Secrecy in Communication Networks: Being Cooperative or Competitive?

Yanling Chen[1], O. Ozan Koyluoglu[2], and A. J. Han Vinck[1]

[1] Insititute of Digital Signal Processing, University of Duisburg-Essen, Germany
[2] Department of Electrical Engineering and Computer Sciences
University of California at Berkeley, USA
{yanling.chen, han.vinck}@uni-due.de, ozan.koyluoglu@berkeley.edu

Abstract. Communication networks have had a transformative impact on our society as they have revolutionized almost all aspects of human interaction. The explosive growth of data traffic has led to an increased demand on improving the reliability, efficiency and security aspects of the systems. In this paper, we focus on the multiple access channel, a communication model where several transmitters communicate to a common receiver (e.g.: a cellular telephone network) in the presence of an external eavesdropper. The goal is to explore the competitive yet cooperative relationship between the transmitters in order to obtain an efficient communication under a certain reliability and security guarantee.

Keywords: Communication network · Multiple access channel · Secrecy.

1 Introduction

1.1 Ubiquitous communication in the era of Internet of Things

Over the last decades, wireless communication has transformed from a niche technology into an indispensable part of life. The combination of ubiquitous cellular phone service and rapid growth of the Internet has created an environment where consumers desire seamless, high quality connectivity at all times and from virtually all locations. Most traditional wireless systems are based on the cellular methodology, where the area to be covered is broken into geographical cells. A base station (or access point) is placed in each cell, and the wireless users in each cell communicate exclusively with the corresponding base station, which acts as a gateway to the rest of the network. The single cell model shown in Fig. 1, in which there is a base station and multiple mobile devices. When the base station is transmitting messages to the mobiles, the channel is referred to as a downlink or broadcast channel (BC). Conversely, when the mobiles are transmitting messages to the base station, the channel is referred to as an uplink or multiple-access channel (MAC). Both BC and MAC are two important branches in the extensive field of the multiple-user communication. In this paper, we will mainly focus on the MAC.

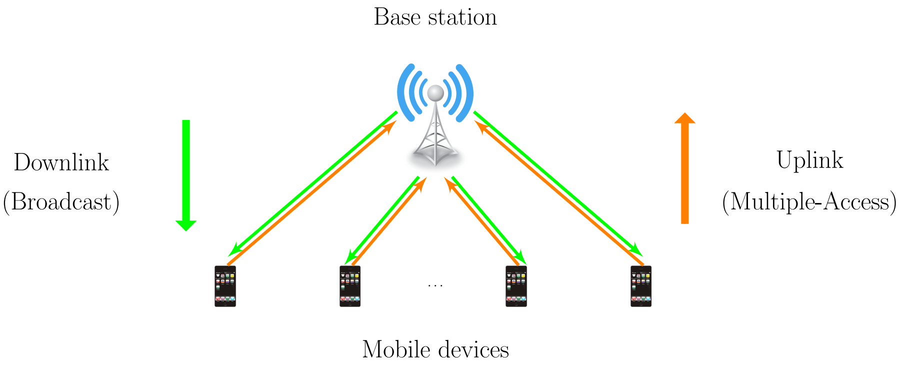

Fig. 1. Cellular channel model.

1.2 Previous studies on MAC

The study of MAC can be traced back to the classic papers from the 70s. For the discrete memoryless MAC (DM-MAC) with independent messages, Ahlswede [1] first studied the 2-transmitter and 3-transmitter cases and determined the respective capacity regions; whilst Liao [2] considered the general K-transmitter DM-MAC and fully characterized its capacity region. There are also many studies on different extensions of MAC, such as MAC with correlated sources [3–5], the Gaussian MAC [6], and etc. An extensive survey on the information-theoretic aspects of MAC was given in [7].

Another remarkable result on MAC is that the capacity region of a memoryless MAC can be increased by feedback, unlike the capacity of a single user memoryless channel. Especially, Gaarder and Wolf [8], Cover and Leung-Yan-Cheong [9], providing examples of the binary erasure MAC and the Gaussian MAC, respectively, showed that feedback will enlarge the capacity region of the 2-transmitter MAC. Several general achievable rate regions for the 2-transmitter MAC with noiseless feedback (MAC-FB) were established by Cover and Leung [10], Carleial [11], Bross and Lapidoth [12], Venkataramanan and Pradhan [13]; a dependence balance based outer bound was provided in [14]; and constructive coding strategies that exploit feedback were discussed in [15–18]. Nevertheless, the capacity region of the 2-transmitter MAC-FB remains unknown in general, except for a special class, say class $\mathcal{D}$, in which at least one input is a function of the output and the other input [19].

1.3 Secrecy over MAC: transmitting confidential information

Nowadays, general awareness of user privacy in society has increased, leading to a greater focus on the protection of user metadata and communication. Inspired by the pioneering works of Wyner [20] and Csiszár and Körner [21] that studied the information theoretic secrecy for a point-to-point communication in the presence of an external eavesdropper, MAC with an external eavesdropper was

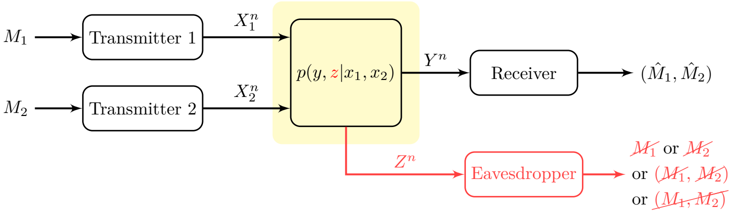

Fig. 2. 2-transmitter DM-MAC with an external eavesdropper.

first introduced in [22]. In particular, [22] focused on a K-transmitter Gaussian MAC with a degraded external eavesdropper and established several achievable rate regions subject to pre-specified secrecy levels; while a later work [23] extends the results of [22] to the general Gaussian MAC and general Gaussian two-way channel (TWC).

For the discrete case, a 2-transmitter DM-MAC with an external eavesdropper was considered in [24]. Note that the model in [24] took into account the generalized feedback that may enable cooperation between transmitters; and, a *joint* secrecy constraint (i.e., information leakage rate from *both* messages to the eavesdropper is made vanishing) was imposed at the eavesdropper. Achievable secrecy rate regions were derived in [24]. Additional studies include [25] and [26] that investigated MAC with a stronger secrecy criteria (i.e., the *amount* of information leakage from both messages to the eavesdropper is made vanishing). Nevertheless, for the general 2-transmitter DM-MAC (e.g., with an eavesdropper not necessarily degraded), the *joint* secrecy capacity region still remains open.

2 Secure communication over 2-transmitter DM-MAC

2.1 System model

In this paper, we focus on the 2-transmitter DM-MAC with an external eavesdropper, the model of which is shown in Fig. 2. As its name suggests, it consists of 2 transmitters, one legitimate receiver, and one passive eavesdropper, which is defined by the transition probability $p(y, z|x_1, x_2)$. The transmitter i, aims to send message m_i, to the legitimate receiver, where $i \in \{1, 2\}$. Define rate R_i at transmitter i by

$$R_i = \frac{1}{n} H(M_i), \quad \text{for } i = 1, 2, \tag{1}$$

where $H(\cdot)$ is the entropy function [27]. Suppose that x_i^n is the channel input at transmitter i, and the channel outputs at the legitimate receiver and eavesdropper are y^n and z^n, respectively. By the *discrete memoryless* nature of the channel (without any feedback), we have

$$p(y^n, z^n|x_1^n, x_2^n) = \prod_{i=1}^{n} p(y_i, z_i|x_{1,i}, x_{2,i}). \tag{2}$$

Over such a channel model, the goal is to achieve a reliable and secure communication. To do it, we first define a secrecy code. More specifically, a $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code $\mathcal{C}_n$ for the 2-transmitter DM-MAC consists of

- 2 message sets $\mathcal{M}_1, \mathcal{M}_2$, where $m_i \in \mathcal{M}_i = [1 : 2^{nR_i}]$ for $i = 1, 2$;
- 2 encoders each assigning a codeword x_i^n to message m_i for $i = 1, 2$; and
- 1 decoder at the legitimate receiver that declares an estimate of (m_1, m_2), say $(\hat{m}_1, \hat{m}_2)$, to the received sequence y^n.

2.2 System requirements

Reliability at the legitimate receiver: Define the *average probability of decoding error* at the legitimate receiver by

$$P_e^n(\mathcal{C}_n) = \frac{1}{2^{n[R_1+R_2]}} \Pr\left\{ \bigcup_{i\in\{1,2\}} \{m_i \neq \hat{m}_i\} | \mathcal{C}_n \right\}. \tag{3}$$

Note that $P_e^n(\mathcal{C}_n) = \Pr\left\{\{M_1 \neq \hat{M}_1\} \bigcup \{M_2 \neq \hat{M}_2\} | \mathcal{C}_n\right\}$ if M_1, M_2 are uniformly distributed over their corresponding message sets.

Secrecy against the eavesdropper: Suppose that the transmitters are aware of the presence of the passive eavesdropper. Briefly, we have the following scenarios:

- The secrecy of the messages is not of concern to both transmitters; or,
- The secrecy of the respective message is of concern only to one transmitter. In more details, we have the following possibilities:
  - Secrecy of M_1 is required, but not M_2. We dfine the *information leakage rate* of M_1 from transmitter 1 to the eavesdropper by

    $$R_{L,\{1\}}(\mathcal{C}_n) = \frac{1}{n} I(M_1; Z^n | \mathcal{C}_n), \tag{4}$$

    where $I(\cdot)$ is the mutual information function [27].
  - Secrecy of M_2 is required, but not M_1. We define the *information leakage rate* of M_2 from transmitter 2 to the eavesdropper by

    $$R_{L,\{2\}}(\mathcal{C}_n) = \frac{1}{n} I(M_2; Z^n | \mathcal{C}_n). \tag{5}$$

- The secrecy of the messages is of concern to both transmitters. In this scenario, we have the following two cases:
  - From end user point of view, each transmitter only cares about the secrecy of its own message. This is equivalent to limit

    $$R_{L,\{1\},\{2\}}(\mathcal{C}_n) = R_{L,\{1\}}(\mathcal{C}_n) + R_{L,\{2\}}(\mathcal{C}_n). \tag{6}$$

    In this case, the correlation information between M_1 and M_2 may be leaked to the eavesdropper, say $M_1 \oplus M_2$ but not M_1, M_2 individually.

- From the system designer's perspective, the information leakage of M_1, M_2 is considered jointly by defining

$$R_{L,\{1,2\}}(\mathcal{C}_n) = \frac{1}{n} I(M_1, M_2; Z^n|\mathcal{C}_n). \tag{7}$$

  Imposing a limit on (7) implies limits on (4), (5) and (6) as well. As the limit becomes arbitrarily small, the correlation information between M_1 and M_2 may not be leaked to the eavesdropper in this case.

Cooperative or competitive transmission strategy at the transmitters: If there is no secrecy concern, the transmitters are competitive since they have to share the same channel resource. However, in case of a secure communication, the transmitters can be also cooperative since the transmission of one user essentially helps to hide the other user's message from the eavesdropper. Especially in case that only one message is required to be kept confidential from the eavesdropper, the other transmitter may

- use a deterministic encoder (which is conventionally used for DM-MAC without secrecy), competing for the channel resource (i.e., being competitive); or,
- use a stochastic encoder (which is common in achieving information theoretic secrecy), helping to hide other transmitter' message from the eavesdropper (i.e., being cooperative).

Considering that secrecy does not come for free, we assume that the transmitter who demands secrecy for its message, will use the stochastic encoder. Thus,

- if there is no secrecy requirement from both transmitters, then both use deterministic encoders, i.e., being competitive;
- if only one transmitter demands secrecy for its message, then it uses the stochastic encoder, i.e., being cooperative; while, the other transmitter could be either cooperative or competitive;
- if both transmitters demand secrecy for their messages, (including both the individual or joint secrecy), then both use the stochastic encodes, i.e., being cooperative.

We remark here that the deterministic encoder can be considered as a special case of the stochastic encoder. Therefore, for the transmitter, being cooperative will be as least as good as being competitive in achieving the desired transmission rates. Recall the fact that being competitive is sufficient in achieving the capacity region in case of no secrecy constraints, i.e., being cooperative does not provide any gain in the reliable communication over MAC. However, the problem of our interest is, if there is any gain in secure communication over MAC for being cooperative; and if yes, how much is the gain?

2.3 System throughput

If there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes $\{\mathcal{C}_n\}$ such that

$$P_e^n(\mathcal{C}_n) \leq \epsilon_n \quad \text{and} \quad \lim_{n\to\infty} \epsilon_n = 0, \tag{8}$$

$$R_L(\mathcal{C}_n) \leq \tau_n \quad \text{and} \quad \lim_{n\to\infty} \tau_n = 0, \tag{9}$$

Table 1. 2-transmitter DM-MAC with an external eavesdropper: under different secrecy constraints with both transmitters being cooperative.

	Rate region	Input distribution
$\mathcal{C}$: No secrecy [27, Theorem 4.3]	$R_1 \leq I(X_1;Y\|X_2,Q)$ $R_2 \leq I(X_2;Y\|X_1,Q)$ $R_1 + R_2 \leq I(X_1,X_2;Y\|Q)$	$(Q,X_1,X_2) \sim p(q)p(x_1\|q)p(x_2\|q)$
$\mathcal{R}_{\{1\}}$: $\{1\}-$ collective secrecy $\frac{1}{n}I(M_1;Z^n) \to 0$ [28, Theorem 1]	$R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min \left\{ \begin{array}{l} I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_2;Z\|Q) \leq I(V_2;Y\|V_1,Q)$
$\mathcal{R}_{\{2\}}$: $\{2\}-$ collective secrecy $\frac{1}{n}I(M_2;Z^n) \to 0$ [28, Theorem 1]	$R_1 \leq I(V_1;Y\|V_2,Q)$ $R_2 \leq \min \left\{ \begin{array}{l} I(V_2;Y\|V_1,Q) - I(V_2;Z\|Q) \\ I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_1;Z\|Q) \leq I(V_1;Y\|V_2,Q)$
$\mathcal{R}_{\{1\},\{2\}}$: Individual secrecy [29, Theorem 1] $\frac{1}{n}I(M_1;Z^n) \to 0$ $\frac{1}{n}I(M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q) - I(V_2;Z\|Q)$ $\max\{R_1,R_2\} \leq I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q)$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1;Z\|Q) - I(V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$
$\mathcal{R}_{\{1,2\}}$: $\{1,2\}-$ collective secrecy i.e., joint secrecy [29, Theorem 2] $\frac{1}{n}I(M_1,M_2;Z^n) \to 0$	$R_1 \leq I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,T) - I(V_2;Z\|Q)$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q)$	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$

then the rate pair (R_1, R_2) is said to be *achievable under the secrecy constraint defined by (9)*. Note that (8) is the *reliability constraint*; and (9) is the *secrecy constraint*. In particular, if $R_L(\mathcal{C}_n)$ in (9) is defined by (4), or (5), or (7), it corresponds to the $\mathcal{S}$-collective secrecy that is introduced in [28], for $\mathcal{S}$ being $\{1\}, \{2\}$ or $\{1, 2\}$, respectively. More specifically, (R_1, R_2) is said to be

1) $\{1\}$-collective secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (4);
2) $\{2\}$-collective secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (5);
3) individual secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (6);
4) $\{1, 2\}$-collective or joint secrecy achievable, if $R_L(\mathcal{C}_n)$ is defined by (7).

Clearly, for given reliability and secrecy constraints, the union of all the achievable rate pairs gives the respective achievable rate regions, providing fundamental limits on the system throughput.

3 Discussions

3.1 Impact of different secrecy requirements

Recall that $\mathcal{S}$-collective secrecy is studied in [28], which includes all the instances of the above discussed secrecy requirements except the individual secrecy. Nevertheless, the individual secrecy has been studied in [29] together with joint secrecy for the 2-transmitter DM-MAC with an external eavesdropper. In addition, the capacity region in case of no secrecy constraint has been characterized [1] (or see [27, Theorem 4.3]). Therefore, we could give a rather complete review on the achievable rate regions under different secrecy constraints.

For a fair comparison, we consider the optimistic case that both transmitter are cooperative in all scenarios. In Table 1, we provide the respective regions corresponding to the 5 different secrecy strengths (in which 4 secrecy constraints are as discussed above and the additional one is no secrecy constraint). In particular, we denote the $\mathcal{S}$-collective secrecy region to be $\mathcal{R}_{\mathcal{S}}$ for $\mathcal{S} \in \{1, 2\}$, $\mathcal{S} \neq \emptyset$, $\mathcal{C}$ for the case of no secrecy, and $\mathcal{R}_{\{1\},\{2\}}$ for the individual secrecy rate region.

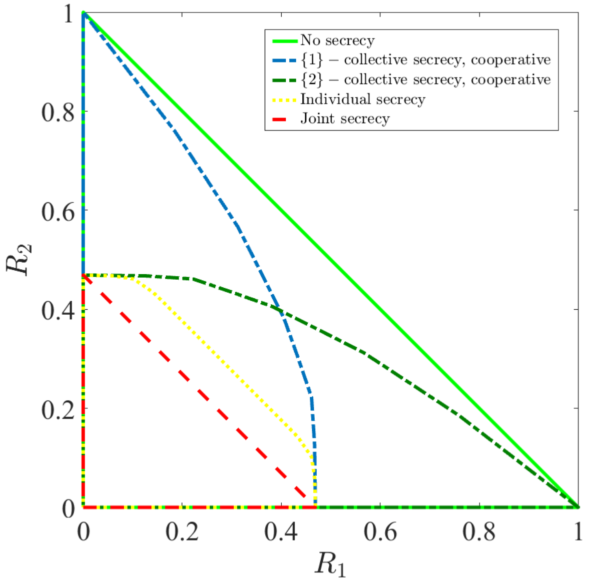

Fig. 3. Achievable rate regions for a binary multiplier 2-transmitter MAC with a degraded eavesdropper, with different secrecy constraints but cooperative transmitters. See [28, Fig. 2(b)].

Moreover, a numerical illustration is provided in Fig. 3, where we plotted all these regions for a 2-transmitter DM-MAC with an external eavesdropper, where the channel from (X_1, X_2) to Y is a binary multiplier MAC, and Z is a degraded version of Y through a binary symmetric channel (BSC) with crossover probability $p = 0.1$. Note that V_1, V_2 are taken as binary for the calculations. Not surprisingly, we observe that $\mathcal{R}_{\{1,2\}} \subseteq \mathcal{R}_{\{1\},\{2\}} \subseteq \mathcal{R}_{\{1\}}$ or $\mathcal{R}_{\{2\}} \subseteq \mathcal{C}$, where $\mathcal{R}_{\{1,2\}}$ is enclosed by (red) dashed lines; $\mathcal{R}_{\{1\},\{2\}}$ by (yellow) dotted lines; $\mathcal{R}_{\{1\}}$ and $\mathcal{R}_{\{2\}}$ by dash-dotted lines (blue for $\mathcal{R}_{\{1\}}$ and forest-green for $\mathcal{R}_{\{2\}}$, respectively); and $\mathcal{C}$ by (green) solid lines. Note that the inclusion relation of these regions is due to the correspondingly relaxed secrecy strengths. That is, more stringent is the secrecy requirement, smaller is the correspondingly achievable secrecy region. Another interesting observation is that $\mathcal{R}_{\{1\},\{2\}} \subset \mathcal{R}_{\{1\}} \cap \mathcal{R}_{\{2\}}$. In other words, $\mathcal{R}_{\{1\},\{2\}} = \mathcal{R}_{\{1\}} \cap \mathcal{R}_{\{2\}}$ does not hold. This implies that there are rate pairs achievable for either the secrecy of M_1 or the secrecy of M_2, but not the secrecy of M_1 and secrecy of M_2 simultaneously (i.e., individual secrecy).

3.2 Impact of transmitters being cooperative or competitive

Recall the fact that being cooperative does not provide any gain in the reliable communication over MAC (i.e., no secrecy requirement). However, we wonder if it is still the case in the secure communication over MAC.

Table 2. 2-transmitter DM-MAC with an external eavesdropper: $\{1\}$-collective secrecy.

	Competitive Transmitter 2, [28, (10) in Theorem 1]	Cooperative Transmitter 2, [28, (11) in Theorem 1]
Rate region	$R_2 \geq I(V_2;Z\|Q)$ $R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min \left\{ \begin{array}{l} I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q) \end{array} \right\}$ $R_1 - R_2 \leq I(V_1;Y\|V_2,Q) - I(V_1,V_2;Z\|Q)$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1;Z\|Q)$	$R_2 \leq I(V_2;Y\|V_1,Q)$ $R_1 \leq \min \left\{ \begin{array}{l} I(V_1;Y\|V_2,Q) - I(V_1;Z\|Q) \\ I(V_1,V_2;Y\|Q) - I(V_1,V_2;Z\|Q) \end{array} \right\}$ $R_1 + R_2 \leq I(V_1,V_2;Y\|Q) - I(V_1;Z\|Q)$
Input distribution	$(Q,V_1,V_2,X_1,X_2) \sim p(q)\prod_{i=1}^{2} p(v_i\|q)p(x_i\|v_i)$ such that $I(V_2;Z\|Q) \leq I(V_2;Y\|V_1,Q)$	

Consider the specific case that transmitter 1 would like to keep its message secret from the eavesdropper; while transmitter 2 not. That is, transmitter 1 uses a stochastic encoder for the purpose of secrecy of M_1; while transmitter 2 may take a conventional deterministic encoder for being competitive for the same channel resource; or take a stochastic encoder for being cooperative to help to hide M_1 from the eavesdropper. According to [28, Theorem 1], we have two achievable regions corresponding to these two different transmission strategies at transmitter 2, and we provide them in Table 2.

Moreover, a numerical illustration is provided in Fig. 4, where we show the advantage of transmitter 2 being cooperative (in obtaining a larger secrecy rate region) by a concrete example. Consider the 2-transmitter DM-MAC with an external eavesdropper, where the channel from (X_1, X_2) to Y is a binary input adder MAC, and Z is a degraded version of Y with $p(z|y) = 1 - p$ for $z = y$ and $p(z|y) = p$ for $z = y + 1 \pmod 3$, where $p = 0.1$. In Fig. 4, we depict the respective achievable regions (with binary V_1, V_2 for the calculations), where the one enclosed by (magenta) dotted lines is for the case of transmitter 2 being competitive; and the one enclosed by (blue) dash-dotted lines is for the case of transmitter 2 being cooperative. The capacity region (without secrecy constraint) is also plotted for reference purpose, which is enclosed by the (green) solid lines.

As one can see in Fig. 4, in case of transmitter 2 being cooperative, the region is strictly larger than the case of transmitter 2 being competitive. In particular, a big gap in the achievable secret rate R_1 can be observed at $R_2 = 0$. The gap indicates that transmitter 2 can indeed help the secret transmission of transmitter 1 by sending random signals to jam the eavesdropper. (This is similar to the cooperative jamming observed in the Gaussian scenario [23], but as its counterpart in the discrete setting.) Even in case that transmitter 2 uses a deterministic encoder, its transmission at low rates to some extent, could help transmitter 1 to achieve a larger secrecy rate. However, the advantage of using cooperative transmission strategy at transmitter 2, diminishes or even vanishes especially when R_2 is at high rates. This is because of the bounded sum rate capacity, due to the fact that the same channel resource is shared by both transmitters. This observation provides interesting insights into the competitive yet cooperative relationship between the transmitters in a secure communication, unlike their simple competitive relationship in a reliable communication.

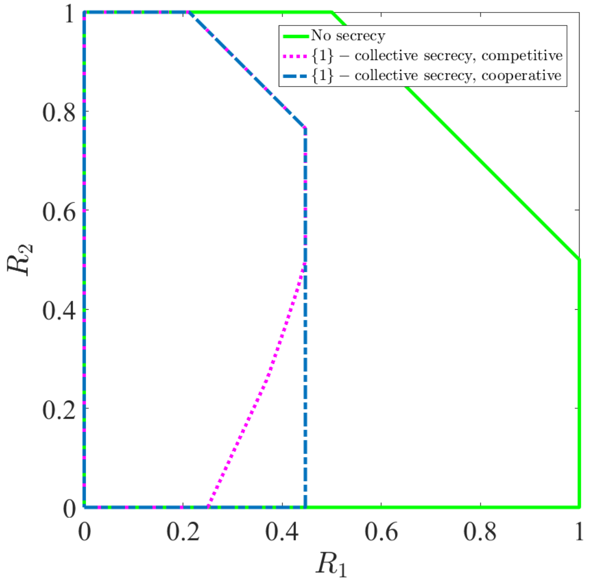

Fig. 4. Achievable rate regions for a binary input adder 2-transmitter MAC with a degraded eavesdropper, where transmitter 1 demands the secrecy but not transmitter 2. See [28, Fig. 2(a)].

4 Concluding remarks

In this paper, we review the secrecy results obtained for the 2-transmitter multiple access channel with an external eavesdropper. In particular, we discuss 5 secrecy strengths, from both the end user's perspective and the system designer's perspective. Both theoretical and numerical results are presented to show the impact of different secrecy requirements on the respective achievable rate regions (or in other words, the price paid for the required secrecy). Moreover, we look into the case where either competitive or cooperative transmission strategies can be employed at the transmitter who does not demand secrecy for its message. Unlike the reliable communication scenario where secrecy is not concerned, and it does not make any difference for the transmitters for being either cooperative or competitive, we show that in a secure communication over MAC, being cooperative can enlarge the corresponding achievable secrecy region.

2-transmitter multiple access channel is a rather simple model, which has been extensively investigated and which results provide insights into the open problems in multi-use communications. For more extended and general results, one can refer to [28], where a class of collective secrecy was introduced and studied in the multiple access channel with arbitrarily many transmitters.

References

1. R. Ahlswede: Multi-way communication channels. *Akadémiai Kiadó*, (1973).
2. H. H.-J. Liao: Multiple Access Channels. Honolulu: *Ph.D. Dissertation*, University of Hawaii, (1972).
3. D. Slepian and J. K. Wolf: A coding theorem for multiple access channels with correlated sources. *Bell Syst. Tech. J.*, **52**(7), 1037–1076 (1973).
4. Te Sun Han: The capacity region of general multiple-access channel with certain correlated sources. *Information and Control*, **40**(1), 37-60 (1979).
5. T. Cover, A. Gamal, and M. Salehi: Multiple access channels with arbitrarily correlated sources. *IEEE Trans. Inf. Theory*, **26**(6), 648–657 (1980).
6. T. M. Cover: Some advances in broadcast channels. *Advances in Communication Systems*, **4**, 229 – 260 (1975).
7. E. van der Meulen: A survey of multi-way channels in information theory: 1961-1976. *IEEE Trans. Inf. Theory*, **23**(1), 1–37 (1977).
8. N. Gaarder and J. Wolf: The capacity region of a multiple-access discrete memoryless channel can increase with feedback. *IEEE Trans. Inf. Theory*, **21**(1), 100–102 (1975).
9. T. M. Cover and S. K. Leung-Yan-Cheong: A scheme for enlarging the capacity region of multiple-access channels using feedback. Dept. of Stat., Stanford Univ., Stanford, CA, *Tech. Rep. 17*, (1976).
10. T. Cover and C. Leung: An achievable rate region for the multiple-access channel with feedback. *IEEE Trans. Inf. Theory*, **27**(3), 292–298 (1981).
11. A. Carleial: Multiple-access channels with different generalized feedback signals. *IEEE Trans. Inf. Theory*, **28**(6), 841–850 (1982).
12. S. I. Bross and A. Lapidoth: An improved achievable region for the discrete memoryless two-user multiple-access channel with noiseless feedback. *IEEE Trans. Inf. Theory*, **51**(3), 811–833 (2005).
13. R. Venkataramanan and S. S. Pradhan: A new achievable rate region for the multiple-access channel with noiseless feedback. *IEEE Trans. Inf. Theory*, **57** (12), 8038–8054 (2011).
14. A. P. Hekstra and F. M. J. Willems: Dependence balance bounds for single-output two-way channels. *IEEE Trans. Info. Theory*, **35**(1), 44–53 (1989).
15. A. J. Vinck: Constructive superposition coding for the binary erasure multiple access channel. *Proc. 4th Symp. Information Theory in Benelux*, 179-188 (1983).
16. A.J. Vinck, W.L.M. Hoeks and K.A. Post: On the capacity of the two-user M-ary multiple-access channel with feedback. *IEEE Trans. Info. Theory*, **31** (4), 540-543 (1985).
17. A. J. Han Vinck: On the multiple access channel. *Proc. of the 2nd Joint Swedish-Soviet Int. Workshop on Info. Theory*, **54** (1), 24-29 (1985).
18. G. Kramer: Feedback strategies for a class of two-user multiple-access channels. *IEEE Trans. Inf. Theory*, **45** (6), 2054–2059 (1999).
19. F. Willems: The feedback capacity region of a class of discrete memoryless multiple access channels. *IEEE Trans. Inf. Theory*, **28** (1), 93–95 (1982).
20. A. D. Wyner: The wire-tap channel. *Bell Syst. Tech. J.*, **54**(8), 1355–1387 (1975).
21. I. Csiszár and J. Körner: Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, **24**(3), 339–348 (1978).
22. E. Tekin and A. Yener: The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, **54**(12), 5747–5755 (2008).

23. E. Tekin and A. Yener: The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, **54**(6), 2735–2751 (2008).
24. X. Tang, R. Liu, P. Spasojevic, and H. Poor: Multiple access channels with generalized feedback and confidential messages. In: *Proc. ITW 2007*, (2007).
25. M. Yassaee and M. Aref: Multiple access wiretap channels with strong secrecy. In: *Proc. ITW 2010*, Dublin, (2010).
26. M. Wiese and H. Boche: Strong secrecy for multiple access channels. In *Information Theory, Combinatorics, and Search Theory*, LNCS. Springer Berlin Heidelberg, **7777**, 71–122 (2013).
27. A. E. Gamal and Y.-H. Kim: *Network Information Theory.* New York, NY, USA: Cambridge University Press, (2012).
28. Y. Chen, O. Ozan Koyluoglu and A. J. Han Vinck: Collective secrecy over the K-transmitter multiple access channel. *IEEE Transactions on Information Forensics and Security*, **13** (9), 2279–2293 (2018).
29. Y. Chen, O. Ozan Koyluoglu and A. J. Han Vinck: On secure communication over the multiple access channel, In *Proc. 2016 IEEE International Symposium on Information Theory and Its Applications (ISITA)*, 355–359 (2016).