IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Multiple access channel with common message and secrecy constraint

ISSN 1751-8628
Received on 17th November 2014
Revised on 3rd September 2015
Accepted on 30th September 2015
doi: 10.1049/iet-com.2015.0468
www.ietdl.org

Hassan Zivari-Fard[1,2], Bahareh Akhbari[2] ✉, Mahmoud Ahmadian-Attari[2], Mohammad Reza Aref[1]

[1]*Information Systems and Security Lab (ISSL), Sharif University of Technology, Tehran, Iran*
[2]*Faculty of Electrical Engineering, K. N. Toosi University of Technology, Tehran, Iran*
✉ *E-mail: akhbari@eetd.kntu.ac.ir*

Abstract: The authors study the problem of secret communication over a multiple-access channel with a common message. Here, the authors assume that two transmitters have confidential messages, which must be kept secret from the wiretapper (the second receiver), and both of them have access to a common message which can be decoded by the two receivers. The authors call this setting as multiple-access wiretap channel with common message (MAWC-CM). For this setting, the authors derive general inner and outer bounds on the secrecy capacity region for the discrete memoryless case and show that these bounds meet each other for a special case called the switch channel. As well, for a Gaussian version of MAWC-CM, the authors derive inner and outer bounds on the secrecy capacity region. Providing numerical results for the Gaussian case, the authors illustrate the comparison between the derived achievable rate region and the outer bound for the considered model and the capacity region of compound multiple access channel.

1 Introduction

In a seminal work, the wire-tap channel was introduced by Wyner [1], where a sender wishes to communicate a message to a receiver while keeping the message secret from an eavesdropper. He established the secrecy capacity for a single-user degraded wire-tap channel. Later, Csiszár and Körner extended the wire-tap channel to a more generalised model called the broadcast channel with confidential messages [2] and computed its secrecy capacity.

The problem of secret communication over multi-user channels has recently attracted remarkable attention [3–13]. In [3, 4], multiple access channel (MAC) with generalised feedback has been considered, where in [3] the encoders do not need to keep their messages secret from each other, but their messages should be kept secret from an external eavesdropper. Whereas in [4] each user views the other user as an eavesdropper and wishes to keep its confidential information as secret as possible from the other user.

The multiple access wire-tap channel (MAWC) (i.e. MAC with an external eavesdropper) under strong secrecy criterion has been studied in [5]. In [6], MAWC has been studied assuming that there exists a common message while the eavesdropper is *unable* to decode it. For this model an achievable rate region for discrete memoryless case under the strong secrecy criterion has been derived. A degraded Gaussian MAWC, in which the eavesdropper receives a degraded version of the legitimate receiver's signal, has been studied in [7] and an achievable rate region for this setting has been established. In [9] general Gaussian MAWC has been considered such that an achievable rate region has been derived. The problem of lossy source transmission over a MAWC was considered in [14].

The influence of partial encoder cooperation on the secrecy capacity of the MAWC has been studied in [10]. In their considered setting, two encoders that are connected by two communication links with finite capacities wish to send secret messages to the common intended decoder in the presence of an eavesdropper. In their model the transmitters do not have any common messages. The compound MAC (CMAC) (two-transmitter/two-receiver MAC) with conferencing links between both encoders and decoders without any secrecy constraint has been studied in [15]. In [16], we have considered compound MAC with confidential messages so that the first transmitter's private message is confidential and are only decoded by the first receiver, and kept secret from the second receiver, while the common message and the private message of the second transmitter are decoded by both receivers.

In this paper, we investigate secrecy constraints in a MAC with a common message. We call our model as MAWC with common message (MAWC-CM). To interpret this model, it can be noted that in wireless networks there may be a scenario in which the users may have a *common message* which can be decoded by *all users* in addition to the confidential information that wish to be kept secret from illegal users. Motivated by this scenario, we consider MAWC-CM as a building block of this setting. In this model, each transmitter sends its own private message while both of them have a common message. Both of the transmitter's private messages (W_1 and W_2) are confidential and are only decoded by the first receiver and kept secret from the second receiver. The common message W_0 is decoded by both receivers (see Fig. 1). For this model, we derive single-letter inner and outer bounds on the secrecy capacity region. We also study a switch channel which is a special case of our model and show that the derived inner and outer bounds meet each other for this case. We also consider Gaussian MAWC-CM and derive inner and outer bounds on its secrecy capacity region. Providing some numerical examples for Gaussian MAWC-CM, we compare the derived achievable rate region and outer bound for the Gaussian case with each other and also with the capacity region of the Gaussian compound MAC. The considered examples illustrate the impact of noise power and secrecy constraints on the rate regions. We show that there are scenarios for which the secret transmissions may increase achievable rate region when compared with the case that requires the second receiver to decode the private messages.

The rest of this paper is organised as follows. In Section 2, the notations and the system model are described. In Section 3, outer and inner bounds on the secrecy capacity region of discrete memoryless MAWC-CM are established and it is shown that these bounds meet each other for the switch channel model. An achievable secrecy rate region and an outer bound on the secrecy capacity region of Gaussian MAWC-CM are derived in Section 4. Finally, Section 5 concludes the paper.

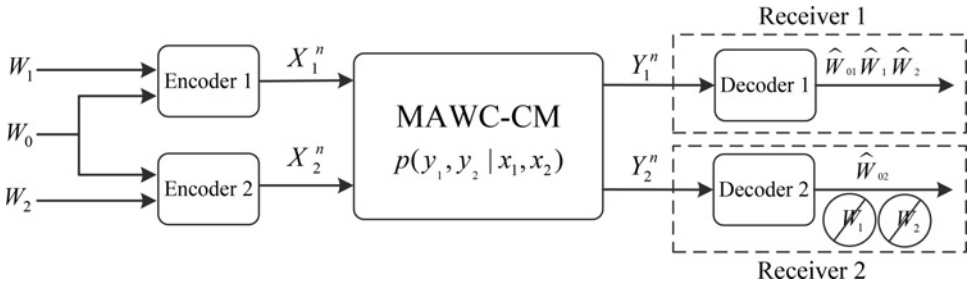

Fig. 1 *Multiple access wire-tap channel with common message*

2 Notations and system model

In this paper, the random variables (RVs) are represented by capital letters, for example, X, the realisations of RVs are represented by lower case letters, for example, x and their alphabets are represented by $\mathcal{X}$. The $\mathcal{T}_\varepsilon^n(P_{XY})$ indicates the set of $\varepsilon-$strongly jointly typical sequences [11] of length n, on joint distribution $P_{X,Y}$. X_i^n indicates vector $(X_{i,1}, X_{i,2}, \ldots, X_{i,n})$, and $X_{i,j}^k$ indicates vector $(X_{i,j}, X_{i,j+1}, \ldots, X_{i,k})$. The cardinality of U is denoted by $|\mathcal{U}|$.

Definition 1: Consider a discrete memoryless MAWC-CM $(\mathcal{X}_1, \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1, \mathcal{Y}_2)$ where $\mathcal{X}_1$ and $\mathcal{X}_2$ are the finite input alphabets of transmitters, $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are the channel output alphabets of receiver 1 and receiver 2, respectively (Fig. 1) and $p(y_1, y_2|x_1, x_2)$ is the channel transition probability distribution.

Definition 2: A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for the MAWC-CM (Fig. 1) consists of the followings: (i) Three message sets $\mathcal{W}_u = \{1, \ldots, 2^{nR_u}\}$ for $u = 0, 1, 2$ where independent messages W_0, W_1 and W_2 are uniformly distributed over respective sets. (ii) Two stochastic encoders g_k, $k = 1, 2$, for transmitter k that are specified by $g_k : \mathcal{W}_0 \times \mathcal{W}_k \to \mathcal{X}_k^n$ for $k = 1, 2$. (iii) Two decoding functions $\phi : \mathcal{Y}_1^n \to \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2$ and $\rho : \mathcal{Y}_2^n \to \mathcal{W}_0$. The first decoder is at the legitimate receiver and assigns $(\widehat{W}_{01}, \widehat{W}_1, \widehat{W}_2) \in \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2$ to each received sequence y_1^n. The second decoder assigns an estimate $\widehat{W}_{02} \in \mathcal{W}_0$ to each received sequence y_2^n. The average probability of error is defined as,

$$P_{e,1}^n = \Pr\{(\widehat{W}_{01}, \widehat{W}_1, \widehat{W}_2) \neq (W_0, W_1, W_2)\} \tag{1}$$

$$P_{e,2}^n = \Pr\{(\widehat{W}_{02}) \neq (W_0)\} \tag{2}$$

$$P_e^n = \max\{P_{e,1}^n, P_{e,2}^n\} \tag{3}$$

The ignorance level of the eavesdropper (Receiver 2), with respect to the confidential messages W_1 and W_2, is measured by equivocation rate $(1/n)H(W_1, W_2|Y_2^n)$.

Definition 3: A rate tuple (R_0, R_1, R_2) is said to be achievable for MAWC-CM, if for any $\varepsilon > 0$ there exists a $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code which satisfies

$$P_e^n < \varepsilon \tag{4}$$

$$R_1 + R_2 - \frac{1}{n}H(W_1, W_2|Y_2^n) \leq \varepsilon \tag{5}$$

for sufficiently large n. Note that secrecy requirement (5) implies

$$R_k - \frac{1}{n}H(W_k|Y_2^n) \leq \varepsilon \quad \text{for} \quad k = 1, 2 \tag{6}$$

that also has been shown in [3]. The secrecy capacity region of the MAWC-CM is defined as the closure of the set of all achievable rate tuples (R_0, R_1, R_2).

3 Discrete memoryless MAWC-CM

In this section, we derive an outer bound on the secrecy capacity region of discrete memoryless MAWC-CM in Theorem 1 and an inner bound in Theorem 2. We show that these bounds meet each other in a special case.

3.1 Outer bound

Theorem 1: (Outer bound) The secrecy capacity region of MAWC-CM is included in the set of rates satisfying

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} \tag{7}$$

$$R_1 \leq I(V_1; Y_1|U) - I(V_1; Y_2|U) \tag{8}$$

$$R_2 \leq I(V_2; Y_1|U) - I(V_2; Y_2|U) \tag{9}$$

$$R_1 + R_2 \leq I(V_1, V_2; Y_1|U) - I(V_1, V_2; Y_2|U) \tag{10}$$

for some joint distribution

$$p(u)p(v_1, v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2) \tag{11}$$

where the auxiliary RVs U, V_1 and V_2 are bounded in cardinality by

$$|\mathcal{U}| \leq |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 7 \tag{12}$$

$$|\mathcal{V}_1| \leq (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 3) \cdot (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 7) \tag{13}$$

$$|\mathcal{V}_2| \leq (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 3) \cdot (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 7). \tag{14}$$

Proof: See Appendix 1. □

Remark 1: If transmitter 1 (or transmitter 2) does not send any messages, by setting $V_1 = \emptyset$ (or $V_2 = \emptyset$) in Theorem 1 the region reduces to the capacity region of the broadcast channel with confidential messages discussed in [2].

3.2 Achievability

Theorem 2: (Achievability) For a discrete memoryless MAWC-CM, the secrecy rate region $\mathcal{R}(\pi_I)$ is achievable, where $\mathcal{R}(\pi_I)$ is the closure of the convex hull of all non-negative (R_0, R_1, R_2) satisfying

$$R_0 \leq I(U; Y_2) \tag{15}$$

$$R_1 \leq I(V_1; Y_1|V_2, U) - I(V_1; Y_2|U) \tag{16}$$

$$R_2 \leq I(V_2; Y_1|V_1, U) - I(V_2; Y_2|U) \tag{17}$$

$$R_1 + R_2 \le I(V_1, V_2; Y_1|U) - I(V_1, V_2; Y_2|U) \quad (18)$$

$$R_0 + R_1 + R_2 \le I(V_1, V_2; Y_1) - I(V_1, V_2; Y_2|U) \quad (19)$$

and π_I denotes the class of joint probability mass functions $p(u, v_1, v_2, x_1, x_2, y_1, y_2)$ that factor as

$$p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2) \quad (20)$$

in which the auxiliary RVs U, V_1 and V_2 are bounded in cardinality by

$$|\mathcal{U}| \le |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 6 \quad (21)$$

$$|\mathcal{V}_1| \le (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 5) \cdot (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 6) \quad (22)$$

$$|\mathcal{V}_2| \le (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 5) \cdot (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 6). \quad (23)$$

Proof: In the following, we provide outlines of our achievable scheme and the details of the proof are referred to Appendix 2. In the coding scheme we use superposition technique and Wyner's wiretap coding [1], as the secrecy achievability method. We illustrate the common message w_0 with the auxiliary codeword u^n. All receivers are able to decode this codeword. Therefore, it does not need to be protected from the illegal user by Wyner's coding technique. The auxiliary codeword v_1^n, which illustrates the private message w_1, is superimposed on top of u^n and is decoded only by receiver 1. Moreover, the auxiliary codeword v_2^n, which illustrates the message w_2, is superimposed on top of u^n and is decoded only by receiver 1. These codewords are protected from the illegal user by Wyner's coding technique. The structure of the encoder is depicted in Fig. 7 in Appendix 2. Transmitted codewords x_1^n and x_2^n are drawn based on v_1^n and v_2^n respectively, according to (20). □

Remark 2: If we convert our model to a MAWC without common message, by setting $U = \emptyset$, $V_1 = X_1$ and $V_2 = X_2$ in Theorem 2, the region reduces to the achievable secrecy rate region of the MAWC without common message that is reported in [3] and its Gaussian version is first introduced in [7, 9].

Remark 3: If we convert the model to a broadcast channel with confidential messages, our region includes the region discussed by Csiszár and Körner in [2]. It can be verified by setting $V_1 = \emptyset$ or $V_2 = \emptyset$ in (15)–(19).

3.3 Switch channel

Now, we obtain the secrecy capacity region for a switch channel. In the switch channel (see Fig. 2) the receivers cannot listen to both transmitters at the same time. For example, each receiver can listen to only one frequency whereas each transmitter can broadcast at various frequencies during the symbol time i. We assume that at each symbol time i, each receiver t for $t \in \{1, 2\}$ has access to a random switch $s_t \in \{1, 2\}$, which independently is set to t or $\bar{t}$ with probabilities

$$P(S_{t,i} = t) = \tau_t \quad (24)$$

$$P(S_{t,i} = \bar{t}) = 1 - \tau_t, \quad i = 1, \ldots, n \quad (25)$$

where $\bar{t}$ is complement of t. Hence, if $S_{t,i} = t$, receiver t for $t \in \{1, 2\}$ listens to the signal sent by the transmitter t (i.e. $x_{t,i}$) and if $S_{t,i} = \bar{t}$, receiver t listens to the signal sent by the transmitter $\bar{t}$ (i.e. $x_{\bar{t},i}$). The switch channel is investigated in [12] as a special case of Interference channel. We generalise the interpretation of a switch channel to our model as follows: Consider a MAC with a common message and an eavesdropper that the legal receiver (receiver 1) can listen to only one of the transmitters at each time instant that is determined by the first switch state. The illegal receiver (in terms of private messages) can eavesdrop only one of the transmitters which is determined by the second switch state. We also assume that both receivers have access to switch state information. Thus, we have

$$\begin{aligned} P(y_{t,i}|x_{1,i}, x_{2,i}, s_{t,i}) &= P(y_{t,i}|x_{1,i})1(s_{t,i} = 1) \\ &\quad + P(y_{t,i}|x_{2,i})1(s_{t,i} = 2) = P(y_{t,i}|x_{s_{t,i},i}) \end{aligned} \quad (26)$$

where 1(.) is the indicator function. The switch state information $\{S_{t,i}\}_{i=1}^n$ is an i.i.d. process known at receiver t. Therefore, we can assume that $s_{t,i}$ is a part of the channel output. In other words, we set

$$y_{t,i} \triangleq \{k_{t,i}, s_{t,i}\} \quad (27)$$

where $k_{t,i}$ indicates the received signal at receiver t. For the described switch channel, we have the following theorem for the secrecy capacity region.

Theorem 3: For the switch channel with two confidential messages and one common message, the secrecy capacity region $\mathcal{C}_S$ is the union of all (R_0, R_1, R_2) satisfying

$$R_0 \le I(U; Y_2) \quad (28)$$

$$R_1 \le I(V_1; Y_1|U) - I(V_1; Y_2|U) \quad (29)$$

$$R_2 \le I(V_2; Y_1|U) - I(V_2; Y_2|U) \quad (30)$$

$$R_1 + R_2 \le I(V_1, V_2; Y_1|U) - I(V_1, V_2; Y_2|U) \quad (31)$$

$$R_0 + R_1 + R_2 \le I(V_1, V_2; Y_1) - I(V_1, V_2; Y_2|U) \quad (32)$$

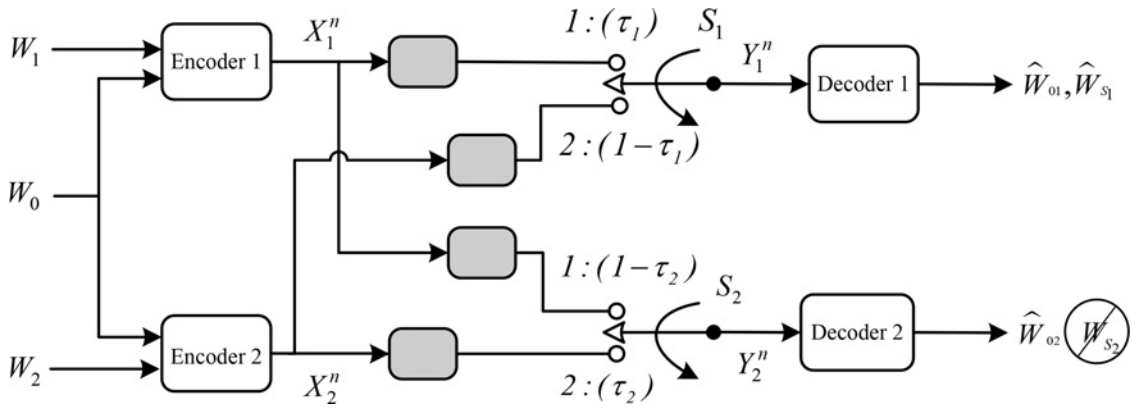

Fig. 2 *Switch channel model*

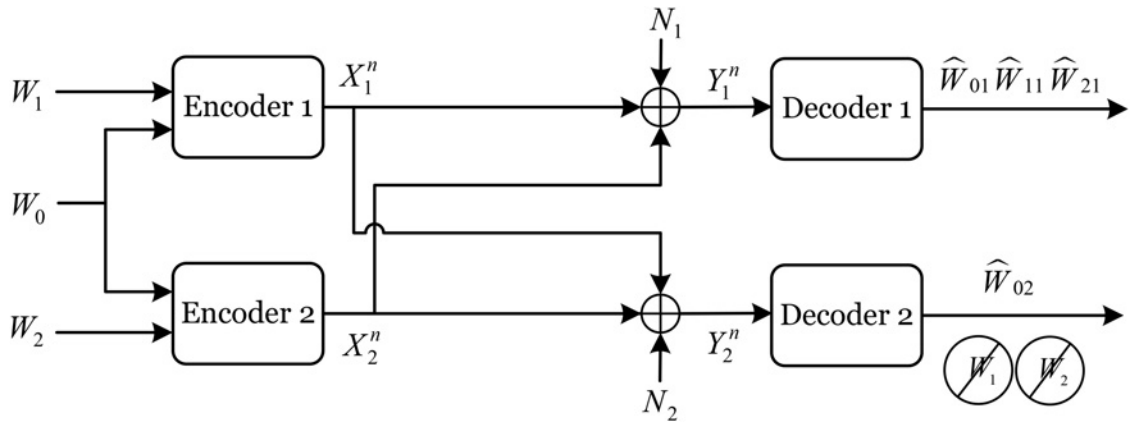

Fig. 3 *Gaussian MAWC-CM*

over all distributions

$$p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2) \tag{33}$$

where the auxiliary RVs U, V_1 and V_2 are bounded in cardinality by

$$|\mathcal{U}| \leq |\mathcal{X}_1| \cdot |\mathcal{X}_2| + 6 \tag{34}$$

$$|\mathcal{V}_1| \leq (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 4) \cdot (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 6) \tag{35}$$

$$|\mathcal{V}_2| \leq (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 4) \cdot (|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 6). \tag{36}$$

Proof: See Appendix 3.

4 Gaussian MAWC-CM

In this section, we consider Gaussian MAWC-CM as shown in Fig. 3, and derive inner and outer bounds on its secrecy capacity region. Relationships between the inputs and outputs of the channel, as shown in Fig. 3, are given by

$$Y_1 = X_1 + X_2 + N_1 \tag{37}$$

$$Y_2 = X_1 + X_2 + N_2 \tag{38}$$

where N_1 and N_2 are independent zero-mean Gaussian RVs, with variances σ_1^2 and σ_2^2, and independent of the RVs X_1, X_2. We impose the power constraints $(1/n)\sum_{i=1}^{n} E[X_{j,i}^2] \leq P_j$, $j = 1, 2$.

4.1 Outer bound

Theorem 4: (Outer bound) The secrecy capacity region for the Gaussian MAWC-CM is included in the set of rates satisfying (see (39))

where $C(x) = (1/2)\log(1 + x)$ and the union is taken over all $0 \leq \beta_1 \leq 1$, $0 \leq \beta_2 \leq 1$ and $0 \leq \rho \leq 1$.

Proof: See Appendix 4. □

4.2 Inner bound

Theorem 5: (Achievability) An inner bound on the secrecy capacity region of Gaussian MAWC-CM is: (see (40))

where $C(x) = (1/2)\log(1 + x)$ and the union is taken over all $0 \leq \beta_1 \leq 1$ and $0 \leq \beta_2 \leq 1$.

Proof: The achievable rate region in Theorem 2 can be extended to the discrete-time Gaussian memoryless case with continuous alphabets by standard arguments [17]. Hence, it is sufficient to

$$\bigcup \begin{cases} R_0 \leq \min\left\{ C\left(\dfrac{(1-\beta_1)P_1 + (1-\beta_2)P_2 + (1-\beta_1\beta_2)\rho\sqrt{P_1P_2}}{\beta_1P_1 + \beta_2P_2 + 2\beta_1\beta_2\rho\sqrt{P_1P_2} + \sigma_1^2}\right), C\left(\dfrac{(1-\beta_1)P_1 + (1-\beta_2)P_2 + (1-\beta_1\beta_2)\rho\sqrt{P_1P_2}}{\beta_1P_1 + \beta_2P_2 + 2\beta_1\beta_2\rho\sqrt{P_1P_2} + \sigma_2^2}\right)\right\} \\ R_1 + R_2 \leq \left[C\left(\dfrac{\beta_1P_1 + \beta_2P_2 + 2\beta_1\beta_2\rho\sqrt{P_1P_2}}{\sigma_1^2}\right) - C\left(\dfrac{\beta_1P_1 + \beta_2P_2 + 2\beta_1\beta_2\rho\sqrt{P_1P_2}}{\sigma_2^2}\right)\right] \end{cases} \tag{39}$$

$$\bigcup \begin{cases} R_0 \leq C\left(\dfrac{\beta_1^2P_1 + \beta_2^2P_2 + 2\beta_1\beta_2\sqrt{P_1P_2}}{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2 + \sigma_2^2}\right) \\ R_1 \leq C\left(\dfrac{(1-\beta_1^2)P_1}{\sigma_1^2}\right) - C\left(\dfrac{(1-\beta_1^2)P_1}{(1-\beta_2^2)P_2 + \sigma_2^2}\right) \\ R_2 \leq C\left(\dfrac{(1-\beta_2^2)P_2}{\sigma_1^2}\right) - C\left(\dfrac{(1-\beta_2^2)P_2}{(1-\beta_1^2)P_1 + \sigma_2^2}\right) \\ R_1 + R_2 \leq C\left(\dfrac{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2}{\sigma_1^2}\right) - C\left(\dfrac{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2}{\sigma_2^2}\right) \\ R_0 + R_1 + R_2 \leq C\left(\dfrac{P_1 + P_2 + 2\beta_1\beta_2\sqrt{P_1P_2}}{\sigma_1^2}\right) - C\left(\dfrac{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2}{\sigma_2^2}\right) \end{cases} \tag{40}$$

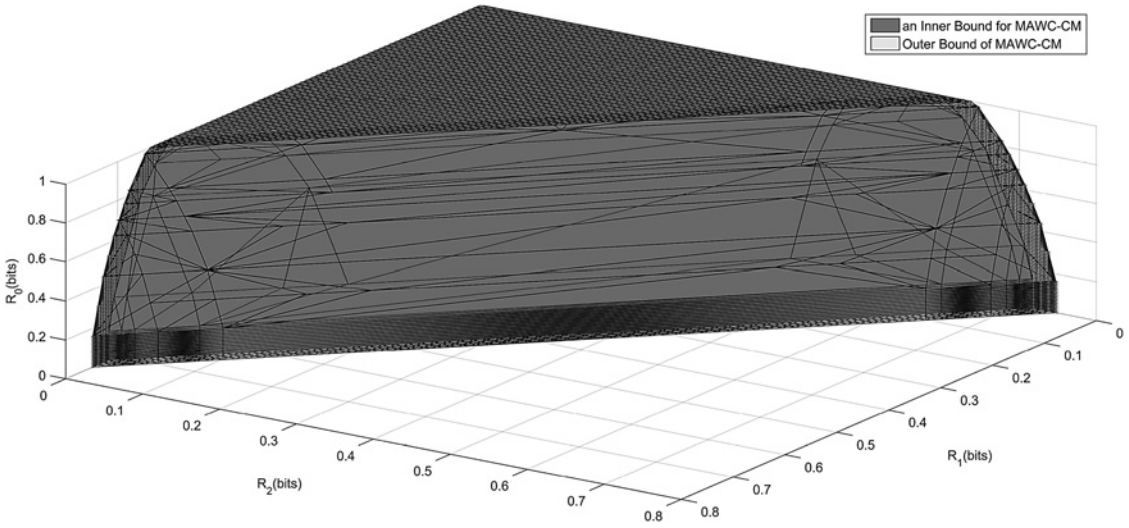

Fig. 4 *Achievable rate region and Outer bound of Gaussian MAWC-CM for $P_1 = P_2 = 1$, $\sigma_1^2 = 0.1$ and $\sigma_2^2 = 0.3$*

evaluate (15)–(19) with appropriate choice of input distribution to reach (40). We constrain all the inputs to be Gaussian. For certain $0 \le \beta_1 \le 1$ and $0 \le \beta_2 \le 1$ consider the following mapping in (41)–(44) for the generated codebook in Theorem 2 with respect to the p.m.f (20), which contains the Gaussian version of the superposition coding and random binning

$$V_1 = \sqrt{P_1}\beta_1 U + \sqrt{P_1(1-\beta_1^2)}K_1 \tag{41}$$

$$X_1 = V_1 \tag{42}$$

$$V_2 = \sqrt{P_2}\beta_2 U + \sqrt{P_2(1-\beta_2^2)}K_2 \tag{43}$$

$$X_2 = V_2. \tag{44}$$

where U, K_1 and K_2 are independent, zero-mean and unit variance Gaussian RVs. Using the above mapping with the channel model in (37)–(38), and by calculating mutual information functions for Gaussian RVs similar to the method in [17], we have

$$I(U; Y_2) = C\left(\frac{\beta_1^2 P_1 + \beta_2^2 P_2 + 2\beta_1\beta_2\sqrt{P_1P_2}}{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2 + \sigma_2^2}\right) \tag{45}$$

$$I(V_1; Y_1|V_2, U) = C\left(\frac{(1-\beta_1^2)P_1}{\sigma_1^2}\right) \tag{46}$$

$$I(V_1; Y_2|U) = C\left(\frac{(1-\beta_1^2)P_1}{(1-\beta_2^2)P_2 + \sigma_2^2}\right) \tag{47}$$

$$I(V_2; Y_1|V_1, U) = C\left(\frac{(1-\beta_2^2)P_2}{\sigma_1^2}\right) \tag{48}$$

$$I(V_2; Y_2|U) = C\left(\frac{(1-\beta_2^2)P_2}{(1-\beta_1^2)P_1 + \sigma_2^2}\right) \tag{49}$$

$$I(V_1, V_2; Y_1|U) = C\left(\frac{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2}{\sigma_1^2}\right) \tag{50}$$

$$I(V_1, V_2; Y_2|U) = C\left(\frac{(1-\beta_1^2)P_1 + (1-\beta_2^2)P_2}{\sigma_2^2}\right) \tag{51}$$

$$I(V_1, V_2; Y_1) = C\left(\frac{P_1 + P_2 + 2\beta_1\beta_2\sqrt{P_1P_2}}{\sigma_1^2}\right) \tag{52}$$

where $C(x) = (1/2)\log(1+x)$. Considering Theorem 2 and (45)–(52) completes the proof. □

As mentioned in Section 1 we aim to compare our derived bounds with each other and also with the capacity region of the Gaussian compound MAC. Hence, we first derive this region as follows.

Theorem 6: The capacity region of Gaussian compound MAC with common information is given by: (see equation (53) at the bottom of the next page)

where $C(x) = (1/2)\log(1+x)$ and the union is taken over all $0 \le \beta_1 \le 1$ and $0 \le \beta_2 \le 1$.

Proof: It is clear that to obtain this capacity region, Propositions 6.1 and 6.2 in [15], which are outer and inner bounds on the capacity region of the Gaussian compound MAC with conferencing links, can be modified by setting $C_{12} = C_{21} = 0$ in them (i.e. ignoring conferencing links) and by adopting them to our defined channel parameters in (37) and (38). □

4.3 Examples

In this part, we provide numerical examples and compare our derived inner and outer bounds on the secrecy capacity region of Gaussian MAWC-CM. We also compare these bounds with the capacity region of the Gaussian compound MAC illustrated in (53). As an example, for the values $P_1 = P_2 = 1$, $\sigma_1^2 = 0.1$ and $\sigma_2^2 = 0.3$ the outer bound in Theorem 4 and the achievable rate region in Theorem 5 are depicted in Fig. 4. To illustrate the effect of secrecy constraint and noise power on the rate region of MAWC-CM, we also compare our derived regions with the capacity region of the Gaussian compound MAC in (53). These comparisons are shown in Figs. 5 and 6. Actually, in the CMAC both receivers should decode W_0, W_1, W_2 reliably, while in the defined MAWC-CM model the messages W_1 and W_2 should be kept secret from receiver 2. As it can be seen in Fig. 5 for channel parameters $P_1 = P_2 = 1$, $\sigma_1^2 = 0.1$ and $\sigma_2^2 = 0.3$ (i.e. the same as for Fig. 4) the achievable rates and outer bounds on R_1 and R_2 (rate of W_1 and W_2 respectively, which are decoded by receiver 1) for MAWC-CM is less than that for CMAC due to secrecy constraint for decoding messages W_1 and W_2. Note that in Figs. 5 and 6 we present the regions in two-dimensional by projecting on R_0 plane to have a better illustration. Based on (53) it is clear that if the noise power of receiver 2 (i.e. σ_2^2) increases, the capacity region of Gaussian CMAC may remain as before or decreases (i.e. it does not increase). On the other hand, there exist scenarios for

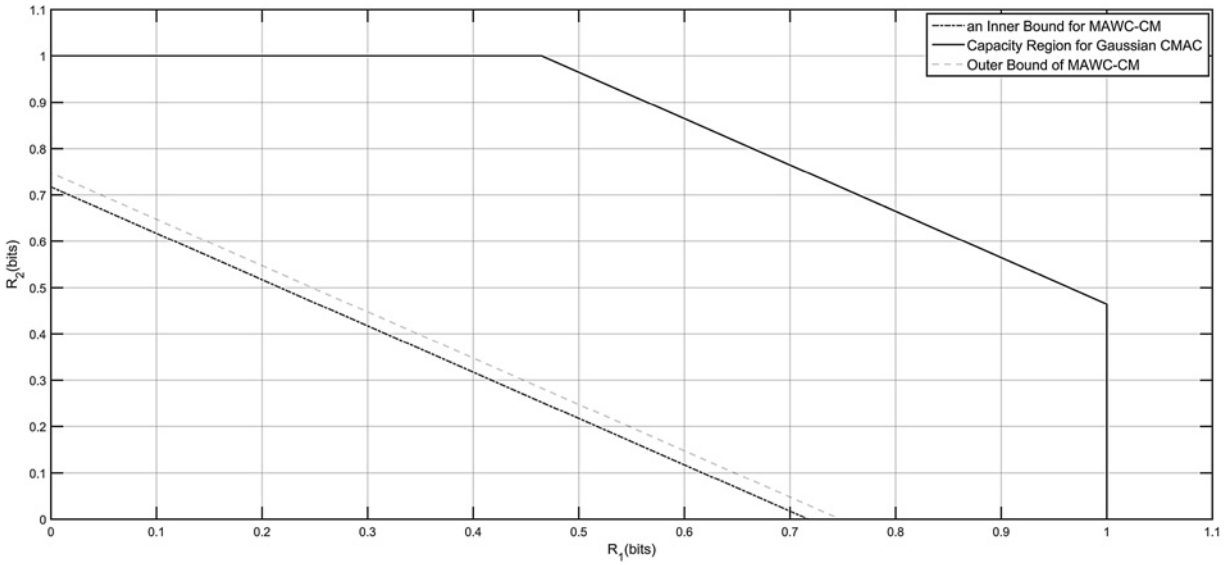

Fig. 5 *Achievable rate region of Gaussian MAWC-CM and the Capacity region of Gaussian CMAC for $P_1 = P_2 = 1$, $\sigma_1^2 = 0.1$ and $\sigma_2^2 = 0.6$*

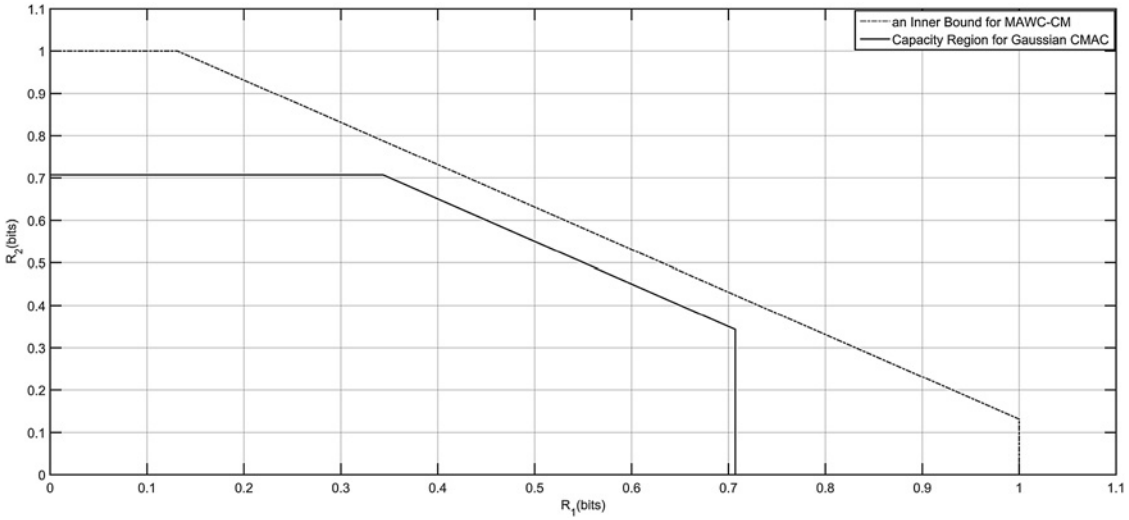

Fig. 6 *Achievable rate region of Gaussian MAWC-CM and the capacity region of Gaussian CMAC for $P_1 = P_2 = 1$, $\sigma_1^2 = 0.1$ and $\sigma_2^2 = 0.6$*

MAWC-CM (see (40)) for which increasing σ_2^2 results in increasing its achievable rate region. For comparison, assume changing $\sigma_2^2 = 0.3$ to $\sigma_2^2 = 0.6$ in the above example. As it can be seen in Fig. 6, the achievable rate region of MAWC-CM is larger than the capacity region of CMAC for the new parameters. This can be interpreted as follows: the transmitted signals from transmitters 1 and 2 are extremely attenuated at the receiver 2 in comparison with the investigated case shown in Fig. 5. Hence, for this case the requirement of secrecy of W_1 and W_2 from receiver 2 in MAWC-CM can increase the achievable rate region in comparison with that of CMAC wherein W_1 and W_2 should be reliably decoded by receiver 2.

5 Conclusions

In this paper, we have studied the secrecy capacity region of MAWC-CM. We have obtained inner and outer bounds on the secrecy capacity region for the general MAWC-CM and showed that these bounds meet each other for the switch channel model.

$$\bigcup \begin{cases} R_1 \le \min\left\{C\left(\frac{P_1(1-\beta_1^2)}{\sigma_1^2}\right), C\left(\frac{P_1(1-\beta_1^2)}{\sigma_2^2}\right)\right\} \\ R_2 \le \min\left\{C\left(\frac{P_2(1-\beta_2^2)}{\sigma_1^2}\right), C\left(\frac{P_2(1-\beta_2^2)}{\sigma_2^2}\right)\right\} \\ R_1 + R_2 \le \min\left\{C\left(\frac{P_1(1-\beta_1^2)+P_2(1-\beta_2^2)}{\sigma_1^2}\right), C\left(\frac{P_1(1-\beta_1^2)+P_2(1-\beta_2^2)}{\sigma_2^2}\right)\right\} \\ R_0 + R_1 + R_2 \le \min\left\{C\left(\frac{P_1+P_2+2\sqrt{P_1P_2}\beta_1\beta_2}{\sigma_1^2}\right), C\left(\frac{P_1+P_2+2\sqrt{P_1P_2}\beta_1\beta_2}{\sigma_2^2}\right)\right\} \end{cases} \tag{53}$$

As well, we have studied Gaussian MAWC-CM and derived inner and outer bounds on its secrecy capacity region. Providing numerical examples for the Gaussian case, we have illustrated the impact of noise and secrecy constraint on the capacity region. We have shown that there are scenarios for which the secret transmissions may increase achievable rate region in compare with the case that requires receiver 2 to decode the private messages.

6 Acknowledgment

This work was partially supported by Iran NSF under Grant number 92-32575 and by Iran Telecom Research Center (ITRC).

7 References

1 Wyner, A.D.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **57**, (8), pp. 1355–1367
2 Csiszár, I., Körner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, (3), pp. 339–348
3 Tang, X., Liu, R., Spasojević, P., *et al.*: 'Multiple access channels with generalized feedback and confidential messages'. Proc. IEEE Info. Theory Workshop (ITW), CA, USA, September 2007, pp. 608–613
4 Liang, L., Poor, H.V.: 'Multiple-access channels with confidential messages', *IEEE Trans. Inf. Theory*, 2008, **3**, pp. 976–1002
5 Yassaee, M.H., Aref, M.R.: 'Multiple access wiretap channels with strong secrecy'. Proc. IEEE ITW, Dublin, Ireland, September 2010, pp. 1–5
6 Wiese, M., Boche, H.: 'An achievable region for the wiretap multiple-access channel with common message'. Proc. IEEE Int. Symp. on Info. Theory (ISIT), Cambridge, MA, July 2012, pp. 249–253
7 Tekin, E., Yener, A.: 'The Gaussian multiple access wire-tap channel', *IEEE Trans. Inf. Theory*, 2008, **54**, (12), pp. 5747–5755
8 Liu, R., Marić, I., Yates, R.D., *et al.*: 'The discrete memoryless multiple access channel with confidential messages'. Proc. IEEE Int. Symp. on Information Theory (ISIT), Seattle, WA, September 2006, pp. 957–961
9 Tekin, E., Yener, A.: 'The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2735–2751
10 Xu, P., Ding, Z., Dai, X.: 'Rate regions for multiple access channel with conference and secrecy constraints', *IEEE Trans. Inf. Forensics Sec.*, 2013, **8**, (12), pp. 1961–1974
11 Bloch, M., Barros, J.: 'Physical-layer security: from information theory to security engineering' (Cambridge University Press, 2011)
12 Liu, R., Marić, I., Spasojević, P., *et al.*: 'Discrete memoryless interference and broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2493–2507
13 Salehkalaibar, S., Aref, M.R.: 'Physical layer security for some classes of three-receiver broadcast channels', *IET Commun.*, 2014, **8**, pp. 1965–1976
14 Salehkalaibar, S., Aref, M.R.: 'Joint source-channel coding for multiple-access wiretap channels'. Proc. IEEE Int. Symp. on Information Theory (ISIT), Cambridge, MA, July 2013, pp. 369–373
15 Simeone, O., Gündüz, D., Poor, H.V., *et al.*: 'Compound multiple-access channels with partial cooperation', *IEEE Trans. Inf. Theory*, 2009, **55**, (6), pp. 2425–2441
16 Zivari-Fard, H., Akhbari, B., Ahmadian-Attari, M., *et al.*: 'Compound multiple access channel with confidential messages'. Proc. IEEE Int. Conf. on Communication (ICC), Sydney, Australia, June 2014, pp. 1922–1927
17 Cover, T., Thomas, J.: 'Elements of information theory' (John Wiley, Hoboken, New Jersey, 2006, 2nd edn.)
18 El Gamal, A., H-Kim, Y.: 'Network information theory' (Cambridge University Press, Cambridge, U.K, 2012, 1st edn.)
19 Csiszár, I., Körner, J.: 'Information theory: coding theorems for discrete memoryless systems' (Cambridge University Press, Cambridge, U.K, 2011, 2nd edn.)

8 Appendices

8.1 Appendix 1: Proof for Theorem 1

The basis for deriving our outer bound is using Fano's inequality [18] and applying the techniques in [2] to consider the secrecy constraints.

Consider a $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n, P_e^n)$ code for the MAWC-CM. Applying Fano's inequality results in

$$H(W_0, W_1, W_2|Y_1^n) \le n\varepsilon_1 \tag{54}$$

$$H(W_0|Y_2^n) \le n\varepsilon_2. \tag{55}$$

where $\varepsilon_i \to 0$, $i = 1, 2$ as $P_e^n \to 0$.

To derive the upper bound on R_1, we first present the bound on $H(W_1|Y_2^n)$ as follows

$$\begin{aligned}
H(W_1|Y_2^n) &= H(W_1|Y_2^n, W_0) + I(W_1; W_0|Y_2^n) \\
&= H(W_1|Y_2^n, W_0) + H(W_0|Y_2^n) - H(W_0|Y_2^n, W_1) \\
&\overset{(a)}{\le} H(W_1|Y_2^n, W_0) + n\varepsilon_2 \\
&\overset{(b)}{\le} H(W_1|Y_2^n, W_0) - H(W_1|Y_1^n, W_0) + n(\varepsilon_1 + \varepsilon_2) \\
&= I(W_1; Y_1^n|W_0) - I(W_1; Y_2^n|W_0) + n(\varepsilon_1 + \varepsilon_2) \\
&= \sum_{i=1}^{n} [I(W_1; Y_{1,i}|W_0, Y_1^{i-1}) - I(W_1; Y_{2,i}|W_0, Y_{2,i+1}^n)] \\
&\quad + n(\varepsilon_1 + \varepsilon_2) \\
&\overset{(c)}{=} \sum_{i=1}^{n} [I(W_1; Y_{1,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n) \\
&\quad - I(W_1; Y_{2,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n)] + n\varepsilon' \\
&\overset{(d)}{=} \sum_{i=1}^{n} [I(V_{1,i}; Y_{1,i}|U_i) - I(V_{1,i}; Y_{2,i}|U_i)] + n\varepsilon'
\end{aligned} \tag{56}$$

where (a) and (b) result from Fano's inequality in (54) and (55). The equality (c) results from [19, Lemma 17.12] (i.e. Csiszár's sum Lemma [2]), and setting $\varepsilon' = \varepsilon_1 + \varepsilon_2$. The equality ($d$) results from the following definitions of the RVs in (57)–(59).

$$U_i = W_0, Y_1^{i-1}, Y_{2,i+1}^n \tag{57}$$

$$V_{1,i} = (W_1, U_i) \tag{58}$$

$$V_{2,i} = (W_2, U_i). \tag{59}$$

Now, we have

$$\begin{aligned}
H(W_1|Y_2^n) &\overset{(a)}{\le} n \sum_{i=1}^{n} p(Q = i)[I(V_{1,Q}; Y_{1,Q}|U_Q, Q = i) \\
&\quad - I(V_{1,Q}; Y_{2,Q}|U_Q, Q = i)] + n\varepsilon' \\
&= n[I(V_{1,Q}; Y_{1,Q}|U_Q, Q) \\
&\quad - I(V_{1,Q}; Y_{2,Q}|U_Q, Q)] + n\varepsilon' \\
&\overset{(b)}{=} n[I(V_1; Y_1|U) - I(V_1; Y_2|U)] + n\varepsilon'
\end{aligned} \tag{60}$$

where (a) results from considering Q with a uniform distribution over $\{1, 2, \ldots, n\}$ outcomes and (b) is due to defining $V_{1,Q} = V_1$, $V_{2,Q} = V_2$, $Y_{1,Q} = Y_1$, $Y_{2,Q} = Y_2$ and $(U_Q, Q) = U$. Using (6) and (60) we derive the bound on R_1 as follows

$$R_1 \le I(V_1; Y_1|U) - I(V_1; Y_2|U). \tag{61}$$

Now, we derive the bound on R_2. Using (6) and proceeding the same way as for deriving the bound on $H(W_1|Y_2^n)$, the bound on $H(W_2|Y_2^n)$ and hence the bound on R_2 can be derived as follows

$$R_2 \le I(V_2; Y_1|U) - I(V_2; Y_2|U) \tag{62}$$

Based on (5) we have: for any $\varepsilon > 0$,

$$n(R_1 + R_2) - n\varepsilon \le H(W_1, W_2|Y_2^n) \tag{63}$$

for all sufficiently large n. Hence, to derive the bound on $R_1 + R_2$ we

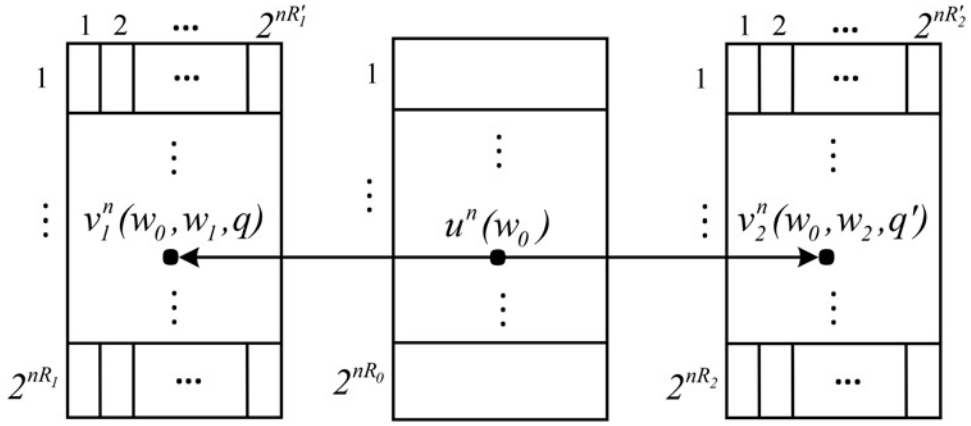

Fig. 7 *Coding scheme*

first derive the bound on $H(W_1, W_2|Y_2^n)$ as follows

$$\begin{aligned}
H(W_1, W_2|Y_2^n) &= H(W_1, W_2|Y_2^n, W_0) + I(W_1, W_2; W_0|Y_2^n) \\
&\overset{(a)}{\leq} H(W_1, W_2|Y_2^n, W_0) + n\varepsilon_2 \\
&\overset{(b)}{\leq} H(W_1, W_2|Y_2^n, W_0) - H(W_1, W_2|Y_1^n, W_0) \\
&\quad + n(\varepsilon_1 + \varepsilon_2) \\
&= I(W_1, W_2; Y_1^n|W_0) - I(W_1, W_2; Y_2^n|W_0) \\
&\quad + n(\varepsilon_1 + \varepsilon_2) \\
&= \sum_{i=1}^{n} [I(W_1, W_2; Y_{1,i}|W_0, Y_1^{i-1}) \\
&\quad - I(W_1, W_2; Y_{2,i}|W_0, Y_{2,i+1}^n)] + n(\varepsilon_1 + \varepsilon_2) \\
&\overset{(c)}{=} \sum_{i=1}^{n} [I(W_1, W_2; Y_{1,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n) \\
&\quad - I(W_1, W_2; Y_{2,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n)] + n\varepsilon' \\
&\overset{(d)}{=} \sum_{i=1}^{n} [I(V_{1,i}, V_{2,i}; Y_{1,i}|U_i) - I(V_{1,i}, V_{2,i}; Y_{2,i}|U_i)] + n\varepsilon'
\end{aligned} \tag{64}$$

where (a) and (b) result from Fano's inequality in (54) and (55) respectively. The equality (c) results from Csiszár's sum Lemma, and setting $\varepsilon' = \varepsilon_1 + \varepsilon_2$. The equality ($d$) results from the definitions of the RVs as (57)–(59). Using (63) and (64) and by applying the same time-sharing strategy as before, we have

$$R_1 + R_2 \leq I(V_1, V_2; Y_1|U) - I(V_1, V_2; Y_2|U) + \varepsilon^{\star} \tag{65}$$

where $\varepsilon^{\star} = \varepsilon + \varepsilon'$. Finally, we derive the bound on R_0 as follows

$$\begin{aligned}
nR_0 &= H(W_0) \\
&= I(W_0; Y_1^n) + H(W_0|Y_1^n) \\
&\leq I(W_0; Y_1^n) + n\varepsilon_1 \\
&= \sum_{i=1}^{n} I(W_0; Y_{1,i}|Y_1^{i-1}) + n\varepsilon_1 \\
&= \sum_{i=1}^{n} [I(W_0, Y_1^{i-1}; Y_{1,i}) - I(Y_1^{i-1}; Y_{1,i})] + n\varepsilon_1.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
nR_0 &\leq \sum_{i=1}^{n} I(W_0, Y_1^{i-1}; Y_{1,i}) + n\varepsilon_1 \\
&= \sum_{i=1}^{n} [I(W_0, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1,i}) - I(Y_{2,i+1}^n; Y_{1,i}|W_0, Y_1^{i-1})] + n\varepsilon_1 \\
&\leq \sum_{i=1}^{n} I(W_0, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1,i}) + n\varepsilon_1 \\
&= \sum_{i=1}^{n} I(U_i; Y_{1,i}) + n\varepsilon_1.
\end{aligned} \tag{66}$$

By applying the same time-sharing strategy as before, we have

$$R_0 \leq I(U; Y_1) + \varepsilon_1. \tag{67}$$

Moreover we have,

$$\begin{aligned}
nR_0 &= H(W_0) \\
&= I(W_0; Y_2^n) + H(W_0|Y_2^n) \\
&\leq I(W_0; Y_2^n) + n\varepsilon_2 \\
&= \sum_{i=1}^{n} I(W_0; Y_{2,i}|Y_{2,i+1}^n) + n\varepsilon_2 \\
&= \sum_{i=1}^{n} [I(W_0, Y_{2,i+1}^n; Y_{2,i}) - I(Y_{2,i+1}^n; Y_{2,i})] + n\varepsilon_2.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
nR_0 &\leq \sum_{i=1}^{n} I(W_0, Y_{2,i+1}^n; Y_{2,i}) + n\varepsilon_2 \\
&= \sum_{i=1}^{n} [I(W_0, Y_1^{i-1}, Y_{2,i+1}^n; Y_{2,i}) - I(Y_1^{i-1}; Y_{2,i}|W_0, Y_{2,i+1}^n)] + n\varepsilon_2 \\
&\leq \sum_{i=1}^{n} I(W_0, Y_1^{i-1}, Y_{2,i+1}^n; Y_{2,i}) + n\varepsilon_2 \\
&= \sum_{i=1}^{n} I(U_i; Y_{2,i}) + n\varepsilon_2.
\end{aligned} \tag{68}$$

By applying the same time-sharing strategy as before, we have

$$R_0 \leq I(U; Y_2) + \varepsilon_2. \tag{69}$$

Therefore, from (67) and (69) we have

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\}. \tag{70}$$

Considering (61), (62), (65) and (70), the region in (7)–(10) is obtained. The bounds on cardinality of $|\mathcal{U}|$, $|\mathcal{V}_1|$ and $|\mathcal{V}_2|$ can be derived by following the steps in [2, Appendix]. This completes the proof. □

8.2 Appendix 2: Proof for Theorem 2

As described in Section 3.2, we use the coding structure as illustrated in Fig. 7. More precisely, the codebook generation is as follows

(i) *Codebook generation:* Fix $p(u)$, $p(v_1|u)$, $p(v_2|u)$, $p(x_1|v_1)$ and $p(x_2|v_2)$. Let

$$R_1' + R_2' = I(V_1, V_2; Y_2|U) - \varepsilon, \tag{71}$$

where $\varepsilon > 0$ and $\varepsilon \to 0$ as $n \to \infty$.

- Generate 2^{nR_0} length-n codewords u^n through $p(u^n) = \prod_{i=1}^n p(u_i)$ and index them as $u^n(w_0)$, $w_0 \in \{1, \ldots, 2^{nR_0}\}$.
- For each codeword $u^n(w_0)$, generate $2^{n\widetilde{R}_1}$ length-n codewords v_1^n through $p(v_1^n|u^n) = \prod_{i=1}^n p(v_{1,i}|u_i)$, where $\widetilde{R}_1 = R_1 + R_1'$. Then, randomly bin $2^{n\widetilde{R}_1}$ codewords into 2^{nR_1} bins, and index them as $v_1^n(w_0, w_1, q)$, where $w_1 \in \{1,\ldots, 2^{nR_1}\}$ is the bin number and $q \in \mathcal{Q} = \{1, \ldots, 2^{nR_1'}\}$ is the index of codewords in the bin number w_1.

The codebook for user 2 is generated in the same way.

(ii) *Encoding:* Assume that (w_0, w_1) is the message pair to be transmitted, the encoder g_1 randomly chooses index q corresponding to (w_0, w_1) and then generates a codeword X_1^n at random according to $\prod_{i=1}^n p(x_{1,i}|v_{1,i})$. Transmitter 2 uses the same way to encode (w_0, w_2).

(iii) *Decoding and probability of error*:

Decoding:

- The legitimate receiver (receiver 1) decodes $(\widehat{w}_{01}, \widehat{w}_1, \widehat{w}_2)$ by looking for the unique (u^n, v_1^n, v_2^n) such that $(u^n(\widehat{w}_{01}), v_1^n(\widehat{w}_{01}, \widehat{w}_1, q), v_2^n(\widehat{w}_{01}, \widehat{w}_2, q'), y_1^n) \in T_\varepsilon^n(P_{UV_1V_2Y_1})$.
- Receiver 2 decodes $\hat{w}_{02}$ by looking for the unique u^n such that $(u^n(\widehat{w}_{02}), y_2^n) \in T_\varepsilon^n(P_{UY_2})$.

Probability of error analysis: Define the events

$$\begin{aligned} E_{r,w_0,w_1,w_2} = \{&(u^n(\widehat{w}_{01}), v_1^n(\widehat{w}_{01}, \widehat{w}_{11}, q), \\ &v_2^n(\widehat{w}_{01}, \widehat{w}_{21}, q'), y_1^n) \in T_\varepsilon^n(P_{UV_1V_2Y_1})\} \end{aligned} \tag{72}$$

$$E_{e,w_0} = \{(u^n(\widehat{w}_{02}), y_2^n) \in T_\varepsilon^n(P_{UY_2})\}. \tag{73}$$

Without loss of generality, we assume that $(w_0, w_1, w_2) = (1, 1, 1)$ was sent. We can bound the probability of error in receiver 1 using the union bound (see (74))

(see (75))

In the same way we can bound the probability of error in receiver 2 using the union bound as

$$\begin{aligned} P_{e,2}^n(1, 1, 1) &= \Pr\{E_{e,1}^c \bigcup_{w_0 \neq 1} E_{e,w_0}\} \\ &\leq \Pr\{E_{e,1}^c\} + \sum_{w_0 \neq 1} \Pr\{E_{e,w_0}\} \end{aligned} \tag{76}$$

From the Asymptotic Equipartition Property [17, Chapter 3] and [17, Thm. 15.2.1, 15.2.3], it follows that

$$\Pr\{E_{r,1,1,1}^c\} \leq \varepsilon \tag{77}$$

$$\Pr\{E_{r,w_0,1,1}\} \leq 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} \tag{78}$$

$$\Pr\{E_{r,1,w_1,1}\} \leq 2^{-n[I(V_1;Y_1|V_2,U)-\varepsilon]} \tag{79}$$

$$\Pr\{E_{r,w_0,w_1,1}\} \leq 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon} \tag{80}$$

$$\Pr\{E_{r,1,1,w_2}\} \leq 2^{-n[I(V_2;Y_1|V_1,U)-\varepsilon]} \tag{81}$$

$$\Pr\{E_{r,w_0,1,w_2}\} \leq 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} \tag{82}$$

$$\Pr\{E_{r,1,w_1,w_2}\} \leq 2^{-n[I(V_1,V_2;Y_1|U)-\varepsilon]} \tag{83}$$

$$\Pr\{E_{r,w_0,w_1,w_2}\} \leq 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} \tag{84}$$

$$\Pr\{E_{e,1}^c\} \leq \varepsilon \tag{85}$$

$$\Pr\{E_{e,w_0}\} \leq 2^{-n[I(U;Y_2)-\varepsilon]} \tag{86}$$

where $\varepsilon > 0$ and $\varepsilon \to 0$ as $n \to \infty$. Hence, (75) and (76) are

$$P_{e,1}^n(1, 1, 1) = \Pr\{E_{r,1,1,1}^c \bigcup_{w_0 \neq 1} E_{r,w_0,1,1} \bigcup_{w_1 \neq 1} E_{r,1,w_1,1} \bigcup_{\substack{w_0 \neq 1 \\ w_1 \neq 1}} E_{r,w_0,w_1,1} \bigcup_{w_2 \neq 1} E_{r,1,1,w_2} \bigcup_{\substack{w_0 \neq 1 \\ w_2 \neq 1}} E_{r,w_0,1,w_2} \bigcup_{\substack{w_1 \neq 1 \\ w_2 \neq 1}} E_{r,1,w_1,w_2} \bigcup_{\substack{w_0 \neq 1 \\ w_1 \neq 1 \\ w_2 \neq 1}} E_{r,w_0,w_1,w_2}\} \tag{74}$$

$$\begin{aligned} &\leq \Pr\{E_{r,1,1,1}^c\} + \sum_{w_0 \neq 1} \Pr\{E_{r,w_0,1,1}\} + \sum_{w_1 \neq 1} \sum_{q} \Pr\{E_{r,1,w_1,1}\} \\ &+ \sum_{w_0 \neq 1} \sum_{w_1 \neq 1} \sum_{q} \Pr\{E_{r,w_0,w_1,1}\} \\ &+ \sum_{w_2 \neq 1} \sum_{q'} \Pr\{E_{r,1,1,w_2}\} + \sum_{w_0 \neq 1} \sum_{w_2 \neq 1} \sum_{q'} \Pr\{E_{r,w_0,1,w_2}\} \\ &+ \sum_{w_1 \neq 1} \sum_{q} \sum_{w_2 \neq 1} \sum_{q'} \Pr\{E_{r,1,w_1,w_2}\} \\ &+ \sum_{w_0 \neq 1} \sum_{w_1 \neq 1} \sum_{q} \sum_{w_2 \neq 1} \sum_{q'} \Pr\{E_{r,w_0,w_1,w_2}\}. \end{aligned} \tag{75}$$

respectively bounded by

$$P_{e,1}^{n}(1,1,1) \le \varepsilon + 2^{nR_0} \times 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} + 2^{n\tilde{R}_1} \times 2^{-n[I(V_1;Y_1|V_2,U)-\varepsilon]} + 2^{nR_0+\tilde{R}_1} \times 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} + 2^{n\tilde{R}_2} \times 2^{-n[I(V_2;Y_1|V_1,U)-\varepsilon]} + 2^{nR_0+\tilde{R}_2} \times 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} + 2^{n(\tilde{R}_1+\tilde{R}_2)} \times 2^{-n[I(V_1,V_2;Y_1|U)-\varepsilon]} + 2^{n(R_0+\tilde{R}_1+\tilde{R}_2)} \times 2^{-n[I(U,V_1,V_2;Y_1)-\varepsilon]} \tag{87}$$

and

$$P_{e,2}^{n}(1) \le \varepsilon + 2^{nR_0} \times 2^{-n[I(U;Y_2)-\varepsilon]}. \tag{88}$$

Due to (88) and (87), to generate $P_e^n \to 0$ as $n \to \infty$, we must choose

$$R_0 \le I(U; Y_2) \tag{89}$$

$$\tilde{R}_1 \le I(V_1; Y_1|V_2, U) \tag{90}$$

$$\tilde{R}_2 \le I(V_2; Y_1|V_1, U) \tag{91}$$

$$\tilde{R}_1 + \tilde{R}_2 \le I(V_1, V_2; Y_1|U) \tag{92}$$

$$R_0 + \tilde{R}_1 + \tilde{R}_2 \le I(U, V_1, V_2; Y_1), \tag{93}$$

and

$$R_0 \le I(U, V_1, V_2; Y_1) \tag{94}$$

$$R_0 + \tilde{R}_1 \le I(U, V_1, V_2; Y_1) \tag{95}$$

$$R_0 + \tilde{R}_2 \le I(U, V_1, V_2; Y_1) \tag{96}$$

then $P_{e,1}^n \le \varepsilon$ and $P_{e,2}^n \le \varepsilon$, and from (3) we have: $P_e^n \le \varepsilon$. Note that in (89)–(96), we have these Markov chains $V_1 - U - V_2$ and $U - (V_1, V_2) - (Y_1, Y_2)$, and the bounds (94)–(96) are redundant because of (93). Therefore, we need to consider only (89)–(93). Moreover $\tilde{R}_1 = R_1 + R_1'$ and $\tilde{R}_2 = R_2 + R_2'$ that by replacing these into (89)–(93) we have

$$R_0 \le I(U; Y_2) \tag{97}$$

$$R_1 + R_1' \le I(V_1; Y_1|V_2, U) \tag{98}$$

$$R_2 + R_2' \le I(V_2; Y_1|V_1, U) \tag{99}$$

$$R_1 + R_1' + R_2 + R_2' \le I(V_1, V_2; Y_1|U) \tag{100}$$

$$R_0 + R_1 + R_1' + R_2 + R_2' \le I(U, V_1, V_2; Y_1) \tag{101}$$

(iv) *Equivocation computation*

$$\begin{aligned} H(W_1, W_2|Y_2^n) &\ge H(W_1, W_2|Y_2^n, U^n) \\ &= H(W_1, W_2, Y_2^n|U^n) - H(Y_2^n|U^n) \\ &= H(W_1, W_2, Y_2^n, V_1^n, V_2^n|U^n) - H(V_1^n, V_2^n|W_1, W_2, Y_2^n, U^n) \\ &\quad - H(Y_2^n|U^n) \\ &= H(W_1, W_2, V_1^n, V_2^n|U^n) + H(Y_2^n|W_1, W_2, V_1^n, V_2^n, U^n) \\ &\quad - H(V_1^n, V_2^n|W_1, W_2, Y_2^n, U^n) - H(Y_2^n|U^n) \\ &\overset{(a)}{\ge} H(V_1^n, V_2^n|U^n) - H(V_1^n, V_2^n|W_1, W_2, Y_2^n, U^n) \\ &\quad + H(Y_2^n|V_1^n, V_2^n, U^n) - H(Y_2^n|U^n) \\ &= H(V_1^n, V_2^n|U^n) - H(V_1^n, V_2^n|W_1, W_2, Y_2^n, U^n) \\ &\quad - I(V_1^n, V_2^n; Y_2^n|U^n) \end{aligned} \tag{102}$$

where (a) is due to $I(Y_2^n; W_1, W_2|V_1^n, V_2^n, U^n) = 0$.

The first term in (102) is given by

$$H(V_1^n, V_2^n|U^n) = n\widetilde{R}_1 + n\widetilde{R}_2 = n(R_1 + R_1' + R_2 + R_2'). \tag{103}$$

We then show that the second term in (102) can be bounded by $H(V_1^n, V_2^n|W_1, W_2, Y_2^n, U^n) \le n\varepsilon_1$, as $n \to \infty$ then $\varepsilon_1 \to 0$. To this aim, it can be noted that given the message $(W_1, W_2) = (w_1, w_2)$ and assuming that receiver 2 knows the sequence $U^n = u^n$, it can decode (q, q') with small probability of error if

$$R_1' \le I(V_1; Y_2|V_2, U) \tag{104}$$

$$R_2' \le I(V_2; Y_2|V_1, U) \tag{105}$$

$$R_1' + R_2' \le I(V_1, V_2; Y_2|U). \tag{106}$$

for sufficiently large n.

Using Fano's inequality implies that $H(V_1^n, V_2^n|W_1 = w_1, W_2 = w_2, Y_2^n, U^n) \le n\varepsilon_1$. Hence,

$$\begin{aligned} &H(V_1^n, V_2^n|W_1, W_2, Y_2^n, U^n) \\ &= \sum_{w_1}\sum_{w_2} p(W_1 = w_1)p(W_2 = w_2) \\ &\times H(V_1^n, V_2^n|W_1 = w_1, W_2 = w_2, Y_2^n, U^n) \le n\varepsilon_1. \end{aligned} \tag{107}$$

The last term in (102) is bounded as

$$I(V_1^n, V_2^n; Y_2^n|U^n) \le nI(V_1, V_2; Y_2|U) + n\varepsilon_2, \tag{108}$$

as $n \to \infty$ then $\varepsilon_2 \to 0$ similar to [1, Lemma 1]. By replacing (103), (107) and (108) in (102) we have

$$\begin{aligned} H(W_1, W_2|Y_2^n) &\ge n(R_1 + R_1' + R_2 + R_2') \\ &\quad - n\varepsilon_1 - nI(V_1, V_2; Y_2|U) - n\varepsilon_2 \end{aligned} \tag{109}$$

$$= n(R_1 + R_2 + R_1' + R_2' - I(V_1, V_2; Y_2|U)) - n\delta \tag{110}$$

$$= n(R_1 + R_2) - 2n\delta \tag{111}$$

where $\delta = \varepsilon_1 + \varepsilon_2$. Finally, by using the Fourier–Motzkin procedure [18] to eliminate R_1' and R_2' in (71), (97)–(101) and (104)–(106) we obtain the five inequalities in Theorem 2. The bounds on cardinality of $|\mathcal{U}|$, $|\mathcal{V}_1|$ and $|\mathcal{V}_2|$ can be derived by following the steps in [2, Appendix]. This completes the proof of Theorem 2.

8.3 Appendix 3: Proof for Theorem 3

To prove this theorem, we concentrate on outer bound (Theorem 1) and inner bound (Theorem 2) and we prove that these bounds are identical for the switch channel case. The method of our proof is similar to the method in [12]. According to the distribution (20), for a known auxiliary random variable U, auxiliary RVs V_1 and V_2 are independent, but this is not true for distribution (11). Therefore, we first show that these distributions are identical for a switch channel case. Therefore, we show that,

$$I(V_1;\, V_2|U) = 0 \tag{112}$$

holds for the outer bound of switch channel case. Moreover, if

$$I(V_1;\, V_2|Y_1,\, U) = 0, \tag{113}$$

holds for the outer bound of the switch channel, then

$$I(V_1;\, Y_1|V_2,\, U) = I(V_1;\, Y_1|U) \tag{114}$$

$$I(V_2;\, Y_1|V_1,\, U) = I(V_2;\, Y_1|U) \tag{115}$$

that is, for the switch channel case, (8)–(9) in the outer bound and (16)–(17) in the inner bound are identical.

Now, we prove that (112) and (113) hold for outer bound of switch channel model. From definitions (57)–(59) we need to show that

$$I(W_1;\, W_2|U_i) = 0 \tag{116}$$

$$I(W_1;\, W_2|U_i,\, Y_{1,i}) = 0 \tag{117}$$

where according to (57), $U_i = W_0,\, Y_1^{i-1},\, Y_{2,i+1}^n$. We first show that (116) holds for switch channel. From definition (27) we have,

$$\{Y_1^{i-1},\, Y_{2,i+1}^n\} = \{K_1^{i-1},\, K_{2,i+1}^n,\, S_1^{i-1},\, S_{2,i+1}^n\} \tag{118}$$

therefore,

$$\begin{aligned} I(W_1;\, W_2|U_i) &= I(W_1;\, W_2|W_0,\, K_1^{i-1},\, K_{2,i+1}^n,\, S_1^{i-1},\, S_{2,i+1}^n) \\ &= \sum_{s_1^{i-1}} \sum_{s_{2,i+1}^n} P(S_1^{i-1} = s_1^{i-1},\, S_{2,i+1}^n = s_{2,i+1}^n) \\ &I(W_1;\, W_2|W_0,\, K_1^{i-1},\, K_{2,i+1}^n,\, s_1^{i-1},\, s_{2,i+1}^n) \\ &= \sum_{s_1^{i-1}} \sum_{s_{2,i+1}^n} \left[\prod_{a=1}^{i-1} P(S_{1,a} = s_{1,a}) \prod_{b=i+1}^{n} P(S_{2,b} = s_{2,b}) \right] \\ &I(W_1;\, W_2|W_0,\, K_1^{i-1},\, K_{2,i+1}^n,\, s_1^{i-1},\, s_{2,i+1}^n). \end{aligned} \tag{119}$$

Now, for known $s_{t,i}$, the switch channel model (26) shows that $k_{t,i}$ depends only on the channel input $x_{s_{t,i}},\, i$. From [12], and for known switch state information s_1^{i-1} and $s_{2,i+1}^n$ we can easily show that

$$I(W_1;\, W_2|W_0,\, K_1^{i-1},\, K_{2,i+1}^n,\, s_1^{i-1},\, s_{2,i+1}^n) = 0. \tag{120}$$

This proves the equality (112). Proceeding the same way, we can show that equality (113) holds. Hence, the equalities (114)–(115) hold for the switch channel. Moreover, (7) implies (15). Moreover, in the derived outer bound in Theorem 1, adding (7) to the (10) subject to the existing Markov chain $U - (V_1,\, V_2) - (Y_1,\, Y_2)$ gives: $R_0 + R_1 + R_2 \le I(V_1,\, V_2; Y_1) - I(V_1,\, V_2; Y_2|U)$ that is identical to (19) in the derived inner bound. The bounds on cardinality of $|\mathcal{U}|$, $|\mathcal{V}_1|$ and $|\mathcal{V}_2|$ can be derived by following the steps in [2, Appendix]. This completes the proof.

8.4 Appendix 4: Proof for Theorem 4

To derive an outer bound for the Gaussian case we can follow the steps of deriving an outer bound for discrete memoryless case (i.e. Theorem 1) that are based on the basic properties of mutual information (the chain rule and positivity) and hold irrespective of the continuous or discrete nature of the channel. Therefore, by following (64), (66) and (68), it can be seen that if a rate tuple $(R_0,\, R_1,\, R_2)$ is achievable for the Gaussian MAWC-CM, it must hold that

$$R_0 \le \min\left\{ \frac{1}{n}\sum_{i=1}^{n} I(U_i;\, Y_{1,i}),\, \frac{1}{n}\sum_{i=1}^{n} I(U_i;\, Y_{2,i}) \right\} \tag{121}$$

$$R_1 + R_2 \le \frac{1}{n}\sum_{i=1}^{n} [I(V_{1,i},\, V_{2,i};\, Y_{1,i}|U_i) - I(V_{1,i},\, V_{2,i};\, Y_{2,i}|U_i)] \tag{122}$$

It remains to upper bound (121) and (122) with terms that depend on the power constraints P_1 and P_2. We first assume that $\sigma_1^2 \le \sigma_2^2$ so that the eavesdropper's channel is stochastically degraded with respect to the main channel. We expand $\frac{1}{n}\sum_{i=1}^{n} I(U_i;\, Y_{1,i})$ in terms of the differential entropy as

$$\frac{1}{n}\sum_{i=1}^{n} I(U_i;\, Y_{1,i}) = \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}) - \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|U_i) \tag{123}$$

and we bound each sum separately. Due to channel model definition and assumptions, we have

$$\mathrm{var}\,(Y_{1,i}) = E[X_{1,i}^2] + E[X_{2,i}^2] + \sigma_1^2 + 2\lambda_i \tag{124}$$

where $\lambda_i = E[X_{1,i}X_{2,i}]$. Hence, the differential entropy of $Y_{1,i}$ is upper bounded by the entropy of a Gaussian random variable with the same variance. Hence,

$$\begin{aligned} \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}) &\le \frac{1}{n}\sum_{i=1}^{n} \frac{1}{2}\log\left(2\pi e(E[X_{1,i}^2] + E[X_{2,i}^2] + \sigma_1^2 + 2\lambda_i)\right) \\ &\overset{(a)}{\le} \frac{1}{2}\log\left(2\pi e\left(\frac{1}{n}\sum_{i=1}^{n} E[X_{1,i}^2] + \frac{1}{n}\sum_{i=1}^{n} E[X_{2,i}^2] + \frac{2}{n}\sum_{i=1}^{n} \lambda_i + \sigma_1^2\right)\right), \end{aligned}$$

where (a) results since $x \mapsto \log(2\pi e x)$ is a concave function of x as using Jensen's inequality. Also, by setting $Q_1 \triangleq (1/n)\sum_{i=1}^{n} E[X_{1,i}^2]$, $Q_2 \triangleq (1/n)\sum_{i=1}^{n} E[X_{2,i}^2]$, $Q_3 \triangleq (1/n)\sum_{i=1}^{n} \lambda_i$ and $\rho = Q_3/\sqrt{Q_1 Q_2}$ we finally obtain

$$\frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}) \le \frac{1}{2}\log\left(2\pi e(Q_1 + Q_2 + 2\rho\sqrt{Q_1 Q_2} + \sigma_1^2)\right). \tag{125}$$

To bound the second sum $(1/n)\sum_{i=1}^{n} h(Y_i|U_i)$, note that

$$\begin{aligned} \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|U_i) &\le \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}) \\ &\le \frac{1}{2}\log\left(2\pi e(Q_1 + Q_2 + 2\rho\sqrt{Q_1 Q_2} + \sigma_1^2)\right). \end{aligned} \tag{126}$$

Moreover, because $U_i \to (V_{1,i},\, V_{2,i}) \to (X_{1,i},\, X_{2,i}) \to (Y_{1,i},\, Y_{2,i})$ forms

IET Commun., 2016, Vol. 10, Iss. 1, pp. 98–110

a Markov chain, we have

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|U_i) &\geq \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|U_i, X_{1,i}, X_{2,i}) \\ &= \frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|X_{1,i}, X_{2,i}) \\ &= \frac{1}{2}\log(2\pi e\sigma_1^2).\end{aligned} \tag{127}$$

Since $x, y \mapsto (1/2)\log(2\pi e(xQ_1 + yQ_2 + 2xy\rho\sqrt{Q_1Q_2} + \sigma_1^2))$ is a continuous function on interval $x \in [0, 1]$ and $y \in [0, 1]$, a two-dimensional intermediate-value theorem ensures the existence of $\beta_1, \beta_2 \in [0, 1]$ such that

$$\begin{aligned}\frac{1}{n}\sum_{i=1}^{n} h(Y_{1,i}|U_i) = \frac{1}{2}\log(2\pi e(&\beta_1 Q_1 + \beta_2 Q_2 \\ &+ 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_1^2)).\end{aligned} \tag{128}$$

By substituting (125) and (128) into (123), we obtain

$$\begin{aligned}&\frac{1}{n}\sum_{i=1}^{n} I(U_i; Y_{1,i}) \\ &\leq \frac{1}{2}\log(2\pi e(Q_1 + Q_2 + 2\rho\sqrt{Q_1Q_2} + \sigma_1^2)) \\ &\quad - \frac{1}{2}\log(2\pi e(\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_1^2)) \\ &= \frac{1}{2}\log\left(1 + \frac{(1-\beta_1)Q_1 + (1-\beta_2)Q_2 + 2(1-\beta_1\beta_2)\rho\sqrt{Q_1Q_2}}{\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_1^2}\right).\end{aligned} \tag{129}$$

Now, we need to upper bound $(1/n)\sum_{i=1}^{n} I(U_i; Y_{2,i})$. Note that we can repeat the steps leading to (125) with $Y_{2,i}$ instead of $Y_{1,i}$ to obtain

$$\frac{1}{n}\sum_{i=1}^{n} h(Y_{2,i}) \leq \frac{1}{2}\log(2\pi e(Q_1 + Q_2 + 2\rho\sqrt{Q_1Q_2} + \sigma_2^2)). \tag{130}$$

Hence, we need to derive a lower bound for $(1/n)\sum_{i=1}^{n} h(Y_{2,i}|U_i)$ as a function of Q_1, Q_2, β_1, β_2 and ρ. Since we have assumed that the eavesdropper's channel is stochastically degraded with respect to the main channel, we can write $Y_{2,i} = Y_{1,i} + N_i'$ with $N_i' \sim \mathcal{N}(0, \sigma_2^2 - \sigma_1^2)$. Applying the Entropy Power Inequality (EPI) [18] to the RV $Y_{2,i}$ conditioned on $U_i = u_i$, we have

$$\begin{aligned}h(Y_{2,i}|U_i = u_i) &= h(Y_{1,i} + N_i'|U_i = u_i) \\ &\geq \frac{1}{2}\log\left(2^{2h(Y_{1,i}|U_i=u_i)} + 2^{2h(N_i'|U_i=u_i)}\right) \\ &= \frac{1}{2}\log\left(2^{2h(Y_{1,i}|U_i=u_i)} + 2\pi e(\sigma_2^2 - \sigma_1^2)\right).\end{aligned} \tag{131}$$

Hence,

$$\begin{aligned}&\frac{1}{n}\sum_{i=1}^{n} h(Y_{2,i}|U_i) = \frac{1}{n}\sum_{i=1}^{n} E_{U_i}[h(Y_{2,i}|U_i)] \\ &\overset{(a)}{\geq} \frac{1}{2n}\sum_{i=1}^{n} E_{U_i}\left[\log\left(2^{2h(Y_{1,i}|U_i)} + 2\pi e\left(\sigma_2^2 - \sigma_1^2\right)\right)\right] \\ &\overset{(b)}{\geq} \frac{1}{2n}\sum_{i=1}^{n} \log\left(2^{2E_{U_i}[h(Y_{1,i}|U_i)]} + 2\pi e\left(\sigma_2^2 - \sigma_1^2\right)\right) \\ &= \frac{1}{2n}\sum_{i=1}^{n} \log\left(2^{2h(Y_{1,i}|U_i)} + 2\pi e(\sigma_2^2 - \sigma_1^2)\right) \\ &\overset{(c)}{\geq} \frac{1}{2}\log\left(2^{(2/n)\sum_{i=1}^{n} h(Y_{1,i}|U_i)} + 2\pi e(\sigma_2^2 - \sigma_1^2)\right) \\ &\overset{(d)}{=} \frac{1}{2}\log(2\pi e(\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_2^2)),\end{aligned} \tag{132}$$

where (a) follows from EPI and (131). Both (b) and (c) follow from the convexity of the function $x \mapsto \log(2^x + c)$ for $c \in \mathbb{R}_+$ and Jensen's inequality, while (d) follows from (128). Hence,

$$\begin{aligned}&\frac{1}{n}\sum_{i=1}^{n} I(U_i; Y_{2,i}) = \frac{1}{n}\sum_{i=1}^{n} h(Y_{2,i}) - h(Y_{2,i}|U_i) \\ &\leq \frac{1}{2}\log(2\pi e(Q_1 + Q_2 + 2\rho\sqrt{Q_1Q_2} + \sigma_2^n)) \\ &\quad - \frac{1}{2}\log(2\pi e(\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_2^2)) \\ &= \frac{1}{2}\log\left(1 + \frac{(1-\beta_1)Q_1 + (1-\beta_2)Q_2 + 2(1-\beta_1\beta_2)\rho\sqrt{Q_1Q_2}}{\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_2^2}\right)\end{aligned} \tag{133}$$

where the inequality follows from (130) and (132). By substituting (129) and (133) into (121), we obtain (see (134))

Now, we derive the bound on $R_1 + R_2$,

$$\begin{aligned}&\frac{1}{n}\sum_{i=1}^{n} [I(V_{1,i}, V_{2,i}; Y_{1,i}|U_i) - I(V_{1,i}, V_{2,i}; Y_{2,i}|U_i)] \\ &= \frac{1}{n}\sum_{i=1}^{n} [I(V_{1,i}, V_{2,i}, X_{1,i}, X_{2,i}; Y_{1,i}|U_i) \\ &\quad - I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i, V_{1,i}, V_{2,i}) \\ &\quad - I(V_{1,i}, V_{2,i}, X_{1,i}, X_{2,i}; Y_{2,i}|U_i) \\ &\quad + I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i})]\end{aligned}$$

$$R_0 \leq \min\left\{\begin{array}{l}\frac{1}{2}\log\left(1 + \frac{(1-\beta_1)Q_1 + (1-\beta_2)Q_2 + 2(1-\beta_1\beta_2)\rho\sqrt{Q_1Q_2}}{\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_1^2}\right), \\ \frac{1}{2}\log\left(1 + \frac{(1-\beta_1)Q_1 + (1-\beta_2)Q_2 + 2(1-\beta_1\beta_2)\rho\sqrt{Q_1Q_2}}{\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1Q_2} + \sigma_2^2}\right)\end{array}\right\}. \tag{134}$$

$$
\begin{aligned}
&= \frac{1}{n}\sum_{i=1}^{n}[I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i) \\
&\quad + I(V_{1,i}, V_{2,i}; Y_{1,i}|U_i, X_{1,i}, X_{2,i}) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i, V_{1,i}, V_{2,i}) - I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i) \\
&\quad - I(V_{1,i}, V_{2,i}; Y_{2,i}|U_i, X_{1,i}, X_{2,i}) \\
&\quad + I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i})] \\
&\overset{(a)}{=} \frac{1}{n}\sum_{i=1}^{n}[I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i, V_{1,i}, V_{2,i}) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i) + I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i})] \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{1,i}, Y_{2,i}|U_i, V_{1,i}, V_{2,i}) \\
&\quad + I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i}, Y_{1,i}) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i) + I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i})] \\
&\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^{n}[I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{1,i}, Y_{2,i}|U_i, V_{1,i}, V_{2,i}) \\
&\quad - I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i) + I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i})] \\
&\overset{(c)}{\leq} \frac{1}{n}\sum_{i=1}^{n}[I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i) - I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i)]
\end{aligned} \tag{135}
$$

where (a) follows from $I(V_{1,i}, V_{2,i}; Y_{1,i}|U_i, X_{1,i}, X_{2,i}) = I(V_{1,i}, V_{2,i}; Y_{2,i}|U_i, X_{1,i}, X_{2,i}) = 0$ since $U_i \to (V_{1,i}, V_{2,i}) \to (X_{1,i}, X_{2,i}) \to (Y_{1,i}, Y_{2,i})$ forms a Markov chain, (b) follows from $I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i}, Y_{1,i}) = 0$ since $Y_{2,i}$ is stochastically degraded with respect to $Y_{1,i}$, and (c) follows from $I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i, V_{1,i}, V_{2,i}) \leq I(X_{1,i}, X_{2,i}; Y_{1,i}, Y_{2,i}|U_i, V_{1,i}, V_{2,i})$. Next, we use (128) and (132) to substitute Q_1, Q_2, ρ, β_1 and β_2 as follows

$$
\begin{aligned}
&\frac{1}{n}\sum_{i=1}^{n}[I(V_{1,i}, V_{2,i}; Y_{1,i}|U_i) - I(V_{1,i}, V_{2,i}; Y_{2,i}|U_i)] \\
&\overset{(a)}{\leq} \frac{1}{n}\sum_{i=1}^{n}[I(X_{1,i}, X_{2,i}; Y_{1,i}|U_i) - I(X_{1,i}, X_{2,i}; Y_{2,i}|U_i)] \\
&= \frac{1}{n}\sum_{i=1}^{n}[h(Y_{1,i}|U_i) - h(Y_{1,i}|U_i, X_{1,i}, X_{2,i}) \\
&\quad - h(Y_{2,i}|U_i) + h(Y_{2,i}|U_i, X_{1,i}, X_{2,i})] \\
&\overset{(b)}{\leq} \frac{1}{2}\log\left(1 + \frac{\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1 Q_2}}{\sigma_1^2}\right) \\
&\quad - \frac{1}{2}\log\left(1 + \frac{\beta_1 Q_1 + \beta_2 Q_2 + 2\beta_1\beta_2\rho\sqrt{Q_1 Q_2}}{\sigma_2^2}\right)
\end{aligned} \tag{136}
$$

where (a) is due to (135), and (b) results from (127), (128) and (132).

If $\sigma_1^2 \geq \sigma_2^2$, then the main channel is stochastically degraded with respect to the eavesdropper's channel and $R_1 = R_2 = 0$ by virtue of [11, Proposition 3.4]. By swapping the roles of $Y_{1,i}$ and $Y_{2,i}$ in the proof, it can be verified that (134) still holds. We combine the two cases $\sigma_1^2 \leq \sigma_2^2$ and $\sigma_1^2 \geq \sigma_2^2$ by writing (39). Note that (134) and (136) are increasing functions of Q_1 and Q_2. Hence, by defining $Q_j = (1/n)\sum_{i=1}^{n} E[X_{j,i}^2] \leq P_j$, $j = 1, 2$ the inequalities in Theorem 4 hold. This completes the proof.

IET Commun., 2016, Vol. 10, Iss. 1, pp. 98–110