Degraded Gaussian MIMO Multi-Receiver Wiretap Channel with Public and Confidential Messages

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 multi-receiver wiretap channel with public and confidential messages. In this channel, there is a transmitter that wishes to communicate with two legitimate users in the presence of an external eavesdropper. The legitimate users and the eavesdropper satisfy a certain degradation order. In this paper, we study this channel model for the scenario where the transmitter sends a pair of public and confidential messages to each legitimate user. While there are no secrecy constraints on the public messages, confidential messages need to be transmitted in perfect secrecy. First, we obtain an inner bound for the capacity region of the discrete memoryless channel by using an achievable scheme that uses superposition coding and binning. Next, we obtain an outer bound for the capacity region of the degraded discrete memoryless channel. We show that this outer bound partially matches the inner bound. Consequently, we provide a partial characterization of the capacity region of the degraded discrete memoryless channel. Finally, we consider the degraded Gaussian multi-input multi-output (MIMO) wiretap channel with public and confidential messages. We show that, to evaluate both the inner and outer bounds for the Gaussian MIMO case, considering only jointly Gaussian auxiliary random variables and channel input is sufficient. Since the inner and outer bounds provided earlier for the degraded discrete memoryless channel partially match, these sufficiency results provide a partial characterization of the capacity region of the degraded Gaussian MIMO channel.**

I. Introduction

Information theoretic secrecy is initiated by Wyner in [1], where he introduces the wiretap channel and obtains the capacity-equivocation region of the wiretap channel. Wyner considers the degraded wiretap channel, where the eavesdropper's observation is a degraded version of the legitimate user's observation. His result is generalized to arbitrary, *not necessarily degraded*, wiretap channels in [2]. Recently, the wiretap channel gathered a renewed interest, and many multi-user extensions of the wiretap channel have been considered. One particular multi-user extension of the wiretap channel, that is relevant to our work here, is the multi-receiver wiretap channel considered in [3]–[5]. A recent survey on the secure broadcasting problem (including the multi-receiver wiretap channel) can be found in [6].

In the multi-receiver wiretap channel, see Figure 1, different from the basic wiretap channel in [1], [2], there are multiple legitimate users to which the transmitter sends confidential messages in the presence of an external eavesdropper. These multiple confidential messages need to be kept secret from the eavesdropper. References [3]–[5] consider the degraded multi-receiver wiretap channel, where the observations of the legitimate users and the eavesdropper are arranged according to a degradedness order. According to this degradation order, the eavesdropper has the worst observation, i.e., the eavesdropper's observation is degraded with respect to both legitimate users' observation. References [3]–[5] study the scenario where the transmitter sends a confidential message to each legitimate user where these confidential messages are kept perfectly secret from the eavesdropper, see Figure 2. The capacity region of the degraded multi-receiver wiretap channel for this scenario, i.e., the secrecy capacity region of the degraded multi-receiver wiretap channel, is obtained in [3] for two legitimate users, and in [4], [5] for an arbitrary number of legitimate users.

Here we study the degraded multi-receiver wiretap channel for the two legitimate user case, see Figure 3. We consider the scenario where the transmitter sends a pair of public and confidential messages to each legitimate user. While there are no secrecy concerns on the public messages, confidential messages need to be transmitted in perfect secrecy, i.e., confidential messages need to be kept perfectly secret from the eavesdropper. We call the channel model arising from this scenario the *degraded multi-receiver wiretap channel with public and confidential messages*. This model generalizes previous works on the degraded multi-receiver wiretap channel [3]–[5], where there were no public messages.

First, we propose an inner bound for the capacity region of the discrete memoryless channel. This inner bound results from an achievable scheme that combines superposition coding for broadcast channels [7] and binning. Binning has been used previously for the multi-receiver wiretap channel in [1]–[5] to associate each confidential message with many codewords, and hence to provide randomness for the confidential message to confuse the eavesdropper, and protect the confidential message from it. In other words, by means of binning, the confidential message is embedded into a doubly indexed codeword where one index denotes the confidential message and the other index (dummy index), denotes the necessary randomness to ensure the confidentiality of the

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

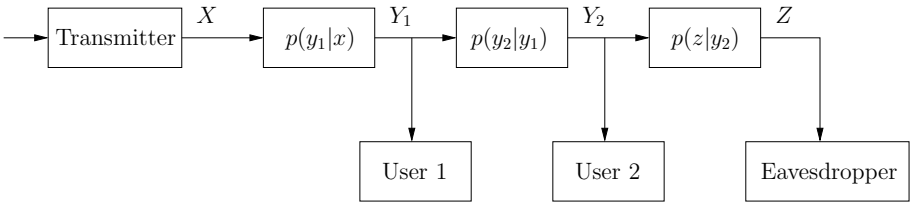

Fig. 1. Degraded multi-receiver wiretap channel.

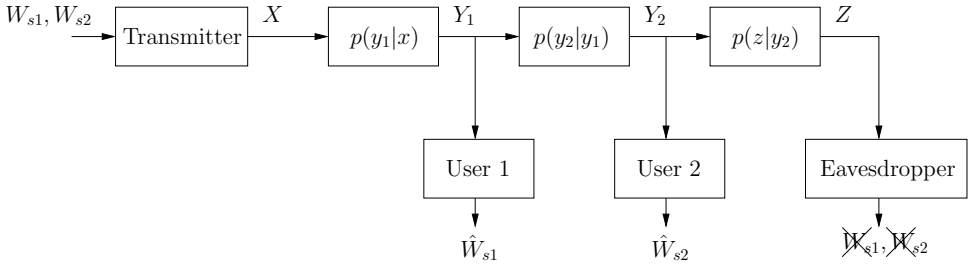

Fig. 2. Degraded multi-receiver wiretap channel with only confidential messages.

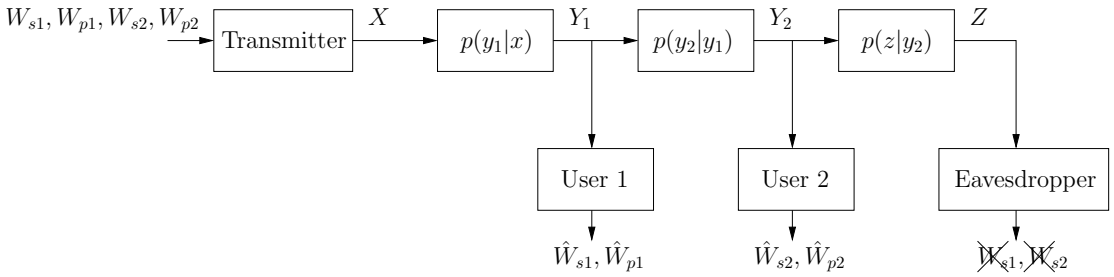

Fig. 3. Degraded multi-receiver wiretap channel with public and confidential messages.

message. This second index (dummy index) does not have any information content.

Since in our channel model there are public messages, on which there are no secrecy constraints, the protection of the confidential messages from the eavesdropper can be accomplished by using these public messages instead of dummy (no information bearing) messages. Thus, the difference of binning used here from the binning used in [3]–[5] is that, here, the confusion messages carry information, although there are no security guarantees on this information. Consequently, the injection of public messages into the degraded multi-receiver wiretap channel can be viewed as an effort to use the *wasted* transmission rate due to no-information bearing dummy indices, since these dummy indices are replaced with information bearing public messages on which there are no secrecy guarantees.

Next, we propose an outer bound for the capacity region of the degraded discrete memoryless channel. We obtain this outer bound by combining the converse proof techniques for the broadcast channel with degraded message sets [8] and the broadcast channel with confidential messages [2]. This outer bound partially matches the inner bound we propose, and therefore, it provides a partial characterization of the capacity region of the degraded discrete memoryless channel. In particular, when we specialize these inner and outer bounds by setting either the public message rate of the second legitimate user or the confidential message rate of the first legitimate user to zero, they match, i.e., provide the exact capacity regions for these two scenarios. Moreover, when we set the rates of both of the public messages to zero, these inner and outer bounds match, and yield the secrecy capacity region of the degraded discrete memoryless channel. This result was previously obtained in [3]–[5].

Finally, we consider the degraded Gaussian multi-input multi-output (MIMO) multi-receiver wiretap channel with public and confidential messages, see Figure 4. This model generalizes our work in [9], where we consider the general, i.e., *not necessarily degraded*, Gaussian MIMO channel only with confidential messages. For the degraded Gaussian MIMO channel in this paper, we first show that it is sufficient to consider the jointly Gaussian auxiliary random variables and channel input for the evaluation of the inner bound we proposed for the degraded discrete memoryless channel. In other words, we prove that there is no other possible

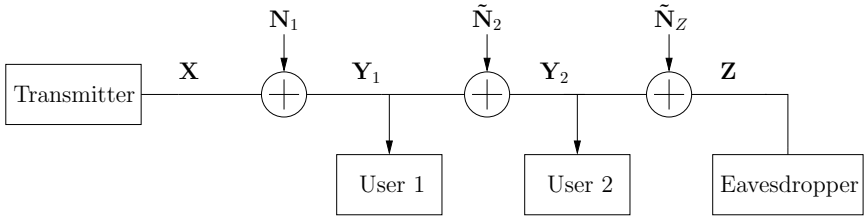

Fig. 4. Degraded Gaussian MIMO multi-receiver wiretap channel with public and confidential messages.

selection of auxiliary random variables and channel input which can provide a rate vector outside the Gaussian rate region that is obtained by using jointly Gaussian auxiliary random variables and channel input. We prove the sufficiency of Gaussian auxiliary random variables and channel input by using the de Bruijn identity [10], [11], a differential relationship between the differential entropy and the Fisher information matrix, in conjunction with the properties of the Fisher information matrix. We note that this proof technique was used in [9] to evaluate the secrecy capacity region of the degraded Gaussian MIMO channel, i.e., the capacity region of the degraded Gaussian MIMO channel only with confidential messages.

Next, we consider the outer bound we proposed for the degraded discrete memoryless channel. We show that, similar to the inner bound, considering only jointly Gaussian auxiliary random variables and channel input is sufficient to evaluate this outer bound for the degraded Gaussian MIMO channel. Indeed, this sufficiency result is already implied by the sufficiency of jointly Gaussian auxiliary random variables and channel input for the inner bound, because of the partial match between the inner and the outer bounds. Moreover, this partial match also gives us a partial characterization of the capacity region of the degraded Gaussian MIMO channel. Similar to the degraded discrete memoryless channel, the inner and outer bounds for the degraded Gaussian MIMO channel completely match, i.e., we obtain the exact capacity region, when we set either the public message rate of the second legitimate user or the confidential message rate of the first legitimate user to zero. Moreover, these inner and outer bounds match for the secrecy capacity region of the degraded Gaussian MIMO channel, which we obtain when we set the rates of both of the public messages to zero. This result was previously obtained in [12] for the degraded Gaussian MIMO multi-receiver wiretap channel with two legitimate users, and in [9] for the general, i.e., *not necessarily degraded*, Gaussian MIMO multi-receiver wiretap channel with an arbitrary number of legitimate users.

II. Degraded Multi-Receiver Wiretap Channels

In this section, we study degraded multi-receiver wiretap channels which consist of a transmitter with input alphabet $\mathcal{X}$, two legitimate users with output alphabets $\mathcal{Y}_1, \mathcal{Y}_2$, and an eavesdropper with output alphabet $\mathcal{Z}$. The channel is memoryless with a transition probability $p(y_1, y_2, z|x)$, where $X \in \mathcal{X}$ is the channel input, and $Y_1 \in \mathcal{Y}_1, Y_2 \in \mathcal{Y}_2, Z \in \mathcal{Z}$ denote the channel outputs of the first legitimate user, the second legitimate user, and the eavesdropper, respectively. We study degraded channels which satisfy the following Markov chain

$$X \to Y_1 \to Y_2 \to Z \tag{1}$$

We consider the scenario in which, the transmitter sends a pair of public and confidential messages to each legitimate user. While there are no secrecy constraints on the public messages, the confidential messages need to be transmitted in perfect secrecy. We call the channel model arising from this scenario the *degraded multi-receiver wiretap channel with public and confidential messages*.

An $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code for this channel consists of four message sets, $\mathcal{W}_{p1} = \{1, \ldots, 2^{nR_{p1}}\}$, $\mathcal{W}_{s1} = \{1, \ldots, 2^{nR_{s1}}\}$, $\mathcal{W}_{p2} = \{1, \ldots, 2^{nR_{p2}}\}$, $\mathcal{W}_{s2} = \{1, \ldots, 2^{nR_{s2}}\}$, one encoder at the transmitter $f : \mathcal{W}_{p1} \times \mathcal{W}_{s1} \times \mathcal{W}_{p2} \times \mathcal{W}_{s2} \to \mathcal{X}^n$, and one decoder at each legitimate user $g_j : \mathcal{Y}_j^n \to \mathcal{W}_{pj} \times \mathcal{W}_{sj}$, for $j = 1, 2$. The probability of error is defined as $P_e^n = \max\{P_{e,1}^n, P_{e,2}^n\}$, where $P_{e,j}^n = \Pr[g_j(Y_j^n) \neq (W_{pj}, W_{sj})]$, for $j = 1, 2$, and $W_{p1}, W_{s1}, W_{p2}, W_{s2}$ are uniformly distributed random variables in $\mathcal{W}_{p1}, \mathcal{W}_{s1}, \mathcal{W}_{p2}, \mathcal{W}_{s2}$, respectively. A rate tuple $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is said to be achievable if there exists an $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code which satisfies $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s1}, W_{s2}; Z^n) = 0 \tag{2}$$

We note that the perfect secrecy requirement given by (2) implies the following individual perfect secrecy requirements

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s1}; Z^n) = 0 \quad \text{and} \quad \lim_{n\to\infty} \frac{1}{n} I(W_{s2}; Z^n) = 0 \tag{3}$$

The capacity region of the degraded multi-receiver wiretap channel with public and confidential messages is defined as the convex closure of all achievable rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$, and is denoted by $\mathcal{C}$. We first present an inner bound for $\mathcal{C}$, i.e., an achievable rate region for the degraded multi-receiver wiretap channel with public and confidential messages, in the following theorem.

Theorem 1: An achievable rate region for the multi-

receiver wiretap channel with public and confidential messages is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying[1]

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{4}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{5}$$

$$R_{p2} + R_{s2} \leq I(U;Y_2) \tag{6}$$

$$R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z|U) \tag{7}$$

$$R_{p1} + R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{8}$$

where (U, X) satisfy the following Markov chain

$$U \rightarrow X \rightarrow (Y_1, Y_2, Z) \tag{9}$$

Due to space limitations here, we omit the proof of this theorem as well as the proofs of all upcoming results. The omitted proofs can be found in [13]. We prove Theorem 1 in two steps. As a first step, using superposition coding, one can show that the rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{p2} \leq I(U;Z) \tag{10}$$

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{11}$$

$$R_{p1} \leq I(X;Z|U) \tag{12}$$

$$R_{s1} \leq I(X;Y_1|U) - I(X;Z|U) \tag{13}$$

are achievable, where (U, X) satisfy (9). We show the achievability of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying (10)-(13) by using superposition coding. The differences of the superposition coding used here from the original superposition coding that attains the capacity region of the degraded broadcast channel [7] are that both public and confidential messages of a legitimate user are transmitted by the same layer of the codebook, and the public messages provide the necessary randomness to protect the confidential messages from the eavesdropper. In other words, in addition to their information content, the public messages also serve as the confusion messages that prevent the eavesdropper from decoding the confidential messages.

We also note that the achievability of the region given in (10)-(13) can be concluded by using the achievable scheme in [3]–[5], which was designed for the degraded multi-receiver wiretap channel only with confidential messages. This achievable scheme also uses superposition coding and binning. In this scheme, to achieve the following confidential message rates

$$R_{s2} = I(U;Y_2) - I(U;Z) \tag{14}$$

$$R_{s1} = I(X;Y_1|U) - I(X;Z|U) \tag{15}$$

each confidential message rate is equipped with the rate of some dummy messages, where these dummy messages provide the necessary protection of the confidential messages from the eavesdropper. In particular, the confidential message rates R_{s2} and R_{s1} are equipped with the following dummy message rates

$$\tilde{R}_{s2} = I(U;Z) \tag{16}$$

$$\tilde{R}_{s1} = I(X;Z|U) \tag{17}$$

where $\tilde{R}_{sj}$ is the dummy message rate spent for the jth legitimate user's confidential message rate R_{sj}. Since in our channel model there are public messages on which there are no secrecy constraints, these dummy message rates can be used as public message rates yielding the achievable rate region given in (10)-(13). We note that the presence of public messages in our channel model prevents the waste of resources due to the transmission of the dummy messages at rates given by (16)-(17) to protect the confidential messages.

As the second step to prove Theorem 1, one can use the following facts

- since confidential messages can be considered as public messages as well, each legitimate user's confidential message rate R_{sj} can be given up in favor of its public message rate R_{pj}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1} + \alpha_1, R_{s1} - \alpha_1, R_{p2} + \alpha_2, R_{s2} - \alpha_2)$ is also achievable for any non-negative (α_1, α_2) pairs satisfying $\alpha_j \leq R_{sj}$,
- since the channel is degraded, the second legitimate user's confidential message rate R_{s2} can be given up in favor of the first legitimate user's public and confidential message rates R_{p1} and R_{s1}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha, R_{s1}+\beta, R_{p2}, R_{s2}-\alpha-\beta)$ is also achievable for any non-negative (α, β) pairs satisfying $\alpha + \beta \leq R_{s2}$,
- since the channel is degraded, the second legitimate user's public message rate R_{p2} can be given up in favor of the first legitimate user's public message rate R_{p1}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1} + \alpha, R_{s1}, R_{p2} - \alpha, R_{s2})$ is also achievable for any non-negative α satisfying $\alpha \leq R_{p2}$,

in conjunction with Fourier-Motzkin elimination, and show that the region given in (10)-(13) is equivalent to the one given in (4)-(8).

The reason we state the achievable rate region by using the bounds in (4)-(8) instead of the bounds in (10)-(13) is that the former expressions simplify the comparison of the inner bound with the outer bound which will be introduced in the sequel. Another reason that we state achievable region by using the bounds in (4)-(8) is that they are more convenient for an explicit evaluation for the case of degraded Gaussian MIMO channel, which will be considered in the next section.

Now we introduce the following outer bound for the capacity region of the degraded discrete memoryless multi-receiver wiretap channel with public and confidential messages.

Theorem 2: The capacity region of the degraded multi-receiver wiretap channel with public and confidential messages is contained in the union of rate tuples

[1]We note that the achievable rate region given in Theorem 1 is valid not only for the degraded multi-receiver wiretap channel but also for the general, i.e., *not necessarily degraded*, multi-receiver wiretap channel.

$(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{18}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{19}$$

$$R_{p2} + R_{s2} \leq I(U;Y_2) \tag{20}$$

$$R_{p1} + R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{21}$$

for some (U, X) such that U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z \tag{22}$$

This outer bound provides a partial converse for the capacity region of the degraded multi-receiver wiretap channel because the only difference between the inner bound in Theorem 1 and the outer bound in Theorem 2 is the bound on $R_{s1}+R_{p2}+R_{s2}$ given by (7). In particular, in addition to the bounds defining the outer bound for the capacity region, the inner bound includes the following constraint

$$R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z|U) \tag{23}$$

Besides that, the inner and outer bounds are identical.

Despite this difference, there are cases for which the exact capacity region can be obtained. First, we note that the inner bound in Theorem 1 and the outer bound in Theorem 2 match when the confidential message rate of the first legitimate user is zero, i.e., $R_{s1} = 0$.

Corollary 1: The capacity region of the degraded multi-receiver wiretap channel without the first legitimate user's confidential message is given by the union of rate triples (R_{p1}, R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{24}$$

$$R_{s2} + R_{p2} \leq I(U;Y_2) \tag{25}$$

$$R_{p1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{26}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z \tag{27}$$

Corollary 1 can be proved by setting $R_{s1} = 0$ in both Theorem 1 and Theorem 2 and eliminating the redundant bounds.

Next, we note that the inner bound in Theorem 1 and the outer bound in Theorem 2 match when the public message rate of the second legitimate user is zero, i.e., $R_{p2} = 0$.

Corollary 2: The capacity region of the degraded multi-receiver wiretap channel without the second legitimate user's public message is given by the union of rate triples (R_{p1}, R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{28}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{29}$$

$$R_{p1} + R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{30}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z \tag{31}$$

Corollary 2 can be proved by setting $R_{p2} = 0$ in both Theorem 1 and Theorem 2 and eliminating the redundant bounds.

Corollary 2 also implies that the inner bound in Theorem 1 and the outer bound in Theorem 2 match on the secrecy capacity region of the degraded multi-receiver wiretap channel. In particular, the inner bound in Theorem 1 and the outer bound in Theorem 2 match if the rates of both public messages are set to zero, i.e., $R_{p1} = R_{p2} = 0$. The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the following corollary.

Corollary 3 ([3]–[5]): The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of rate pairs (R_{s1}, R_{s2}) satisfying[2]

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{32}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{33}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z \tag{34}$$

We note that in addition to its representation in Corollary 3, the secrecy capacity region of the degraded multi-receiver wiretap channel can be stated in an alternative form as the union of rate pairs (R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{35}$$

$$R_{s1} \leq I(X;Y_1|U) - I(X;Z|U) \tag{36}$$

where U, X exhibit the Markov chain in (34).

III. Degraded Gaussian MIMO Multi-Receiver Wiretap Channels

Here, we consider the degraded Gaussian MIMO multi-receiver wiretap channel which is defined by

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1 \tag{37}$$

$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2 \tag{38}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{39}$$

where the channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{40}$$

where $\mathbf{S} \succ 0$, and $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2, \mathbf{\Sigma}_Z$, respectively, which satisfy the following order

$$\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z \tag{41}$$

In a multi-receiver wiretap channel, since the capacity region depends only on the conditional marginal distributions of the transmitter-receiver links, but not on the entire joint distribution of the channel, the correlations among $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$

[2]The secrecy capacity region of the degraded multi-receiver wiretap channel for an arbitrary number of legitimate users, i.e., for more than two legitimate users, can be found in [4], [5].

do not affect the capacity region. Thus, without changing the corresponding capacity region, we can adjust the correlation structure among these noise vectors to ensure that they satisfy the following Markov chain

$$\mathbf{X} \rightarrow \mathbf{Y}_1 \rightarrow \mathbf{Y}_2 \rightarrow \mathbf{Z} \tag{42}$$

which is always possible because of our assumption about the covariance matrices in (41). Moreover, the Markov chain in (42) implies that any Gaussian MIMO multi-receiver wiretap channel satisfying the semi-definite order in (41) can be treated as a degraded multi-receiver wiretap channel, hence Theorem 2 provides an outer bound for the capacity regions of these Gaussian MIMO multi-receiver wiretap channels. We note that contrary to the outer bound in Theorem 2, the inner bound in Theorem 1 can be used for any Gaussian MIMO multi-receiver wiretap channel irrespective of whether the channel is degraded.

We first provide an inner bound for the capacity region of the Gaussian MIMO multi-receiver wiretap channel with public and confidential messages by using Theorem 1. The corresponding achievable rate region is stated in the following theorem.

Theorem 3: An achievable rate region for the Gaussian MIMO multi-receiver wiretap channel with public and confidential messages is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{43}$$

$$R_{s1}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| - \frac{1}{2}\log|\mathbf{S}+\mathbf{\Sigma}_Z| \tag{44}$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} \tag{45}$$

$$R_{s1}+R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| - \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_Z| \tag{46}$$

$$R_{s1}+R_{s2}+R_{p1}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| \tag{47}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$.

This achievable rate region given in Theorem 3 can be obtained by evaluating the achievable rate region in Theorem 1 for the degraded Gaussian MIMO multi-receiver wiretap channel by using the following selection for $U, \mathbf{X}$: i) U is a zero-mean Gaussian random vector with covariance matrix $\mathbf{S}-\mathbf{K}$, ii) $\mathbf{X} = U + U'$ where U' is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}$, and is independent of U. We note that besides this jointly Gaussian $(U, \mathbf{X})$ selection, there might be other possible $(U, \mathbf{X})$ selections which may yield a larger region than the one obtained by using jointly Gaussian $(U, \mathbf{X})$. However, we show that jointly Gaussian $(U, \mathbf{X})$ selection is sufficient to evaluate the achievable rate region in Theorem 1 for the degraded Gaussian MIMO multi-receiver wiretap channel. In other words, jointly Gaussian $(U, \mathbf{X})$ selection exhausts the achievable rate region in Theorem 1 for the degraded Gaussian MIMO multi-receiver wiretap channel. This sufficiency result is stated in the following theorem.

Theorem 4: For the degraded Gaussian MIMO multi-receiver wiretap channel, the achievable rate region in Theorem 1 is exhausted by jointly Gaussian $(U, \mathbf{X})$. In particular, for any non-Gaussian $(U, \mathbf{X})$, there exists a Gaussian $(U^G, \mathbf{X}^G)$ which yields a larger region than the one obtained by using the non-Gaussian $(U, \mathbf{X})$.

Next, we provide an outer bound for the capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. This outer bound can be obtained by evaluating the outer bound given in Theorem 2 for the degraded Gaussian MIMO multi-receiver wiretap channel. This evaluation is tantamount to finding the optimal $(U, \mathbf{X})$ which exhausts the outer bound in Theorem 2 for the degraded Gaussian MIMO multi-receiver wiretap channel. We show that jointly Gaussian $(U, \mathbf{X})$ is sufficient to exhaust the outer bound in Theorem 2 for the degraded Gaussian MIMO channel. The corresponding outer bound is stated in the following theorem.

Theorem 5: The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is contained in the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{48}$$

$$R_{s1}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| - \frac{1}{2}\log|\mathbf{S}+\mathbf{\Sigma}_Z| \tag{49}$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} \tag{50}$$

$$R_{s1}+R_{s2}+R_{p1}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| \tag{51}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$.

We prove Theorem 4 and Theorem 5 by using the de Bruijn identity [10], [11], a differential relationship between differential entropy and the Fisher information matrix, in conjunction with the properties of the Fisher information matrix. In particular, to prove Theorem 4, we consider the region in Theorem 1, and show that for any non-Gaussian $(U, \mathbf{X})$, there exists a Gaussian $(U^G, \mathbf{X}^G)$ which yields a larger region than the one that is obtained by evaluating the region in Theorem 1 with the non-Gaussian $(U, \mathbf{X})$. We note that this proof of Theorem 4 implies the proof of Theorem 5. In particular, since the region in Theorem 1 includes all the constraints involved in the outer bound given in Theorem 2, the proof of Theorem 4 reveals that for any non-Gaussian $(U, \mathbf{X})$, there exists a Gaussian $(U^G, \mathbf{X}^G)$ which yields a larger region than the one that is obtained by evaluating the region in Theorem 2 with the non-Gaussian $(U, \mathbf{X})$.

We note that the only difference between the inner and the outer bounds for the degraded Gaussian MIMO multi-receiver wiretap given in Theorem 3 and Theorem 5, respectively, comes from the bound in (46). In other words, there is one more constraint in the inner bound given by Theorem 3 than the outer bound given by Theorem 5. This additional constraint is

$$R_{s1}+R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}+\frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| - \frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_Z| \quad (52)$$

Besides this constraint on $R_{s1}+R_{s2}+R_{p2}$, the inner bound in Theorem 3 and the outer bound in Theorem 5 are the same.

We conclude this section by providing the cases where the inner bound in Theorem 3 and the outer bound in Theorem 5 match. We first note that the inner bound in Theorem 3 and the outer bound in Theorem 5 match when the confidential message rate of the first legitimate user is zero, i.e., $R_{s1}=0$. The corresponding capacity region is given by the following corollary.

Corollary 4: The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel without the first legitimate user's confidential message is given by the union of rate tuples (R_{p1},R_{p2},R_{s2}) satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}-\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \quad (53)$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} \quad (54)$$

$$R_{s2}+R_{p1}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}+\frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| \quad (55)$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K}\preceq\mathbf{S}$.

We note that Corollary 4 is the Gaussian MIMO version of Corollary 1 which obtains the capacity region of the degraded discrete memoryless multi-receiver wiretap channel without the first legitimate user's confidential message. Corollary 4 can be proved by setting $R_{s1}=0$ in both Theorem 3 and Theorem 5 and eliminating the redundant bounds.

We next note that the inner bound in Theorem 3 and the outer bound in Theorem 5 match when the public message rate of the second legitimate user is zero, i.e., $R_{p2}=0$. The corresponding capacity region is stated in the following corollary.

Corollary 5: The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel without the second legitimate user's public message is given by the union of rate tuples (R_{p1},R_{s1},R_{s2}) satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}-\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \quad (56)$$

$$R_{s1}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}+\frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| - \frac{1}{2}\log|\mathbf{S}+\mathbf{\Sigma}_Z| \quad (57)$$

$$R_{s1}+R_{s2}+R_{p1} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}+\frac{1}{2}\log|\mathbf{K}+\mathbf{\Sigma}_1| \quad (58)$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K}\preceq\mathbf{S}$.

We note that Corollary 5 is the Gaussian MIMO version of Corollary 2 which obtains the capacity region of the degraded discrete memoryless multi-receiver wiretap channel without the second legitimate user's public message. Corollary 5 can be proved by setting $R_{p2}=0$ in both Theorem 3 and Theorem 5 and eliminating the redundant bounds.

Corollary 5 also implies that the inner bound in Theorem 3 and the outer bound in Theorem 5 match for the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. In particular, the inner bound Theorem 3 and the outer bound in Theorem 5 match if the rates of both public messages are set to zero, i.e., $R_{p1}=R_{p2}=0$. The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the following corollary.

Corollary 6 ([9], [12]): The secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is given by the union of rate pairs (R_{s1},R_{s2}) satisfying[3]

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}-\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \quad (59)$$

$$R_{s2}+R_{s1} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}+\frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (60)$$

where $\mathbf{K}$ satisfies $\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}$.

We note that in addition to its representation in Corollary 6, the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel can be stated in an alternative form as the union of rate pairs (R_{s1},R_{s2}) satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|}-\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \quad (61)$$

$$R_{s1} \leq \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|}-\frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (62)$$

IV. Conclusions

We study the degraded multi-receiver wiretap channel with public and confidential messages. We first consider the degraded discrete memoryless channel. We provide inner and outer bounds for the capacity region of the degraded discrete memoryless multi-receiver wiretap channel, where these inner and outer bounds partially match. Thus, we provide a partial characterization of the capacity region of the degraded discrete memoryless multi-receiver wiretap channel with public and confidential messages. Next, we consider the degraded Gaussian MIMO multi-receiver wiretap channel. We show that, to evaluate the proposed inner and outer bounds for the Gaussian MIMO case, it is sufficient to consider only the jointly Gaussian auxiliary random variables

[3]The secrecy capacity region of the general, not necessarily degraded, Gaussian MIMO multi-receiver wiretap channel for an arbitrary number of legitimate users can be found in [9].

and channel input. Consequently, since these inner and outer bounds partially match, we obtain a partial characterization of the capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel with public and confidential messages.

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] 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.

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

[5] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Communications and Networking*, 2009:Article ID 824235, 2009.

[6] E. Ekrem and S. Ulukus. Secure broadcasting using multiple antennas. *Journal of Communications and Networks*. To appear.

[7] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley & Sons, 2006. 2nd edition.

[8] J. Korner and K. Marton. General broadcast channels with degraded message sets. *IEEE Trans. Inf. Theory*, 23(1):60–64, Jan. 1977.

[9] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*. To appear. Also available at [arXiv:0903.3096].

[10] N. M. Blachman. The convolution inequality for entropy powers. *IEEE Trans. Inf. Theory*, IT-11(2):267–271, Apr. 1965.

[11] D. P. Palomar and S. Verdu. Gradient of mutual information in linear vector Gaussian channels. *IEEE Trans. Inf. Theory*, 52(1):141–154, Jan. 2006.

[12] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz). A vector generalization of Costa's entropy-power inequality with applications. *IEEE Trans. Inf. Theory*, 56(4):1865–1879, Apr. 2010.

[13] E. Ekrem and S. Ulukus. Gaussian MIMO multi-receiver wiretap channel with public and confidential messages. In preparation.