Secrecy Capacity Region of the Degraded Compound Multi-receiver Wiretap Channel

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu *ulukus@umd.edu*

***Abstract*— We study the degraded compound multi-receiver wiretap channel, which consists of two groups of users and a group of eavesdroppers. We consider two different communication scenarios. In both scenarios, the transmitter sends two confidential messages, one for each group of users. In the first scenario, both messages need to be kept confidential from the eavesdroppers. For this scenario, we assume that there is only one eavesdropper. We obtain the secrecy capacity region for the general discrete memoryless channel model, the parallel channel model, and the Gaussian parallel channel model. For the Gaussian multi-input multi-output (MIMO) channel model, we obtain the secrecy capacity region when there is only one user in the second group. In the second scenario, the message sent to the first group of users needs to be kept confidential from both the second group of users and eavesdroppers, whereas the message sent to the second group of users needs to be kept confidential only from the eavesdroppers. For this scenario, we do not put any restriction on the number of eavesdroppers. We find the secrecy capacity region for the general discrete memoryless channel model, the parallel channel model, and the Gaussian parallel channel model. For the Gaussian MIMO channel model, we obtain the secrecy capacity region when there is only one user in the second group.**

I. Introduction

In recent years, multi-user versions of the wiretap channel [1], [2] have attracted a considerable amount of research interest; see for example references [3-21] in [3]. Among all these extensions, two natural extensions of the wiretap channel to the multi-user setting are particularly of interest here: *secure broadcasting* and *compound wiretap channels*.

Secure broadcasting refers to the situation where a transmitter wants to communicate with several legitimate receivers confidentially in the presence of an external eavesdropper. We call this channel model the *multi-receiver wiretap channel*. Since the underlying channel model without an eavesdropper is the broadcast channel, which is not understood to the full extent even for the two-user case, most works on *secure broadcasting* have focused on some special classes of multi-receiver wiretap channels, where these classes are identified by certain degradation orders [4]–[7]. In particular, [5]–[7] consider the *degraded* multi-receiver wiretap channel. In [5], the secrecy capacity region of the degraded multi-receiver wiretap channel is derived for the two-user case, and in [6], [7], the secrecy capacity region is established for an arbitrary number of legitimate users. The importance of this result lies in the facts that the Gaussian multi-receiver wiretap channel belongs to this class, and the secrecy capacity region of the degraded multi-receiver wiretap channel serves as a crucial step in establishing the secrecy capacity region of the Gaussian multi-input multi-output (MIMO) multi-receiver wiretap channel [3], though the latter channel is not necessarily degraded. In [3], besides proving the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel, we also present new optimization results regarding extremal properties of Gaussian random vectors, which we generalize here.

Another extension of the wiretap channel that we are particularly interested in here, is the *compound wiretap channel*. In compound wiretap channels, there are a finite number of channel states determining the channel transition probability. The channel takes a certain fixed state for the entire duration of the transmission, and the transmitter does not have any knowledge about the channel state realization. Thus, the aim of the transmitter is to ensure the secrecy of messages irrespective of the channel state realization. In addition to this definition, the compound wiretap channel admits another interpretation. Consider the multi-receiver wiretap channel with several legitimate users and many eavesdroppers, where the transmitter wants to send a common confidential message to legitimate users while keeping all of the eavesdroppers totally ignorant of the message. Since each eavesdropper and legitimate user pair can be regarded as a different channel state realization, this channel is equivalent to a compound wiretap channel. Therefore, one can interpret a compound wiretap channel as multicasting a common confidential message to several legitimate receivers in the presence of one or more eavesdroppers [8]. In this work, we mostly refer to this interpretation, which is also the reason why we classify the compound wiretap channel as an extension of the wiretap channel to a multi-user setting.

Keeping this interpretation in mind, the works which implicitly study the compound wiretap channel are [4], [6], [7], [9]–[11]. In [9], [10], parallel wiretap channels with two sub-channels, where each sub-channel is being wiretapped by a different eavesdropper, is studied. Reference [11] considered the fading wiretap channel with many receivers, and in [4], [6], [7], the transmission of a common confidential message to many legitimate receivers in the presence of a single

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

eavesdropper is studied. Reference [8] considers the general discrete compound wiretap channel and provides inner and outer bounds for the secrecy capacity. Moreover, [8] establishes the secrecy capacity of the degraded compound wiretap channel as well as its degraded Gaussian MIMO instance. Reference [12] obtains the secrecy capacity of a class of non-degraded Gaussian parallel compound wiretap channels.

Here, we consider compound broadcast channels from a secrecy point of view, which enables us to study the *secure broadcasting* problem over *compound channels*. We note that the current literature regarding the compound wiretap channel considers the transmission of only one confidential message, whereas here, we study the transmission of multiple confidential messages, where each of these messages needs to be delivered to a different group of users in perfect secrecy. Hereafter, we call this channel model the *compound multi-receiver wiretap channel* to emphasize the presence of more than one confidential message. The compound multi-receiver wiretap channel we study here consists of two groups of users and a group of eavesdroppers, see Figure 1. We focus on a class of compound multi-receiver wiretap channels which exhibits a certain degradation order. In particular, we assume that there exist two fictitious users. The first fictitious user is degraded with respect to any user from the first group, and any user from the second group is degraded with respect to the first fictitious user. There exists a similar degradedness structure for the second fictitious user in the sense that it is degraded with respect to any user from the second group, and any eavesdropper is degraded with respect to it. Without eavesdroppers, this channel model reduces to the degraded compound broadcast channel in [13]. Adapting their terminology, we call our channel model the *degraded compound multi-receiver wiretap channel*. Here, we consider the general discrete memoryless channel model as well as its specializations to the parallel channel model, the Gaussian parallel channel model, and the Gaussian MIMO channel model. We study two different communication scenarios for each version of the degraded compound multi-receiver channel model.

In the first scenario, see Figure 2, the transmitter wants to send a confidential message to users in the first group, and a different confidential message to users in the second group, where both messages need to be kept confidential from the eavesdroppers. For this scenario, we assume that there exists only one eavesdropper and obtain the secrecy capacity region in a single-letter form. While obtaining this result, the presence of the fictitious user between two groups of users plays a crucial role in the converse proof by providing a conditional independence structure in the channel, which enables us to define an auxiliary random variable that yields a tight outer bound. After establishing single-letter expressions for the secrecy capacity region, we consider the parallel channel model. For the parallel channel model, we obtain the secrecy capacity region in a single-letter form as well. Though the general discrete memoryless channel model encompasses the parallel channel model as a special case, we still need a converse proof to establish the optimality of independent signalling in each sub-channel. After we obtain the secrecy capacity region for the parallel channel model, we evaluate this single-letter description of the secrecy capacity region for the Gaussian case, which is tantamount to finding the optimal joint distribution of auxiliary random variables and channel inputs, which is shown to be Gaussian. We accomplish this by using Costa's entropy power inequality [14]. Finally, we consider the Gaussian MIMO channel model, and evaluate its secrecy capacity region when there is only one user in the second group. We show the optimality of a jointly Gaussian distribution for auxiliary random variables and channel inputs by generalizing our optimization results in [3].

In the second scenario, see Figure 3, the transmitter wants to send a confidential message to users in the first group which needs to be kept confidential from users in the second group and eavesdroppers. Moreover, the transmitter sends a different confidential message to users in the second group, which needs to be kept confidential from the eavesdroppers. If there were only one user in each group and one eavesdropper, this channel model would reduce to the channel model that was studied in [15]. However, here, there are an arbitrary number of users in each group and an arbitrary number of eavesdroppers. Hence, our model can be viewed as a generalization of [15] to a compound setting. Adapting their terminology, we call this channel model the *degraded compound multi-receiver wiretap channel with layered messages*. We first obtain the secrecy capacity region in a single-letter form for a general discrete memoryless setting, where again the presence of fictitious users plays a key role in the converse proof. Next, we consider the parallel channel model and establish its secrecy capacity region in a single-letter form. In this case as well, we provide the converse proof which is again necessary to show the optimality of independent signalling in each sub-channel. After we obtain the secrecy capacity region of the parallel channel model, we evaluate it for the Gaussian case by showing the optimality of a jointly Gaussian distribution for auxiliary random variables and channel inputs. For that purpose, we again use Costa's entropy power inequality [14]. Finally, we consider the Gaussian MIMO channel model, and evaluate its secrecy capacity region when there is only one user in the second group. To this end, we show that jointly Gaussian auxiliary random variables and channel inputs is optimal by extending our optimization results in [3].

II. System Model

We consider the degraded compound multi-receiver wiretap channel, see Figure 1, which consists of two groups of users and a group of eavesdroppers. There are K_1 users in the first group, K_2 users in the second group, and K_Z eavesdroppers. The channel is memoryless with a transition probability

$$p(y_1^1, \ldots, y_{K_1}^1, y_1^2, \ldots, y_{K_2}^2, z_1, \ldots, z_{K_Z}|x) \qquad (1)$$

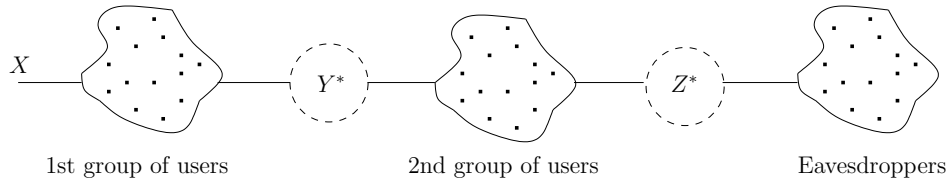

Fig. 1. The degraded compound multi-receiver wiretap channel.

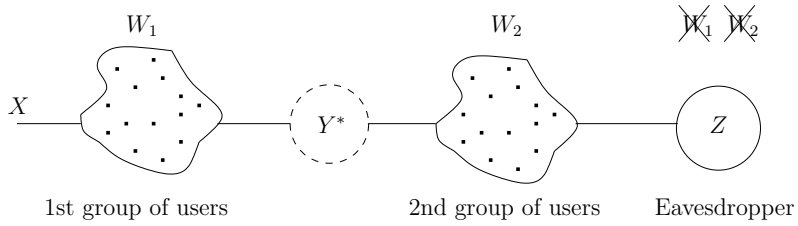

Fig. 2. The first scenario for the degraded compound multi-receiver wiretap channel.

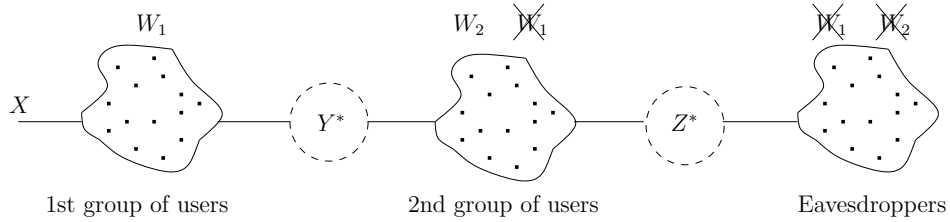

Fig. 3. The second scenario for the degraded compound multi-receiver wiretap channel.

where $X \in \mathcal{X}$ is the channel input, $Y_j^1 \in \mathcal{Y}_j^1$ is the channel output of the jth user in the first group, $j = 1, \ldots, K_1$, $Y_k^2 \in \mathcal{Y}_k^2$ is the channel output of the kth user in the second group, $k = 1, \ldots, K_2$, and $Z_t \in \mathcal{Z}_t$ is the channel output of the tth eavesdropper, $t = 1, \ldots, K_Z$.

We assume that there are two fictitious users with observations $Y^* \in \mathcal{Y}^*, Z^* \in \mathcal{Z}^*$ such that they satisfy the Markov chain

$$X \to Y_j^1 \to Y^* \to Y_k^2 \to Z^* \to Z_t, \quad \forall (j,k,t) \tag{2}$$

This Markov chain is the reason why we call this channel model the *degraded compound multi-receiver wiretap channel*. Actually, there is a slight inexactness in the terminology here because the Markov chain in (2) is more restrictive than the Markov chain

$$X \to Y_j^1 \to Y_k^2 \to Z_t, \quad \forall (j,k,t) \tag{3}$$

and it might be more natural to define the degradedness of the compound multi-receiver wiretap channel by the Markov chain in (3). However, in this work, we adapt the terminology of the previous work on compound broadcast channels [13], and call the channel satisfying (2) the degraded compound multi-receiver wiretap channel. Finally, we note that when there is no eavesdropper, this channel reduces to the degraded compound broadcast channel that was studied in [13].

A. Parallel Degraded Compound Multi-receiver Wiretap Channels

The parallel degraded compound multi-receiver wiretap channel, where each user's and each eavesdropper's channel consists of L independent sub-channels, i.e.,

$$Y_j^1 = (Y_{j1}^1, \ldots, Y_{jL}^1), \quad j = 1, \ldots, K_1 \tag{4}$$

$$Y_k^2 = (Y_{k1}^2, \ldots, Y_{kL}^2), \quad k = 1, \ldots, K_2 \tag{5}$$

$$Z_t = (Z_{t1}, \ldots, Z_{tL}), \quad t = 1, \ldots, K_Z \tag{6}$$

has the following overall transition probability

$$p(y_1^1, \ldots, y_{K_1}^1, y_1^2, \ldots, y_{K_2}^2, z_1, \ldots, z_{K_Z}|x) = \prod_{\ell=1}^{L} p(y_{1\ell}^1, \ldots, y_{K_1\ell}^1, y_{1\ell}^2, \ldots, y_{K_2\ell}^2, z_{1\ell}, \ldots, z_{K_Z\ell}|x_\ell) \tag{7}$$

where $X_\ell,\ \ell = 1, \ldots, L$, is the ℓth sub-channel's input. We again define the degradedness in a similar fashion. We call a parallel compound multi-receiver wiretap channel degraded, if there exist two sequences of random variables

$$Y^* = (Y_1^*, \ldots, Y_L^*) \tag{8}$$

$$Z^* = (Z_1^*, \ldots, Z_L^*) \tag{9}$$

which satisfy Markov chains

$$X_\ell \to Y_{j\ell}^1 \to Y_\ell^* \to Y_{k\ell}^2 \to Z_\ell^* \to Z_{t\ell}, \quad \forall (j,k,t,\ell) \tag{10}$$

B. Gaussian Parallel Degraded Compound Multi-receiver Wiretap Channels

The Gaussian parallel compound multi-receiver wiretap channel is defined by

$$\mathbf{Y}_j^1 = \mathbf{X} + \mathbf{N}_j^1, \quad j = 1, \ldots, K_1 \tag{11}$$

$$\mathbf{Y}_k^2 = \mathbf{X} + \mathbf{N}_k^2, \quad k = 1, \ldots, K_2 \tag{12}$$

$$\mathbf{Z}_t = \mathbf{X} + \mathbf{N}_t^Z, \quad t = 1, \ldots, K_Z \tag{13}$$

where all column vectors $\{\mathbf{Y}_j^1\}_{j=1}^{K_1}, \{\mathbf{Y}_k^1\}_{k=1}^{K_2}, \{\mathbf{Z}_t\}_{t=1}^{K_Z}$, $\mathbf{X}, \{\mathbf{N}_j^1\}_{j=1}^{K_1}, \{\mathbf{N}_k^2\}_{k=1}^{K_2}, \{\mathbf{N}_t^Z\}_{t=1}^{K_Z}$ are of dimensions $L \times 1$. $\{\mathbf{N}_j^1\}_{j=1}^{K_1}, \{\mathbf{N}_k^2\}_{k=1}^{K_2}, \{\mathbf{N}_t^Z\}_{t=1}^{K_Z}$ are Gaussian random vectors with diagonal covariance matrices $\{\mathbf{\Lambda}_j^1\}_{j=1}^{K_1}, \{\mathbf{\Lambda}_k^2\}_{j=1}^{K_2}, \{\mathbf{\Lambda}_t^Z\}_{t=1}^{K_Z}$, respectively. The channel input $\mathbf{X}$ is subject to a trace constraint as

$$E\left[\mathbf{X}^\top \mathbf{X}\right] = \mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \leq P \tag{14}$$

In this paper, we will be interested in Gaussian parallel *degraded* compound multi-receiver wiretap channels which means that the covariance matrices satisfy the following order

$$\mathbf{\Lambda}_j^1 \preceq \mathbf{\Lambda}_k^2 \preceq \mathbf{\Lambda}_t^Z, \quad \forall (j,k,t) \tag{15}$$

Since noise covariance matrices are diagonal, (15) implies

$$\Lambda_{j,\ell\ell}^1 \leq \Lambda_{k,\ell\ell}^2 \leq \Lambda_{t,\ell\ell}^Z, \quad \forall (j,k,t,\ell) \tag{16}$$

where $\Lambda_{j,\ell\ell}^1, \Lambda_{k,\ell\ell}^2, \Lambda_{t,\ell\ell}^Z$ denote the ℓth diagonal element of $\mathbf{\Lambda}_j^1, \mathbf{\Lambda}_k^2, \mathbf{\Lambda}_t^Z$, respectively.

The diagonality of noise covariance matrices also ensures the existence of diagonal matrices $\mathbf{\Lambda}_Y^*$ and $\mathbf{\Lambda}_Z^*$ such that

$$\mathbf{\Lambda}_j^1 \preceq \mathbf{\Lambda}_Y^* \preceq \mathbf{\Lambda}_k^2 \preceq \mathbf{\Lambda}_Z^* \preceq \mathbf{\Lambda}_t^Z, \quad \forall (k,j,t) \tag{17}$$

For example, we can select $\mathbf{\Lambda}_Y^*$ as $\Lambda_{Y,\ell\ell}^* = \max_{j=1,\ldots,K_1} \Lambda_{j,\ell\ell}^1$ which already satisfies (17) because of $\max_{j=1,\ldots,K_1} \Lambda_{j,\ell\ell}^1 \leq \min_{k=1,\ldots,K_2} \Lambda_{k,\ell\ell}^2$ which is due to (16). Similarly, we can select $\mathbf{\Lambda}_Z^*$. Thus, for Gaussian parallel compound multi-receiver channels, two ways of defining degradedness, i.e., (2) and (3), are equivalent due to the equivalence of (15) and (17).

C. Gaussian MIMO Degraded Compound Multi-receiver Wiretap Channels

The Gaussian MIMO degraded compound multi-receiver wiretap channel is defined by

$$\mathbf{Y}_j^1 = \mathbf{X} + \mathbf{N}_j^1, \quad j = 1, \ldots, K_1 \tag{18}$$

$$\mathbf{Y}_k^2 = \mathbf{X} + \mathbf{N}_k^2, \quad k = 1, \ldots, K_2 \tag{19}$$

$$\mathbf{Z}_t = \mathbf{X} + \mathbf{N}_t^Z, \quad t = 1, \ldots, K_Z \tag{20}$$

where all column vectors $\{\mathbf{Y}_j^1\}_{j=1}^{K_1}, \{\mathbf{Y}_k^2\}_{k=1}^{K_2}, \{\mathbf{Z}_t\}_{t=1}^{K_Z}$, $\mathbf{X}, \{\mathbf{N}_j^1\}_{j=1}^{K_1}, \{\mathbf{N}_k^2\}_{k=1}^{K_2}, \{\mathbf{N}_t^Z\}_{t=1}^{K_Z}$ are of dimensions $M \times 1$. $\{\mathbf{N}_j^1\}_{j=1}^{K_1}, \{\mathbf{N}_k^2\}_{k=1}^{K_2}, \{\mathbf{N}_t^Z\}_{t=1}^{K_Z}$ are Gaussian random vectors with covariance matrices $\{\mathbf{\Sigma}_j^1\}_{j=1}^{K_1}, \{\mathbf{\Sigma}_k^2\}_{k=1}^{K_2}, \{\mathbf{\Sigma}_t^Z\}_{t=1}^{K_Z}$, respectively. Unlike in the case of Gaussian parallel channels, these covariance matrices are not necessarily diagonal. The channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{21}$$

where $\mathbf{S} \succeq \mathbf{0}$.

In this paper, we study Gaussian MIMO *degraded* compound multi-receiver wiretap channels for which there exist covariance matrices $\mathbf{\Sigma}_Y^*$ and $\mathbf{\Sigma}_Z^*$ such that

$$\mathbf{\Sigma}_j^1 \preceq \mathbf{\Sigma}_Y^* \preceq \mathbf{\Sigma}_k^2 \preceq \mathbf{\Sigma}_Z^* \preceq \mathbf{\Sigma}_t^Z, \quad \forall (j,k,t) \tag{22}$$

We note that the order in (22), by which we define the degradedness, is more restrictive than the other possible order that can be used to define the degradedness, i.e.,

$$\mathbf{\Sigma}_j^1 \preceq \mathbf{\Sigma}_k^2 \preceq \mathbf{\Sigma}_t^Z, \quad \forall (j,k,t) \tag{23}$$

In [13], a specific numerical example is provided to show that the order in (23) subsumes the one in (22).

D. Comments on Gaussian MIMO Degraded Compound Multi-receiver Wiretap Channels

The first comment is about the covariance constraint in (21). Though it is more common to use a total power constraint, i.e., $\mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \leq P$, the covariance constraint in (21) is more general and it subsumes the total power constraint as a special case [16].

The second comment is about the assumption that the transmitter and all receivers have the same number of antennas, see (18)-(20). We can extend the channel definition in (18)-(20) to let the transmitter and receivers have different number of antennas as follows

$$\mathbf{Y}_j^1 = \mathbf{H}_j^1 \mathbf{X} + \mathbf{N}_j^1, \quad j = 1, \ldots, K_1 \tag{24}$$

$$\mathbf{Y}_k^2 = \mathbf{H}_k^2 \mathbf{X} + \mathbf{N}_k^2, \quad k = 1, \ldots, K_2 \tag{25}$$

$$\mathbf{Z}_t = \mathbf{H}_t^Z \mathbf{X} + \mathbf{N}_t^Z, \quad t = 1, \ldots, K_Z \tag{26}$$

where $\mathbf{H}_j^1, \mathbf{H}_k^2, \mathbf{H}_t^Z$ are of sizes $r_j^1 \times t, r_k^2 \times t, r_t^Z \times t$, respectively, and $\mathbf{X}$ is of size $t \times 1$. $\mathbf{Y}_j^1, \mathbf{Y}_k^2, \mathbf{Z}_t$ are of sizes $r_j^1 \times 1, r_k^2 \times 1, r_t^Z \times 1$, respectively. Gaussian noise vectors $\mathbf{N}_j^1, \mathbf{N}_k^2, \mathbf{N}_t^Z$ are assumed to have identity covariance matrices. In this case, observations of the fictitious users are

$$\mathbf{Y}^* = \mathbf{H}_Y^* \mathbf{X} + \mathbf{N}_Y^* \tag{27}$$

$$\mathbf{Z}^* = \mathbf{H}_Z^* \mathbf{X} + \mathbf{N}_Z^* \tag{28}$$

For the channel model in (24)-(26), we can define degradedness accordingly using the definition in [13] which states that $\mathbf{Y}_a = \mathbf{H}_a \mathbf{X} + \mathbf{N}_a$ is said to be degraded with respect to $\mathbf{Y}_b = \mathbf{H}_b \mathbf{X} + \mathbf{N}_b$, if there exists a matrix $\mathbf{D}$ such that $\mathbf{D}\mathbf{H}_b = \mathbf{H}_a$ and $\mathbf{D}\mathbf{D}^\top \preceq \mathbf{I}$. We note that the channel model in (24)-(26) subsumes the channel model in (18)-(20). Nevertheless, we note that if we establish the secrecy capacity region for the channel model defined by (18)-(20), we can also obtain the secrecy capacity region for the channel model defined by (24)-(26) using the analysis in [3], [13]. Thus, focusing on the channel model in (18)-(20) does not result in any loss of generality.

III. Problem Statement and Main Results

We consider two different communication scenarios for the degraded compound multi-receiver wiretap channel.

A. The First Scenario: External Eavesdroppers

In the first scenario, see Figure 2, the transmitter wants to send a confidential message to users in the first group and a different confidential message to users in the second group,

where both messages need to be kept confidential from the eavesdroppers. In this case, we assume that there is only one eavesdropper, i.e., $K_Z = 1$.

An $(n, 2^{nR_1}, 2^{nR_2})$ code for the first scenario consists of two message sets $\mathcal{W}_1 = \{1, \ldots, 2^{nR_1}\}, \mathcal{W}_2 = \{1, \ldots, 2^{nR_2}\}$, an encoder $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, one decoder for each legitimate user in the first group $g_j^1 : \mathcal{Y}_j^{1,n} \to \mathcal{W}_1,\ j = 1, \ldots, K_1$, and one decoder for each legitimate user in the second group $g_k^2 : \mathcal{Y}_k^{2,n} \to \mathcal{W}_2,\ k = 1, \ldots, K_2$. The probability of error, P_e^n, is defined as the maximum error probability among the legitimate users.

A secrecy rate pair (R_1, R_2) is said to be achievable if there exists an $(n, 2^{nR_1}, 2^{nR_2})$ code which has $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} I(W_1, W_2; Z^n) = 0 \tag{29}$$

where we dropped the subscript of Z_t since $K_Z = 1$. We note that (29) implies $\lim_{n\to\infty}(1/n)I(W_1; Z^n) = 0$ and $\lim_{n\to\infty}(1/n)I(W_2; Z^n) = 0$. From these definitions, it is clear that we are only interested in perfect secrecy rates of the channel. The secrecy capacity region is defined as the closure of all achievable secrecy rate pairs. A single-letter characterization of the secrecy capacity region is given as follows.

Theorem 1: The secrecy capacity region of the degraded compound multi-receiver wiretap channel is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} I(X; Y_j^1 | U, Z) \tag{30}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} I(U; Y_k^2 | Z) \tag{31}$$

where the union is over all (U, X) such that

$$U \to X \to Y_j^1 \to Y^* \to Y_k^2 \to Z \tag{32}$$

for any (j, k) pair.

We omit the proof of this theorem as well as the proofs of upcoming theorems due to lack of space. All of the proofs can be found in [17]. Showing the achievability is rather standard. We just comment about the converse proof, where the presence of the fictitious user with observation Y^* is critical. Essentially, it brings a conditional independence structure to the channel, which enables us to define the auxiliary random variable U, which, in turn, provides the converse proof.

As a side note, if we disable the eavesdropper by setting $Z = \phi$, the region in Theorem 1 reduces to the capacity region of the underlying degraded compound broadcast channel which was established in [13].

1) Parallel Degraded Compound Multi-Receiver Wiretap Channels: In the upcoming section, we will consider the Gaussian parallel degraded compound multi-receiver wiretap channel. For that purpose, here, we provide the secrecy capacity region of the parallel degraded compound multi-receiver wiretap channel in a single-letter form.

Theorem 2: The secrecy capacity region of the parallel degraded compound multi-receiver wiretap channel is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1 | U_\ell, Z_\ell) \tag{33}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2 | Z_\ell) \tag{34}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$ such that

$$U_\ell \to X_\ell \to Y_{j\ell}^1 \to Y_\ell^* \to Y_{k\ell}^2 \to Z_\ell \tag{35}$$

for any (j, k, ℓ) triple.

Though Theorem 1 provides the secrecy capacity region for a rather general channel model including the parallel degraded compound multi-receiver channel as a special case, we still need a converse proof to show that the region in Theorem 1 reduces to the region in Theorem 2 for parallel channels. In other words, we still need to show the optimality of independent signalling on each sub-channel.

2) Gaussian Parallel Degraded Compound Multi-Receiver Wiretap Channels: We now obtain the secrecy capacity region of the parallel Gaussian degraded compound multi-receiver wiretap channel. To that end, we need to evaluate the region given in Theorem 2, i.e., we need to find the optimal joint distribution $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. We first introduce the following theorem which will be instrumental in evaluating the region in Theorem 2 for Gaussian parallel channels.

Theorem 3: Let N_1, N^*, N_2, N_Z be zero-mean Gaussian random variables with variances $\sigma_1^2, \sigma_*^2, \sigma_2^2, \sigma_Z^2$, respectively, where

$$\sigma_1^2 \leq \sigma_*^2 \leq \sigma_2^2 \leq \sigma_Z^2 \tag{36}$$

Let (U, X) be an arbitrarily dependent random variable pair, which is independent of (N_1, N^*, N_2, N_Z), and the second-moment of X be constrained as $E\left[X^2\right] \leq P$. Then, for any feasible (U, X), we can find a $P^* \leq P$ such that

$$h(X + N_Z|U) - h(X + N^*|U) = \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_*^2} \tag{37}$$

and

$$h(X + N_Z|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_1^2} \tag{38}$$

$$h(X + N_Z|U) - h(X + N_2|U) \leq \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_2^2} \tag{39}$$

as long as (σ_1^2, σ_2^2) satisfy (36).

Costa's entropy-power inequality [14] plays a key role in the proof of this theorem.

We are now ready to establish the secrecy capacity region of the Gaussian parallel degraded compound multi-receiver wiretap channel.

Theorem 4: The secrecy capacity region of the Gaussian parallel degraded compound multi-receiver wiretap channel

is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} \frac{1}{2}\log\left(1+\frac{\beta_\ell P_\ell}{\Lambda^1_{j,\ell\ell}}\right) - \frac{1}{2}\log\left(1+\frac{\beta_\ell P_\ell}{\Lambda_{Z,\ell\ell}}\right) \tag{40}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} \frac{1}{2}\log\left(1+\frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda^2_{k,\ell\ell}}\right) - \frac{1}{2}\log\left(1+\frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda_{Z,\ell\ell}}\right) \tag{41}$$

where the union is over all $\{P_\ell\}_{\ell=1}^L$ such that $\sum_{\ell=1}^L P_\ell = P$ and $\bar{\beta}_\ell = 1-\beta_\ell \in [0,1],\ \ell = 1,\ldots,L$.

In Theorem 4, P_ℓ denotes the part of the total available power P which is devoted to the transmission in the ℓth sub-channel. Furthermore, β_ℓ denotes the fraction of the power P_ℓ of the ℓth sub-channel spent for the transmission to users in the first group.

3) Gaussian MIMO Degraded Compound Multi-receiver Wiretap Channels: We now obtain the secrecy capacity region of the Gaussian MIMO degraded compound multi-receiver wiretap channel. To that end, we need to evaluate the region given in Theorem 1. In other words, we need to find the optimal random variable pair $(U, \mathbf{X})$. We are able to do this when there is only one user in the second group, i.e., $K_2 = 1$. To prove this claim, we need the following theorem.

Theorem 5: Let $(\mathbf{N}_1, \mathbf{N}^*, \mathbf{N}_Z)$ be zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_1, \mathbf{\Sigma}^*, \mathbf{\Sigma}_Z$, respectively, where

$$\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}^* \preceq \mathbf{\Sigma}_Z \tag{42}$$

Let $(U, \mathbf{X})$ be arbitrarily dependent random vector, which is independent of $(\mathbf{N}_1, \mathbf{N}^*, \mathbf{N}_Z)$, and let the second moment of $\mathbf{X}$ be constrained as $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$. Then, for any feasible $(U, \mathbf{X})$, we can find a positive semi-definite matrix $\mathbf{K}^*$ such that $\mathbf{K}^* \preceq \mathbf{S}$, and it satisfies

$$h(\mathbf{X}+\mathbf{N}_Z|U) - h(\mathbf{X}+\mathbf{N}^*|U) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}^*|} \tag{43}$$

and

$$h(\mathbf{X}+\mathbf{N}_Z|U) - h(\mathbf{X}+\mathbf{N}_1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{44}$$

for any $\mathbf{\Sigma}_1$ satisfying the order in (42).

The proof of this theorem can be found in [3]. Using this theorem, we can establish the secrecy capacity region of the Gaussian MIMO degraded compound multi-receiver wiretap channel when $K_2 = 1$ as follows.

Theorem 6: The secrecy capacity region of the Gaussian MIMO degraded compound channel when $K_2 = 1$ is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}^1_j|}{|\mathbf{\Sigma}^1_j|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{45}$$

$$R_2 \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}^2|}{|\mathbf{K}+\mathbf{\Sigma}^2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{46}$$

where we dropped the subscript of $\mathbf{\Sigma}^2_k$ since $K_2 = 1$, and the union is over all positive semi-definite matrices $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$.

B. The Second Scenario: Layered Confidential Messages

In the second scenario, see Figure 3, the transmitter wants to send a confidential message to users in the first group which needs to be kept confidential from the second group of users and eavesdroppers. The transmitter also wants to send a different confidential message to users in the second group, which needs to be kept confidential from the eavesdroppers. As opposed to the first scenario, in this case, we do not put any restriction on the number of eavesdroppers. The situation where there is only one user in each group and one eavesdropper was investigated in [15]. Hence, this second scenario can be seen as a generalization of the model in [15] to a compound channel setting. Following the terminology of [15], we call this channel model the degraded compound multi-receiver wiretap channel with *layered messages*.

An $(n, 2^{nR_1}, 2^{nR_2})$ code for the degraded compound multi-receiver wiretap channel with *layered messages* consists of two message sets $\mathcal{W}_1 = \{1,\ldots,2^{nR_1}\}, \mathcal{W}_2 = \{1,\ldots,2^{nR_2}\}$ and an encoder $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, one decoder for each legitimate user in the first group $g^1_j : \mathcal{Y}^{1,n}_j \to \mathcal{W}_1,\ j = 1,\ldots,K_1$, and one decoder for each legitimate user in the second group $g^2_k : \mathcal{Y}^{2,n}_k \to \mathcal{W}_2,\ k = 1,\ldots,K_2$. The probability of error, P^n_e, is defined as the maximum error probability among the legitimate users.

A secrecy rate pair is said to be achievable if there exists an $(n, 2^{nR_1}, 2^{nR_2})$ code which has $\lim_{n\to\infty} P^n_e = 0$,

$$\lim_{n\to\infty} \frac{1}{n} I(W_2; Z^n_t) = 0, \quad t = 1,\ldots,K_Z \tag{47}$$

and

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; Y^{2,n}_k | W_2) = 0, \quad k = 1,\ldots,K_2 \tag{48}$$

We note that these two secrecy conditions imply that $\lim_{n\to\infty} \frac{1}{n} I(W_1, W_2; Z^n_t) = 0, \quad t = 1,\ldots,K_Z$. Furthermore, it is clear that we are only interested in perfect secrecy rates of the channel. The secrecy capacity region is defined as the closure of all achievable secrecy rate pairs. A single-letter characterization of the secrecy capacity region is given as follows.

Theorem 7: The secrecy capacity region of the degraded compound multi-receiver wiretap channel with layered messages is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} I(X; Y^1_j | U, Y^2_k) \tag{49}$$

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} I(U; Y^2_k | Z_t) \tag{50}$$

where the union is over all random variable pairs (U, X) such that

$$U \to X \to Y^1_j \to Y^* \to Y^2_k \to Z^* \to Z_t \tag{51}$$

for any triple (j, k, t).

Similar to the converse proof of Theorem 1, the presence of the fictitious users Y^* and Z^* plays an important role here as well. In particular, these two random variables introduce a conditional independence structure to the channel which enables us to define the auxiliary random variable U that yields a tight outer bound. Despite this similarity in the role of fictitious users in converse proofs, there is a significant difference between Theorems 1 and 7; in particular, it does not seem to be possible to extend Theorem 1 to an arbitrary number of eavesdroppers, while Theorem 7 holds for any number of eavesdroppers. This is due to the difference of two communication scenarios. In the second scenario, since we assume that users in the second group as well as the eavesdroppers wiretap users in the first group, we are able to provide a converse proof for the general situation of arbitrary number of eavesdroppers.

As an aside, if we set $K_1 = K_2 = K_Z = 1$, then as the degraded compound multi-receiver wiretap channel with layered messages reduces to the degraded multi-receiver wiretap channel with layered messages of [15], the secrecy capacity region in Theorem 7 reduces to the secrecy capacity region of the channel model in [15].

1) Parallel Degraded Compound Multi-receiver Wiretap Channels with Layered Messages: In the next section, we investigate the Gaussian parallel degraded compound multi-receiver wiretap channel with layered messages. To that end, here we obtain the secrecy capacity region of the parallel degraded compound multi-receiver wiretap channel with layered messages in a single-letter form as follows.

Theorem 8: The secrecy capacity region of the parallel degraded compound multi-receiver wiretap channel with layered messages is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1\\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1 | U_\ell, Y_{k\ell}^2) \tag{52}$$

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2\\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2 | Z_{t\ell}) \tag{53}$$

where the union is over all $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$ such that

$$U_\ell \to X_\ell \to Y_{j\ell}^1 \to Y_\ell^* \to Y_{k\ell}^2 \to Z_\ell^* \to Z_{t\ell} \tag{54}$$

for any (ℓ, j, k, t).

Since parallel degraded compound multi-receiver wiretap channels with layered messages is a special case of the degraded compound multi-receiver wiretap channel, Theorem 7 implicitly gives the secrecy capacity region of parallel degraded compound multi-receiver wiretap channels with layered messages. However, we still need to show that the region in Theorem 7 is equivalent to the region in Theorem 8. That is, we need to prove the optimality of independent signalling in each sub-channel.

2) Gaussian Parallel Degraded Compound Multi-receiver Wiretap Channels with Layered Messages: We now obtain the secrecy capacity region of Gaussian parallel degraded compound multi-receiver wiretap channels with layered messages. To that end, we need to evaluate the region given in Theorem 8, i.e., we need to find the optimal distribution $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. We first introduce the following theorem, which is an extension of Theorem 3.

Theorem 9: Let $N_1, N^*, N_2, \tilde{N}, N_Z$ be zero-mean Gaussian random variables with variances $\sigma_1^2, \sigma_*^2, \sigma_2^2, \tilde{\sigma}^2, \sigma_Z^2$, respectively, where

$$\sigma_1^2 \leq \sigma_*^2 \leq \sigma_2^2 \leq \tilde{\sigma}^2 \leq \sigma_Z^2 \tag{55}$$

Let (U, X) be an arbitrarily dependent random variable pair, which is independent of $(N_1, N^*, N_2, \tilde{N}, N_Z)$, and the second moment of X be constrained as $E\left[X^2\right] \leq P$. Then, for any feasible (U, X), we can find a $P^* \leq P$ such that

$$h(X + \tilde{N}|U) - h(X + N^*|U) = \frac{1}{2} \log \frac{P^* + \tilde{\sigma}^2}{P^* + \sigma_*^2} \tag{56}$$

and

$$h(X + N_Z|U) - h(X + N_2|U) \leq \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_2^2} \tag{57}$$

$$h(X + N_2|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_2^2}{P^* + \sigma_1^2} \tag{58}$$

as long as $(\sigma_1^2, \sigma_2^2, \sigma_Z^2)$ are in the range given in (55).

The proof of this theorem basically relies on Theorem 3 and Costa's entropy-power inequality [14].

Using this theorem, we can establish the secrecy capacity region of the Gaussian parallel degraded compound multi-receiver wiretap channel with layered messages as follows.

Theorem 10: The secrecy capacity region of the Gaussian parallel degraded compound multi-receiver wiretap channel with layered messages is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j,k} \sum_{\ell=1}^{L} \frac{1}{2} \log \left(1 + \frac{\beta_\ell P_\ell}{\Lambda_{j,\ell\ell}^1}\right) - \frac{1}{2} \log \left(1 + \frac{\beta_\ell P_\ell}{\Lambda_{k,\ell\ell}^2}\right) \tag{59}$$

$$R_2 \leq \min_{k,t} \sum_{\ell=1}^{L} \frac{1}{2} \log \left(1 + \frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda_{k,\ell\ell}^2}\right) - \frac{1}{2} \log \left(1 + \frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda_{t,\ell\ell}^Z}\right) \tag{60}$$

where $\bar{\beta}_\ell = 1 - \beta_\ell \in [0, 1],\ \ell = 1, \ldots, L$, and the union is over all $\{P_\ell\}_{\ell=1}^L$ such that $\sum_{\ell=1}^{L} P_\ell = P$.

Similar to Theorem 4, here also, P_ℓ denotes the amount of power P devoted to the transmission in the ℓth sub-channel. Similarly, β_ℓ is the fraction of the power P_ℓ of the ℓth sub-channel spent for the transmission to users in the first group.

3) Gaussian MIMO Degraded Compound Multi-receiver Wiretap Channels with Layered Messages: We now obtain the secrecy capacity region of the Gaussian MIMO degraded compound multi-receiver wiretap channel with layered messages. To that end, we need to evaluate the region given in Theorem 7, i.e., find the optimal random vector pair $(U, \mathbf{X})$. We are able to find the optimal random vector pair

$(U, \mathbf{X})$ when there is only one user in the second group, i.e., $K_2 = 1$. To obtain that result, we first need the following generalization of Theorem 5.

Theorem 11: Let $(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}^*, \mathbf{N}_Z)$ be Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2, \mathbf{\Sigma}^*, \mathbf{\Sigma}_Z$, respectively, where

$$\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}^* \preceq \mathbf{\Sigma}_Z \tag{61}$$

Let $(U, \mathbf{X})$ be an arbitrarily dependent random vector pair, which is independent of $(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}^*, \mathbf{N}_Z)$, and the second moment of $\mathbf{X}$ be constrained as $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$. Then, for any feasible $(U, \mathbf{X})$, there exists a positive semi-definite matrix $\mathbf{K}^*$ such that $\mathbf{K}^* \preceq \mathbf{S}$, and it satisfies

$$h(\mathbf{X} + \mathbf{N}^*|U) - h(\mathbf{X} + \mathbf{N}_2|U) = \frac{1}{2} \log \frac{|\mathbf{K}^* + \mathbf{\Sigma}^*|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{62}$$

and

$$h(\mathbf{X} + \mathbf{N}_Z|U) - h(\mathbf{X} + \mathbf{N}_2|U) \leq \frac{1}{2} \log \frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{63}$$

$$h(\mathbf{X} + \mathbf{N}_2|U) - h(\mathbf{X} + \mathbf{N}_1|U) \geq \frac{1}{2} \log \frac{|\mathbf{K}^* + \mathbf{\Sigma}_2|}{|\mathbf{K}^* + \mathbf{\Sigma}_1|} \tag{64}$$

for any $(\mathbf{\Sigma}_1, \mathbf{\Sigma}_Z)$ satisfying the order in (61).

Using this theorem, we can find the secrecy capacity region of the Gaussian MIMO degraded compound multi-receiver wiretap channel with layered messages when $K_2 = 1$ as follows.

Theorem 12: The secrecy capacity region of the Gaussian MIMO degraded compound multi-receiver wiretap channel with layered messages when $K_2 = 1$ is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}^2|}{|\mathbf{\Sigma}^2|} \tag{65}$$

$$R_2 \leq \min_{t=1,\ldots,K_Z} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}^2|}{|\mathbf{K} + \mathbf{\Sigma}^2|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_t^Z|}{|\mathbf{K} + \mathbf{\Sigma}_t^Z|} \tag{66}$$

where the union is over all positive semi-definite matrices $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$.

As an aside, if we set $K_1 = K_Z = 1$ in this theorem, we can recover the secrecy capacity region of the degraded multi-receiver wiretap channel with layered messages that was established in [15].

IV. Conclusions

In this paper, we studied two different communication scenarios for the degraded compound multi-receiver wiretap channel. In the first scenario, the transmitter wants to send a confidential message to users in the first group, and a different confidential message to users in the second group, where both messages are to be kept confidential from an eavesdropper. We establish the secrecy capacity region of the general discrete memoryless channel model, the parallel channel model, and the Gaussian parallel channel model. For the Gaussian MIMO channel model, we obtain the secrecy capacity region when there is only one user in the second group.

In the second scenario we study, the transmitter wants to sends a confidential message to users in the first group which is wiretapped by both users in the second group and eavesdroppers. In addition to this message sent to the first group of users, the transmitter sends a different message to users in the second group which needs to be kept confidential from only eavesdroppers. In this case, we do not put any restriction on the number of eavesdroppers. Similar to the first scenario, we establish the secrecy capacity region for the general discrete memoryless channel model, the parallel channel model, and the Gaussian parallel channel model. For the Gaussian MIMO channel model, we obtain the secrecy capacity region when there is only one user in the second group.

References

[1] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[3] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2009. Also available at [arXiv:0903.3096].

[4] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, Jun. 2008.

[5] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. The secrecy rate region of the broadcast channel. In *46th Annual Allerton Conf. Commun., Contr. and Comput.*, Sep. 2008. Also available at [arXiv:0806.4200].

[6] E. Ekrem and S. Ulukus. On secure broadcasting. In *42th Asilomar Conf. Signals, Syst. and Comp.*, Oct. 2008.

[7] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Communications and Networking*, 2009(824235), Oct. 2009.

[8] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Compound wire-tap channels. Submitted to *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, Dec. 2008. Also available at http://www-ee.eng.hawaii.edu/ yingbinl/papers/CompSecurity.pdf.

[9] H. Yamamoto. Coding theorem for secret sharing communication systems with two noisy channels. *IEEE Trans. Inf. Theory*, 35(3):572–578, May 1989.

[10] H. Yamamoto. A coding theorem for secret sharing communication systems with two Gaussian wiretap channels. *IEEE Trans. Inf. Theory*, 37(3):634–638, May 1991.

[11] P. Wang, G. Yu, and Z. Zhang. On the secrecy capacity of fading wireless channel with multiple eavesdroppers. In *IEEE Intnl. Symp. Inf. Theory*, pages 1301–1305, Jun. 2007.

[12] T. Liu, V. Prabhakaran, and S. Viswanath. The secrecy capacity of a class of parallel Gaussian compound wiretap channels. In *IEEE Intnl. Symp. Inf. Theory*, pages 116–120, Jul. 2008.

[13] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath. The capacity region of the degraded multi-input multi-output compound broadcast channel. *IEEE Trans. Inf. Theory*, to appear. Also available at http://www.ifp.illinois.edu/∼pramodv/pubs/WLSSV.pdf.

[14] M. Costa. A new entropy power inequality. *IEEE Trans. Inf. Theory*, 31(6):751–760, Nov. 1985.

[15] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz). A vector generalization of Costa's entropy-power inequality with applications. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2009. Also available at [arXiv:0903.3024].

[16] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.

[17] E. Ekrem and S. Ulukus. Degraded compound multi-receiver wiretap channels. To be submitted.