

Physical Layer Security in Broadcast Networks ¹

Yingbin Liang, H. Vincent Poor and Shlomo Shamai (Shitz) ²

Abstract

This paper reviews the information theoretic characterization of security in broadcast channels, in which a transmitter has both public and confidential messages intended for multiple receivers. All messages must be successfully received by their intended receivers, and the confidential messages must be kept as secret as possible from non-intended recipients. Various scenarios are considered in the context of two-user broadcast channels, for which known results on the secrecy capacity region are reviewed and corresponding coding schemes for achieving rates in these regions are described.

1 Introduction and System Model

Broadcast channels model communication networks in which one transmitter sends information to multiple receivers. The transmitter has information flows intended for all receivers or for only a subset of receivers, and the transmitter must guarantee that all information flows are successfully received by their corresponding intended receivers. Broadcast arises as a basic mode of communication in many practical networks such as downlink communication from a base station to cell phones in cellular networks and communication from access points to mobile users in wireless local networks (WLANs).

Security issues arise naturally in broadcast channels due to the open nature of such communication. Each receiver is able to receive signals that contain all information flows from the transmitter, although sometimes with weak signal strength. Hence, some receivers may decode information flows that are not intended for them. However, confidential information flows should be kept as secret as possible from non-intended receivers. This requires that the transmitter employ techniques to guarantee such security constraints. Information theoretic

¹The work of Y. Liang was supported by the National Science Foundation CAREER Award under Grant CCF-08-46028. The work of H. V. Poor was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637 and CCF-07-28208. The work of S. Shamai was supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++.

²Yingbin Liang is with the Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822, USA; yingbinl@hawaii.edu; H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544; e-mail: poor@princeton.edu; Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel; email: sshlomo@ee.technion.ac.il

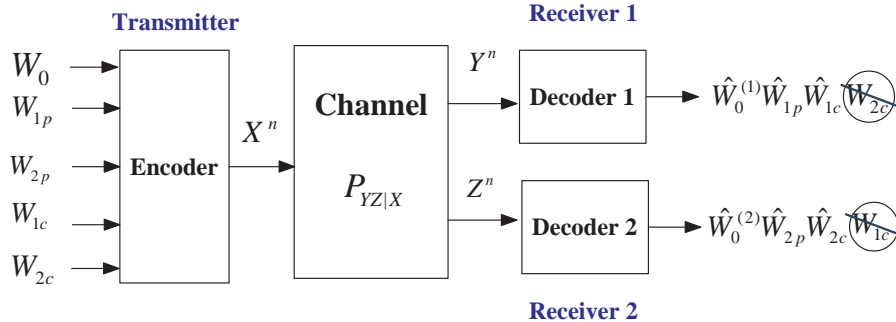


Figure 1: The two-user broadcast channel with confidential messages

approaches have been developed to achieve secure communication, initially over broadcast channels in [1, 2] and later on over other communication channels (see [3] for a general treatment of this problem). In this paper, we review information theoretic approaches to security for broadcast channels. We focus on the two-user broadcast channel referred to as the broadcast channel with confidential messages (BCC), which includes a rich set of scenarios as special cases. We first describe the general two-user BCC model, and then address the secrecy performance (i.e., the secrecy capacity region) and design of secure communication schemes for several special scenarios.

The two-user BCC model is depicted in Fig. 1, in which a transmitter has a common (public) message W_0 intended for receivers 1 and 2, two individual (public) messages W_{1p} and W_{2p} respectively for receivers 1 and 2, and two confidential messages W_{1c} and W_{2c} respectively for receivers 1 and 2. In particular, the confidential messages W_{1c} and W_{2c} should be kept as secret as possible from the other non-intended receiver, i.e., W_{1c} should be hidden from receiver 2 and W_{2c} should be hidden from receiver 1. Hence, a receiver is regarded as an eavesdropper with respect to a confidential message that is not intended for it.

The five messages W_0 , W_{1p} , W_{1c} , W_{2p} and W_{2c} are assumed to be uniformly distributed over finite sets \mathcal{W}_0 , \mathcal{W}_{1p} , \mathcal{W}_{1c} , \mathcal{W}_{2p} and \mathcal{W}_{2c} , respectively. A (stochastic) encoder at the transmitter $f : (\mathcal{W}_0, \mathcal{W}_{1p}, \mathcal{W}_{1c}, \mathcal{W}_{2p}, \mathcal{W}_{2c}) \rightarrow \mathcal{X}^n$ maps each message tuple $(w_0, w_{1p}, w_{1c}, w_{2p}, w_{2c}) \in (\mathcal{W}_0, \mathcal{W}_{1p}, \mathcal{W}_{1c}, \mathcal{W}_{2p}, \mathcal{W}_{2c})$ to a length- n codeword $x^n \in \mathcal{X}^n$, where \mathcal{X} is an input alphabet. The input x^n is transmitted over a broadcast channel having the transition probability $P_{YZ|X}(\cdot|\cdot)$, and there are corresponding output sequences y^n and z^n at receivers 1 and 2, respectively. At receiver 1, decoder 1 maps a received sequence $y^n \in \mathcal{Y}^n$ to a message triple $(\hat{w}_0^{(1)}, \hat{w}_{1p}, \hat{w}_{1c}) \in (\mathcal{W}_0, \mathcal{W}_{1p}, \mathcal{W}_{1c})$; i.e., decode 1 is a mapping $g_1: \mathcal{Y}^n \rightarrow (\mathcal{W}_0, \mathcal{W}_{1p}, \mathcal{W}_{1c})$. Similarly, at receiver 2, decoder 2 maps a received sequence $z^n \in \mathcal{Z}^n$ to a message triple

$(\hat{w}_0^{(2)}, \hat{w}_{2p}, \hat{w}_{2c}) \in (\mathcal{W}_0, \mathcal{W}_{2p}, \mathcal{W}_{2c})$; i.e., decoder 2 is a mapping $g_2: \mathcal{Z}^n \rightarrow (\mathcal{W}_0, \mathcal{W}_{2p}, \mathcal{W}_{2c})$.

A *rate-equivocation tuple* $(R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c}, R_{1e}, R_{2e})$ is *achievable* if there exists a sequence of message sets $(\mathcal{W}_{0n}, \mathcal{W}_{1pn}, \mathcal{W}_{1cn}, \mathcal{W}_{2pn}, \mathcal{W}_{2cn})$ with $|\mathcal{W}_{0n}| = 2^{nR_0}$, $|\mathcal{W}_{1pn}| = 2^{nR_{1p}}$, $|\mathcal{W}_{1cn}| = 2^{nR_{1c}}$, $|\mathcal{W}_{2pn}| = 2^{nR_{2p}}$ and $|\mathcal{W}_{2cn}| = 2^{nR_{2c}}$, and encoder-decoder triples (f_n, g_{1n}, g_{2n}) such that the average error probability

$$P_e^{(n)} = Pr \left\{ (\hat{W}_0^{(1)}, \hat{W}_0^{(2)}, \hat{W}_{1p}, \hat{W}_{1c}, \hat{W}_{2p}, \hat{W}_{2c}) \neq (W_0, W_0, W_{1p}, W_{1c}, W_{2p}, W_{2c}) \right\} \rightarrow 0$$

as n goes to infinity and the equivocation rates R_{1e} and R_{2e} satisfy

$$R_{1e} \leq \liminf_{n \rightarrow \infty} \frac{1}{n} H(W_{1c} | Z^n) \quad \text{and} \quad (1)$$

$$R_{2e} \leq \liminf_{n \rightarrow \infty} \frac{1}{n} H(W_{2c} | Y^n). \quad (2)$$

We note that the equivocation rates R_{1e} and R_{2e} measure the secrecy levels respectively for the confidential messages W_{1c} and W_{2c} (see [3] for further discussion of the notion of equivocation). The larger the equivocation rate, the higher the secrecy level of the confidential message.

The *capacity-equivocation region* \mathcal{C} is the closure of the set that consists of all achievable rate-equivocation tuples $(R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c}, R_{1e}, R_{2e})$. The *secrecy capacity region* \mathcal{C}_s is the region that includes all achievable rate tuples $(R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c})$ such that perfect secrecy is achieved, i.e., $R_{1e} = R_{1c}$ and $R_{2e} = R_{2c}$. The secrecy capacity region can be expressed as:

$$\mathcal{C}_s = \{(R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c}) : (R_0, R_{1p}, R_{1c}, R_{2p}, R_{2c}, R_{1c}, R_{2c}) \in \mathcal{C}\}. \quad (3)$$

Characterizing the capacity-equivocation region for the general two-user BCC with five messages is difficult, considering that its special case of the capacity region of the two-user broadcast channel remains unknown [4]. In the following sections, we review the capacity-equivocation regions and secrecy capacity regions that have been characterized for some special cases of the general BCC. In doing so, we will introduce basic techniques to address secure communication over broadcast channels, which will also provide insight into the solution to the general problem.

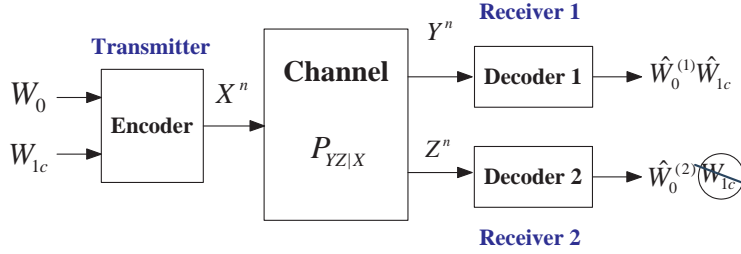


Figure 2: The BCC with one common and one confidential messages

2 BCCs with One Common and One Confidential Messages

The BCC was first studied by Csiszár and Körner [2] for the case in which the transmitter has a common message W_0 for both receivers and a confidential message W_{1c} for receiver 1, and wishes to keep W_{1c} as secret as possible from receiver 2 (see Fig. 2). This model can be specialized from the general model described in Section 1 by setting $R_{1p} = 0$, $R_{2p} = 0$, and $R_{2c} = 0$. The rate-equivocation tuple now contains three components (R_0, R_{1c}, R_{1e}) . The capacity-equivocation region for this model has been obtained in [2] and is given in the following theorem.

Theorem 1. [2] *The capacity-equivocation region of the BCC with one common and one confidential messages is given by*

$$\mathcal{C} = \bigcup_{P_{QU} P_{X|U} P_{YZ|X}} \left\{ \begin{array}{l} (R_0, R_{1c}, R_{1e}) : \\ R_0 \geq 0, R_{1c} \geq 0, R_{1e} \geq 0 \\ R_0 \leq \min\{I(Q; Y), I(Q; Z)\} \\ R_0 + R_{1c} \leq I(U; Y|Q) + \min\{I(Q; Y), I(Q; Z)\} \\ R_{1e} \leq I(U; Y|Q) - I(U; Z|Q) \end{array} \right\}, \quad (4)$$

where the auxiliary random variables U and Q satisfy the Markov chain relationship $Q \rightarrow U \rightarrow X \rightarrow (Y, Z)$, and are bounded in cardinality by $|\mathcal{Q}| \leq |\mathcal{X}| + 3$ and $|\mathcal{U}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$, respectively.

The roles of the auxiliary random variables U and Q in Theorem 1 can be understood in the context of the coding scheme that achieves the region (4). The variable U represents the total information contained in the channel input, including both the common and confidential messages. The variable Q represents the common message W_0 that is part of the information represented by U , and is incorporated into U by superposition coding. The remaining part

of the information represented by U is constructed to be hidden to the extent possible (measured by the secrecy level) from receiver 2.

We note that two additional techniques have also been employed to improve the achievable scheme. The first one involves introducing a prefix channel from U to X , i.e., the equivalent channel becomes $P_{YZ|U}(\cdot|\cdot)$. Such an equivalent channel is at least as good as the original channel by setting $U = X$, but may be better. The second technique involves moving bits from the common rate to the confidential rate, which is based on the fact that if the rate-equivocation triple (R_0, R_{1c}, R_{1e}) is achievable, then $(R_0 - \Delta, R_{1c} + \Delta, R_{1e})$ is also achievable, where $0 \leq \Delta \leq R_0$. This follows because a part Δ of the common rate R_0 is clearly decodable at receiver 1, and hence can be moved to be a part of the rate R_{1c} . This is reflected by the bound on the sum rate $R_0 + R_{1c}$ in (4), as R_0 and R_{1c} share a total rate. However, since this part Δ of the common rate R_0 is known at receiver 2 (the eavesdropper with respect to the confidential message), it does not change the equivocation rate R_{1e} .

The fact that the above scheme achieves the secrecy capacity region, i.e., is optimal, was shown by a converse proof given in [2], which is omitted here. We note that this converse proof provides important techniques to construct auxiliary random variables and exploit properties of the summation of mutual information terms, which are very useful for proving converse and outer bounds on the (secrecy) capacity region for multi-user channels in general. We refer the reader to Reference [2] for details.

The following secrecy capacity region corresponding to the case of perfect secrecy follows directly from Theorem 1 by setting $R_{1e} = R_{1c}$.

Corollary 1. [2] *The secrecy capacity region of the BCC with one common and one confidential messages is given by*

$$\mathcal{C}_s = \bigcup_{P_{QU}P_{X|U}P_{YZ|X}} \left\{ \begin{array}{l} (R_0, R_{1c}) : \\ 0 \leq R_0 \leq \min\{I(Q; Y), I(Q; Z)\} \\ 0 \leq R_{1c} \leq I(U; Y|Q) - I(U; Z|Q) \end{array} \right\}, \quad (5)$$

where the auxiliary random variables Q and U satisfy the Markov chain relationship $Q \rightarrow U \rightarrow X \rightarrow (Y, Z)$, and are bounded in cardinality by $|\mathcal{Q}| \leq |\mathcal{X}| + 3$ and $|\mathcal{U}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$, respectively.

Remark 1. *If there is no secrecy constraint for the confidential message W_{1c} , i.e., replacing W_{1c} with W_{1p} , the above BCC model becomes the broadcast channel with degraded message sets, for which the capacity region has been obtained in [5].*

We next consider the Gaussian and multiple-input multiple-output (MIMO) channel examples of the BCC with one common and one confidential messages.

2.1 Gaussian BCC

We consider the Gaussian BCC, in which the channel outputs at each symbol time (i.e., channel use) are given by

$$Y = X + W \quad \text{and} \quad Z = X + V, \quad (6)$$

where the noise variables W and V are Gaussian with respective variances μ^2 and ν^2 , and each is independent and identically distributed (i.i.d.) over channel uses. The channel input sequence X^n is subject to the average power constraint P , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E}[X_i^2] \leq P \quad (7)$$

where i denotes the symbol time index.

The secrecy capacity region for the Gaussian BCC can be obtained from Corollary 1 by choosing Gaussian input distribution, i.e., choosing $Q \sim \mathcal{N}(0, (1-\beta)P)$ and $X = Q + X'$ with $X' \sim \mathcal{N}(0, \beta P)$ and independent of Q . The converse proof can be found in Reference [6].

Theorem 2. [6] *The secrecy capacity region of the Gaussian BCC with one common and one confidential messages is given by*

$$\mathcal{C}_s = \bigcup_{0 \leq \beta \leq 1} \left\{ \begin{array}{l} (R_0, R_1) : \\ 0 \leq R_0 \leq \min \left\{ \frac{1}{2} \log \left(1 + \frac{(1-\beta)P}{\mu^2 + \beta P} \right), \frac{1}{2} \log \left(1 + \frac{(1-\beta)P}{\nu^2 + \beta P} \right) \right\} \\ 0 \leq R_1 \leq \left[\frac{1}{2} \log \left(1 + \frac{\beta P}{\mu^2} \right) - \frac{1}{2} \log \left(1 + \frac{\beta P}{\nu^2} \right) \right]^+ \end{array} \right\} \quad (8)$$

In the above region, β represents power allocation between common and confidential messages. As β increases, R_1 increases and R_0 decreases. It is also clear that positive secrecy rate is achieved only if $\mu^2 < \nu^2$.

Remark 2. *The above Gaussian BCC model becomes the Gaussian wire-tap channel if there is no common message W_0 , for which the secrecy capacity has been obtained in [7].*

2.2 MIMO BCC

We consider the MIMO BCC, in which N_T , N_{R1} , and N_{R2} antennas are deployed at the transmitter, receiver 1, and receiver 2, respectively. The channel input-output relationship

for one channel use is given by

$$\begin{aligned}\underline{Y} &= H\underline{X} + \underline{W} \\ \underline{Z} &= G\underline{X} + \underline{V}\end{aligned}\tag{9}$$

where \underline{X} is the channel input vector with N_T components, and \underline{Y} is the channel output vector at receiver 1 with N_{R1} components, and \underline{Z} is the channel output vector at receiver 2 with N_{R2} components. The channel matrices H and G are fixed $N_{R1} \times N_T$ and $N_{R2} \times N_T$ matrices, respectively. The noise vectors \underline{W} and \underline{V} consist of i.i.d. Gaussian components with zero means and unit variances. As in the scalar model, the noise vectors are i.i.d. over channel uses as well. The channel input is assumed to be subject to an average matrix power constraint:

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\underline{X}_i \underline{X}_i^T] \preceq S,\tag{10}$$

where S is a positive semidefinite matrix, and $A \preceq B$ denotes that $B - A$ is a positive semidefinite matrix.

For the MIMO BCC, the following secrecy capacity region was established in [8].

Theorem 3. [8] *The secrecy capacity region of the MIMO BCC with one common and one confidential messages is given by*

$$\mathcal{C}_s = \bigcup_{0 \preceq K \preceq S} \left\{ \begin{array}{l} (R_0, R_{1c}) : \\ 0 \leq R_0 \leq \min \left\{ \frac{1}{2} \log \left| \frac{HSH^T + I}{HKH^T + I} \right|, \frac{1}{2} \log \left| \frac{GSG^T + I}{GKG^T + I} \right| \right\} \\ 0 \leq R_{1c} \leq \frac{1}{2} \log |HKH^T + I| - \frac{1}{2} \log |GKG^T + I| \end{array} \right\}.\tag{11}$$

As for the Gaussian BCC, the achievability of the above region follows from Corollary 1 by choosing jointly Gaussian input vectors, i.e., choosing Q to be a Gaussian vector with mean zero and covariance matrix $S - K$ and choosing $X = Q + X'$ with X' being a Gaussian vector with mean zero and covariance matrix K and independent of Q . We note that the covariance matrix K plays the same role as the parameter β for the Gaussian BCC, and hence represents resource allocation between common and confidential messages. To show the Gaussian input is optimal, i.e., achieves the secrecy capacity region, a proof of the converse was provided in [8]. The proof is based on the converse techniques for proving Theorem 1 and the channel enhancement approach, which was first proposed to establish the capacity region for the MIMO broadcast channel in [9]. The details can be found in [8].

Remark 3. *The above MIMO BCC model becomes the MIMO wire-tap channel if there is no common message W_0 , for which the secrecy capacity has been obtained in [10, 11]. An*

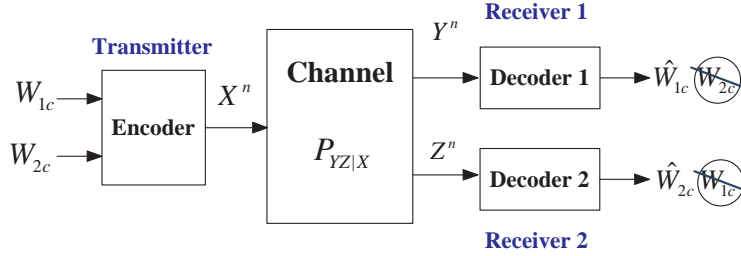


Figure 3: The broadcast channel with two confidential messages

alternative converse proof based on a channel enhancement idea [9] and an extremal entropy inequality [12, 13] was provided in [14], and a MMSE approach has been proposed in [15]. The secrecy capacity of a special case of the MIMO wire-tap channel in which the transmitter and the receiver each has two antennas and the eavesdropper has one antenna is given in [16].

3 BCCs with Two Confidential Messages

In this section, we consider the BCC with two confidential messages, i.e., the transmitter has two confidential messages W_{1c} and W_{2c} for respective receivers 1 and 2, and wishes to keep each message secret from the non-intended receiver (see Fig. 3). This model can be specialized from the general two-user BCC model described in Section 1 by setting $R_0 = 0$, $R_{1p} = 0$, and $R_{2p} = 0$. This model has been studied in [17] for the case of perfect secrecy, i.e., each confidential message is perfectly hidden from the non-intended receiver. The secrecy capacity region for this model includes all achievable secrecy rate pairs (R_{1c}, R_{2c}) . The following inner and outer bounds on the secrecy capacity region were obtained in [17].

Theorem 4. [17] *For the BCC with two confidential messages, an inner bound on the secrecy capacity region is given by*

$$\mathcal{R} = \bigcup_{P_{QU_1U_2}P_{X|U_1U_2}P_{YZ|X}} \left\{ \begin{array}{l} (R_{1c}, R_{2c}) : \\ 0 \leq R_{1c} \leq I(U_1; Y|Q) - I(U_1; U_2|Q) - I(U_1; Z|U_2, Q) \\ 0 \leq R_{2c} \leq I(U_2; Z|Q) - I(U_1; U_2|Q) - I(U_2; Y|U_1, Q) \end{array} \right\}, \quad (12)$$

where Q is a time-sharing auxiliary random variable.

An outer bound on the secrecy capacity region is given by

$$\bar{\mathcal{R}} = \bigcup_{P_{QU_1U_2}P_{X|U_1U_2}P_{YZ|X}} \left\{ \begin{array}{l} (R_{1c}, R_{2c}) : \\ 0 \leq R_{1c} \leq \min\{I(U_1; Y|Q) - I(U_1; Z|Q), \\ \quad I(U_1; Y|U_2, Q) - I(U_1; Z|U_2, Q)\} \\ 0 \leq R_{2c} \leq \min\{I(U_2; Z|Q) - I(U_2; Y|Q), \\ \quad I(U_2; Z|U_1, Q) - I(U_2; Y|U_1, Q)\} \end{array} \right\}. \quad (13)$$

In both the inner and outer bounds, the auxiliary random variables Q , U_1 and U_2 satisfy the Markov chain relationships $Q \rightarrow U_1 \rightarrow X$, $Q \rightarrow U_2 \rightarrow X$, and $(Q, U_1, U_2) \rightarrow X \rightarrow (Y, Z)$.

An encoding scheme that achieves the region (12) uses the *double binning scheme*, which combines the Gel'fand-Pinsker binning [18] and the random binning. This scheme also causes both bounds on R_{1c} and R_{2c} to include a penalty term $I(U_1, U_2|Q)$ in order to guarantee perfect secrecy constraints. This is in contrast to Marton's inner bound [19] on the capacity region of the broadcast channel without secrecy constraints, where only the sum rate includes the penalty term. We refer the reader to [17] for the details of the proof of Theorem 4.

In general, the inner and outer bounds given in Theorem 4 do not match, and hence the secrecy capacity region for the BCC with two confidential messages is not known in general. We next consider multiple-input single-output (MISO) and MIMO channel examples of the BCC with two confidential messages, for which the secrecy capacity region can be characterized.

3.1 MISO BCC

We consider the MISO BCC with two confidential messages, in which the transmitter has N_T antennas, and each receiver has a single antenna. The input-output relationship at one time instant is given by

$$\begin{aligned} Y &= \underline{H}^T \underline{X} + W \\ Z &= \underline{G}^T \underline{X} + V \end{aligned} \quad (14)$$

where \underline{X} is the N_T -dimensional input vector, and \underline{H} and \underline{G} are N_T -dimensional channel vectors. The noise variables W and V are Gaussian with zero mean and unit variance, and are i.i.d. over channel uses. The channel input is subject to an average power constraint:

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\underline{X}_i^T \underline{X}_i] \leq P. \quad (15)$$

The MISO BCC channel was studied in [20] and the following secrecy capacity region was obtained.

Theorem 5. [20] *The secrecy capacity region of the MISO BCC with two confidential messages is given by*

$$\mathcal{C}_s = \mathbf{Conv} \left\{ \bigcup_{0 \leq \alpha \leq 1} \left\{ \begin{array}{l} (R_{1c}, R_{2c}) : \\ 0 \leq R_{1c} \leq \log \gamma_1(\alpha) \\ 0 \leq R_{2c} \leq \log \gamma_2(\alpha) \end{array} \right\} \right\} \quad (16)$$

where $\mathbf{Conv}(A)$ denotes the convex hull of the set A , and

$$\gamma_1(\alpha) = \frac{1 + \alpha P |\underline{H}^T \underline{e}_1|^2}{1 + \alpha P |\underline{G}^T \underline{e}_1|^2} \quad (17)$$

with \underline{e}_1 being the normalized eigenvector corresponding to the largest generalized eigenvalue (see the definition of the generalized eigenvalue in [20, Appendix A]) of the pencil

$$(I + P \underline{H} \underline{H}^T, I + P \underline{G} \underline{G}^T).$$

In equation (16), $\gamma_2(\alpha)$ is the largest generalized eigenvalue of the pencil

$$\left(I + \frac{(1 - \alpha)P}{1 + \alpha P |\underline{G}^T \underline{e}_1|^2} \underline{G} \underline{G}^T, I + \frac{(1 - \alpha)P}{1 + \alpha P |\underline{H}^T \underline{e}_1|^2} \underline{H} \underline{H}^T \right).$$

The achievable scheme for the secrecy capacity region given in (16) involves design of a dirty paper coding strategy [21, 22] jointly with a double binning strategy proposed to achieve the rate region given in (12) for the BCC with two confidential messages in general. To show this scheme is optimal, i.e., achieves the secrecy capacity region, a converse proof was provided in [20], which is based on the Sato-type outer bound [23]. In particular, an enhanced BCC was considered, in which receiver 1 also obtains the output at receiver 2, and hence the performance of the enhanced channel provides an outer bound on that of the original channel. This proof is similar to the technique applied in [10, 11] to prove the secrecy capacity for the MIMO wire-tap channel.

3.2 MIMO BCCs

We consider the MIMO BCC with two confidential messages, which is a generalization of the model addressed in the preceding subsection. The MIMO BCC model here is exactly the same as that described in Section 2.2 except that now the transmitter has two confidential messages with each intended for one receiver and hidden from the other (non-intended) receiver. The secrecy capacity region of this channel was established recently in [24].

Theorem 6. [24] *The secrecy capacity region of the MIMO BCC with two confidential messages is given by*

$$\mathcal{C}_s = \bigcup_{0 \preceq B_1, 0 \preceq B_2, B_1 + B_2 \preceq S} \left\{ \begin{array}{l} (R_{1c}, R_{2c}) : \\ 0 \leq R_{1c} \leq \frac{1}{2} \log |HB_1H^T + I| - \frac{1}{2} \log |GB_1G^T + I| \\ 0 \leq R_{2c} \leq \frac{1}{2} \log \frac{|G(B_1 + B_2)G^T + I|}{|GB_1G^T + I|} - \frac{1}{2} \log \frac{|H(B_1 + B_2)H^T + I|}{|HB_1H^T + I|} \end{array} \right\} \quad (18)$$

As for the MISO BCC with two confidential messages studied in Section 3.1, the achievable scheme applies the double binning strategy. The region (18) follows by choosing the Gaussian input for the region (12). However, the converse proof for the MIMO BCC requires further technicality than that for the MISO BCC, and it further applies the channel enhancement technique, which was first introduced in [9] for the converse proof for the MIMO Gaussian broadcast channel without secrecy constraints. The details of the proof can be found in [24].

4 BCCs with Full Message Sets

In this section, we consider the BCC with full message sets, i.e., with one common, two private, and two confidential messages. As we commented before, a precise characterization of the secrecy capacity region for this general model is very difficult. In such circumstances, it may be useful to study specific channels to obtain some understanding of the issues involved. This motivates the study of the MIMO linear deterministic BCC in [8], which may serve as an approximate characterization for the Gaussian MIMO BCC in the high SNR regime [25, 26]. To be specific, the channel input-output relationship of the MIMO linear deterministic BCC considered in [8] is given by

$$\begin{aligned} \underline{Y} &= H\underline{X} \\ \underline{Z} &= G\underline{X} \end{aligned} \quad (19)$$

where H and G are respectively $N_{R1} \times N_T$ and $N_{R2} \times N_T$ matrices both with entries in \mathbb{F}^m , where \mathbb{F} is a finite field. We note that the additive noise is suppressed as an approximation of the high SNR limit for the Gaussian MIMO BCC. The channel input \underline{X} is a vector in \mathbb{F}^m . The operation of the multiplication ³ is over \mathbb{F}^m . The transmission rates $(R_0, R_{1p}, R_{2p}, R_{1c}, R_{2c})$

³In a more rigorous sense, the input vector \underline{X} is a super-vector with each entry being an m -dimensional vector with components in \mathbb{F} , and the matrices H and G are super-matrices with each entry being an

are expressed in terms of $\log_2 |\mathbb{F}|$ bits per channel use. Hence, the capacity result is not affected by the size of the field.

We use \mathcal{A}_k for $k = 1, 2$ to denote the vector spaces spanned by the row vectors in H and G , respectively, and use \mathcal{A}_k^\perp , $k = 1, 2$, to denote the corresponding null spaces. Let a_k be the dimension of the space \mathcal{A}_k for $k = 1, 2$. We note that $a_1 = \text{Rank}(H)$ and $a_2 = \text{Rank}(G)$ are the capacities for the point-to-point channels from the transmitter to receivers 1 and 2, respectively. Similarly, let a_{12} be the dimension of the linear space $\mathcal{A}_1 \cup \mathcal{A}_2$. Then

$$a_{12} = \text{Rank} \left(\begin{bmatrix} H \\ G \end{bmatrix} \right)$$

is the capacity for the channel from the transmitter to receivers 1 and 2 if the two receivers perfectly cooperate to decode the messages. The following secrecy capacity region for the MIMO linear deterministic BCC was given in [8].

Theorem 7. [8] *The secrecy capacity region of the MIMO linear deterministic BCC with full message sets is given by*

$$\mathcal{C}_s = \left\{ \begin{array}{l} (R_0, R_{1p}, R_{2p}, R_{1c}, R_{2c}) : \\ R_0 \geq 0, R_{1p} \geq 0, R_{2p} \geq 0, R_{1c} \geq 0, R_{2c} \geq 0 \\ R_0 + R_{1p} + R_{1c} \leq a_1 \\ R_0 + R_{2p} + R_{2c} \leq a_2 \\ R_{1c} \leq a_{12} - a_2 \\ R_{2c} \leq a_{12} - a_1 \\ R_0 + R_{1p} + R_{1c} + R_{2p} + R_{2c} \leq a_{12} \end{array} \right\} \quad (20)$$

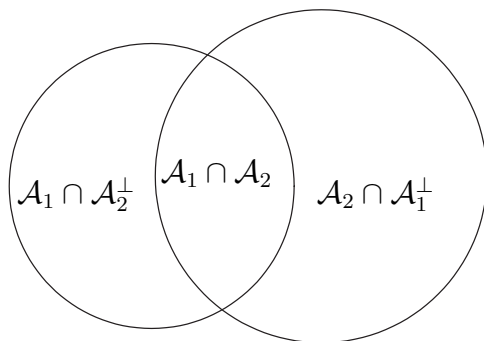


Figure 4: Illustration of vector spaces associated with the channel matrices H and G .

$m \times m$ matrix with components in \mathbb{F} . Hence the multiplication of an entry in H and an entry in \underline{X} is the multiplication of an $m \times m$ matrix with an m -dimensional vector over the finite field \mathbb{F} , which results in an m -dimensional vector, i.e., a symbol in \mathbb{F}^m .

The achievable scheme uses beamforming techniques to transmit the messages along basis vectors chosen from the linear vector spaces $\mathcal{A}_1 \cap \mathcal{A}_2^\perp$, $\mathcal{A}_1 \cap \mathcal{A}_2$, and $\mathcal{A}_2 \cap \mathcal{A}_1^\perp$ (see Fig. 4). These basis vectors are referred to as *beamforming directions*. It is clear that information bits transmitted along beamforming directions (basis vectors) in $\mathcal{A}_1 \cap \mathcal{A}_2$ can be received by both receivers, information bits transmitted along directions in $\mathcal{A}_1 \cap \mathcal{A}_2^\perp$ is received by receiver 1, but not by receiver 2. Hence these information bits are perfectly secret from receiver 2. Similarly, information bits transmitted along directions in $\mathcal{A}_2 \cap \mathcal{A}_1^\perp$ is received by receiver 2, but not receiver 1, and hence are perfectly secret from receiver 1. Therefore, the common message W_0 can be sent along all directions, the private messages W_{1p} and W_{2p} can be sent along directions in \mathcal{A}_1 and \mathcal{A}_2 , respectively, and the confidential messages W_{1c} and W_{2c} must be sent along directions in $\mathcal{A}_1 \cap \mathcal{A}_2^\perp$ and $\mathcal{A}_2 \cap \mathcal{A}_1^\perp$, respectively. We refer the reader to [8] for details of this scheme.

The fact that the above scheme achieves the secrecy capacity region, i.e., is optimal, follows from several straightforward upper bounds. The first two inequalities in (20) follow from the point-to-point capacity constraints for receivers 1 and 2, respectively. The next two inequalities in (20) follow from the capacity of the wire-tap channel if W_{1c} (respectively W_{2c}) is sent to receiver 1 (respectively receiver 2) and needs to be secret from receiver 2 (respectively receiver 1). The last inequality in (20) follows from the channel capacity if two receivers perfectly cooperate to decode information from the transmitter.

5 BCCs with One Common and Two Confidential Messages

In this section, we consider the BCC with one common and two confidential messages, i.e., the transmitter has one common message for both receivers, and two confidential messages intended for each receiver and hidden from the other (non-intended receiver). This model can be specialized from the general model described in Section 1 by setting $R_{1p} = 0$, $R_{2p} = 0$. This model was studied in [34], in which lower and upper bounds on the capacity-equivocation region were derived that generalize the corresponding bounds given in Theorem 4.

In this section, we focus on the case of the Gaussian compound MIMO BCC studied in Reference [27], in which the channel from the transmitter to two receivers takes one state from a finite set of states. The transmitter knows the state set, but does not know the realization of the channel state. It is required that no matter which channel state occurs, all messages must be successfully transmitted to corresponding receivers and the confidential

messages must be kept secret from the corresponding non-intended receiver. In particular, the channel outputs of receivers 1 and 2 at each channel use are given by

$$\begin{aligned}\underline{Y} &= H_j \underline{X} + \underline{W} \quad \text{for } j = 1, \dots, J_1 \\ \underline{Z} &= G_l \underline{X} + \underline{V} \quad \text{for } l = 1, \dots, J_2\end{aligned}\tag{21}$$

where J_1 and J_2 denote respectively the number of possible channel states of receivers 1 and 2, H_j denotes the channel matrix at state j with dimension $N_{R1} \times N_T$, and G_l denotes the channel matrix at state l with dimension $N_{R2} \times N_T$. The noise vectors \underline{W} and \underline{V} consist of i.i.d. Gaussian components with zero means and unit variances. As in the scalar model, the noise is i.i.d. over channel uses as well, and the source input is subject to an average power constraint:

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\underline{X}_i^T \underline{X}_i] \leq P.\tag{22}$$

A precise characterization of the secrecy capacity region for this channel is difficult, considering the capacity region of its special case of the MIMO Gaussian broadcast channel with common and two private (not confidential) messages is unknown [28]. This motivates the study in [27] of the degree of freedom (d.o.f.) that characterizes the rate region in the high SNR regime. The degrees of freedom (d.o.f.s) of the common and confidential messages are defined, respectively, as

$$r_0 = \lim_{P \rightarrow \infty} \frac{R_0(P)}{\log(P)} \quad \text{and} \quad r_{kc} = \lim_{P \rightarrow \infty} \frac{R_{kc}(P)}{\log(P)}, \quad \text{for } k = 1, 2.$$

We first note that the secrecy rate region in Reference [34] was extended to yield the following secrecy rate region in [27] for the compound BCC with one common and two confidential messages:

$$\mathcal{R}_s = \bigcup_{P_{QU_1U_2} P_{X|U_1U_2} P_{YZ|X}} \left\{ \begin{array}{l} (R_0, R_{1c}, R_{2c}) : \\ R_0 \geq 0, R_{1c} \geq 0, R_{2c} \geq 0 \\ R_0 \leq \min_j I(Q; Y_j) \\ R_0 \leq \min_l I(Q; Z_l) \\ R_1 \leq \min_{j,l} [I(U_1; Y_j|Q) - I(U_1; Z_l, U_2|Q)] \\ R_2 \leq \min_{j,l} [I(U_2; Z_l|Q) - I(U_2; Y_j, U_1|Q)] \end{array} \right\}\tag{23}$$

Based on the preceding region, the following secrecy d.o.f. region was given in [27].

Theorem 8. [27] *Consider the Gaussian compound MIMO BCC with one common and two confidential messages, in which any set of N_T rows taken from the matrices $H_1, \dots, H_{J_1}, G_1, \dots, G_{J_2}$ has rank N_T . If $J_1 N_{R1} < N_T$ and $J_2 N_{R2} < N_T$, an achievable secrecy d.o.f. region is given*

by

$$r_s = \left\{ \begin{array}{l} (r_0, r_{1c}, r_{2c}) : \\ r_0 \geq 0, r_{1c} \geq 0, r_{2c} \geq 0 \\ r_1 \leq \min(N_{R1}, N_T - J_2 N_{R2}) \\ r_2 \leq \min(N_{R2}, N_T - J_1 N_{R1}) \\ r_0 + r_1 \leq N_{R1} \\ r_0 + r_2 \leq N_{R2} \end{array} \right\} \quad (24)$$

The achievable scheme uses a simple linear beamforming strategy. The beamforming directions for sending messages are chosen as follows. It can be shown that for $0 \leq r_1 \leq \min(N_{R1}, N_T - J_2 N_{R2})$ and $0 \leq r_2 \leq \min(N_{R2}, N_T - J_1 N_{R1})$, there exist $\underline{a}_k^1, \dots, \underline{a}_k^{r_k}$ for $k = 1, 2$, each with dimension N_T that form a matrix $A_k = [\underline{a}_k^1 \cdots \underline{a}_k^{r_k}]$, such that

$$H_j A_2 = 0 \quad \text{for } j = 1, \dots, J_1, \quad (25)$$

$$G_l A_1 = 0 \quad \text{for } l = 1, \dots, J_2, \quad (26)$$

and $\text{Rank}(H_j A_1) = r_1$ for $j = 1, \dots, J_1$ and $\text{Rank}(G_l A_2) = r_2$ for $l = 1, \dots, J_2$. Hence, vectors in A_2 are in the null space of all row vectors in H_1, \dots, H_{J_1} , and vectors in A_1 are in the null space of all row vectors in G_1, \dots, G_{J_2} . Based on A_1 and A_2 , we let $\underline{a}_0^1, \dots, \underline{a}_0^{N_T - \text{Rank}[A_1 \ A_2]}$ be orthonormal vectors in the null space of $[A_1 \ A_2]$.

The confidential messages W_{1c} and W_{2c} are transmitted respectively along the vectors in A_1 and A_2 . It is clear that receiver 1 cannot receive message W_{2c} due to (25), and receiver 2 cannot receive message W_{1c} due to (26), thus achieving secrecy for the two confidential messages. The common information W_0 is transmitted along the directions $\underline{a}_0^1, \dots, \underline{a}_0^{N_T - \text{Rank}[A_1 \ A_2]}$. Further details about this scheme can be found in [27].

Theorem 8 addressed the case when $J_1 N_{R1} < N_T$ and $J_2 N_{R2} < N_T$. By using the beamforming scheme similar to that used for achieving the d.o.f. region given in Theorem 8, we obtain the achievable d.o.f. regions for other cases, as follows.

Corollary 2. [27] *For the Gaussian compound MIMO BCC with one common and two confidential messages, if $J_1 N_{R1} < N_T$ and $J_2 N_{R2} \geq N_T$, an achievable d.o.f. region includes all nonnegative triples of the form $(r_0, 0, r_2)$ that satisfy $r_0 \leq \min(N_{R1}, N_{R2} - r_2)$ and $r_2 \leq \min(N_{R2}, N_T - J_1 N_{R1})$.*

Corollary 3. [27] *For the Gaussian compound MIMO-BCC with one common and two confidential messages, if $J_1 N_{R1} \geq N_T$ and $J_2 N_{R2} \geq N_T$, an achievable d.o.f. region includes all nonnegative triples of the form $(r_0, 0, 0)$ with r_0 satisfying $r_0 \leq \min(N_T, N_{R1}, N_{R2})$.*

We now consider the special case in which $J_1 = J_2 = 1$, i.e., the Gaussian MIMO BCC. The above beamforming strategy suggests to transmit confidential message W_{kc} in the null

space of the channel matrix of the other receiver. This yields the achievable d.o.f. conditions $r_1 \leq \min(N_{R1}, N_T - N_{R2})$ and $r_2 \leq \min(N_{R2}, N_T - N_{R1})$ for $N_T > \max(N_{R1}, N_{R2})$. We note that this beamforming strategy is in fact optimal for this case, which follows from the secrecy capacity of the MIMO wire-tap channel [10, 11, 14]. Furthermore, for the case in which $J_1 = J_2 = 1$ and $N_{R1} + N_{R2} > N_T$, Theorem 8 implies the sum-d.o.f. is N_T , which is also the maximum achievable sum-d.o.f.

Remark 4. *The above Gaussian compound MIMO BCC model can specialize to the Gaussian compound MIMO wire-tap channel if there is no common message and only one confidential message. The secrecy capacity for this channel has been obtained in [29] if the channel is also degraded.*

Remark 5. *The above Gaussian compound MIMO BCC model can specialize to the Gaussian compound MIMO broadcast channel if the confidential messages need not to be kept secret from the non-intended receivers. Such a broadcast channel has been studied in [13, 30], and the capacity region has been obtained for some special cases.*

6 Other Models and Associated Issues

In the previous sections, we have focused on the general discrete memoryless BCC and its Gaussian and MIMO channel examples. Based on these basic channels, other interesting specific channels and scenarios have been studied, many of which are motivated by applications in wireless networks, and address secrecy issues with other communication issues such as power allocation, scheduling, and delay constraints. In this section, we briefly review these studies.

For the BCC with one common and one confidential messages, the parallel BCC with L independent subchannels was studied in [6]. The secrecy capacity region for this case was given in [6], and it was shown that having independent inputs for each subchannel is optimal. The fading BCC was further studied in [6], in which the channels from the transmitter to receivers 1 and 2 are corrupted by multiplicative fading gain processes in addition to additive white Gaussian noise processes. The fading BCC can be viewed as a parallel Gaussian BCC with each fading state corresponding to one subchannel. The ergodic performance, i.e., the secrecy capacity region, of the fading BCC was obtained in [6] for the case when both the transmitter and receivers know the channel state information. The boundary of the secrecy capacity region was characterized by the optimal transmitter power allocations among fading states. The outage performance of the fading BCC was also studied

in [6], where messages must be transmitted over a certain time to satisfy the delay constraint. Under the assumption of long term average power constraint over multiple blocks, the power allocations that minimize the outage probability were obtained under several performance requirements.

For the BCC with two confidential messages, the ergodic fading compound MISO channel was studied in [27], in which the channel state to each receiver at each block is randomly uniformly chosen from a finite set of states. The transmitter is assumed to know the state sets, but not the realization of states. An achievable d.o.f. region was derived based on the zero-forcing beamforming idea, similar to the approach discussed in Section 5. The achievable scheme also applied the variable-rate transmission proposed in [31] to achieve better rates. It was demonstrated that the time variation of the channel state creates an additional temporal dimension, and significantly improves the d.o.f. region with respect to the same model but with constant channel state.

The fading BCC with more than two confidential messages was studied in [32], in which each confidential message is intended for one receiver and must be kept secret from other receivers. For this channel, the joint design of the physical layer coding schemes and the medium access control layer scheduling protocols are proposed to achieve reliability (small probability of error), security (perfect secrecy), and network stability (finite queue length) simultaneously. A throughput optimal queue length based scheduling algorithm was derived that stabilizes all arrival rate vectors contained in the secrecy capacity region.

We finally note that a different class of broadcast channels with confidential messages was studied in [33], in which an eavesdropper is not a legitimate receiver in the broadcast network. In this model, a transmitter broadcasts to multiple receivers with one confidential message intended for each receiver, and wants to keep each message secret from the eavesdropper even when all of the other messages are known to the eavesdropper. The secrecy sum-capacity for a special case of broadcast channels was obtained in [33], and the fading channel case was studied in [33] as well.

7 Concluding Remarks

In this paper, we have reviewed recent results on the broadcast channel with confidential messages. Several special cases of the general channel model have been described, and the characterization of the secrecy capacity region for these cases has been discussed. Interaction between public and confidential messages, impact of multiple antennas on the secrecy capac-

ity region, as well as basic achievability and converse proof techniques have been discussed.

We note that the general model of the BCC with confidential messages includes a rich set of communication scenarios, and those that have been studied so far are only small part of this set. It is also clear that even for some scenarios that have been studied, such as the model in Section 5, the secrecy capacity region is still unknown. Furthermore, as we have discussed in Section 6, wireless applications motivate the study of secrecy issues in BCC models jointly with other issues in wireless communications such as power control and outage probability. Applications to wireless networks also motivate the study of the BCC model with more than two receivers and network models with secrecy constraints, which may include broadcast, multiple access, relay, and interference channels as basic components. Hence, the BCC and general network models with confidential messages are far from being fully understood and need to be further explored from both fundamental theoretical aspects and practical application aspects.

References

- [1] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, October 1975.
- [2] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inform. Theory*, 24(3):339–348, May 1978.
- [3] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Information theoretic security. *Foundations and Trends in Communications and Information Theory*, Now Publishers, Hanover, MA, USA, Feb. 2009, submitted.
- [4] T. M. Cover. Comments on broadcast channels. *IEEE Trans. Inform. Theory*, 44(6):2524–2530, October 1998.
- [5] J. Körner and K. Marton. Comparison of two noisy channels. In *Topics in Information Theory*, pages 411–423, 1975, Keszthely, Hungary. Colloquia Math. Soc. János Bolyai, Amsterdam: North-Holland Publ., 1977.
- [6] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Secure communication over fading channels. *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, 54(6):2470–2492, June 2008.

- [7] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inform. Theory*, 24(4):451–456, July 1978.
- [8] H. D. Ly, T. Liu, and Y. Liang. MIMO broadcasting with common, private and confidential messages. In *Proc. International Symposium on Information Theory and its Applications (ISITA)*, Auckland, New Zealand, December 2008.
- [9] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inform. Theory*, 52(9):3936–3964, September 2006.
- [10] A. Khisti and G. Wornell. The MIMOME channel. In *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, USA, September 2007.
- [11] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wire-tap channel. In *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, USA, September 2007.
- [12] T. Liu and P. Viswanath. An extremal inequality motivated by multiterminal information-theoretic problems. *IEEE Trans. Inform. Theory*, 53(5):1839–1851, May 2007.
- [13] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath. The capacity region of the degraded MIMO compound broadcast channel. In *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 2007.
- [14] T. Liu and S. Shamai (Shitz). A note on the secrecy capacity of the multi-antenna wire-tap channel. To appear in *IEEE Trans. Inform. Theory*, June 2009.
- [15] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz). A MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel. *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, submitted in December 2008.
- [16] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inform. Theory*, 2007, submitted.
- [17] R. Liu, I. Maric, P. Spasojevic, and R. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, 54(6):2493–2507, June 2008.

- [18] S. I. Gel'fand and M. S. Pinsker. Coding for channel with random parameters. *Probl. Contr. Inform. Th.*, 9(1):19–31, 1980.
- [19] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inform. Theory*, 25(3):306–311, May 1979.
- [20] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inform. Theory*, 55(3):1235–1249, March 2009.
- [21] G. Caire and S. Shamai (Shitz). On the achievable throughput of a multiantenna Gaussian broadcast channel. *IEEE Trans. Inform. Theory*, 49(7):1691–1706, July 2003.
- [22] W. Yu and J. M. Cioffi. Sum capacity of Gaussian vector broadcast channels. *IEEE Trans. Inform. Theory*, 50(9):1875–1892, September 2004.
- [23] H. Sato. An outer bound to the capacity region of broadcast channels. *IEEE Trans. Inform. Theory*, 24(3):374–377, May 1978.
- [24] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz). MIMO Gaussian broadcast channels with confidential messages. In *Proceedings of IEEE Int. Symp. Information Theory (ISIT)*, Seoul, Korea, June-July 2009.
- [25] D. Tse. A deterministic model for wireless channels and its applications. In *Proc. IEEE Information Theory Workshop (ITW)*, Lake Tahoe, CA, USA, September 2007.
- [26] A. Avestimehr, S. Diggavi, and D. Tse. Wireless network information flow. In *Proc. 45th Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, USA, September 2007.
- [27] M. Kobayashi, Y. Liang, S. Shamai (Shitz), and M. Debbah. On the compound MIMO broadcast channels with confidential messages. In *Proceedings of IEEE Int. Symp. Information Theory (ISIT)*, Seoul, Korea, June-July 2009.
- [28] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). On the capacity region of the multi-antenna broadcast channel with common messages. In *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, Washington, USA, June 2007.
- [29] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Recent results on compound wire-tap channels. In *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, September 2008.

- [30] H. Weingarten, S. Shamai (Shitz), and G. Kramer. On the compound MIMO broadcast channel. In *Proc. Information Theory and Applications Workshop (ITA)*, La Jolla, CA, USA, June 2007.
- [31] P. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inform. Theory*, 54(10):4687–4698, October 2008.
- [32] Y. Liang, H. V. Poor, and L. Ying. Wireless broadcast networks: Reliability, security and stability. In *Proc. of 3rd Workshop on Information Theory and Applications (ITA)*, La Jolla, CA, USA, Jan.-Feb. 2008.
- [33] A. Khisti, A. Tchamkerten, and G. Wornell. Secure broadcasting. *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, 54(6):2453–2469, June 2008.
- [34] J. Xu, Y. Cao, B. Chen. Capacity bounds for broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, submitted in May 2008.