On Secure Broadcasting

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 security of communication between a single transmitter and multiple receivers in a broadcast channel in the presence of an eavesdropper. We consider several special classes of channels. As the first model, we consider the degraded multi-receiver wiretap channel where the legitimate receivers exhibit a degradedness order while the eavesdropper is more noisy with respect to all legitimate receivers. We establish the secrecy capacity region of this channel model. Secondly, we consider the parallel multi-receiver wiretap channel with a less noisiness order in each sub-channel, where this order is not necessarily the same for all sub-channels. We establish the common message secrecy capacity and sum secrecy capacity of this channel. Thirdly, we study a special class of degraded parallel multi-receiver wiretap channels and provide a stronger result. In particular, we study the case with two sub-channels two users and one eavesdropper, where there is a degradedness order in each sub-channel such that in the first (resp. second) sub-channel the second (resp. first) receiver is degraded with respect to the first (resp. second) receiver, while the eavesdropper is degraded with respect to both legitimate receivers in both sub-channels. We determine the secrecy capacity region of this channel.**

I. Introduction

Information theoretic secrecy was initiated by Wyner in [1] where he introduced the wiretap channel and established the capacity-equivocation region of the *degraded* wiretap channel. Later, his result was generalized to arbitrary, *not necessarily degraded*, wiretap channels by Csiszar and Korner [2]. One basic extension of the wiretap channel to the multiuser environment is *secure broadcasting to many users* in the presence of an eavesdropper. In the most general form of this problem, one transmitter wants to have confidential communication with an arbitrary number of users in a broadcast channel, while this communication is being eavesdropped by an external entity. Characterizing the secrecy capacity region of this channel model in its most general form is difficult, because the version of this problem without any secrecy constraints, is the broadcast channel with an arbitrary number of receivers, whose capacity region is open. Consequently, to have progress in understanding the limits of secure broadcasting, we resort to studying several special classes of channels, with increasing generality. The approach of studying special channel structures was also followed in the existing literature on secure broadcasting [3], [4].

Reference [3] first considers an arbitrary wiretap channel with two legitimate receivers and one eavesdropper, and provides an achievable scheme when each user wishes to receive an independent message. Secondly, [3] focuses on the degraded wiretap channel with two receivers and one eavesdropper, where there is a degradedness order among the receivers, and the eavesdropper is degraded with respect to both users (see Figure 1 for a more general version of the problem that we study). For this setting, [3] finds the secrecy capacity region. This result is concurrently and independently obtained in this work as a special case, see Corollary 1.

Another related work is [4] which considers secure broadcasting to K users using M sub-channels (see Figure 2) for two different scenarios: In the first scenario, the transmitter wants to convey only a common confidential message to all users, and in the second scenario, the transmitter wants to send independent messages to all users. For both scenarios, [4] considers a sub-class of parallel multi-receiver wiretap channels, where in any given sub-channel there is a degradation order such that each receiver's observation (except the best one) is a degraded version of some other receiver's observation, and this degradation order is not necessarily the same for all sub-channels. For this sub-class of channels, [4] finds the common message secrecy capacity and the sum secrecy capacity, for the first and second scenarios, respectively.

Here, our approach would be two-fold: First, we will identify more general channel models than considered in [3], [4] and generalize the results in [3], [4] to those channel models, and secondly, we will consider a somewhat more specialized channel model than in [4] and provide a more comprehensive result. More precisely, our contributions in this paper are:

1) We consider the degraded multi-receiver wiretap channel with an arbitrary number of users and one eavesdropper, where users are arranged according to a degradedness order, and each user has a less noisy channel with respect to the eavesdropper, see Figure 1. We find the secrecy capacity region when each user receives both an independent message and a common message. Since degradedness implies less noisiness [2], this channel model contains the sub-class of channel models where in addition to the degradedness order users exhibit, the eavesdropper is degraded with respect to all users. Consequently, our result can be specialized to the degraded multi-receiver wiretap channel with an arbitrary number of users and a degraded eavesdropper, see Corollary 1.
2) We then focus on a class of parallel multi-receiver wiretap channels with an arbitrary number of legitimate

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

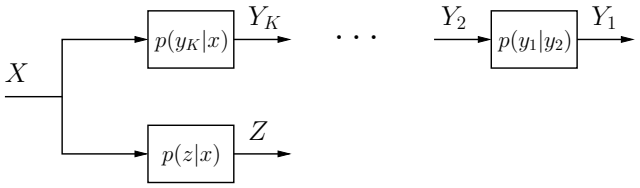

Fig. 1. Degraded multi-receiver wiretap channel with a more noisy eavesdropper.

receivers and an eavesdropper, see Figure 2, where in each sub-channel, for any given user, either the user's channel is less noisy with respect to the eavesdropper's channel, or vice versa. We establish the common message secrecy capacity of this channel, which is a generalization of the corresponding capacity result in [4] to a broader class of channels. Secondly, we study the scenario where each legitimate receiver wishes to receive an independent message for another sub-class of parallel multi-receiver wiretap channels. For channels belonging to this sub-class, in each sub-channel, there is a less noisiness order which is not necessarily the same for all sub-channels. Consequently, this ordered class of channels is a subset of the class for which we establish the common message secrecy capacity. We find the sum secrecy capacity for this class, which is again a generalization of the corresponding result in [4] to a broader class of channels.

3) We also investigate a class of parallel multi-receiver wiretap channels with two sub-channels, two users and one eavesdropper, see Figure 3. For the channels in this class, there is a specific degradation order in each sub-channel such that in the first (resp. second) sub-channel the second (resp. first) user is degraded with respect to the first (resp. second) user, while the eavesdropper is degraded with respect to both users in both sub-channels. This is the model of [4] for $K = 2$ users and $M = 2$ sub-channels. For this class, we determine the entire secrecy capacity region when each user receives both an independent message and a common message. In contrast, [4] gives the common message secrecy capacity and sum secrecy capacity of this class.

II. Degraded Multi-receiver Wiretap Channels

We first consider the channel model given in Figure 1. This channel consists of a transmitter with an input alphabet $x \in \mathcal{X}$, K legitimate receivers with output alphabets $y_k \in \mathcal{Y}_k,\ k = 1, \ldots, K,$ and an eavesdropper with output alphabet $z \in \mathcal{Z}$. The transmitter sends a confidential message to each user, say $w_k \in \mathcal{W}_k$ to the kth user, and a common confidential message to all users, both of which need to be kept secret from the eavesdropper. The channel is assumed to be memoryless with a transition probability $p(y_1, y_2, \ldots, y_K, z|x)$.

Moreover, users exhibit a certain degradation order, i.e., their channel outputs satisfy the following Markov chain

$$X \to Y_K \to \ldots \to Y_1 \tag{1}$$

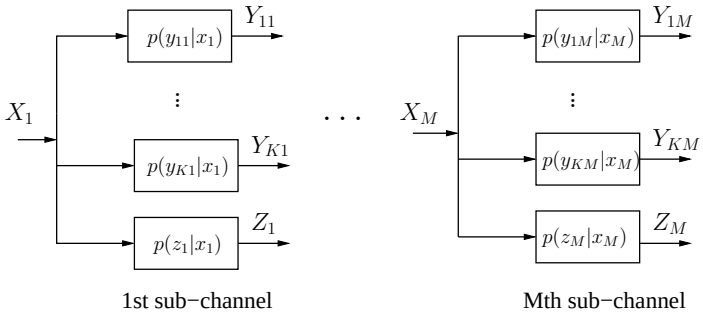

Fig. 2. Parallel multi-receiver wiretap channel.

and each user has a less noisy channel with respect to the eavesdropper, i.e., we have

$$I(U; Y_k) > I(U; Z) \tag{2}$$

for every U such that $U \to X \to (Y_k, Z)$. In fact, since a degradation order exists among the users, it is sufficient to say that user 1 has a less noisy channel with respect to the eavesdropper to guarantee that all users do. Hereafter, we call this channel *the degraded multi-receiver wiretap channel with a more noisy eavesdropper*. We note that this channel model contains the degraded multi-receiver wiretap channel which is defined through the Markov chain

$$X \to Y_K \to \ldots \to Y_1 \to Z \tag{3}$$

because the Markov chain in (3) implies the less noisiness condition in (2).

A $(n, 2^{nR_0}, 2^{nR_1}, \ldots, 2^{nR_K})$ code for this channel consists of $K + 1$ message sets, $\mathcal{W}_k = \{1, \ldots, 2^{nR_k}\}$, $k = 0, \ldots, K$, an encoder $f : \mathcal{W}_0 \times \mathcal{W}_1 \ldots \times \mathcal{W}_K \to \mathcal{X}^n$, K decoders, one at each legitimate receiver, $g_k : \mathcal{Y}_k \to \mathcal{W}_0 \times \mathcal{W}_k$, $k = 1, \ldots, K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[g_k(Y_k^n) \neq (W_0, W_k)\right]$. A rate tuple $(R_0, R_1, \ldots, R_K)$ is said to be achievable if there exists a code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{k \in \mathcal{S}(W)} R_k, \quad \forall\ \mathcal{S}(W) \tag{4}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_0, W_1, \ldots, W_K\}$. Hence, we consider only perfect secrecy rates. The secrecy capacity region is defined as the closure of all achievable rate tuples, and is given by the following theorem.

Theorem 1 The secrecy capacity region of the degraded multi-receiver wiretap channel with a more noisy eavesdropper is given by the union of the tuples $(R_1, \ldots, R_K)$ satisfying

$$R_0 + \sum_{k=1}^{\ell} R_k \leq \sum_{k=1}^{\ell} I(U_k; Y_k|U_{k-1}) - I(U_\ell; Z), \qquad \ell = 1, \ldots, K \tag{5}$$

where the maximization is over $\prod_{i=1}^{K} p(u_i|u_{i-1})$, and $U_0 = \phi, U_K = X$.

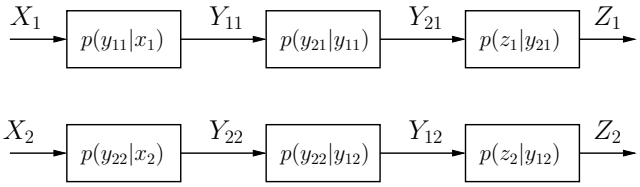

Fig. 3. Parallel degraded multi-receiver wiretap channel.

Remark 1 Theorem 1 implies that a modified version of superposition coding can achieve the boundary of the capacity region. The difference between the superposition coding scheme used to achieve (5) and the standard one [5] is that the former uses stochastic encoding in each layer of the code to associate each message with many codewords. This controlled amount of redundancy prevents the eavesdropper from being able decode the message.

As stated earlier, the degraded multi-receiver wiretap channel with a more noisy eavesdropper contains the degraded multi-receiver wiretap channel which requires the eavesdropper to be degraded with respect to all users as stated (3). Thus, we can specialize our result in Theorem 1 to the degraded multi-receiver wiretap channel as given below.

Corollary 1 The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of the tuples $(R_0, R_1, \ldots, R_K)$ satisfying

$$R_0 + \sum_{k=1}^{\ell} R_k \leq \sum_{k=1}^{\ell} I(U_k; Y_k|U_{k-1}, Z), \quad \ell = 1, \ldots, K \quad (6)$$

where the maximization is over $\prod_{i=1}^{K} p(u_i|u_{i-1})$, and $U_0 = \phi, U_K = X$.

We acknowledge an independent and concurrent work regarding the degraded multi-receiver wiretap channel. Reference [3] considers the two-user case and establishes the secrecy capacity region as well.

III. Parallel Multi-receiver Wiretap Channels

Here, we investigate the parallel multi-receiver wiretap channel where the transmitter communicates with K legitimate receivers using M independent sub-channels in the presence of an eavesdropper, see Figure 2. The channel transition probability of a parallel multi-receiver wiretap channel is

$$p\left(\{y_{1m}, \ldots, y_{Km}, z_m\}_{m=1}^{M} \,|\, \{x_m\}_{m=1}^{M}\right) = \prod_{m=1}^{M} p\left(y_{1m}, \ldots, y_{Km}, z_m|x_m\right) \quad (7)$$

where $x_m \in \mathcal{X}_m$ is the input in the mth sub-channel, $y_{km} \in \mathcal{Y}_{km}$ (resp. $z_m \in \mathcal{Z}_m$) is the output in the kth user's (resp. eavesdropper's) mth sub-channel.

In this section, we investigate special classes of parallel multi-receiver wiretap channels, and our emphasis will be on the common message secrecy capacity and the sum secrecy capacity of these special classes.

A. The Common Message Secrecy Capacity

We first consider the simplest possible scenario where the transmitter sends a common confidential message to all users. The common message secrecy capacity for a special class of parallel multi-receiver wiretap channels was studied in [4]. In this class of parallel multi-receiver wiretap channels [4], each sub-channel exhibits a certain degradation order which is not necessarily the same for all sub-channels, i.e., the following Markov chain is satisfied

$$X_l \rightarrow Y_{\pi_l(1)} \rightarrow Y_{\pi_l(2)} \rightarrow \ldots \rightarrow Y_{\pi_l(K+1)} \quad (8)$$

in the lth sub-channel, where $(Y_{\pi_l(1)}, Y_{\pi_l(2)}, \ldots, Y_{\pi_l(K+1)})$ is a permutation of $(Y_{1l}, \ldots, Y_{Kl}, Z_l)$. Hereafter, we call this channel *the parallel degraded multi-receiver wiretap channel*. Although [4] established the common message secrecy capacity for this class of channels, in fact, their result is valid for the broader class in which we have one of the following two Markov chains

$$X_l \rightarrow Y_{kl} \rightarrow Z_l, \quad \text{or} \quad X_l \rightarrow Z_l \rightarrow Y_{kl} \quad (9)$$

valid for every X_l and for any (k, l) pair where $k \in \{1, \ldots, K\}$, $l \in \{1, \ldots, M\}$. Thus, it is sufficient to have a degradedness order between each user and the eavesdropper in any sub-channel instead of the long Markov chain between all users and the eavesdropper as in (8).

Here, we focus on a broader class of channels where in each sub-channel, for any given user, either the user's channel is less noisy than the eavesdropper's channel, or vice versa. More formally, we have either

$$I(U; Y_{kl}) > I(U; Z_l) \quad (10)$$

or

$$I(U; Y_{kl}) < I(U; Z_l) \quad (11)$$

for all $U \rightarrow X_l \rightarrow (Y_{kl}, Z)$ and any (k, l) pair where $k \in \{1, \ldots, K\}$, $l \in \{1, \ldots, M\}$. Hereafter, we call this channel *the parallel multi-receiver wiretap channel with a more noisy eavesdropper*. Since the Markov chain in (8) implies either (10) or (11), the parallel multi-receiver wiretap channel with a more noisy eavesdropper contains the parallel degraded multi-receiver wiretap channel studied in [4].

A $(2^{nR}, n)$ code for this channel consists of a message set, $\mathcal{W}_0 = \{1, \ldots, 2^{nR}\}$, an encoder, $f : \mathcal{W}_0 \rightarrow \mathcal{X}_1^n \times \ldots \times \mathcal{X}_M^n$, K decoders, one at each legitimate receiver $g_k : \mathcal{Y}_{k1} \times \ldots \times \mathcal{Y}_{kM} \rightarrow \mathcal{W}_0, k = 1, \ldots, K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[\hat{W}_{k0} \neq W_0\right]$ where $\hat{W}_{k0}$ is the k-th user's decoder output. The secrecy of the common message is measured through the equivocation rate which is defined as $\frac{1}{n} H(W_0|Z_1^n, \ldots, Z_M^n)$. A common message secrecy rate, R, is said to be achievable if there exists a code such that $\lim_{n\rightarrow\infty} P_e^n = 0$, and

$$\lim_{n\rightarrow\infty} \frac{1}{n} H(W_0|Z_1^n, \ldots, Z_M^n) \geq R \quad (12)$$

The common message secrecy capacity is the supremum of all achievable secrecy rates, and is given by the following theorem.

Theorem 2 The common message secrecy capacity, C_0, of the parallel multi-receiver wiretap channel with a more noisy eavesdropper is given by

$$C_0 = \max \min_{k=1,\ldots,K} \sum_{l=1}^{M} \left[I(X_l;Y_{kl}) - I(X_l;Z_l)\right]^+ \qquad (13)$$

where the maximization is over $\prod_{l=1}^{M} p(x_l)$.

Remark 2 Theorem 2 implies that we should not use the sub-channels in which there is no user that has a less noisy channel than the eavesdropper. Moreover, Theorem 2 shows that the use of independent inputs in each sub-channel is sufficient to achieve the capacity.

As stated earlier, the parallel multi-receiver wiretap channel with a more noisy eavesdropper contains the parallel degraded multi-receiver wiretap channel studied in [4]. Hence, we can specialize Theorem 2 to recover the common message secrecy capacity of the parallel degraded multi-receiver wiretap channel established in [4]. This is stated in the following corollary.

Corollary 2 The common message secrecy capacity of the parallel degraded multi-receiver wiretap channel is given by

$$C_0 = \max \min_{k=1,\ldots,K} \sum_{l=1}^{M} I(X_l;Y_{kl}|Z_l) \qquad (14)$$

where the maximization is over $\prod_{l=1}^{M} p(x_l)$.

B. The Sum Secrecy Capacity

We now consider the scenario where the transmitter sends an independent confidential message to each legitimate receiver, and focus on the sum secrecy capacity. We consider a class of parallel multi-receiver wiretap channels where the legitimate receivers and the eavesdropper exhibit a certain less noisiness order in each sub-channel. These less noisiness orders are not necessarily the same for all sub-channels. Thus, the overall channel is not less noisy. In the lth sub-channel, for all $U \rightarrow X_l \rightarrow (Y_{1l},\ldots,Y_{Kl},Z_l)$, we have

$$I(U;Y_{\pi_l(1)}) > I(U;Y_{\pi_l(2)}) > \ldots > I(U;Y_{\pi_l(K+1)}) \qquad (15)$$

where $(Y_{\pi_l(1)},Y_{\pi_l(2)},\ldots,Y_{\pi_l(K+1)})$ is a permutation of $(Y_{1l},\ldots,Y_{Kl},Z_l)$. We call this class of channels *the parallel multi-receiver wiretap channel with a less noisiness order in each sub-channel*. We note that this class of channels is a subset of the parallel multi-receiver wiretap channel with a more noisy eavesdropper studied in Section III-A, because of the additional ordering imposed between users' sub-channels. We also note that the class of parallel degraded multi-receiver wiretap channels with a degradedness order in each sub-channel studied in [4] is not only a subset of parallel multi-receiver wiretap channels with a more noisy eavesdropper studied in Section III-A but also a subset of parallel multi-receiver wiretap channels with a less noisiness order in each sub-channel studied in this section.

A $(2^{nR_1}\ldots,2^{nR_K},n)$ code for this channel consists of K message sets, $\mathcal{W}_k = \{1,\ldots,2^{nR_k}\}$, $k=1,\ldots,K$, an encoder, $f : \mathcal{W}_1 \times \ldots \times \mathcal{W}_K \rightarrow \mathcal{X}_1^n \times \ldots \times \mathcal{X}_M^n$, K decoders, one at each legitimate receiver $g_k : \mathcal{Y}_{k1} \times \ldots \times \mathcal{Y}_{kM} \rightarrow \mathcal{W}_k, k=1,\ldots,K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[\hat{W}_k \neq W_k\right]$ where $\hat{W}_k$ is the kth user's decoder output. The secrecy is measured through the equivocation rate which is defined as $\frac{1}{n}H(W_1,\ldots,W_K|Z_1^n,\ldots,Z_M^n)$. A sum secrecy rate, R_s, is said to be achievable if there exists a code such that $\lim_{n\rightarrow\infty} P_e^n = 0$, and

$$\lim_{n\rightarrow\infty} \frac{1}{n} H(W_1,\ldots,W_K|Z_1^n,\ldots,Z_M^n) \geq R_s \qquad (16)$$

The sum secrecy capacity is the supremum of all achievable sum secrecy rates, and is given by the following theorem.

Theorem 3 The sum secrecy capacity of the parallel multi-receiver wiretap channel with a less noisiness order in each sub-channel is given by

$$\max \sum_{l=1}^{M} \left[I(X_l;Y_{\rho(l)l}) - I(X_l;Z_l)\right]^+ \qquad (17)$$

where the maximization is over $\prod_{l=1}^{M} p(x_l)$ and $\rho(l)$ is the index of the strongest user in the lth sub-channel such that

$$I(U;Y_{kl}) \leq I(U;Y_{\rho(l)l}) \qquad (18)$$

for all $U \rightarrow X_l \rightarrow (Y_{1l},\ldots,Y_{Kl},Z_l)$ and any $k \in \{1,\ldots,K\}$.

Remark 3 Theorem 3 implies that the sum secrecy capacity is achieved by sending information only to the strongest user in each sub-channel. As in Theorem 2, here also, the use of independent inputs for each sub-channel is capacity-achieving.

As mentioned earlier, since the class of parallel multi-receiver wiretap channels with a less noisiness order in each sub-channel contains the class of parallel degraded multi-receiver wiretap channels studied in [4], Theorem 3 can be specialized to give the sum secrecy capacity of the latter class of channels as well, which was originally obtained in [4].

Corollary 3 The sum secrecy capacity of the parallel degraded multi-receiver wiretap channel is given by

$$\max \sum_{l=1}^{M} I(X_l;Y_{\rho(l)l}|Z_l) \qquad (19)$$

where the maximization is over $\prod_{l=1}^{M} p(x_l)$ and $\rho(l)$ is the index of the strongest user in the lth sub-channel such that

$$X_l \rightarrow Y_{\rho(l)l} \rightarrow Y_{kl} \qquad (20)$$

for all input distributions on X_l and any $k \in \{1,\ldots,K\}$.

IV. Parallel Degraded Multi-receiver Wiretap Channels

We consider a special class of parallel degraded multi-receiver wiretap channels with two sub-channels, two users and one eavesdropper. We consider the scenario where each user receives both an independent message and a common message, which need be kept secret from the eavesdropper.

For the special class of channels in consideration, there is a specific degradation order in each sub-channel. Particularly, we have the following Markov chain

$$X_1 \to Y_{11} \to Y_{21} \to Z_1 \tag{21}$$

in the first sub-channel, and the following Markov chain

$$X_2 \to Y_{22} \to Y_{12} \to Z_2 \tag{22}$$

in the second sub-channel. Consequently, although in each sub-channel, one user is degraded with respect to the other one, this does not hold for the overall channel, and the overall channel is not degraded for any user. The corresponding transition probability of the channel is

$$p(y_{11}|x_1)p(y_{21}|y_{11})p(z_1|y_{21})p(y_{22}|x_2)p(y_{12}|y_{22})p(z_2|y_{12}) \tag{23}$$

A $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code for this channel consists of three message sets, $\mathcal{W}_j = \{1, \ldots, 2^{nR_j}\}, j = 0, 1, 2$, one encoder $f : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}_1^n \times \mathcal{X}_2^n$, two decoders one at each legitimate receiver $g_j : \mathcal{Y}_{j1}^n \times \mathcal{Y}_{j2}^n \to \mathcal{W}_0 \times \mathcal{W}_j, j = 1, 2$. The probability of error is defined as $P_e^n = \max_{j=1,2} \Pr\left[g_j(Y_{j1}^n, Y_{j2}^n) \neq (W_0, W_j)\right]$. A rate tuple (R_0, R_1, R_2) is said to be achievable if there exists a code such that $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z_1^n, Z_2^n) \geq \sum_{i\in\mathcal{S}(W)} R_i, \quad \forall\ \mathcal{S}(W) \tag{24}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_0, W_1, W_2\}$. The secrecy capacity region is the closure of all achievable secrecy rate tuples, and is given in the following theorem.

Theorem 4 The secrecy capacity region of the parallel degraded multi-receiver wiretap channel defined by (23) is the union of the rate tuples (R_0, R_1, R_2) satisfying

$$R_0 \leq I(U_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{25}$$

$$R_0 \leq I(U_1; Y_{21}|Z_1) + I(U_2; Y_{22}|Z_2) \tag{26}$$

$$R_0 + R_1 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{27}$$

$$R_0 + R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1) \tag{28}$$

$$R_0 + R_1 + R_2 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) + I(X_2; Y_{22}|U_2, Z_2) \tag{29}$$

$$R_0 + R_1 + R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1) + I(X_1; Y_{11}|U_1, Z_1) \tag{30}$$

where the union is over all $p(u_1)p(u_2)p(x_1|u_1)p(x_2|u_2)$.

Remark 4 If we let the encoder use an arbitrary joint distribution $p(u_1, x_1, u_2, x_2)$ instead of the ones that satisfy $p(u_1, x_1, u_2, x_2) = p(u_1, x_1)p(u_2, x_2)$, this would not enlarge the region given in Theorem 4, because all rate expressions in Theorem 4 depend on either $p(u_1, x_1)$ or $p(u_2, x_2)$ but not on the joint distribution $p(u_1, u_2, x_1, x_2)$.

Remark 5 The capacity achieving scheme uses either superposition coding in both sub-channels or superposition coding in one of the sub-channels, and a dedicated transmission in the other one. We again note that this superposition coding is different from the standard one [5] in the sense that it associates each message with many codewords by using stochastic encoding at each layer of the code due to secrecy concerns.

Remark 6 If we ignore the eavesdropper by setting $Z_1 = Z_2 = \phi$, this channel model reduces to the broadcast channel that was studied in [6], [7]. We recover the capacity region of the underlying broadcast channel [7] by setting $Z_1 = Z_2 = \phi$ in Theorem 4.

Remark 7 If we disable one of the sub-channels by setting $Y_{11} = Y_{21} = Z_1 = \phi$, the channel model of interest in this section reduces to the degraded multi-receiver wiretap channel. The corresponding secrecy capacity region is the union of the tuples (R_0, R_1, R_2) satisfying

$$R_0 + R_1 \leq I(U_2; Y_{12}|Z_2) \tag{31}$$

$$R_0 + R_1 + R_2 \leq I(X_2; Y_{22}|U_2, Z_2) + I(U_2; Y_{12}|Z_2) \tag{32}$$

where the union is over all $p(u_2, x_2)$. This region can be obtained through either Corollary 1 or Theorem 4 implying the consistency of the results.

V. Conclusions

In this paper, we studied secure broadcasting to many users in the presence of an eavesdropper. We took the approach of considering special classes of channels. In particular, we considered degraded multi-receiver wiretap channels, parallel multi-receiver wiretap channels with a more noisy eavesdropper, parallel multi-receiver wiretap channels with less noisiness orderings in each sub-channel, and parallel degraded multi-receiver wiretap channels. For each of these channels, we obtained either partial characterization of the secrecy capacity region or the entire region.

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 *Allerton Conf. Commun., Control and Computing*, Jul. 2008.

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

[6] G. S. Poltyrev. Capacity for a sum of certain broadcast channels. *Problemy Peredachi Informatsii*, 15(2):40–44, Apr.-Jun. 1979.

[7] A. El Gamal. Capacity of the product and sum of two unmatched broadcast channels. *Problemy Peredachi Informatsii*, 16(1):3–23, Jan.-Mar. 1980.