1^n), (b) follows because $(r_1^o, r_1^p, r_1^r, S_1^n) \to X_1^n \to Z^n$ form a Markov chain, (c)

follows because r_1^r is independent of (S_1^n, r_1^o), (d) follows from [8, Lecture Note 13] and the fact that $H(r_1^r) = nR_1^r$. Next, consider the second term of (22)

$$\begin{aligned}
&H(r_1^r, r_1^p | r_1^o, S_1^n, Z^n) \\
&= H(r_1^p, r_1^r | r_1^o) - I(r_1^p, r_1^r; S_1^n, Z^n | r_1^o) \\
&\overset{(a)}{=} n(R_1^r + R_1^p) - I(r_1^p, r_1^r; S_1^n, Z^n | r_1^o) \\
&\overset{(b)}{=} n(R_1^r + R_1^p) - I(r_1^p, r_1^r, V_1^n; S_1^n, Z^n | r_1^o) \\
&\leq n(R_1^r + R_1^p) - I(V_1^n; S_1^n, Z^n | r_1^o) \\
&= n(R_1^r + R_1^p) - H(V_1^n | r_1^o) + H(V_1^n | r_1^o, S_1^n, Z^n) \\
&\leq n(R_1^r + R_1^p) - n(R_1^r + R_1^p) + H(V_1^n | r_1^o, S_1^n, Z^n) \\
&\overset{(c)}{\leq} n[R_1^r + R_1^p - I(V_1; S_1, Z | W_1)]^+ + n\epsilon
\end{aligned}$$

where (a) follows from the independence of (r_1^p, r_1^r) and r_1^o, and the fact that $H(r_1^r, r_1^p) = n(R_1^r + R_1^p)$, (b) follows because V_1^n is a deterministic function of (r_1^o, r_1^p, r_1^r), (c) holds because if $R_1^r + R_1^p \geq I(V_1; S_1, Z | W_1)$, then we have $H(V_1^n | r_1^o, S_1^n, Z^n) \leq n(R_1^r + R_1^p - I(V_1; S_1, Z | W_1))$. In summary, we have

$$\begin{aligned}
R_{e1} < {} & H(S_1 | W_1) - I(X_1; Z | W_1) + R_1^r \\
& - [R_1^r + R_1^p - I(V_1; S_1, Z | W_1)]^+ \qquad (23)
\end{aligned}$$

Similarly, we get

$$\begin{aligned}
R_{e2} < {} & H(S_2 | W_2) - I(X_2; Z | W_2) + R_2^r \\
& - [R_2^r + R_2^p - I(V_2; S_2, Z | W_2)]^+ \qquad (24) \\
R_{e12} < {} & H(S_1, S_2 | W_1, W_2) - I(X_1, X_2; Z | W_1, W_2) \\
& + R_1^r + R_2^r - [R_1^r + R_1^p + R_2^r + R_2^p \\
& - I(V_1, V_2; S_1, S_2, Z | W_1, W_2)]^+ \qquad (25)
\end{aligned}$$

Collecting the terms in (9)-(18), (23)-(25) and performing Fourier-Motzkin elimination, we find the terms in the theorem. ■

IV. Special Cases

In this section, we consider some special cases of Theorem 1. First, we show that our proposed inner bound includes some previous bounds as special cases.

Remark 1: Suppose that the eavesdropper is neutral. Also, let $W_1 = W_2 = 0$ and $Z = 0$ in Theorem 1. Then, (D_1, D_2) is achievable if

$$I(V_1; S_1) < I(V_1; V_2, Y) \qquad (26)$$

$$I(V_2; S_2) < I(V_2; V_1, Y) \qquad (27)$$

$$I(V_1; S_1) + I(V_2; S_2) < I(V_1, V_2; Y) + I(V_1; V_2) \qquad (28)$$

for some pmf $p(s_1, s_2)p(v_1, x_1 | s_1)p(v_2, x_2 | s_2)$ and functions $\hat{s}_1(v_1, v_2, y)$ and $\hat{s}_2(v_1, v_2, y)$ such that $E[d_j(S_j, \hat{S}_j)] \leq D_j$, $j = 1 : 2$. The conditions in (26)-(28) have been found in [5] for the lossless transmission of the sources over the MAC. As it is stated in [5], the conditions (26)-(28) imply the conditions of [9] with $V_j = (X_j, S_j)$ and $\hat{S}_j = S_j$, $j = 1 : 2$. The conditions of (26)-(28) also imply the Berger-Tung inner bound [8, Lecture Note 12] with $Y = (X_1, X_2)$, $\log |\mathcal{X}_1| = R_1$, $\log |\mathcal{X}_2| = R_2$ and $V_j = (X_j, U_j), j = 1 : 2$.

Next, we consider the special case of uncoded transmission. Suppose that the receiver's channel is defined as $Y = (X_1, X_2)$.

Corollary 1: Let $W_j = 0$, $V_j = X_j = S_j$ and $\hat{S}_j = S_j$, $j = 1 : 2$, in Theorem 1. Therefore, tuple $(D_1 = 0, D_2 = 0, R_{e1}, R_{e2}, R_{e12})$ is achievable for the MAC-WT where $Y = (X_1, X_2)$ if

$$R_{e1} < H(S_1 | Z) \qquad (29)$$

$$R_{e2} < H(S_2 | Z) \qquad (30)$$

$$R_{e12} < H(S_1, S_2 | Z) - I(S_1; S_2) \qquad (31)$$

for some pmf $p(s_1, s_2)$. As it can be seen in (31), the term $I(S_1; S_2)$ appears when bounding the secrecy rate R_{e12}. This is because of the fact that the correlation of the sources helps the eavesdropper to obtain some information about the sources.

V. Conclusion

We studied lossy communication over a MAC-WT. We proposed a joint source-channel scheme based on hybrid coding of [5]. We also discussed some special cases of the proposed scheme.

VI. Acknowledgement

This work was partially supported by Iranian NSF under contract no. 88114/46 and by Iran Telecom Research Center (ITRC) and by Cryptography chair and by Iran's National Elites Foundation.

References

[1] T. M. Cover, A. El Gamal and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Trans. on Info. Theory*, vol. 26, no. 6, pp. 648-657, Nov. 1980.

[2] D. Gunduz, E. Erkip, A. Goldsmith and H. V. Poor, "Source and channel coding for correlated sources over multiuser channels," *IEEE Trans. on Info. Theory*, vol. 55, no. 9, pp. 3927-3944, Sept. 2009.

[3] S. Salehkalaibar and M. R. Aref, "On the transmission of correlated sources over relay channel," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, St. Petersburg, Russia, Jul.-Aug. 2011, pp. 1409-1413.

[4] S. Salehkalaibar and M. R. Aref, "On the reliable transmission of correlated sources over relay channel," *To appear in IEEE Trans. on Info. Theory*, revised, Sept. 2012.

[5] S. H. Lim, P. Minero and Y. H. Kim, "Lossy communication of correlated sources over multiple access channels," *48th Allerton Conf. on Comm., Cont. and Computing*, Sept.-Oct. 2010, pp. 851-858.

[6] J. Villard, P. Piantanida and S. Shamai, "Secure transmission of sources over noisy channels with side information at the receivers," *Submitted to IEEE Trans. on Info. Theory*, Jan. 2012, available at http://arxiv.org/abs/1201.2315.

[7] A. Wyner, "The wiretap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[8] A. El Gamal and Y. H. Kim, "Lecture notes on network information theory," Cambridge University Press, 2011.

[9] T. M. Cover, A. El Gamal and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Trans. on Info. Theory*, vol. 26, no. 6, pp. 648-657, Nov. 1980.