IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Lossy transmission of correlated sources over multiple-access wiretap channels

ISSN 1751-8628
Received on 22nd May 2014
Accepted on 12th November 2014
doi: 10.1049/iet-com.2014.0518
www.ietdl.org

Sadaf Salehkalaibar ✉, *Mohammad Reza Aref*

Information Systems and Security Lab (ISSL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
✉ *E-mail: sadaf_sk86@yahoo.com*

Abstract: In this study, the authors study lossy communication of correlated sources over a multiple-access wiretap channel (MAC-WT). Consider a system with two transmitters, a receiver and an eavesdropper. There are two correlated sources where each of them is observed by the corresponding transmitter, separately. Each transmitter wishes to describe its source sequence to the receiver with a desired distortion. The sources need to be kept secret from the eavesdropper. They find an achievable region for the MAC-WT with correlated sources by separation. A joint source-channel coding scheme for the MAC-WT is also proposed. They consider lossy communication of a bivariate Gaussian source over Gaussian MAC-WT (GMAC-WT). They propose a separation-based achievable scheme for the GMAC-WT. An achievable region for the GMAC-WT based on uncoded transmission is also found. They compare the separate and the uncoded schemes for the symmetric GMAC-WT, where the same constraint on the power of each transmitter is imposed and the same distortion on each source is achieved. For another case of source correlation coefficient, they compare the separate, uncoded and hybrid schemes. They obtain outer bounds to the rate-distortion-equivocation region of: (i) the degraded MAC-WT where the output at the eavesdropper is a degraded version of the output at the receiver, (ii) the GMAC-WT with independent sources and (iii) the symmetric GMAC-WT when the correlation of the sources is maximum. Optimal regions for some cases are established.

1 Introduction

Consider a multiple-access channel (MAC) where there are two transmitters, a receiver and two sources. Each transmitter observes its source component, separately and tries to describe its source to the receiver. The receiver wishes to reconstruct both sources with desired distortions. There is also an eavesdropper (wiretapper) from which, the sources need to be kept secret. The whole system is referred to as multiple-access wiretap channel (MAC-WT). The motivation of this model is given by an example in the following (see Fig. 1). Consider a wireless sensor network where the sensors collect environmental conditions and send them to a main location. The data of the sensors may have correlated with each other. Also, suppose that there is another location that eavesdrops the data of the sensors. Fig. 1 illustrates such a network with two sensors.

The coding scheme for the above model includes three major concepts: secret communication, joint (or separate) source-channel coding and lossy communication over noisy (wireless) channels. The information theoretic secrecy was first introduced by Shannon [1]. Wyner [2] studied the so-called wiretap channel (WTC) where there are a transmitter, a receiver and an eavesdropper. He determined the capacity of the degraded WTC where the channel of the eavesdropper is a degraded version of the channel of the receiver. The achievable scheme involves adding randomness to the transmitted codeword so that the eavesdropper cannot obtain enough information about the source. Csiszar and Korner [3] considered the general WTC and established the secrecy capacity. There are some works that extended the secrecy problem to MAC-WTs [4–6] and MACs with confidential messages [7, 8].

Source-channel separation theorem states that a source sequence can be reliably transmitted over a single-user channel if and only if the minimum source coding rate is below the channel capacity [9]. Optimality of the separation does not hold for general multi-user channels. However, the separate scheme has been considered in several multi-user networks, for example, in relay channels [10–12], compound MACs, two-way channels and interference channels [9]. Cover *et al.* [13] showed by an example that the separation is not optimal in the MAC with correlated sources. Therefore, joint source-channel coding received considerable attention, for example, in broadcast channels [14, 15] and relay channels [16]. Lim *et al.* [17] proposed a hybrid scheme for the transmission of correlated sources over MAC. In this scheme, each transmitter compresses its source component to a codeword. It then maps the observed sequence and the compressed codeword to the channel codeword, symbol-by-symbol. Recently, the hybrid scheme of [17] has been employed to find sufficient conditions for the transmission of a source over WTC with side information at the receivers [18].

Lossy communication of correlated sources has been studied in different multi-terminal channels, for example, WTCs [19], interference channels [20] and Gaussian sensor networks [21]. Lossy transmission of Gaussian correlated sources over a Gaussian MAC (GMAC) has been considered in [22]. Necessary and sufficient conditions for the achievability of a distortion pair have been found in [22]. The coding of [22] is related to the quadratic Gaussian two-terminal source-coding problem [23, 24]. In this problem, correlated Gaussian sources are described to a central receiver. It has been shown that the Berger-Tung inner bound [25] is optimal in this case.

In this paper, we consider lossy communication of correlated sources over MAC-WT. Comparing to [4], we consider the correlation between the sources, and comparing to [17], we introduce some secrecy constraints. First, the separate scheme is employed to find an achievable rate-distortion-equivocation region. For the achievability, each source is compressed into common and private codewords. The common codeword can be decoded by the eavesdropper. The private codeword needs to be kept secret from the eavesdropper using Wyner's wiretap coding [2]. The corresponding indices are sent to the receiver through channel codewords. Next, we propose a joint scheme based on hybrid coding of [17]. In this scheme, each transmitter compresses its source into common and private codewords. It then maps the source and the codewords to the channel codeword,

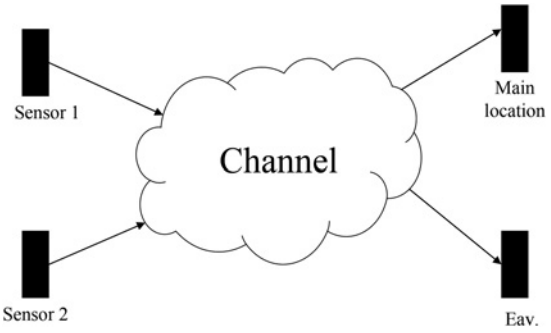

Fig. 1 *Two-sensor wireless network with an eavesdropper*

symbol-by-symbol. In this case, the analysis of the probability of error is not the same as the conventional random coding proof, since the transmitted codeword depends on the entire codebook [26]. The secrecy analysis of this work is different from standard Wyner's proof. In this analysis, we find sufficient conditions so that the eavesdropper can find the private indices, given the common indices. Then, we consider lossy transmission of a bivariate Gaussian source over Gaussian MAC-WT (GMAC-WT). An inner bound to the distortion-equivocation region of the GMAC-WT is proposed using the separate scheme. The optimal rate-distortion region of the Gaussian two-terminal source coding problem [23, 24] is combined with other achievable region which is based on separation. We also obtain an achievable region for the GMAC-WT using uncoded transmission. The achievable region of the separate scheme is compared with that of uncoded transmission for the symmetric GMAC-WT, where the same constraint on the power of each transmitter is satisfied and the same distortion on each source is achieved. We derive the results of the comparison when: (i) the sources are independent, in this case, the distortion at the receiver for the separate scheme is smaller than the uncoded scheme. However, the secrecy rate of the separate scheme is larger than the uncoded scheme, (ii) the correlation of the sources is maximum, in this case, the distortion at the receiver for the uncoded scheme is smaller than the separate scheme. Moreover, the secrecy rate of the separate scheme is larger than the uncoded scheme. We also compare the separate, the uncoded and the hybrid schemes for another case of source correlation coefficient. An outer bound to the rate-distortion-equivocation region of the degraded MAC-WT is proposed, where the eavesdropper's output is a degraded version of the receiver's output. This bound is extended to some other cases of GMAC-WT.

This paper is organised as follows:

- In Section 2, we present a mathematical framework for our work.
- In Section 3, we propose an achievable scheme for the MAC-WT using separate scheme. We also discuss some special cases of the inner bound.
- In Section 4, we obtain an achievable region for the MAC-WT using hybrid scheme. We also propose an outer bound to the rate-distortion-equivocation region of a class of MAC-WTs.
- In Section 5, we consider the lossy transmission of a bivariate Gaussian source over a GMAC-WT. We propose outer bounds to the rate-distortion-equivocation region of: (i) the GMAC-WT with independent sources and (ii) the symmetric GMAC-WT when the correlation of the sources is maximum. We also find achievable regions for the GMAC-WT using separate scheme, uncoded transmission and hybrid scheme. We compare the achievable regions of the uncoded transmission and the separate scheme for the cases of: (i) independent sources and (ii) maximum correlation of the sources. Also, the separate, the uncoded and the hybrid schemes are compared with each other for a special case of source correlation coefficient. Optimal regions for some cases are established.
- Conclusions are provided in Section 6.

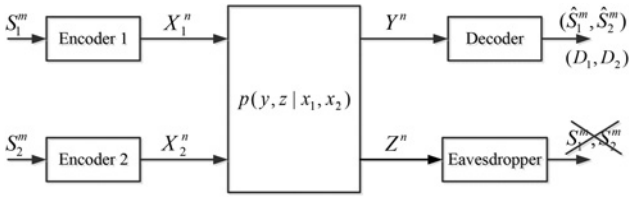

Fig. 2 *Lossy source transmission over MAC-WT*

2 Preliminaries and definitions

We denote discrete random variables with capital letters, for example, X, Y and their realisations with lower case letters x, y. X_i^j indicates a sequence of random variables $(X_i, \ldots, X_j)$. We use $H(.)$ to denotes the entropy of a discrete random variable and $I(.;.)$ to denotes the mutual information between two discrete random variables. We denote by $A_\epsilon^n(X, Y)$ 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 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. 2. Moreover, the sources are independent over time. Each transmitter 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 $0 \le d_{\max} < \infty$. 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 $d_j(s_j^n, \hat{s}_j^n) = (1/n)\sum_{i=1}^n d_j(s_{j,i}, \hat{s}_{j,i})$.

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

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

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

$$\frac{n}{m} \le \kappa \tag{1}$$

$$\mathbb{E}[d_1(S_1^m, \hat{S}_1^m)] \le D_1 \tag{2}$$

$$\mathbb{E}[d_2(S_2^m, \hat{S}_2^m)] \le D_2 \tag{3}$$

$$\frac{1}{m}H(S_1^m|Z^n) \ge R_{e1} \tag{4}$$

$$\frac{1}{m}H(S_2^m|Z^n) \ge R_{e2} \tag{5}$$

$$\frac{1}{m}H(S_1^m, S_2^m|Z^n) \ge R_{e12} \tag{6}$$

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

3 Separate scheme

In this section, we first find an inner bound to the rate-distortion-equivocation region of the MAC-WT using the separate scheme. Then, we discuss some special cases of the proposed scheme. The achievable region is given in the following.

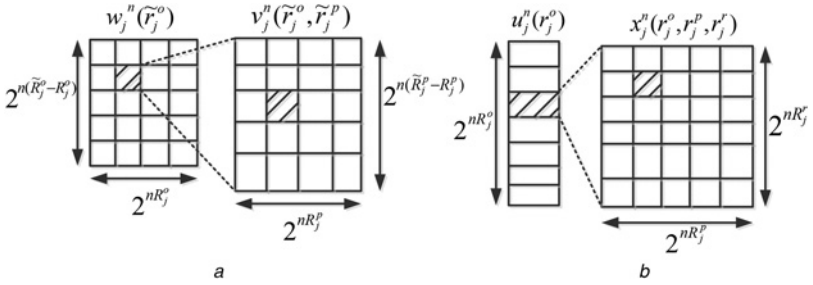

Fig. 3 *Codebook of separate scheme*

a Source Codebook
b Channel Codebook

Theorem 1: A tuple (κ, D_1, D_2, R_{e1}, R_{e2}, R_{e12}) is achievable for the MAC-WT if (see (7))

where V_1, V_2, W_1, W_2, U_1, U_2 are auxiliary random variables with the distribution $p(v_1, w_1|s_1)\ p(v_2, w_2|s_2)p(x_1, u_1)p(x_2, u_2)$ and $\mathbb{E}[d_j(S_j, \hat{S}_j)] \le D_j$, $j = 1{:}2$, where $[x]^+ = \max 0, x$ and $I_i (i = 1{:}11)$ are shown in (8) at the top of next page

$$\begin{aligned}
I_1 &= \kappa I(X_1; Y|X_2)\\
I_2 &= \kappa I(X_2; Y|X_1)\\
I_3 &= \kappa I(X_1, X_2; Y|U_1)\\
I_4 &= \kappa I(X_1, X_2; Y|U_2)\\
I_5 &= \kappa I(X_1, X_2; Y)\\
I_6 &= \kappa I(X_1, X_2; Y|U_1, U_2)\\
I_7 &= \kappa I(X_1; Y|X_2, U_1)\\
I_8 &= \kappa I(X_2; Y|X_1, U_2)\\
I_9 &= \kappa I(X_1; Z|U_1)\\
I_{10} &= \kappa I(X_2; Z|U_2)\\
I_{11} &= \kappa I(X_1, X_2; Z|U_1, U_2)
\end{aligned} \tag{8}$$

Proof: Each source $S_j, j = 1{:}2$, is compressed into codewords (W_j, V_j), with V_j on the top of W_j. The corresponding bin indices (r_j^o, r_j^p) are transmitted to the receiver through variables (U_j, X_j). The codeword U_j can be decoded by the eavesdropper, but the codeword X_j needs to be kept secret from the eavesdropper by a random noise r_j^r. The Wyner's wiretap coding [2] is used to protect X_j from the eavesdropper. □

3.1 Codebook generation

(1) Source codewords: Fix a conditional pmf $p(v_1, w_1|s_1)p(v_2, w_2|s_2)$ 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 $\mathbb{E}[d_j(S_j, \hat{S}_j)] \le D_j/(1+\varepsilon)$, $j = 1{:}2$. For $j = 1{:}2$, randomly and independently generate $2^{m\tilde{R}_j^o}$ sequences $w_j^m(\tilde{r}_j^o)$, $\tilde{r}_j^o \in \left[1{:}2^{m\tilde{R}_j^o}\right]$ each according to $\prod_{i=1}^m p(w_{ji})$. Partition the set of indices $\tilde{r}_j^o \in \left[1{:}2^{m\tilde{R}_j^o}\right]$ into equal-size bins $\mathcal{C}_j^o(r_j^o)$, $r_j^o \in \left[1{:}2^{mR_j^o}\right]$, where $R_j^o \le \tilde{R}_j^o$. For each $w_j^m(\tilde{r}_j^o)$, randomly and independently generate $2^{m\tilde{R}_j^p}$ sequences $v_j^m(\tilde{r}_j^o, \tilde{r}_j^p)$, $\tilde{r}_j^p \in \left[1{:}2^{m\tilde{R}_j^p}\right]$ each according to $\prod_{i=1}^m p(v_{ji}|w_{ji}(\tilde{r}_j^o))$. Partition the set of indices $\tilde{r}_j^p \in \left[1{:}2^{m\tilde{R}_j^p}\right]$ into equal-size bins $\mathcal{C}_j^p(r_j^p)$, $r_j^p \in \left[1{:}2^{mR_j^p}\right]$, where $R_j^p \le \tilde{R}_j^p$. See Fig. 3*a*.

(2) Channel codewords: Randomly and independently generate $2^{mR_j^o}$, $j = 1{:}2$, sequences $u_j^n(r_j^o)$, $r_j^o \in \left[1{:}2^{mR_j^o}\right]$, each according to $\prod_{i=1}^n p(u_{ji})$. For each $u_j^n(r_j^o)$, randomly and independently generate $2^{m(R_j^p + R_j^r)}$ sequences $x_j^n\left(r_j^o, r_j^p, r_j^r\right)$, $r_j^p \in \left[1{:}2^{mR_j^p}\right]$, $r_j^r \in [1{:}2^{mR_j^r}]$, each according to $\prod_{i=1}^n p(x_{ji}|u_{ji}(r_j^o))$. See Fig. 3*b*.

3.2 Encoding

Sender $j, j = 1{:}2$, first finds codewords $w_j^m(\tilde{r}_j^o)$ and $v_j^m(\tilde{r}_j^o, \tilde{r}_j^p)$ such that

$$(w_j^m(\tilde{r}_j^o), v_j^m(\tilde{r}_j^o, \tilde{r}_j^p), s_j^m) \in A_\varepsilon^m(W_j, V_j, S_j)$$

This can be done with an arbitrarily small probability of error as $n \to \infty$ if

$$\tilde{R}_j^p > I(V_j; S_j|W_j) \tag{9}$$

$$\tilde{R}_j^o > I(W_j; S_j) \tag{10}$$

Sender j then finds r_j^o and r_j^p, the bin indices of $\tilde{r}_j^o$ and $\tilde{r}_j^p$, respectively. Transmitter j randomly selects an index r_j^r from $\left[1{:}2^{mR_j^r}\right]$ and sends $x_j^n\left(r_j^o, r_j^p, r_j^r\right)$.

$$\left\{\begin{array}{c}
I(V_1; S_1|V_2) < I_1,\ I(V_2; S_2|V_1) < I_2\\
I(V_1, V_2; S_1, S_2|W_1) < I_3,\ I(V_1, V_2; S_1, S_2|W_2) < I_4\\
I(V_1, V_2; S_1, S_2) < I_5,\ I(V_1, V_2; S_1, S_2|W_1, W_2) < I_6\\
I(V_1; S_1|V_2, W_1) - I(W_1; V_2|W_2) < I_7\\
I(V_2; S_2|V_1, W_2) - I(W_2; V_1|W_1) < I_8\\
R_{e1} < H(S_1|W_1) - I(V_1; S_1|W_1) + I_7 - I_9\\
R_{e1} < H(S_1|W_1) - I(V_1; S_1|W_1) - I(W_1; S_1|W_2) + I_1 - I_9\\
R_{e2} < H(S_2|W_2) - I(V_2; S_2|W_2) + I_8 - I_{10}\\
R_{e2} < H(S_2|W_2) - I(V_2; S_2|W_2) - I(W_2; S_2|W_1) + I_2 - I_{10}\\
R_{e12} < H(S_1, S_2|W_1, W_2) - \max\{[I(V_1; S_1|W_1) + I(V_2; S_2|W_2) - I_6 + I_{11}\\
I(V_1; S_1|W_1) + I(V_2; S_2|W_2) + I(W_1, W_2; S_1, S_2) - I_5 + I_{11}\\
I(V_1; S_1|W_1) + I(V_2; S_2|W_2) + I(W_2; S_2|W_1) - I_3 + I_{11}\\
I(V_1; S_1|W_1) + I(V_2; S_2|W_2) + I(W_1; S_1|W_2) - I_4 + I_{11}\}
\end{array}\right\} \tag{7}$$

3.3 Decoding

The receiver looks for unique indices r_j^o, r_j^p and r_j^r, $j = 1{:}2$, such that

$$(\{u_j^n(r_j^o), x_j^n(r_j^o, r_j^p, r_j^r) | j = 1{:}2\}, y^n) \in A_\varepsilon^n(U_1, U_2, X_1, X_2, Y)$$

This can be done with an arbitrarily small probability of error as $n \to \infty$ if

$$R_1^o + R_1^p + R_1^r < \kappa I(X_1; Y|X_2) \tag{11}$$

$$R_2^o + R_2^p + R_2^r < \kappa I(X_2; Y|X_1) \tag{12}$$

$$R_1^o + R_1^p + R_1^r + R_2^o + R_2^p + R_2^r < \kappa I(X_1, X_2; Y) \tag{13}$$

$$R_1^p + R_1^r < \kappa I(X_1; Y|U_1, X_2) \tag{14}$$

$$R_2^p + R_2^r < \kappa I(X_2; Y|U_2, X_1) \tag{15}$$

$$R_1^p + R_1^r + R_2^p + R_2^r < \kappa I(X_1, X_2; Y|U_1, U_2) \tag{16}$$

$$R_1^p + R_1^r + R_2^o + R_2^p + R_2^r < \kappa I(X_1, X_2; Y|U_1) \tag{17}$$

$$R_1^o + R_1^p + R_1^r + R_2^p + R_2^r < \kappa I(X_1, X_2; Y|U_2) \tag{18}$$

The receiver then looks for indices $(\tilde{r}_j^o, \tilde{r}_j^p)$, $j = 1{:}2$, such that

$$\tilde{r}_j^o \in \mathcal{C}_j^o(r_j^o), \ \tilde{r}_j^p \in \mathcal{C}_j^p(r_j^p)$$

and

$$(w_1^m(\tilde{r}_1^o), v_1^m(\tilde{r}_1^o, \tilde{r}_1^p), w_2^m(\tilde{r}_2^o), v_2^m(\tilde{r}_2^o, \tilde{r}_2^p)) \in A_\varepsilon^m(W_1, W_2, V_1, V_2)$$

This can be done with an arbitrarily small probability of error as $n \to \infty$ if

$$\sum_{i=1}^{2} (\tilde{R}_i^o - R_i^o) + (\tilde{R}_i^p - R_i^p) < I(W_1, V_1; W_2, V_2) \tag{19}$$

$$\sum_{i=1}^{2} (\tilde{R}_i^p - R_i^p) < I(W_1, V_1; W_2, V_2) - I(W_1; W_2) \tag{20}$$

$$\sum_{i=1}^{2} (\tilde{R}_i^o - R_i^o) < I(W_1; W_2) \tag{21}$$

3.4 Secrecy analysis

Consider the following equivocation rate at the eavesdropper

$$H(S_1^m|Z^n) = H(S_1^m|r_1^o, r_1^p, Z^n) + I(S_1^m; r_1^o, r_1^p|Z^n) \tag{22}$$

Now, we study the first term of (22)

$$\begin{aligned} H(S_1^m|r_1^o, r_1^p, Z^n) &\geq H(S_1^m|\tilde{r}_1^o, \tilde{r}_1^p, r_1^o, r_1^p, Z^n) \\ &\overset{(a)}{=} H(S_1^m|\tilde{r}_1^o, \tilde{r}_1^p, Z^n) \\ &\overset{(b)}{=} H(S_1^m|\tilde{r}_1^o, \tilde{r}_1^p) \\ &\overset{(c)}{=} H(S_1^m|\tilde{r}_1^o) - H(\tilde{r}_1^p|\tilde{r}_1^o) \\ &\overset{(d)}{=} H(S_1^m|\tilde{r}_1^o) - m\tilde{R}_1^p \\ &\overset{(e)}{\geq} m[H(S_1|W_1) - \varepsilon] - m\tilde{R}_1^p \end{aligned}$$

where (a) follows because r_1^o and r_1^p are deterministic functions of $\tilde{r}_1^o$ and $\tilde{r}_1^p$, respectively, (b) follows because $S_1^m \to (\tilde{r}_1^o, \tilde{r}_1^p) \to Z^n$ form a Markov chain, (c) follows because $\tilde{r}_1^p$ is a deterministic function of S_1^m, (d) follows because $\tilde{r}_1^p$ is independent of $\tilde{r}_1^o$, and the fact that $\tilde{r}_1^p \in [1{:}2^{n\tilde{R}_1^p}]$ (e) follows from [25, Lecture Note 13]. Next, consider the second term of (22)

$$\begin{aligned} I(S_1^m; r_1^o, r_1^p|Z^n) &\overset{(a)}{=} H(r_1^o, r_1^p|Z^n) \\ &\geq H(r_1^p|r_1^o, Z^n) \\ &= H(r_1^p|r_1^o) - I(r_1^p; Z^n|r_1^o) \\ &\overset{(b)}{=} mR_1^p - I(r_1^p; Z^n|r_1^o) \\ &\overset{(c)}{=} mR_1^p - I(X_1^n; Z^n|r_1^o) + I(X_1^n; Z^n|r_1^o, r_1^p) \\ &= mR_1^p - H(X_1^n|r_1^o) + H(X_1^n|r_1^o, Z^n) \\ &\quad + I(X_1^n; Z^n|r_1^o, r_1^p) \\ &\overset{(d)}{\geq} mR_1^p - n[H(X_1|U_1) + \varepsilon] \\ &\quad + n[H(X_1|U_1, Z) - \varepsilon] + I(X_1^n; Z^n|r_1^o, r_1^p) \\ &= mR_1^p - nI(X_1; Z|U_1) \\ &\quad + I(X_1^n; Z^n|r_1^o, r_1^p) - 2n\varepsilon \\ &= mR_1^p - nI(X_1; Z|U_1) + H(X_1^n|r_1^o, r_1^p) \\ &\quad - H(X_1^n|Z^n, r_1^o, r_1^p) - 2n\varepsilon \\ &= mR_1^p - nI(X_1; Z|U_1) + mR_1^r \\ &\quad - H(X_1^n|Z^n, r_1^o, r_1^p) - 2n\varepsilon \\ &\overset{(e)}{\geq} mR_1^p - nI(X_1; Z|U_1) + mR_1^r - m\varepsilon - 2n\varepsilon \end{aligned}$$

where (a) follows because (r_1^o, r_1^p) is a deterministic function of S_1^m, (b) follows from the independence of r_1^p and r_1^o and the fact that $H(r_1^p) = mR_1^p$, (c) follows because $(r_1^o, r_1^p, r_1^r) \to X_1^n \to Z^n$ forms a Markov chain, (d) follows from [25, Lecture Note 13] and (e) follows because if $R_1^r < \kappa I(X_1; Z|U_1)$, then from Fano's inequality, we have

$$H(X_1^n|Z^n, r_1^o, r_1^p) \leq m\varepsilon$$

This can be proved as the following: the eavesdropper, knowing (r_1^o, r_1^p), tries to find r_1^r. By the analysis of the error event, it can be easily shown that if the above condition on R_1^r is satisfied, then from Fano's inequality, we obtain the above bound on the entropy. We choose $R_1^r = \kappa I(X_1; Z|U_1) - \delta'$ for $\delta' > 0$. Therefore we have

$$R_{e1} < H(S_1|W_1) - \tilde{R}_1^p + R_1^p \tag{23}$$

Similarly, if

$$R_2^r = \kappa I(X_2; Z|U_2) - \delta'' \tag{24}$$

then we have

$$R_{e2} < H(S_2|W_2) - \tilde{R}_2^p + R_2^p \tag{25}$$

$$\begin{aligned} R_{e12} < &H(S_1, S_2|W_1, W_2) - \tilde{R}_1^p - \tilde{R}_2^p + R_1^p \\ &+ R_2^p + \kappa I(X_1; Z|U_1) + \kappa I(X_2; Z|U_2) \\ &- \kappa I(X_1, X_2; Z|U_1, U_2) \end{aligned} \tag{26}$$

Collecting the terms in (9)–(26) and performing Fourier–Motzkin elimination, we obtain the terms in the theorem.

Application of Theorem 1 yields the following results as special cases.

Lossy communication over WTC [19]: Let $W_j = U_j = 0$, $j = 1{:}2$, $V_2 = 0$, $S_2 = 0$, $X_2 = 0$, $R_{e2} = R_{e12} = 0$ and $D_2 \to \infty$ in Theorem 1. Therefore a tuple (κ, D_1, R_{e1}) is achievable if

$$I(V_1; S_1) < \kappa I(X_1; Y) \tag{27}$$

$$R_{e1} < H(S_1) - [I(S_1; V_1) - \kappa[I(X_1; Y) - I(X_1; Z)]^+]^+ \tag{28}$$

for some $p(v_1|s_1)p(x_1)$ such that $\mathbb{E}[d_1(S_1, \hat{S}_1)] \le D_1$.

Berger-Tung inner bound [25, Lecture Note 12]: Let $W_j = U_j = 0$, $j = 1{:}2$, $R_{e1} = R_{e2} = R_{e12} = 0$, $\kappa = 1$, $Y = (X_1, X_2)$, $\log|\mathcal{X}_j| = R_j$ and $V_j = (X_j, U_j)$ in Theorem 1. Therefore a pair (R_1, R_2) is achievable if

$$R_1 > I(S_1; U_1|U_2) \tag{29}$$

$$R_2 > I(S_2; U_2|U_1) \tag{30}$$

$$R_1 + R_2 > I(S_1, S_2; U_1, U_2) \tag{31}$$

for some $p(u_1|s_1)p(u_2|s_2)$ and functions $\hat{s}_j(u_1, u_2)$, $j = 1{:}2$, such that $\mathbb{E}[d_j(S_j, \hat{S}_j)] \le D_j$.

4 Hybrid scheme and an outer bound

In this section, we first review hybrid coding for a point-to-point channel which was introduced in [17]. Then, we propose an achievable region for the MAC-WT. Finally, we derive an outer bound to the rate-distortion-equivocation region of a class of MAC-WTs. Suppose that a source $S \sim p(s)$ is to be sent over the discrete memoryless channel $(\mathcal{X}, p(y|x), \mathcal{Y})$. The decoder reconstructs the sequence S by $\hat{S}$. The average distortion must satisfy $\mathbb{E}[d(S, \hat{S})] \le D$, where d is a distortion measure. In the hybrid scheme of [17], 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, symbol-by-symbol. 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 [17], averaging over all codebooks is not the same as the conventional random coding proof. Let P_e be the probability of the event that there exists $\hat{T} \neq T$ such that $(U^n(\hat{T}), Y^m) \in A_\varepsilon^n$. Then, we have the following lemma.

Lemma 1 [17]: The probability P_e is upper bounded as

$$P_e < 4.2^{n(R - I(U;Y) + \varepsilon)} \tag{32}$$

for $\varepsilon > 0$.

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

Theorem 2: A tuple $(\kappa = 1, D_1, D_2, R_{e1}, R_{e2}, R_{e12})$ is achievable for MAC-WT if (see (33))

where V_1, V_2, W_1 and W_2 are auxiliary random variables with the distribution $p(s_1, s_2)p(x_1, v_1, w_1|s_1)\, p(x_2, v_2, w_2|s_2)$ 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 $\mathbb{E}[d_j(S_j, \hat{S}_j)] \le D_j$, $j = 1{:}2$, where $I_i (i = 1{:}11)$ are shown in (34)

$$\begin{aligned}
I_1 &= I(W_1, V_1; W_2, V_2, Y)\\
I_2 &= I(W_2, V_2; W_1, V_1, Y)\\
I_3 &= I(V_1; W_2, V_2, Y|W_1)\\
I_4 &= I(V_2; W_1, V_1, Y|W_2)\\
I_5 &= I(W_1, V_1, W_2, V_2; Y) + I(W_1, V_1; W_2, V_2)\\
I_6 &= I(V_1, V_2; Y|W_1, W_2) + I(W_1, V_1; W_2, V_2) - I(W_1; W_2)\\
I_7 &= I(W_1, V_1, V_2; Y|W_2) + I(W_1, V_1; W_2, V_2)\\
I_8 &= I(V_1, W_2, V_2; Y|W_1) + I(W_1, V_1; W_2, V_2)\\
I_9 &= I(V_1; S_1, Z|W_1)\\
I_{10} &= I(V_2; S_2, Z|W_2)\\
I_{11} &= I(V_1, V_2; S_1, S_2, Z|W_1, W_2)
\end{aligned} \tag{34}$$

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 symbol-by-symbol 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. □

4.1 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 $\mathbb{E}[d_j(S_j, \hat{S}_j)] \le D_j/(1 + \varepsilon)$, $j = 1{:}2$. For $j = 1{:}2$, randomly and independently generate $2^{nR_j^o}$ sequences $w_j^n(r_j^o)$, $r_j^o \in \left[1{:}2^{nR_j^o}\right]$ each according to $\prod_{i=1}^n p(w_{ji})$. For each $w_j^n(r_j^o)$, randomly and independently generate $2^{n\left(R_j^p + R_j^r\right)}$ sequences $v_j^n(r_j^o, r_j^p, r_j^r)$, $r_j^p \in \left[1{:}2^{nR_j^p}\right]$, $r_j^r \in \left[1{:}2^{nR_j^r}\right]$, each according to $\prod_{i=1}^n p(v_{ji}|w_{ji}(r_j^o))$.

4.2 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 $(w_j^n(r_j^o), v_j^n(r_j^o, r_j^p, r_j^r), s_j^n) \in A_\varepsilon^n(W_j, V_j, S_j)$. This can be done with an arbitrarily small probability of error if

$$R_j^o \ge I(W_j; S_j) \tag{35}$$

$$\left\{\begin{array}{c}
I(V_1; S_1) < I_1,\ I(V_2; S_2) < I_2,\ I(V_1; S_1|W_1) < I_3,\ I(V_2; S_2|W_2) < I_4\\
I(V_1; S_1) + I(V_2; S_2) < I_5,\ I(V_1; S_1|W_1) + I(V_2; S_2|W_2) < I_6\\
I(V_1; S_1) + I(V_2; S_2|W_2) < I_7,\ I(V_1; S_1|W_1) + I(V_2; S_2) < I_8\\
R_{e1} < H(S_1|W_1) - I(X_1; Z|W_1) + \min\{I_9 - I(V_1; S_1|W_1), I_3 - I(V_1; S_1|W_1)\\
I_1 - I(V_1; S_1)\}\\
R_{e2} < H(S_2|W_2) - I(X_2; Z|W_2) + \min\{I_{10} - I(V_2; S_2|W_2), I_4 - I(V_2; S_2|W_2)\\
I_2 - I(V_2; S_2)\}\\
R_{e12} < H(S_1, S_2|W_1, W_2) - I(X_1, X_2; Z|W_1, W_2)\\
+ \min\{I_{11} - I(V_1; S_1|W_1) - I(V_2; S_2|W_2), I_5 - I(V_1; S_1) - I(V_2; S_2)\\
I_6 - I(V_1; S_1|W_1) - I(V_2; S_2|W_2), I_{10} - I(V_1; S_1) - I(V_2; S_2|W_2)\\
I_8 - I(V_1; S_1|W_1) - I(V_2; S_2)\}
\end{array}\right\} \tag{33}$$

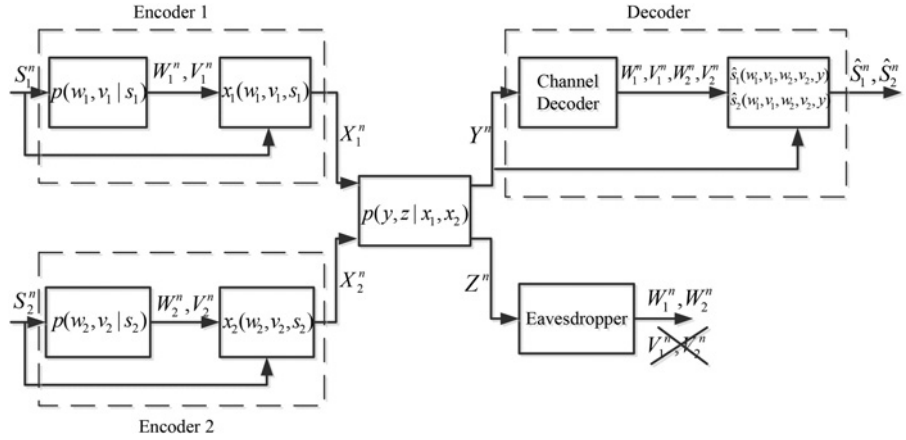

Fig. 4 *Hybrid scheme for MAC-WT*

$$R_j^p \geq I(V_j; S_j|W_j) \tag{36}$$

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 $i = 1, \ldots, n$.

4.3 Decoding

The receiver looks for unique indices r_j^o, r_j^p and r_j^r, j = 1:2, such that

$$(\{w_j^n(r_j^o), v_j^n(r_j^o, r_j^p, r_j^r)|j = 1{:}2\}, y^n) \in A_\varepsilon^n(W_1, W_2, V_1, V_2, Y)$$

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

$$(\{w_j^n(r_j^o)|j = 1{:}2\}, z^n) \in A_\varepsilon^n(W_1, W_2, Z)$$

4.4 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

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

From the Markov lemma [25, Lecture Note 13], $\Pr(\mathcal{E}_1)$ and $\Pr(\mathcal{E}_3)$ tend to zero as $n \to \infty$. The event $\mathcal{E}_2$ occurs in one of the following cases (we use 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 $(\tilde{r}_2^p, \tilde{r}_2^r) \neq (r_2^p, r_2^r)$: The probability of this event goes to zero as $n \to \infty$ if

$$\begin{aligned}
R_1^o + R_1^p + R_1^r + R_2^o + R_2^p + R_2^r < I(W_1, V_1, W_2, V_2; Y)\\
+ I(W_1, V_1; W_2, V_2)
\end{aligned} \tag{37}$$

(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

$$\begin{aligned}
R_1^p + R_1^r + R_2^o + R_2^p + R_2^r < I(V_1, W_2, V_2; Y|W_1)\\
+ I(W_1, V_1; W_2, V_2)
\end{aligned} \tag{38}$$

(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

$$\begin{aligned}
R_1^o + R_1^p + R_1^r + R_2^p + R_2^r < I(W_1, V_1, V_2; Y|W_2)\\
+ I(W_1, V_1; W_2, V_2)
\end{aligned} \tag{39}$$

(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

$$\begin{aligned}
R_1^p + R_1^r + R_2^p + R_2^r < I(V_1, V_2; Y|W_1, W_2)\\
+ I(W_1, V_1; W_2, V_2) - I(W_1; W_2)
\end{aligned} \tag{40}$$

(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

$$R_2^o + R_2^p + R_2^r < I(W_2, V_2; Y, W_1, V_1) \tag{41}$$

(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

$$R_2^p + R_2^r < I(V_2; Y, W_1, V_1|W_2) \tag{42}$$

(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

$$R_1^o + R_1^p + R_1^r < I(W_1, V_1; Y, W_2, V_2) \tag{43}$$

(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

$$R_1^p + R_1^r < I(V_1; Y, W_2, V_2|W_1) \tag{44}$$

Therefore $\Pr(\mathcal{E}_2)$ 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 (we use 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

$$R_1^o + R_2^o < I(W_1, W_2; Z) + I(W_1; W_2) \tag{45}$$

(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

$$R_1^o < I(W_1; Z|W_2) \tag{46}$$

(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

$$R_2^o < I(W_2; Z|W_1) \tag{47}$$

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

4.5 Secrecy analysis

Consider the following equivocation rate

$$\begin{aligned} H(S_1^n|Z^n) &= H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) - H(r_1^o, r_1^p, r_1^r, X_1^n|S_1^n, Z^n) \\ &\overset{(a)}{=} H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) - H(r_1^o, r_1^p, r_1^r|S_1^n, Z^n) \\ &\overset{(b)}{=} H(r_1^o, r_1^p, r_1^r, S_1^n, X_1^n|Z^n) - H(r_1^p, r_1^r|r_1^o, S_1^n, Z^n) \end{aligned} \tag{48}$$

where (a) follows because X_1^n is a deterministic function of $(r_1^o, r_1^p, r_1^r, S_1^n)$ and (b) follows because r_1^o is a deterministic function of S_1^n. Now, consider the first term of (48)

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

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) and (d) follows from [25, Lecture Note 13] and the fact that $H(r_1^r) = nR_1^r$. Next, consider the second term of (48)

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

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 $R_1^r + R_1^p < I(V_1; S_1, Z|W_1)$, then from Fano's inequality we have, $H(V_1^n|r_1^o, S_1^n, Z^n) \leq n\delta$. This can be proved as the following. Suppose that the eavesdropper, knowing r_1^o, tries to find (r_1^p, r_1^r). By the analysis of the error event, it can be easily shown that if the above condition on $R_1^p + R_1^r$ is satisfied, then from Fano's inequality, we can bound the entropy term as the above. In summary, we have

$$R_{e1} < H(S_1|W_1) - I(X_1; Z|W_1) + R_1^r \tag{49}$$

Similarly, if

$$R_2^r + R_2^p < I(V_2; S_2, Z|W_2) \tag{50}$$

$$R_1^r + R_1^p + R_2^r + R_2^p < I(V_1, V_2; S_1, S_2, Z|W_1, W_2) \tag{51}$$

we obtain

$$R_{e2} < H(S_2|W_2) - I(X_2; Z|W_2) + R_2^r \tag{52}$$

$$R_{e12} < H(S_1, S_2|W_1, W_2) - I(X_1, X_2; Z|W_1, W_2) + R_1^r + R_2^r \tag{53}$$

Collecting the terms in (35)–(47), (49)–(53) and performing Fourier–Motzkin elimination, we find the terms in the theorem.

At the end of this section, we find an outer bound to the rate-distortion-equivocation region of the degraded MAC-WT, where $(X_1, X_2) \to Y \to Z$ forms a Markov chain. The outer bound is given in the following theorem.

Theorem 3: If $(\kappa, D_1, D_2, R_{e12})$ is achievable for the degraded MAC-WT where $(X_1, X_2) \to Y \to Z$ forms a Markov chain, then we have

$$\left\{ \begin{array}{c} I(S_1; \hat{S}_1|S_2) \leq \kappa I(X_1; Y|X_2) \\ I(S_2; \hat{S}_2|S_1) \leq \kappa I(X_2; Y|X_1) \\ I(S_1, S_2; \hat{S}_1, \hat{S}_2) \leq \kappa I(X_1, X_2; Y) \\ R_{e12} \leq H(S_1, S_2) - I(S_1, S_2; \hat{S}_1, \hat{S}_2) + \kappa I(X_1, X_2; Y|Z) \end{array} \right\} \tag{54}$$

for some pmf $p(x_1, x_2, s_1, s_2)$, such that $\mathbb{E}[d_j(S_j, \hat{S}_j)] \leq D_j$, $j = 1{:}2$.

Proof: See Appendix 1. □

In the following section, we study lossy transmission of a bivariate Gaussian source over GMAC-WT.

5 Gaussian case

In this section, we consider lossy transmission of correlated sources over a GMAC-WT. First, we derive an outer bound to the rate-distortion-equivocation region of the GMAC-WT. Then, we use the proposed separate and hybrid schemes to find inner bounds to the rate-distortion-equivocation region of the GMAC-WT. An achievable region based on uncoded transmission is also obtained. The separate, the uncoded and the hybrid schemes are compared for different values of source correlation coefficient. Optimal regions for some special cases are established. Suppose that the sources are Gaussian random variables with joint distribution $(S_1, S_2) \sim \mathcal{N}(0, K_S)$, where

$$K_S = \begin{bmatrix} \sigma^2 & \rho\sigma^2 \\ \rho\sigma^2 & \sigma^2 \end{bmatrix} \tag{55}$$

The sources are reconstructed using the quadratic distortion measure $d_j(s_j, \hat{s}_j) = (s_j - \hat{s}_j)^2$, $j = 1{:}2$. We assume that the channel to the legitimate receiver is defined as $Y = X_1 + X_2 + N_y$ with $N_y \sim \mathcal{N}(0, \sigma_y^2)$ and input power constraints $(1/n)\sum_{i=1}^n \mathbb{E}(x_{ji}^2) \leq P_j$,

$j = 1{:}2$. The channel of the eavesdropper is defined as $Z = X_1 + X_2 + N_z$ with $N_z \sim \mathcal{N}(0, \sigma_z^2)$. We define the quantities $D_{e1} = 2^{2R_{e1}}/(2\pi e)$, $D_{e2} = 2^{2R_{e2}}/(2\pi e)$ and $D_{e12} = 2^{2R_{e12}}/(2\pi e)$. A tuple $(D_1, D_2, D_{e1}, D_{e2}, D_{e12})$ is said to be achievable if there exists an (n, n)-code (f_1, f_2, g) such that

$$\mathbb{E}\left[\left\|S_j - \hat{S}_j\right\|^2\right] \leq D_j + \varepsilon, j = 1{:}2 \tag{56}$$

$$\frac{1}{n}H(S_1^n|Z^n) \geq \frac{1}{2}\log(2\pi e D_{e1}) - \varepsilon \tag{57}$$

$$\frac{1}{n}H(S_2^n|Z^n) \geq \frac{1}{2}\log(2\pi e D_{e2}) - \varepsilon \tag{58}$$

$$\frac{1}{n}H(S_1^n, S_2^n|Z^n) \geq \frac{1}{2}\log(2\pi e D_{e12}) - \varepsilon. \tag{59}$$

In the following, we first propose an outer bound to the distortion-equivocation region of the GMAC-WT when $\sigma_y^2 \leq \sigma_z^2$.

Theorem 4: If $(D_1, D_2, D_{e1}, D_{e2}, D_{e12})$ is achievable for the GMAC-WT when $\sigma_y^2 \leq \sigma_z^2$ and $\rho = 0$, then we have

$$\left\{\begin{array}{c} D_1 \geq \dfrac{1}{1+\left(P_1/\sigma_y^2\right)} \cdot \sigma^2 \\ D_2 \geq \dfrac{1}{1+\left(P_2/\sigma_y^2\right)} \cdot \sigma^2 \\ D_1 \cdot D_2 \geq \dfrac{1}{1+\left((P_1+P_2)/\sigma_y^2\right)} \cdot \sigma^4 \\ D_{e1} \leq \min\left\{\sigma^2, D_1 \cdot \dfrac{1+\left((P_1+(1-\beta_1)P_2)/\left(\beta_1 P_2+\sigma_y^2\right)\right)}{1+\left(P_1/\left(P_2+\sigma_z^2\right)\right)}\right\} \\ D_{e2} \leq \min\left\{\sigma^2, D_2 \cdot \dfrac{1+\left((P_2+(1-\beta_2)P_1)/\left(\beta_2 P_1+\sigma_y^2\right)\right)}{1+\left(P_2/\left(P_1+\sigma_z^2\right)\right)}\right\} \\ D_{e12} \leq D_1 \cdot D_2 \cdot \dfrac{1+\left((P_1+P_2)/\sigma_y^2\right)}{1+\left((P_1+P_2)/\sigma_z^2\right)} \end{array}\right\} \tag{60}$$

for some $\beta_1, \beta_2 \in [0, 1]$.

Proof: See Appendix 2. □

Next, we find inner bounds to the rate-distortion-equivocation region of the GMAC-WT. We study three coding schemes: separation approach, uncoded transmission and hybrid schemes. First, consider the separate source-channel coding strategy.

5.1 Source-channel separation

We combine the optimal scheme for the source-coding problem and an achievable scheme for the channel-coding problem. The source-coding problem is explained in Fig. 5. Two source sequences are observed by two encoders. Each encoder maps its source sequence to a rate-limited codeword and sends it through an error-free link. The receiver wishes to reconstruct both sources with desired distortions. This problem has been considered in [25, Lecture Note 12] and the optimal rate-distortion region has been characterised as the following. For the Gaussian two-terminal source-coding problem, a distortion-pair (D_1, D_2) is achievable if and only if [25, Lecture Note 12]

$$(R_1, R_2) \in \mathcal{R}_1(D_1) \bigcap \mathcal{R}_2(D_2) \bigcap \mathcal{R}_{12}(D_1, D_2)$$

where

$$\left\{\begin{array}{c} \mathcal{R}_1(D_1) = \{(R_1, R_2): \\ R_1 \geq \dfrac{1}{2}\log\left[\dfrac{1}{D_1}(1-\rho^2(1-2^{-2R_2}))\right]\right\} \\ \mathcal{R}_2(D_2) = \{(R_1, R_2): \\ R_2 \geq \dfrac{1}{2}\log\left[\dfrac{1}{D_2}(1-\rho^2(1-2^{-2R_1}))\right]\right\} \\ \mathcal{R}_{12}(D_1, D_2) = \{(R_1, R_2): \\ R_1 + R_2 \geq \dfrac{1}{2}\log\left[\dfrac{(1-\rho^2)\phi(D_1, D_2)}{2D_1 D_2}\right]\right\} \end{array}\right\} \tag{61}$$

and

$$\phi(D_1, D_2) = 1 + \sqrt{1 + \frac{4\rho^2 D_1 D_2}{(1-\rho^2)^2}}$$

For the channel-coding problem, we use Theorem 1 to find an achievable region in the following.

Corollary 1: Let $W_j = U_j = 0$, $j = 1{:}2$, and $\kappa = 1$ in Theorem 1, and define $R_j = I(V_j; S_j)$. A tuple $(D_1, D_2, R_{e1}, R_{e2}, R_{e12})$ is achievable for the MAC-WT if

$$\left\{\begin{array}{c} R_{e1} < H(S_1) - [R_1 - [I(X_1; Y|X_2) - I(X_1; Z)]^+]^+ \\ R_{e2} < H(S_2) - [R_2 - [I(X_2; Y|X_1) - I(X_2; Z)]^+]^+ \\ R_{e12} < H(S_1, S_2) - [R_1 + R_2 - [I(X_1, X_2; Y) - I(X_1, X_2; Z)]^+]^+ \end{array}\right\} \tag{62}$$

for some pmf $p(s_1, s_2)p(x_1)p(x_2)$ where R_1 and R_2 are rate-distortion functions of sources S_1 and S_2, respectively, such that

$$\left\{\begin{array}{c} R_1 < I(X_1; Y|X_2) \\ R_2 < I(X_2; Y|X_1) \\ R_1 + R_2 < I(X_1, X_2; Y) \end{array}\right\} \tag{63}$$

$\mathbb{E}[d_1(S_1, \hat{S}_1)] \leq D_1$ and $\mathbb{E}[d_2(S_2, \hat{S}_2)] \leq D_2$.
The remaining problem is to find suitable (R_1, R_2) pair that falls into the capacity region of the GMAC. We will choose the following achievable pairs

$$(R_1, R_2) = \left(\frac{1}{2}\log\left(1 + \frac{P_1}{\sigma_y^2}\right), \frac{1}{2}\log\left(1 + \frac{P_2}{P_1 + \sigma_y^2}\right)\right) \tag{64}$$

$$(R_1, R_2) = \left(\frac{1}{2}\log\left(1 + \frac{P_1}{P_2 + \sigma_y^2}\right), \frac{1}{2}\log\left(1 + \frac{P_2}{\sigma_y^2}\right)\right) \tag{65}$$

Inserting (64) into (61) and (62), we obtain the following achievable distortion tuple.

Theorem 5: The distortion tuple $(D_1^s, D_2^s, D_{e1}^s, D_{e2}^s, D_{e12}^s)$ resulting from the separate scheme satisfies the following (see (66) at the

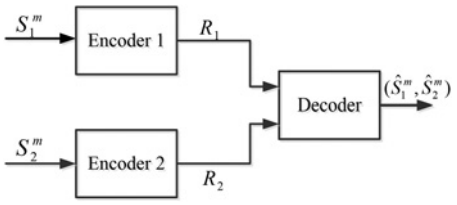

Fig. 5 *Source-coding problem*

bottom of the next page)

Similarly, inserting (65) into (61) and (62), we obtain the achievable distortion tuple $(D_1^{ss}, D_2^{ss}, D_{e1}^{ss}, D_{e2}^{ss}, D_{e12}^{ss})$ that satisfies the following (see (67))

We also find an achievable distortion tuple for the symmetric GMAC-WT where $D_1 = D_2 = D^s$, $P_1 = P_2 = P$, $D_{e1} = D_{e2} = D_e^s$ and $D_{e12} = D_{et}^s$. We assume that $\sigma_z^2 \geq \sigma_y^2$. We choose the achievable rate as $R = (1/4)\log\left(1 + \left(2P/\sigma_y^2\right)\right)$. Inserting this rate into (61) and (62), we obtain the following theorem.

Theorem 6: The distortion tuple (D^s, D_e^s, D_{et}^s) resulting from the separate scheme for the symmetric GMAC-WT when $\sigma_z^2 \geq \sigma_y^2$ is given by

$$\left\{ \begin{array}{c} D^s = \dfrac{\sqrt{1 + \left(2P/\sigma_y^2\right)(1-\rho^2)}}{1 + \left(2P/\sigma_y^2\right)} \cdot \sigma^2 \\ D_e^s = \min\left\{ \sigma^2,\ \dfrac{1 + \left(P/\sigma_y^2\right)}{\sqrt{1 + \left(2P/\sigma_y^2\right)} \cdot \left(1 + \left(P/\left(P + \sigma_z^2\right)\right)\right)} \cdot \sigma^2 \right\} \\ D_{et}^s = \dfrac{(1-\rho^2)}{1 + \left(2P/\sigma_z^2\right)} \cdot \sigma^4 \end{array} \right\} \tag{68}$$

$$\left\{ \begin{array}{c} D_1^s \geq \dfrac{1 + \left(\left((1-\rho^2)P_2\right)/\left(P_1 + \sigma_y^2\right)\right)}{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)} \cdot \sigma^2 \\ D_2^s \geq \dfrac{1 + \left(\left((1-\rho^2)P_1\right)/\sigma_y^2\right)}{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)} \cdot \sigma^2 \\ \dfrac{D_1^s \cdot D_2^s}{\phi(D_1^s, D_2^s)} \geq \dfrac{1-\rho^2}{2\left(1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)\right)} \cdot \sigma^2 \\ D_{e1}^s \leq \dfrac{1}{\max\left\{1,\ \dfrac{1 + \left(P_1/\sigma_y^2\right)}{\max\left\{1,\ \left(\left(1 + \left(P_1/\sigma_y^2\right)\right)/\left(1 + \left(P_1/\left(P_2 + \sigma_z^2\right)\right)\right)\right)\right\}}\right\}} \cdot \sigma^2 \\ D_{e2}^s \leq \dfrac{1}{\max\left\{1,\ \dfrac{1 + \left(P_2/\left(P_1 + \sigma_y^2\right)\right)}{\max\left\{1,\ \left(\left(1 + \left(P_2/\sigma_y^2\right)\right)/\left(1 + \left(P_2/\left(P_1 + \sigma_z^2\right)\right)\right)\right)\right\}}\right\}} \cdot \sigma^2 \\ D_{e12}^s \leq \dfrac{(1-\rho^2)}{\max\left\{1,\ \dfrac{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)}{\max\left\{1,\ \left(\left(1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)\right)/\left(1 + \left(\left(P_1 + P_2\right)/\sigma_z^2\right)\right)\right)\right\}}\right\}} \cdot \sigma^4 \end{array} \right\} \tag{66}$$

$$\left\{ \begin{array}{c} D_1^{ss} \geq \dfrac{1 + \left(\left((1-\rho^2)P_2\right)/\sigma_y^2\right)}{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)} \cdot \sigma^2 \\ D_2^{ss} \geq \dfrac{1 + \left(\left((1-\rho^2)P_1\right)/\left(P_2 + \sigma_y^2\right)\right)}{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)} \cdot \sigma^2 \\ \dfrac{D_1^{ss} \cdot D_2^{ss}}{\phi(D_1^{ss}, D_2^{ss})} \geq \dfrac{1-\rho^2}{2\left(1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)\right)} \cdot \sigma^2 \\ D_{e1}^{ss} \leq \dfrac{1}{\max\left\{1,\ \dfrac{1 + \left(\left(P_1\right)/\left(P_2 + \sigma_y^2\right)\right)}{\max\left\{1,\ \left(\left(1 + \left(P_1/\sigma_y^2\right)\right)/\left(1 + \left(P_1/\left(P_2 + \sigma_z^2\right)\right)\right)\right)\right\}}\right\}} \cdot \sigma^2 \\ D_{e2}^{ss} \leq \dfrac{1}{\max\left\{1,\ \dfrac{1 + \left(P_2/\sigma_y^2\right)}{\max\left\{1,\ \left(\left(1 + \left(P_2/\sigma_y^2\right)\right)/\left(1 + \left(P_2/\left(P_1 + \sigma_z^2\right)\right)\right)\right)\right\}}\right\}} \cdot \sigma^2 \\ D_{e12}^{ss} \leq \dfrac{(1-\rho^2)}{\max\left\{1,\ \dfrac{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)}{\max\left\{1,\ \left(\left(1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)\right)/\left(1 + \left(\left(P_1 + P_2\right)/\sigma_z^2\right)\right)\right)\right\}}\right\}} \cdot \sigma^4 \end{array} \right\}. \tag{67}$$

IET Commun., 2015, Vol. 9, Iss. 6, pp. 754–770

Next, we find an achievable distortion tuple using uncoded transmission. Then, we compare the separate and the uncoded schemes for some special cases.

5.2 Uncoded transmission

We choose $X_{ij} = \sqrt{\frac{P_i}{\sigma^2}} S_{ij}$, for $i = 1{:}2$ and $j = 1, \ldots, n$ and implement a minimum-mean-squared error (MMSE) estimation at the decoder, that is, $\hat{S}^u_{ij} = \mathbb{E}[S_{ij}|Y_j]$, $j = 1, \ldots, n$. Thus, we obtain the following achievable tuple.

Theorem 7: The distortion tuple $(D^u_1, D^u_2, D^u_{e1}, D^u_{e2}, D^u_{e12})$ resulting from the described uncoded scheme is given by

$$\left\{ \begin{array}{l} D^u_1 = \dfrac{1 + \left(\left((1-\rho^2)P_2\right)/\sigma_y^2\right)}{1 + \left(\left(P_1 + P_2 + 2\rho\sqrt{P_1P_2}\right)/\sigma_y^2\right)} \cdot \sigma^2 \\ D^u_2 = \dfrac{1 + \left(\left((1-\rho^2)P_1\right)/\sigma_y^2\right)}{1 + \left(P_1 + P_2 + 2\rho\sqrt{P_1P_2}\right)/\sigma_y^2} \cdot \sigma^2 \\ D^u_{e1} = \dfrac{1 + \left(\left((1-\rho^2)P_2\right)/\sigma_z^2\right)}{1 + \left(\left(P_1 + P_2 + 2\rho\sqrt{P_1P_2}\right)/\sigma_z^2\right)} \cdot \sigma^2 \\ D^u_{e2} = \dfrac{1 + \left(\left((1-\rho^2)P_1\right)/\sigma_z^2\right)}{1 + \left(\left(P_1 + P_2 + 2\rho\sqrt{P_1P_2}\right)/\sigma_z^2\right)} \cdot \sigma^2 \\ D^u_{e12} = \dfrac{(1-\rho^2)}{1 + \left(\left(P_1 + P_2 + 2\rho\sqrt{P_1P_2}\right)/\sigma_z^2\right)} \cdot \sigma^4 \end{array} \right\} \tag{69}$$

for the symmetric GMAC-WT where $D^u_1 = D^u_2 = D^u$, $P_1 = P_2 = P$, $D^u_{e1} = D^u_{e2} = D^u_e$ and $D^u_{e12} = D^u_{et}$, the tuple in (69) reduces to the following

$$\left\{ \begin{array}{l} D^u = \dfrac{1 + \left(\left((1-\rho^2)P\right)/\sigma_y^2\right)}{1 + \left(\left(2(1+\rho)P\right)/\sigma_y^2\right)} \cdot \sigma^2 \\ D^u_e = \dfrac{1 + \left(\left((1-\rho^2)P\right)/\sigma_z^2\right)}{1 + \left(\left(2(1+\rho)P\right)/\sigma_z^2\right)} \cdot \sigma^2 \\ D^u_{et} = \dfrac{(1-\rho^2)}{1 + \left(\left(2(1+\rho)P\right)/\sigma_z^2\right)} \cdot \sigma^4 \end{array} \right\} \tag{70}$$

Remark 1: Consider the symmetric GMAC-WT and let $\rho = 0$ in (68) and (70). Also, assume that $\sigma_z^2 \geq \sigma_y^2$. We obtain the following distortion tuples (see (71) and (72))

It can be easily checked that $D^s < D^u$, therefore, the separate scheme's distortion at the receiver is smaller than the uncoded scheme's. We also have $D^s_e > D^u_e$, that is, the individual secrecy rate of the separation is larger than the rate of uncoded scheme. For both strategies, we have $D^s_{et} = D^u_{et}$. The results of this comparison are numerically evaluated for $\sigma_z^2/\sigma_y^2 = 1.5$ in Fig. 6. As shown in Fig. 6, D^u_e is smaller than D^s_e while D^u dominates D^s.

Now, we find the optimal region for a special case. We simplify Theorem 4 to find an outer bound to the distortion-equivocation region of the symmetric GMAC-WT when $\sigma_y^2 \leq \sigma_z^2$ and $\rho = 0$. In the following theorem, we assume that

$$\sqrt{1 + \left(2P/\sigma_y^2\right)} \leq \frac{1}{1 + \left(P/\left(P + \sigma_z^2\right)\right)}$$

Theorem 8: The tuple (D^s, D^s_e, D^s_{et}) is achievable for the symmetric GMAC-WT when $\sigma_y^2 \leq \sigma_z^2$, $\rho = 0$ and $\sqrt{1 + \left(2P/\sigma_y^2\right)} \leq \left(1/\left(1 + \left(P/\left(P + \sigma_z^2\right)\right)\right)\right)$, if and only if

$$\left\{ \begin{array}{c} D^s \geq \dfrac{1}{\sqrt{1 + \left(2P/\sigma_y^2\right)}} \cdot \sigma^2 \\ D^s_e \leq \sigma^2 \\ D^s_{et} \leq (D^s)^2 \cdot \dfrac{1 + \left(2P/\sigma_y^2\right)}{1 + \left(2P/\sigma_z^2\right)} \end{array} \right\} \tag{73}$$

Proof: For the proof of achievability, consider Theorem 6 with $\rho = 0$. The inequality

$$\sqrt{1 + \left(2P/\sigma_y^2\right)} \leq \frac{1}{1 + \left(P/\left(P + \sigma_z^2\right)\right)}$$

implies that

$$\frac{\sqrt{1 + \left(2P/\sigma_y^2\right)}}{1 + \left(P/\sigma_y^2\right)} \leq \frac{1}{1 + \left(P/\left(P + \sigma_z^2\right)\right)}$$

therefore $D^s_e = \sigma^2$. Also, we have $D^s_{et} = (D^s)^2 \cdot \left(\left(1 + \left(2P/\sigma_y^2\right)\right)\Big/ 1 + \left(2P/\sigma_z^2\right)\right)$. It can be easily checked that Theorem 1 yields similar region. For the proof of converse, consider Theorem 4 with $D_1 = D_2 = D^s$, $P_1 = P_2 = P$, $D_{e1} = D_{e2} = D^s_e$, $D_{e12} = D^s_{et}$ and $\beta_1 = \beta_2 = \beta$. Thus, if the tuple (D^s, D^s_e, D^s_{et}) is achievable, then we have

$$\left\{ \begin{array}{c} D^s \geq \dfrac{1}{\sqrt{1 + \left(2P/\sigma_y^2\right)}} \cdot \sigma^2 \\ D^s_e \leq \min\left\{ \sigma^2, D^s \cdot \dfrac{1 + \left(\left((2-\beta)P\right)/\left(\beta P + \sigma_y^2\right)\right)}{1 + \left(P/\left(P + \sigma_z^2\right)\right)} \right\} \\ D^s_{et} \leq (D^s)^2 \cdot \dfrac{1 + \left(2P/\sigma_y^2\right)}{1 + \left(2P/\sigma_z^2\right)} \end{array} \right\} \tag{74}$$

$$(D^s, D^s_e, D^s_{et}) = \left(\frac{1}{\sqrt{1 + \left(2P/\sigma_y^2\right)}} \cdot \sigma^2, \ \min\left\{ \sigma^2, \ \frac{1 + \left(P/\sigma_y^2\right)}{\sqrt{1 + \left(2P/\sigma_y^2\right)} \cdot \left(1 + \left(P/\left(P + \sigma_z^2\right)\right)\right)} \cdot \sigma^2 \right\}, \ \frac{1}{1 + \left(2P/\sigma_z^2\right)} \cdot \sigma^4 \right) \tag{71}$$

$$(D^u, D^u_e, D^u_{et}) = \left(\frac{1 + \left(P/\sigma_y^2\right)}{1 + \left(2P/\sigma_y^2\right)} \cdot \sigma^2, \ \frac{1 + \left(P/\sigma_z^2\right)}{1 + \left(2P/\sigma_z^2\right)} \cdot \sigma^2, \ \frac{1}{1 + \left(2P/\sigma_z^2\right)} \cdot \sigma^4 \right) \tag{72}$$

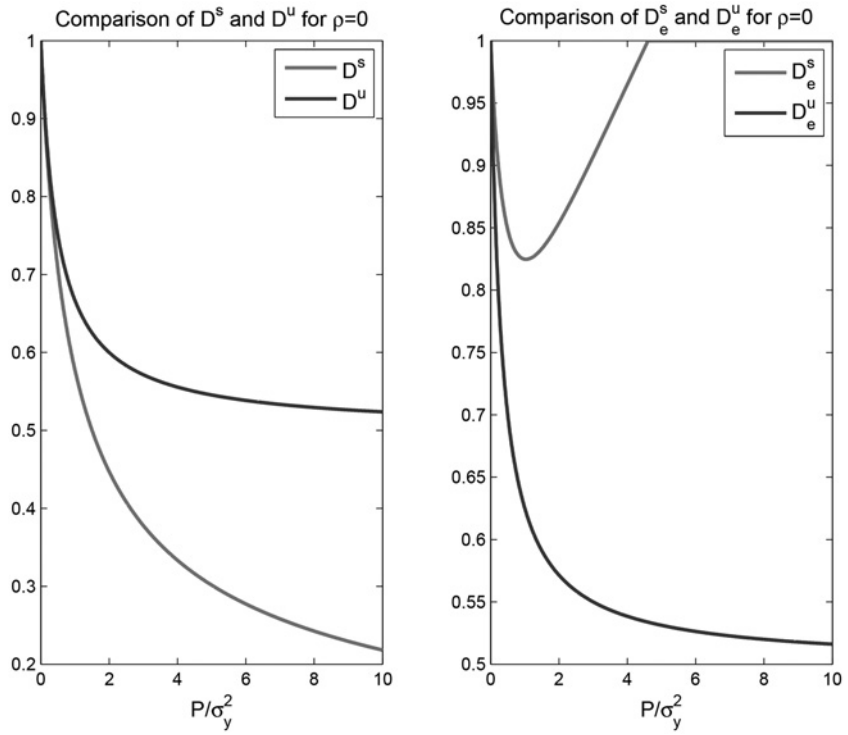

Fig. 6 *Comparison of D^s with D^u, and D_e^s with D_e^u as a function of P/σ_y^2 for $\rho = 0$, $\sigma^2 = 1$ and $\sigma_z^2/\sigma_y^2 = 1.5$*

Also, we have

$$D^s \cdot \frac{1+\left((2-\beta)P\right)/\left(\beta P+\sigma_y^2\right)}{1+\left(P/\left(P+\sigma_z^2\right)\right)} \overset{(a)}{\geq} \frac{1+\left((2-\beta)P\right)/\left(\beta P+\sigma_y^2\right)}{\sqrt{1+\left(2P/\sigma_y^2\right)}\left(1+\left(P/\left(P+\sigma_z^2\right)\right)\right)} \cdot \sigma^2 \overset{(b)}{\geq} \sigma^2 \tag{75}$$

where (a) follows from the first inequality in (74) and (b) follows from the inequality

$$\sqrt{1+\left(2P/\sigma_y^2\right)} \leq \frac{1}{1+\left(P/\left(P+\sigma_z^2\right)\right)}$$

Therefore the second inequality in (74) reduces to $D_e^s \leq \sigma^2$. □

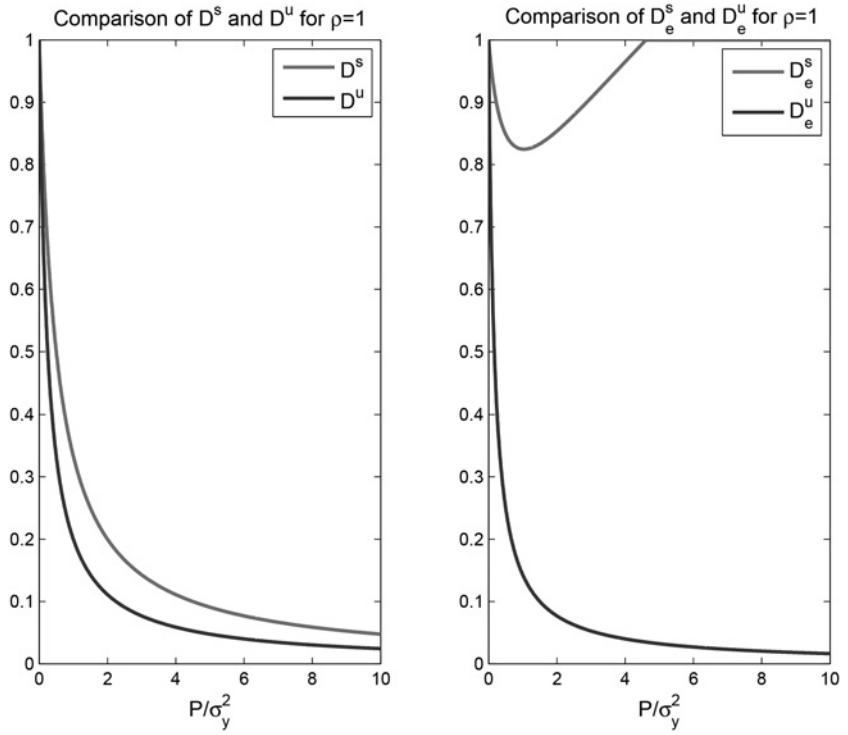

Fig. 7 *Comparison of D^s with D^u, and D_e^s with D_e^u as a function of P/σ_y^2 for $\rho = 1$, $\sigma^2 = 1$ and $\sigma_z^2/\sigma_y^2 = 1.5$*

Remark 2: Consider the symmetric GMAC-WT with $\rho = 1$. Also, let $S_1 = S_2 = S$, that is, the term D_{et}^s is inactive. We obtain the following distortion pairs

$$(D^s, D_e^s) = \left(\frac{1}{1+\frac{2P}{\sigma_y^2}} \cdot \sigma^2, \min\left\{ \sigma^2, \frac{1+\frac{P}{\sigma_y^2}}{\sqrt{1+\frac{2P}{\sigma_y^2}} \cdot \left(1+\frac{P}{P+\sigma_z^2}\right)} \cdot \sigma^2 \right\} \right) \tag{76}$$

$$(D^u, D_e^u) = \left(\frac{1}{1+\left(4P/\sigma_y^2\right)} \cdot \sigma^2, \frac{1}{1+\left(4P/\sigma_z^2\right)} \cdot \sigma^2 \right) \tag{77}$$

The uncoded scheme's distortion at the receiver is smaller than the separate scheme's, that is, $D^s > D^u$. We have $D_e^s > D_e^u$, that is, the individual secrecy rate of the separation is larger than the rate of uncoded scheme. The results of this comparison are numerically evaluated for $\sigma_z^2/\sigma_y^2 = 1.5$ in Fig. 7. As shown in Fig. 7, D_e^s is larger than D_e^u while D^s dominates D^u.

Next, we obtain the optimal region for a special case. We simplify Theorem 3 to find an outer bound to the distortion-equivocation region of the symmetric GMAC-WT when $\rho = 1$ and $\sigma_y^2 \le \sigma_z^2$.

Theorem 9: The pair (D^u, D_e^u) is achievable for the symmetric GMAC-WT when $\rho = 1$ and $\sigma_y^2 \le \sigma_z^2$, if and only if

$$\left\{ \begin{array}{c} D^u \ge \dfrac{1}{1+\left(4P/\sigma_y^2\right)} \cdot \sigma^2 \\ D_e^u \le D^u \cdot \dfrac{1+\left(4P/\sigma_y^2\right)}{1+\left(4P/\sigma_z^2\right)} \end{array} \right\} \tag{78}$$

Proof: For the proof of achievability, let $\rho = 1$ in (70). Also, note that

$$D_e^u = D^u \cdot \frac{1+\left(4P/\sigma_y^2\right)}{1+\left(4P/\sigma_z^2\right)}$$

For the proof of converse, let $S_1 = S_2 = S$, $X_1 = X_2 = X$, $\hat{S}_1 = \hat{S}_2 = \hat{S}$, $\kappa = 1$ and $D_{e12} = D_e^u$ in Theorem 3. □

Finally, we consider the hybrid scheme. In the following, we simplify the conditions of Theorem 2 for the GMAC-WT.

5.3 Hybrid scheme

Consider the conditions of Theorem 2. Given $\alpha_j \in \left[0, \sqrt{P_j/\sigma^2}\right]$ and $R_j > 0$, $j = 1{:}2$, let $W_j = 0$, $j = 1{:}2$, $V_j = \left(1-2^{-2R_j}\right)S_j + N_j$, $j = 1{:}2$ and $X_j = \alpha_j S_j + \beta_j V_j$, $j = 1{:}2$, where N_j are independent Gaussian random variables with zero mean and variance $\sigma^2 2^{-2R_j}(1-2^{-2R_j})$ and

$$\beta_j = \sqrt{\frac{P_j - \alpha_j^2 \sigma^2 2^{-2R_j}}{\sigma^2(1-2^{-2R_j})}} - \alpha_j.$$

Let

$$\boldsymbol{K} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} & k_{15} & k_{16} \\ k_{12} & k_{22} & k_{23} & k_{24} & k_{25} & k_{26} \\ k_{13} & k_{23} & k_{33} & k_{34} & k_{35} & k_{36} \\ k_{14} & k_{24} & k_{34} & k_{44} & k_{45} & k_{46} \\ k_{15} & k_{25} & k_{35} & k_{45} & k_{55} & k_{56} \\ k_{16} & k_{26} & k_{36} & k_{46} & k_{56} & k_{66} \end{bmatrix}$$

denotes the covariance matrix of $(S_1, S_2, V_1, V_2, Y, Z)$, respectively, where

$$\begin{aligned}
k_{jj} &= \sigma^2, j = 1{:}2 \\
k_{12} &= \rho\sigma^2 \\
k_{13} &= k_{33} = \sigma^2(1-2^{-2R_1}) \\
k_{24} &= k_{44} = \sigma^2(1-2^{-2R_2}) \\
k_{14} &= \rho\sigma^2(1-2^{-2R_2}) \\
k_{23} &= \rho\sigma^2(1-2^{-2R_1}) \\
k_{34} &= \rho\sigma^2(1-2^{-2R_1})(1-2^{-2R_2}) \\
k_{15} &= k_{16} = \beta_1 k_{13} + \beta_2 k_{14} + \alpha_1\sigma^2 + \alpha_2\rho\sigma^2 \\
k_{25} &= k_{26} = \beta_2 k_{24} + \beta_1 k_{23} + \alpha_2\sigma^2 + \alpha_1\rho\sigma^2 \\
k_{35} &= k_{36} = (\alpha_1 + \beta_1 + \alpha_2\rho)k_{13} + \beta_2 k_{34} \\
k_{45} &= k_{46} = (\alpha_2 + \beta_2 + \alpha_1\rho)k_{24} + \beta_1 k_{34} \\
k_{55} &= (\beta_1^2 + 2\alpha_1\beta_1 + 2\beta_1\alpha_2\rho)k_{13} \\
&\quad + (\beta_2^2 + 2\alpha_2\beta_2 + 2\alpha_1\beta_2\rho)k_{24} + 2\beta_1\beta_2 k_{34} \\
&\quad + (\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2\rho)\sigma^2 + \sigma_y^2 \\
k_{56} &= (\beta_1^2 + 2\alpha_1\beta_1 + 2\beta_1\alpha_2\rho)k_{13} \\
&\quad + (\beta_2^2 + 2\alpha_2\beta_2 + 2\alpha_1\beta_2\rho)k_{24} + 2\beta_1\beta_2 k_{34} \\
&\quad + (\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2\rho)\sigma^2 \\
k_{66} &= (\beta_1^2 + 2\alpha_1\beta_1 + 2\beta_1\alpha_2\rho)k_{13} \\
&\quad + (\beta_2^2 + 2\alpha_2\beta_2 + 2\alpha_1\beta_2\rho)k_{24} + 2\beta_1\beta_2 k_{34} \\
&\quad + (\alpha_1^2 + \alpha_2^2 + 2\alpha_1\alpha_2\rho)\sigma^2 + \sigma_z^2
\end{aligned} \tag{79}$$

Therefore Theorem 2 reduces to the following.

Corollary 2: The tuple $(D_1, D_2, R_{e1}, R_{e2}, R_{e12})$ is achievable if

$$\left\{ \begin{array}{c} D_j > \sigma^2 - e_{j1}c_{j1} - e_{j2}c_{j2} - e_{j3}c_{j3}, j = 1, 2 \\ R_{e1} < \dfrac{1}{2}\log(\sigma^2) - R_1 - \dfrac{1}{2}\log\left(1+\dfrac{r_{x1}}{P_1 k_{66} - r_{x1}}\right) \\ + \min\left\{ \dfrac{1}{2}\log\left(\dfrac{\beta_1'^2 k_{13}(1-\tilde{\rho}^2)+N'}{N'(1-\tilde{\rho}^2)}\right), \dfrac{1}{2}\log\left(\dfrac{\beta_1^2 k_{13} + 2^{2R_1}N_{e1}}{N_{e1}}\right) \right\} \\ R_{e2} < \dfrac{1}{2}\log(\sigma^2) - R_2 - \dfrac{1}{2}\log\left(1+\dfrac{r_{x2}}{P_2 k_{66} - r_{x2}}\right) \\ + \min\left\{ \dfrac{1}{2}\log\left(\dfrac{\beta_2'^2 k_{24}(1-\tilde{\rho}^2)+N'}{N'(1-\tilde{\rho}^2)}\right), \dfrac{1}{2}\log\left(\dfrac{\beta_2^2 k_{24} + 2^{2R_2}N_{e2}}{N_{e2}}\right) \right\} \\ R_{e12} < \dfrac{1}{2}\log(\sigma^4(1-\rho^2)) - R_1 - R_2 - \dfrac{1}{2}\log\left(1+\dfrac{k_{66}-\sigma_z^2}{\sigma_z^2}\right) \\ + \min\left\{ \dfrac{1}{2}\log\left(\dfrac{\beta_1'^2 k_{13} + \beta_2'^2 k_{24} + 2\tilde{\rho}\beta_1'\beta_2'\sqrt{k_{13}k_{24}} + N'}{N'(1-\tilde{\rho}^2)}\right), \right. \\ \left. \dfrac{1}{2}\log\left(\dfrac{(1-\tilde{\rho}^2)(2^{2(R_1+R_2)}\sigma_z^2 + 2^{2R_2}\beta_1^2 k_{13} + 2^{2R_1}\beta_2^2 k_{24})}{\sigma_z^2}\right) \right\} \end{array} \right\} \tag{80}$$

such that

$$\left\{ \begin{array}{c} R_1 < \dfrac{1}{2}\log\left(\dfrac{\beta_1'^2 k_{13}(1-\tilde{\rho}^2)+N'}{N'(1-\tilde{\rho}^2)}\right) \\ R_2 < \dfrac{1}{2}\log\left(\dfrac{\beta_2'^2 k_{24}(1-\tilde{\rho}^2)+N'}{N'(1-\tilde{\rho}^2)}\right) \\ R_1 + R_2 < \dfrac{1}{2}\log\left(\dfrac{\beta_1'^2 k_{13} + \beta_2'^2 k_{24} + 2\tilde{\rho}\beta_1'\beta_2'\sqrt{k_{13}k_{24}} + N'}{N'(1-\tilde{\rho}^2)}\right) \end{array} \right\} \tag{81}$$

where

$$c_{11} = k_{13}, \quad c_{12} = \rho k_{24}, \quad c_{21} = \rho k_{13}, \quad c_{22} = k_{24}$$
$$c_{13} = (\alpha_1 + \alpha_2\rho)\sigma^2 + \beta_1 k_{13} + \beta_2 k_{24}\rho,$$
$$c_{23} = (\alpha_2 + \alpha_1\rho)\sigma^2 + \beta_2 k_{24} + \beta_1 k_{13}\rho$$
$$\begin{bmatrix} e_{j1} \\ e_{j2} \\ e_{j3} \end{bmatrix} = \begin{bmatrix} k_{33} & k_{34} & k_{35} \\ k_{34} & k_{44} & k_{45} \\ k_{35} & k_{45} & k_{55} \end{bmatrix}^{-1} \begin{bmatrix} c_{j1} \\ c_{j2} \\ c_{j3} \end{bmatrix}$$

and

$$\tilde{\rho} = \rho\sqrt{(1-2^{-2R_1})(1-2^{-2R_2})}$$
$$r_{x1} = ((\alpha_1^2 + \alpha_1\alpha_2\rho)\sigma^2 + (\beta_1^2 + 2\alpha_1\beta_1 + \beta_1\alpha_2\rho)k_{13} + \alpha_1\beta_2\rho k_{24} + \beta_1\beta_2\rho k_{34})^2$$
$$r_{x2} = ((\alpha_2^2 + \alpha_1\alpha_2\rho)\sigma^2 + (\beta_2^2 + 2\alpha_2\beta_2 + \beta_2\alpha_1\rho)k_{24} + \alpha_2\beta_1\rho k_{13} + \beta_1\beta_2\rho k_{34})^2$$
$$N' = \alpha_1^2\nu_1 + \alpha_2^2\nu_2 + 2\alpha_1\alpha_2\nu_3 + \sigma_y^2$$
$$N_{e1} = \alpha_2^2(1-\rho^2)\sigma^2 + \beta_2^2(1-\rho^2(1-2^{-2R_2}))k_{24} + 2\alpha_2\beta_2(1-\rho^2)k_{24} + \sigma_z^2$$
$$N_{e2} = \alpha_1^2(1-\rho^2)\sigma^2 + \beta_1^2(1-\rho^2(1-2^{-2R_1}))k_{13} + 2\alpha_1\beta_1(1-\rho^2)k_{13} + \sigma_z^2$$
$$\nu_1 = \sigma^2 - (1-a_1\rho(1-2^{-2R_2}))^2 k_{13} - 2(1-a_1\rho(1-2^{-2R_2}))a_1 k_{34} - a_1^2 k_{24}$$
$$\nu_2 = \sigma^2 - (1-a_2\rho(1-2^{-2R_1}))^2 k_{24} - 2(1-a_2\rho(1-2^{-2R_1}))a_2 k_{34} - a_2^2 k_{13}$$
$$\nu_3 = \rho\sigma^2 - (1-a_1\rho(1-2^{-2R_2}))(1-a_2\rho(1-2^{-2R_1}))\, k_{34} - a_1a_2k_{34} - (1-a_1\rho(1-2^{-2R_2}))a_2k_{13} - (1-a_2\rho(1-2^{-2R_1}))a_1k_{24}$$
$$\beta_1' = \alpha_1\left(1 - \frac{\rho^2 2^{-2R_1}(1-2^{-2R_2})}{1-\tilde{\rho}^2}\right) + \beta_1 + \frac{\alpha_2\rho 2^{-2R_2}}{1-\tilde{\rho}^2}$$
$$\beta_2' = \alpha_2\left(1 - \frac{\rho^2 2^{-2R_2}(1-2^{-2R_1})}{1-\tilde{\rho}^2}\right) + \beta_2 + \frac{\alpha_1\rho 2^{-2R_1}}{1-\tilde{\rho}^2}a_1$$
$$a_2 = \frac{\rho 2^{-2R_2}(1-2^{-2R_1})}{\eta_2}$$
$$\eta_1 = (1-2^{-2R_2}) - 2\tilde{\rho}^2\sqrt{(1-2^{-2R_1})(1-2^{-2R_2})} + \tilde{\rho}^2(1-2^{-2R_1})$$
$$\eta_2 = (1-2^{-2R_1}) - 2\tilde{\rho}^2\sqrt{(1-2^{-2R_1})(1-2^{-2R_2})} + \tilde{\rho}^2(1-2^{-2R_2})$$

Remark 3: If we assume that the eavesdropper is neutral, that is, the secrecy constraints are omitted from the model, then the conditions of Corollary 2 reduce to the conditions of [22, Theorem IV.6].

In the symmetric case where $P_1 = P_2 = P$, $R_1 = R_2 = R$, $D_1 = D_2 = D^h$, $\alpha_1 = \alpha_2 = \alpha$, $\beta_1 = \beta_2 = \beta$, $R_{e1} = R_{e2} = R_e^h$ and $R_{e12} = R_{et}^h$, the matrix $\boldsymbol{K}$ and other coefficients reduce to

$$\boldsymbol{K} = \begin{bmatrix} k_1 & \rho k_1 & k_2 & \rho k_2 & k_4 & k_4 \\ \rho k_1 & k_1 & \rho k_2 & k_2 & k_4 & k_4 \\ k_2 & \rho k_2 & k_2 & k_3 & k_5 & k_5 \\ \rho k_2 & k_2 & k_3 & k_2 & k_5 & k_5 \\ k_4 & k_4 & k_5 & k_5 & k_7 & k_6 \\ k_4 & k_4 & k_5 & k_5 & k_6 & k_8 \end{bmatrix} \tag{82}$$

where

$$k_1 = \sigma^2$$
$$k_2 = \sigma^2(1-2^{-2R})$$
$$k_3 = \rho\sigma^2(1-2^{-2R})^2$$
$$k_4 = (1+\rho)(\beta k_2 + \alpha\sigma^2)$$
$$k_5 = (\alpha + \beta + \alpha\rho)k_2 + \beta k_3$$
$$k_6 = 2\beta(\beta + 2\alpha(1+\rho))k_2 + 2\beta^2 k_3 + 2\alpha^2(1+\rho)\sigma^2$$
$$k_7 = k_6 + \sigma_y^2$$
$$k_8 = k_6 + \sigma_z^2$$

Therefore, for the symmetric GMAC-WT, Corollary 2 simplifies as follows.

Corollary 3: The tuple (D^h, R_e^h, R_{et}^h) is achievable if (see (83))

such that

$$R < \frac{1}{4}\log\left(\frac{2\beta'^2(1+\tilde{\rho})k_2 + N'}{N'(1-\tilde{\rho}^2)}\right) \tag{84}$$

where

$$c_1 = k_2, \quad c_2 = \rho k_2, \quad c_3 = (1+\rho)\beta k_2 + (1+\rho)\alpha\sigma^2$$
$$\begin{bmatrix} e_1 \\ e_2 \\ e_3 \end{bmatrix} = \begin{bmatrix} k_2 & k_3 & k_5 \\ k_3 & k_2 & k_5 \\ k_5 & k_5 & k_7 \end{bmatrix}^{-1} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

and

$$\tilde{\rho} = \rho(1-2^{-2R})$$
$$r_x = (\alpha^2(1+\rho)\sigma^2 + \beta(\beta + 2\alpha(1+\rho))k_2 + \beta^2\rho k_3)^2$$
$$N' = 2\alpha^2(\nu_1 + \nu_3) + \sigma_y^2$$
$$N_e = \alpha^2(1-\rho^2)\sigma^2 + \beta(1-\rho^2(1-2^{-2R_2}) + 2\alpha(1-\rho^2))k_2 + \sigma_z^2$$

$$\left\{\begin{array}{c} D^h > \sigma^2 - e_1c_1 - e_2c_2 - e_3c_3 \\ R_e^h < \frac{1}{2}\log(\sigma^2) - R - \frac{1}{2}\log\left(1 + \frac{r_x}{Pk_8 - r_x}\right) + \\ \min\left\{\frac{1}{2}\log\left(\frac{\beta'^2 k_2(1-\tilde{\rho}^2) + N'}{N'(1-\tilde{\rho}^2)}\right), \frac{1}{2}\log\left(\frac{\beta'^2 k_2 + 2^{2R}N_e}{N_e}\right)\right\} \\ R_{et}^h < \frac{1}{2}\log(\sigma^4(1-\rho^2)) - 2R - \frac{1}{2}\log\left(1 + \frac{k_8 - \sigma_z^2}{\sigma_z^2}\right) + \\ \min\left\{\frac{1}{2}\log\left(\frac{2\beta'^2 k_2(1+\tilde{\rho}) + N'}{N'(1-\tilde{\rho}^2)}\right), \frac{1}{2}\log\left(\frac{(1-\tilde{\rho}^2)(2^{4R}\sigma_z^2 + 2\beta^2 2^{2R}k_2)}{\sigma_z^2}\right)\right\} \end{array}\right\} \tag{83}$$

IET Commun., 2015, Vol. 9, Iss. 6, pp. 754–770

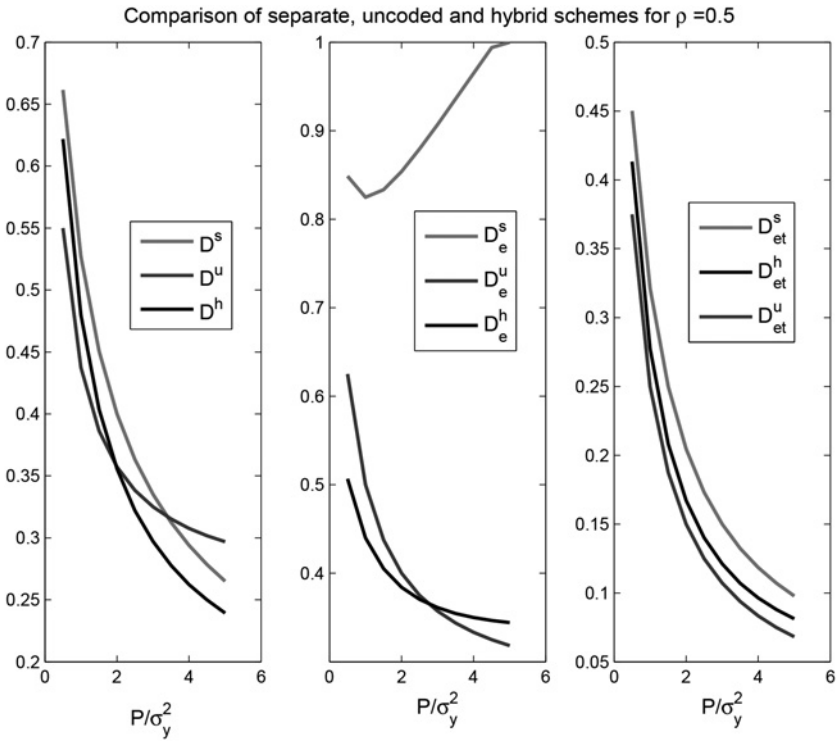

Fig. 8 *Comparison of separate, uncoded and hybrid schemes for $\rho = 0.5$, $\sigma^2 = 1$, $\alpha = 0.1(P/\sigma^2)$ and $\sigma_z^2/\sigma_y^2 = 1.5$*

$$\nu_1 = \sigma^2 2^{-2R}\frac{1-\rho\tilde{\rho}}{1-\tilde{\rho}^2}$$

$$\nu_3 = \sigma^2\rho\frac{2^{-4R}}{1-\tilde{\rho}^2}$$

$$\beta' = \alpha\left(1+\frac{\rho 2^{-2R}}{1+\tilde{\rho}}\right)+\beta$$

for some $\alpha \in [0, (P/\sigma^2)]$ and

$$\beta = \sqrt{\frac{P-\alpha^2\sigma^2 2^{-2R}}{\sigma^2(1-2^{-2R})}} - \alpha$$

Fig. 8 illustrates the separate, uncoded and hybrid schemes for $\rho = 0.5$. As shown in Fig. 8, the term D_e^s is larger than D_e^u and D_e^h with a significant difference. The term D_e^s does not depend on the source correlation coefficient ρ. Also, at high signal-to-noise ratio, this term increases to its maximum value.

6 Conclusion

In this paper, we considered lossy communication of correlated sources over the MAC-WT. We proposed an achievable scheme for the MAC-WT based on the separation. A joint source-channel coding strategy based on the hybrid scheme of [17] was also found. We studied lossy transmission of a bivariate Gaussian source over the GMAC-WT. We found inner bounds to the rate-distortion-equivocation region of the GMAC-WT using three approaches: separation, uncoded transmission and hybrid schemes. The separate, uncoded and hybrid schemes were compared with each other for the symmetric GMAC-WT and different values of the source correlation. We derived outer bounds to the rate-distortion-equivocation region of the degraded MAC-WT and the symmetric GMAC-WT. Optimal regions for some special cases were established.

7 Acknowledgments

This work was partially supported by Iranian NSF under contract no. 92.32575 and by Iran Telecom Research Center (ITRC) under contract no. T.500.12183 and by Cryptography chair. Some of the material in this paper was presented in part at the IEEE International Symposium on Information Theory, Istanbul, Turkey, July 2013.

8 References

1 Shannon, C.: 'Communication theory of secrecy systems', *Bell Syst. Tech. J.*, 1949, **28**, pp. 656–715
2 Wyner, A.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387
3 Csiszar, I., Korner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, (3), pp. 339–348
4 Tekin, E., Yener, A.: 'The general Gaussian multiple access and two-way wire-tap channels: achievables rates and cooperative jamming', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2735–2751
5 Ekrem, E., Ulukus, S.: 'On the secrecy of multiple access wiretap channel'. 46th Annual Allerton Conf. on Comm., Cont. and Computing, September 2008, pp. 1014–1021
6 Liu, N., Kang, W.: 'The secrecy capacity region of a special class of multiple access channels'. IEEE Int. Symp. on Infomation Theory (ISIT), St. Petersburg, Russia, July–August 2011, pp. 622–626
7 Liang, Y., Poor, H.V.: 'Generalized multiple access channels with confidential messages', *IEEE Trans. Inf. Theory*, 2008, **54**, (3), pp. 976–1002
8 Liu, R., Maric, I., Yates, R.D., Spasojevic, P.: 'The discrete memoryless multiple access channel with confidential messages'. IEEE Int. Symp. on Information Theory (ISIT), Seattle, WA, July 2006, pp. 957–961
9 Gunduz, D., Erkip, E., Goldsmith, A., Poor, H.V.: 'Source and channel coding for correlated sources over multiuser channels', *IEEE Trans. Inf. Theory*, 2009, **55**, (9), pp. 3927–3944
10 Gunduz, D., Erkip, E.: 'Reliable cooperative source transmission with side information'. IEEE Infomation. Theory Workshop on Wireless Networks, Bergen, Norway, July 2007, pp. 1–5
11 Mohajer, S., Tian, C., Diggavi, S.N.: 'On source transmission over deterministic relay networks'. Information Theory Workshop (ITW), Cairo, Egypt, January 2010, pp. 1–5
12 Salehkalaibar, S., Aref, M.R.: 'On source transmission over some classes of relay channels'. IEEE Int. Symp. on Information Theory (ISIT), MIT, July 2012, pp. 1942–1946
13 Cover, T., El Gamal, A., Salehi, M.: 'Multiple access channels with arbitrarily correlated sources', *IEEE Trans. Inf. Theory*, 1980, **26**, (6), pp. 648–657

14 Han, T.S., Costa, M.H.M.: 'Broadcast channels with arbitrarily correlated sources', *IEEE Trans. Inf. Theory*, 1987, **33**, (5), pp. 641–650
15 Tuncel, E.: 'Slepian-Wolf coding over broadcast channels', *IEEE Trans. Inf. Theory*, 2006, **52**, (4), pp. 1469–1482
16 Salehkalaibar, S., Aref, M.R.: 'On the transmission of correlated sources over relay channels'. IEEE Int. Symp. on Information Theory (ISIT), St. Petersburg, Russia, July–August 2011, pp. 1409–1413
17 Lim, S.H., Minero, P., Kim, Y.H.: 'Lossy communication of correlated sources over multiple access channels'. 48th Allerton Conf. on Comm., Cont. and Computing, September–October 2010, pp. 851–858
18 Villard, J., Piantanida, P., Shamai, S.: 'Secure transmission of sources over noisy channels with side information at the receivers', *IEEE Trans. Inf. Theory*, 2014, **60**, (1), pp. 713–739
19 Yamamoto, H.: 'Rate-distortion theory for the Shannon cipher system', *IEEE Trans. Inf. Theory*, 1997, **43**, (3), pp. 827–835
20 Liu, W., Chen, B.: 'Communicating correlated sources over interference channels: the lossy case'. IEEE Int. Symp. on Information Theory (ISIT), Austin, Texas, June 2010, pp. 345–349
21 Gastpar, M.: 'Uncoded transmission is exactly optimal for a simple Gaussian sensor network', *IEEE Trans. Inf. Theory*, 2008, **54**, (11), pp. 5247–5251
22 Lapidoth, A., Tinguely, S.: 'Sending bivariate Gaussian over a Gaussian MAC', *IEEE Trans. Inf. Theory*, 2010, **56**, (6), pp. 2714–2752
23 Oohama, Y.: 'Gaussian multiterminal source coding', *IEEE Trans. Inf. Theory*, 1997, **43**, (11), pp. 1912–1923
24 Wagner, A.B., Tavildar, S., Viswanath, P.: 'Rate region of the quadratic Gaussian two-encoder source-coding problem', *IEEE Trans. Inf. Theory*, 2008, **54**, (5), pp. 1938–1961
25 El Gamal, A., Kim, Y.H.: 'Network information theory' (Cambridge University Press, 2011)
26 Salehkalaibar, S., Aref, M.R.: 'Joint source-channel coding for multiple-access wiretap channels'. IEEE Int. Symp. on Information Theory (ISIT), Istanbul, Turkey, July 2013, pp. 369–373

9 Appendix

9.1 Appendix 1: Proof of Theorem 3

We use the fact that a stochastic encoder $p(x_j^n|s_j^n)$, $j=1{:}2$, can be treated as a deterministic mapping from S_j^m and an independent variable T_j onto X_j^n. First, consider the following term

$$\begin{aligned}
&I(S_1^m; Y^n|S_2^m, T_2)\\
&\quad = H(S_1^m|S_2^m, T_2) - H(S_1^m|Y^n, S_2^m, T_2)\\
&\quad \overset{(a)}{=} H(S_1^m|S_2^m) - H(S_1^m|Y^n, S_2^m, T_2)\\
&\quad \overset{(b)}{=} H(S_1^m|S_2^m) - H(S_1^m|Y^n, \hat{S}_1^m, S_2^m, T_2)\\
&\quad \geq H(S_1^m|S_2^m) - H(S_1^m|\hat{S}_1^m, S_2^m)\\
&\quad = I(S_1^m; \hat{S}_1^m|S_2^m)\\
&\quad = \sum_{i=1}^m H(S_{1,i}|S_1^{i-1}, S_2^m) - \sum_{i=1}^m H(S_{1,i}|S_1^{i-1}, S_2^m, \hat{S}_1^m)\\
&\quad \overset{(c)}{=} \sum_{i=1}^m H(S_{1,i}|S_{2,i}) - \sum_{i=1}^m H(S_{1,i}|S_1^{i-1}, S_2^m, \hat{S}_1^m)\\
&\quad \geq \sum_{i=1}^m H(S_{1,i}|S_{2,i}) - \sum_{i=1}^m H(S_{1,i}|S_{2,i}, \hat{S}_{1,i})\\
&\quad = \sum_{i=1}^m I(S_{1,i}; \hat{S}_{1,i}|S_{2,i})
\end{aligned}$$

where (a) follows because T_2 is independent of (S_1^m, S_2^m), (b) follows because $\hat{S}_1^m$ is a deterministic function of Y^n, (c) follows from the independence of random variables $S_{1,i}$ and $S_{2,i}$ over time. Also, we have

$$\begin{aligned}
&I(S_1^m; Y^n|S_2^m, T_2)\\
&\quad = \sum_{i=1}^n I(S_1^m; Y_i|S_2^m, T_2, Y^{i-1})\\
&\quad \overset{(a)}{=} \sum_{i=1}^n I(S_1^m; Y_i|S_2^m, T_2, X_2^n, Y^{i-1})\\
&\quad = \sum_{i=1}^n H(Y_i|S_2^m, T_2, X_2^n, Y^{i-1})\\
&\qquad - \sum_{i=1}^n H(Y_i|S_1^m, S_2^m, T_2, X_2^n, Y^{i-1})\\
&\quad \leq \sum_{i=1}^n H(Y_i|X_{2,i}) - \sum_{i=1}^n H(Y_i|S_1^m, S_2^m, T_2, X_2^n, Y^{i-1})\\
&\quad \leq \sum_{i=1}^n H(Y_i|X_{2,i}) - \sum_{i=1}^n H(Y_i|S_1^m, X_1^n, S_2^m, T_2, X_2^n, Y^{i-1})\\
&\quad \overset{(b)}{=} \sum_{i=1}^n H(Y_i|X_{2,i}) - \sum_{i=1}^n H(Y_i|X_{1,i}, X_{2,i})\\
&\quad = \sum_{i=1}^n I(X_{1,i}; Y_i|X_{2,i})
\end{aligned}$$

where (a) follows because X_2^n is a deterministic function of (S_2^m, T_2), (b) follows because given $(X_{1,i}, X_{2,i})$, Y_i is independent of other variables. Similarly, we have

$$I(S_2^m; Y^n|S_1^m, T_1) \geq \sum_{i=1}^m I(S_{2,i}; \hat{S}_{2,i}|S_{1,i}) \tag{85}$$

$$I(S_1^m, S_2^m; Y^n) \geq \sum_{i=1}^m I(S_{1,i}, S_{2,i}; \hat{S}_{1,i}, \hat{S}_{2,i}) \tag{86}$$

and

$$I(S_2^m; Y^n|S_1^m, T_1) \leq \sum_{i=1}^m I(X_{2,i}; Y_i|X_{1,i}) \tag{87}$$

$$I(S_1^m, S_2^m; Y^n) \leq \sum_{i=1}^m I(X_{1,i}, X_{2,i}; Y_{1,i}) \tag{88}$$

Now, consider the following

$$\begin{aligned}
H(S_1^m, S_2^m|Z^n) &= H(S_1^m, S_2^m) - I(S_1^m, S_2^m; Z^n)\\
&= \underbrace{H(S_1^m, S_2^m)}_{\Delta_1} - \underbrace{I(S_1^m, S_2^m; Y^n)}_{\Delta_2}\\
&\quad + \underbrace{I(S_1^m, S_2^m; Y^n) - I(S_1^m, S_2^m; Z^n)}_{\Delta_3}
\end{aligned} \tag{89}$$

Each term is studied separately. First, consider the term Δ_1

$$\begin{aligned}
\Delta_1 &= H(S_1^m, S_2^m)\\
&= \sum_{i=1}^m H(S_{1,i}, S_{2,i}|S_1^{i-1}, S_2^{i-1})\\
&= \sum_{i=1}^m H(S_{1,i}, S_{2,i})a
\end{aligned}$$

From (86), we have the following bound on Δ_2

$$\Delta_2 = I(S_1^m, S_2^m; Y^n) \geq \sum_{i=1}^m I(S_{1,i}, S_{2,i}; \hat{S}_{1,i}, \hat{S}_{2,i})$$

Finally, consider the term Δ_3

$$\begin{aligned}\Delta_3 &= I(S_1^m, S_2^m; Y^n) - I(S_1^m, S_2^m; Z^n)\\ &\overset{(a)}{=} I(S_1^m, S_2^m; Y^n|Z^n)\\ &\overset{(b)}{\leq} I(X_1^n, X_2^n; Y^n|Z^n)\\ &= \sum_{i=1}^{n} I(X_1^n, X_2^n; Y_i|Z^n, Y^{i-1})\\ &= \sum_{i=1}^{n} [H(Y_i|Z^n, Y^{i-1}) - H(Y_i|Z^n, Y^{i-1}, X_1^n, X_2^n)]\\ &\leq \sum_{i=1}^{n} [H(Y_i|Z_i) - H(Y_i|Z^n, Y^{i-1}, X_1^n, X_2^n)]\\ &\overset{(c)}{=} \sum_{i=1}^{n} [H(Y_i|Z_i) - H(Y_i|Z_i, X_{1,i}, X_{2,i})]\\ &= \sum_{i=1}^{n} I(X_{1,i}, X_{2,i}; Y_i|Z_i)\end{aligned}$$

where (a) follows because $(S_1^m, S_2^m) \to (X_1^n, X_2^n) \to Y^n \to Z^n$ forms a Markov chain from degradedness condition, (b) follows because $(S_1^m, S_2^m) \to (X_1^n, X_2^n, Z^n) \to Y^n$ forms a Markov chain, (c) follows because given $(X_{1,i}, X_{2,i})$, Y_i is independent of other variables. By introducing a time-sharing random variable, we obtain the terms in the theorem.

9.2 Appendix 2: Proof of Theorem 4

Consider the terms in Theorem 3 with $\kappa = 1$ and independent sources, that is, $\rho = 0$ for the GMAC-WT. We have the following sequence of inequalities

$$\begin{aligned}2^{2H(S_1|\hat{S}_1,S_2)}/(2\pi e) \leq 2^{2H(S_1|\hat{S}_1)}/(2\pi e) &\leq \mathrm{Var}[S_1|\hat{S}_1]\\ &\leq \mathbb{E}[d_1(S_1, \hat{S}_1)]\end{aligned} \tag{90}$$

Therefore we have

$$2^{2I(S_1;\hat{S}_1|S_2)} = \frac{2^{2H(S_1|S_2)}}{2^{2H(S_1|\hat{S}_1,S_2)}} \overset{(a)}{=} \frac{2^{2H(S_1)}}{2^{2H(S_1|\hat{S}_1,S_2)}} = \frac{\sigma^2}{2^{2H(S_1|\hat{S}_1,S_2)}} \overset{(b)}{\geq} \frac{\sigma^2}{D_1}$$

where (a) follows from the independence of S_1 and S_2, (b) follows from the inequality in (90). Similarly, we obtain

$$2^{2I(S_2;\hat{S}_2|S_1)} \geq \frac{\sigma^2}{D_2}, \quad 2^{2I(S_1,S_2;\hat{S}_1,\hat{S}_2)} \geq \frac{\sigma^2}{D_1.D_2}$$

Note that the independence of sources S_1 and S_2 implies independence of codewords X_1 and X_2, because X_1 (resp. X_2) is a stochastic function S_1 (resp. S_2). Thus, we have

$$\begin{aligned}I(X_1; Y|X_2) &\leq \frac{1}{2}\log\left(1 + \frac{P_1}{\sigma_y^2}\right)\\ I(X_2; Y|X_1) &\leq \frac{1}{2}\log\left(1 + \frac{P_2}{\sigma_y^2}\right)\\ I(X_1, X_2; Y) &\leq \frac{1}{2}\log\left(1 + \frac{P_1 + P_2}{\sigma_y^2}\right)\end{aligned}$$

From the Markov chain $(X_1, X_2) \to Y \to Z$, there exists a random variable $N \sim \mathcal{N}(0, \sigma_z^2 - \sigma_y^2)$ such that $Z = Y + N$. Thus, we have

$$\begin{aligned}I(X_1,X_2;Y|Z) &= H(Y) - H(Y|X_1,X_2) - H(Z) + H(Z|X_1,X_2)\\ &\overset{(a)}{\leq} H(Y) - H(Y|X_1,X_2) - \frac{1}{2}\log(2^{2H(Y)} + 2^{2H(N)}) + H(N_z)\\ &\overset{(b)}{\leq} \frac{1}{2}\log\left(\frac{1}{1 + \left(\left(\sigma_z^2 - \sigma_y^2\right)/\left(P_1 + P_2 + \sigma_y^2\right)\right)}\frac{\sigma_z^2}{\sigma_y^2}\right)\\ &= \frac{1}{2}\log\left(\frac{1 + \left(\left(P_1 + P_2\right)/\sigma_y^2\right)}{1 + \left(\left(P_1 + P_2\right)/\sigma_z^2\right)}\right)\end{aligned}$$

where (a) follows from the Entropy Power Inequality (EPI) [25, Lecture Note 2], that is, $2^{2H(Z)} \geq 2^{2H(Y)} + 2^{2H(N)}$, (b) follows because $\mathrm{Var}[Y] \leq P_1 + P_2 + \sigma_y^2$. Now, consider the following equivocation rate

$$\begin{aligned}H(S_1^n|Z^n) &= H(S_1^n) - I(S_1^n; Z^n)\\ &= H(S_1^n) - \underbrace{I(S_1^n; Y^n)}_{\Delta_1} + \underbrace{I(S_1^n; Y^n) - I(S_1^n; Z^n)}_{\Delta_2}\end{aligned} \tag{91}$$

Consider the term Δ_1

$$\begin{aligned}\Delta_1 &= I(S_1^n; Y^n)\\ &\overset{(a)}{=} I(S_1^n; Y^n, \hat{S}_1^n)\\ &\geq I(S_1^n; \hat{S}_1^n)\\ &= \sum_{i=1}^{n} I(S_{1,i}; \hat{S}_1^n|S_1^{i-1})\\ &= \sum_{i=1}^{n} [H(S_{1,i}|S_1^{i-1}) - H(S_{1,i}|\hat{S}_1^n, S_1^{i-1})]\\ &\overset{(b)}{=} \sum_{i=1}^{n} [H(S_{1,i}) - H(S_{1,i}|\hat{S}_1^n, S_1^{i-1})]\\ &\geq \sum_{i=1}^{n} [H(S_{1,i}) - H(S_{1,i}|\hat{S}_{1,i})]\\ &= \sum_{i=1}^{n} I(S_{1,i}; \hat{S}_{1,i})\end{aligned}$$

where (a) follows because $\hat{S}_1^n$ is a function of Y^n and (b) follows from the independence of source sequences over time. Consider the following set of inequalities

$$2^{2H(S_1|\hat{S}_1)}/(2\pi e) \leq \mathrm{Var}[S_1|\hat{S}_1] \leq \mathbb{E}[d_1(S_1, \hat{S}_1)]$$

Thus, we obtain

$$2^{2I(S_1;\hat{S}_1)} = \frac{2^{2H(S_1)}}{2^{2H(S_1|\hat{S}_1)}} \geq \frac{\sigma^2}{D_1}$$

Next, consider the term Δ_2

$$\begin{aligned}\Delta_2 &= I(S_1^n; Y^n) - I(S_1^n; Z^n)\\ &\overset{(a)}{=} I(S_1^n; Y^n|Z^n)\\ &\overset{(b)}{\leq} I(X_1^n; Y^n|Z^n)\\ &\overset{(c)}{=} I(X_1^n; Y^n) - I(X_1^n; Z^n)\\ &= H(Y^n) - H(Y^n|X_1^n) - H(Z^n) + H(Z^n|X_1^n)\end{aligned}$$

$$\begin{aligned}
&\overset{(d)}{=} H(Y^n) - H(X_2^n + N_y^n) - H(Z^n) + H(X_2^n + N_z^n)\\
&\overset{(e)}{\leq} H(Y^n) - H(X_2^n + N_y^n)\\
&\quad - \frac{n}{2}\log\left(2^{2H(Y)} + 2^{2H(N)}\right) + H(X_2^n + N_z^n)\\
&\overset{(f)}{=} H(Y^n) - \frac{n}{2}\log\left(\beta_1 P_2 + \sigma_y^2\right)\\
&\quad - \frac{n}{2}\log\left(2^{2H(Y)} + 2^{2H(N)}\right) + H(X_2^n + N_z^n)\\
&\overset{(g)}{\leq} \frac{n}{2}\log\left(\frac{1}{1 + \left(\left(\sigma_z^2 - \sigma_y^2\right)/\left(P_1 + P_2 + \sigma_y^2\right)\right)}\frac{P_2 + \sigma_z^2}{\beta_1 P_2 + \sigma_y^2}\right)\\
&= \frac{n}{2}\log\left(\frac{1 + \left(\left(P_1 + (1-\beta_1)P_2\right)/\left(\beta_1 P_2 + \sigma_y^2\right)\right)}{1 + \left(P_1/\left(P_2 + \sigma_z^2\right)\right)}\right)
\end{aligned}$$

where (a) and (c) follow from the degradedness condition, that is, $S_1^n \to X_1^n \to Y^n \to Z^n$ forms a Markov chain, (b) follows because $S_1^n \to X_1^n \to Y^n$ forms a Markov chain when X_1 and X_2 are independent, (d) follows from the independence of codewords X_1 and X_2, (e) follows from the EPI [25, Lecture Note 2] and (f) follows from the following inequality

$$\frac{n}{2}\log\left(\sigma_y^2\right) \leq H(X_2^n + N_y^n) \leq \frac{n}{2}\log\left(P_2 + \sigma_y^2\right)$$

Thus, there exists $\beta_1 \in [0,\ 1]$ such that $H(X_2^n + N_y^n) = (n/2)\log\left(\beta_1 P_2 + \sigma_y^2\right)$, (g) follows because $\mathrm{Var}[Y^n] \leq n(P_1 + P_2 + \sigma_y^2)$. In summary, we obtain the following bound on $H(S_1^n|Z^n)$

$$H(S_1^n|Z^n) \leq \frac{n}{2}\log\left(D_1 \cdot \frac{1 + \left(\left(P_1 + (1-\beta_1)P_2\right)/\left(\beta_1 P_2 + \sigma_y^2\right)\right)}{1 + \left(P_1/\left(P_2 + \sigma_z^2\right)\right)}\right)$$

for some $\beta_1 \in [0, 1]$. Similarly, we have

$$H(S_2^n|Z^n) \leq \frac{n}{2}\log\left(D_2 \cdot \frac{1 + \left(\left(P_2 + (1-\beta_2)P_1\right)/\left(\beta_2 P_1 + \sigma_y^2\right)\right)}{1 + \left(P_2/\left(P_1 + \sigma_z^2\right)\right)}\right)$$

for some $\beta_2 \in [0, 1]$. In summary, we obtain the terms in the theorem.

IET Commun., 2015, Vol. 9, Iss. 6, pp. 754–770