Secure Broadcasting with Multiuser Diversity

Ashish Khisti, Aslan Tchamkerten, and Gregory Wornell

Abstract— **We investigate the problem of broadcasting secret information to one or more receivers over wireless links in the presence of potential eavesdroppers. A fast fading channel model is assumed, with perfect channel state information (of intended receivers) at the transmitter. Both the case of independent messages and common message are considered.**

For the case of independent messages we propose a scheme that achieves the sum capacity as the number of receivers goes to infinity. We note that in the limit of large number of intended users, capacity scales with the number of intended receivers, but not with power.

For the case where a common message is broadcasted, we present a coding scheme that achieves a certain positive rate independently of the number of intended receivers.

I. Introduction

The problem of broadcasting confidential messages, has been studied for discrete memoryless channels [1], [2] and for the AWGN channel [3]. In these works, an asymptotic secrecy requirement is imposed in addition to the requirement that the probability of error at the receiver vanishes as the block length increases. Many generalizations of this problem have appeared in the literature, including the case of parallel channels [4], [5], secret key distillation using correlated sources [6], [7], and, more recently the multiple access channel with a variety of secrecy constraints [8], [9], [10].

In the present work, we consider an extension of the wiretap channel. Our setup is motivated by a variety of applications that require distribution of secret keys to intended receivers. As an example, in a pay-TV system a content provider wishes to broadcast a decryption key to a subset of users who have subscribed to a particular program. Current solutions rely on off-line key distribution mechanisms, and are vulnerable to piracy [11]. Instead, our approach is to enable a real time key distribution mechanism that uses the knowledge of physical channel to the intended receivers to protect the message against potential eavesdroppers. This application requires the multicast of a common secret message to a set of intended receivers. The users can use the key to decrypt the program, after which the key becomes useless. Another application that could potentially benefit from a real time key distribution solution is sensor networks. In such systems, it is desirable to update the secret key of each node periodically. Such applications require broadcasting of *independent* messages to each receiver, under a secrecy constraint.

In the present work, we model the wireless links between the base stations and all the receivers as independent and i.i.d. Rayleigh faded. Furthermore, we assume that the transmitter and the intended receiver(s) have perfect channel state information (CSI) of the intended links. The eavesdroppers have a channel that is statistically equivalent to the intended users. The eavesdroppers have full CSI of the intended receivers links as well as their own links. The eavesdroppers do not reveal their channel state to the transmitter and/or intended receivers. The eavesdroppers do not collude.

A few words on our model and CSI assumptions. It is unrealistic that the underlying channel changes independently in each symbol, since this requires an unusually large doppler spread. The fast fading model is usually an idealization of a relaxed delay constraint when one can code over several channel coherence intervals. Alternately in a frequency hopping system, one should code over many channel hops to realize the effect of fast fading. We assume that a feedback mechanism is available so that the intended receivers can track the channel coefficients and send them to the transmitter. Since this mechanism can be potentially insecure, we assume that the eavesdropper also knows the coefficients of the intended receivers.

In related works, a quasi-static fading model has been studied very recently in [12] and an outage secrecy formulation has been proposed. The transmitter knows the channel gains of both the receiver and the eavesdropper and declares an outage if the eavesdropper has a stronger channel gain. The role of multiple antennas in secure communications has been recently explored from a detection viewpoint in [13] and from an information theoretic viewpoint in [14], [15], [16]. These works consider the case of one sender and one receiver and explore gains from multiple antennas under different CSI assumptions. Finally in the same conference where this paper was presented, [17] and [18] presented a capacity result for the case of one receiver and one eavesdropper, with the fading coefficients of *both* the receiver and eavesdropper known to the transmitter. The problem was reduced to a set of parallel channels and it was shown that it suffices to use an independent codebook on each parallel channel.

The rest of the paper is organized as follows. In Section II, we present the channel model assumed in our analysis. Upper and lower bounds on the achievable rate with a secrecy constraint for a single user are provided in Section III. In Section IV the achievable rate is generalized to the case of many users with independent messages and its optimality in the limit of large number of users is established. Finally Section V considers the case of multicasting a common

This work was supported in part by NSF under Grant No. CCF-0515109, and by an HP Fellowship

The authors are with the EECS Department, Massachusetts Institute of technology {khisti,tcham,gww}@mit.edu

message to all the receivers.

II. Channel Model

We consider an i.i.d. Rayleigh fading channel [19] model, with channel gains independent in time and across the users. The channel model is given by

$$y_k(t) = h_k(t)x(t) + z_k(t), \quad t = 1,2,\dots,n \quad k = 1,2,\dots,K, \tag{1}$$

where the index t, denotes the time index and the subscript k denotes the user. We assume each $h_k(t)$ to be independently sampled from $\mathscr{CN}(0,1)$. The noise components $z_k(t)$ are also i.i.d. and sampled from $\mathscr{CN}(0,N)$. An average power constraint $E[\sum_{t=1}^{n}|X(t)|^2] \leq nP$ is imposed. Here the expectation is with respect to the set of messages to be transmitted and to any additional randomization at the encoder. While dealing with the case of only one receiver we will drop the subscript k in (1).

In addition to the K intended receivers, we assume the presence of an eavesdropper that has a statistically equivalent channel model as the receivers. We denote the channel model by

$$y_e(t) = h_e(t)x(t) + z_e(t), \qquad t = 1,2,\dots,n, \tag{2}$$

where $h_e(t)$ and $z_e(t)$ are sampled from $\mathscr{CN}(0,1)$ and $\mathscr{CN}(0,N)$ respectively, and are independent of all other channel gains. Finally, without loss of generality assume that $N = 1$. This simply amounts to scaling the power constraint.

We assume that the transmitter has perfect knowledge of the instantaneous channel gains of all the intended receivers, but only statistical knowledge of the eavesdroppers channel. The eavesdropper has perfect channel knowledge of the instantaneous gains of all the intended receivers as well as its own channel.

We provide a formal definition for the achievable rate tuple with independent messages $(M_1, M_2, \dots, M_K)$ to the K users. The definition for a common message rate is analogous, and will be omitted. A length n code for our channel model consists of a set of encoding mappings of the form $x(t) = f_t(m_1, m_2, \dots m_K; h_1^t, h_2^t, \dots h_K^t)$ for $t = 1,2,\dots,n$ that satisfy the average power constraint and a set of decoding mappings $\hat{m}_j = \phi_j(y_j^n; h_1^n, h_2^n, \dots h_K^n)$ for $j = 1,2,\dots K$.

Definition 1: A rate tuple $(R_1, R_2, \dots, R_K)$ is achievable if, for any $\varepsilon > 0$, there is a code of large enough block-length n such that for each $j = 1,2,\dots K$ we have the following: (i) M_j is uniformly distributed over $\{1,2,\dots,2^{nR_j}\}$, (ii) the probability of error $\Pr(\hat{M}_j \neq M_j)$ at each decoder is less than ε, and (iii) the equivocation of each message at the eavesdropper satisfies

$$\frac{1}{n} I\left(M_j; Y_e^n, H_e^n \,\middle|\, \{H_k^n\}_{k=1}^{K}, \{M_k\}_{k\neq j}\right) \leq \varepsilon, \quad j = 1,2,\dots K \tag{3}$$

Remarks

- Our definition for secrecy (3) only depends on the statistical characterization of the eavesdropper. So even though we only consider one eavesdropper in our setup, our proposed coding schemes will be secure against any number of non-colluding eavesdroppers.
- Our requirement on the normalized mutual information in (3) can be replaced by a stronger condition as suggested in Csiszár [20] and Maurer and Wolf [21]. In particular, the normalization by n is not necessary and we can replace the constant ε by a sequence ε_n that tends to zero with n. The coding schemes proposed in this work can also provide secrecy in this stronger sense.

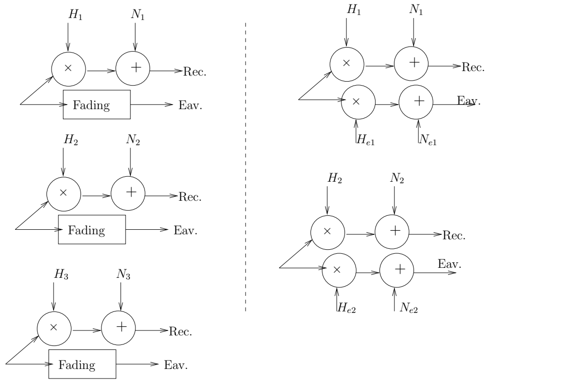

Fig. 1. Parallel channel decomposition of the fading channel with one receiver and one eavesdropper. The decomposition on the left is used in the achievability scheme when the channel coefficients of the intended receiver are known to the sender, the receiver and the eavesdropper. The decomposition on the right is used in the upper bound when the channel coefficients of both the intended receiver and the eavesdropper are known to all the nodes.

III. Single User: Achievable Rates and Upper Bounds

In this section we consider the case when there is only one receiver. The generalization to multiple receivers is considered in the next section. We denote the channel model for the intended receiver as $y(t) = h(t)x(t) + z(t)$.

A. Single User: Achievable Rate

We can view the model (1) as a set of parallel channels in Fig. 1 indexed by the channel gain H of the intended receiver, which is known globally. Thus in each parallel channel the intended receiver's channel is complex Gaussian while the eavesdropper's channel is a fading channel. We propose to use an independent Gaussian codebook on each parallel channel.

Consider a particular sub-channel where the intended receivers experiences a gain of a (i.e. $|H|^2 = a$). Generate an i.i.d. Gaussian wiretap codebook [3] with power P_a and rate $R^I(a, P_a)$. The power P_a is selected to satisfy the average power constraint $E[P_a] = P$. The achievable rate is:

$$\begin{aligned} R^I(a,P_a) &= I(X;Y_r) - I(X;Y_e,H_e) \\ &= \left[\log(1+aP_a) - E[\log(1+|H_e|^2P_a)]\right]^+, \end{aligned} \tag{4}$$

where we use the notation $[v]^+ \overset{\Delta}{=} \max(0,v)$.

From the expression (4), it is clear that our achievable rate $R^I(a,P_a)$ is increasing in a. It is possible to show that if a is fixed and greater than $T \overset{\Delta}{=} \exp(-\gamma)$, where $\gamma = 0.5772$ is the Euler's constant, the supremum of $R^I(a,P_a)$ is obtained in the limit $P_a \to \infty$. On the other hand if $a < T$, then $\sup_{P_a>0} R^I(a,P_a) = 0$. Thus for the proposed scheme, the transmitter will not transmit whenever $a < T$.

It is possible to improve upon the proposed rate in (4) by transmitting artificial noise in addition to the intended codeword. We split the available power P_a into two parts. Generate an i.i.d. Gaussian wiretap codebook with power P_u. Before transmission of a codeword U^n, generate an i.i.d Gaussian noise sequence V^n with power P_v, independent of everything else and not known to the receiver. Our choice of the powers satisfy $P_u + P_v = P_a$. We transmit $X^n = U^n + V^n$. The received symbols at the intended receiver and eavesdropper are

$$\begin{aligned} Y(i) &= HU(i) + HV(i) + Z(i) \\ Y_e(i) &= H_e(i)U(i) + H_e(i)V(i) + Z(i) \end{aligned} \tag{5}$$

Our expression for the achievable rate is given by,

$$\begin{aligned} R^{II}(a,P_a) &= I(U;Y_r) - I(U;Y_e,H_e) \\ &= \left\{ \log\left(1 + \frac{aP_u}{1+aP_v}\right) - E\left[\log\left(1 + \frac{|H_e|^2 P_u}{1+|H_e|^2 P_v}\right)\right]\right\} \end{aligned} \tag{6}$$

We optimize over the choice of P_u and P_v. It can be shown that for any $a > 0$, we have that $\sup_{P_a} R^{II}(a,P_a) > 0$. Thus secret communication is possible for every choice of $a > 0$, provided the available power is sufficiently large. Note that the gain from artificial noise should not be very surprising. As seen in (6), the artificial noise gets amplified by the channel gain of the receivers and hence there is a net gain if the channel gain to the intended receiver is small. The optimal value of P_v is positive only if $a < 1$. Thus if the channel gain of the intended receiver is greater than one, our scheme reduces to the previous one in (4).

To provide an achievable rate for the fading channel of interest (1), we integrate $R(a,P_a)$ with respect to the distribution over a and optimize over all possible power allocations.

$$R^J(P) = \sup_{\{P_v\}:P_v\geq 0, E[P_v]\leq P} \int_{v=0}^{\infty} R^J(v,P_v)\exp(-v)dv, \quad J \in \{I, II\} \tag{7}$$

Numerical evaluation in the high SNR limit yields

$$\begin{aligned} \lim_{P\to\infty} R^I(P) &= 0.7089 \text{ bits/symbol}, \\ \lim_{P\to\infty} R^{II}(P) &= 0.7479 \text{ bits/symbol} \end{aligned} \tag{8}$$

As a final remark, we note that even though our proposed scheme uses an independent codeword for each parallel channel, this is not necessary. In particular following [22], the rate in (7) can also be obtained by using a *single* Gaussian wiretap codebook generated i.i.d. $\mathscr{CN}(0,1)$ and scaling each transmitted symbol by the transmit power P_a depending on the channel state. This reduces the complexity of encoding and decoding significantly.

B. Single User: Upper Bound

To get an upper bound on the secrecy capacity we consider a genie aided channel, where in addition to the receiver channel state, the channel state of the eavesdropper is also globally known. We can view the system as a set of parallel channels as in Fig. 1,indexed by the channel gains of the intended receiver and the eavesdropper (H, H_e). Each of the parallel sub-channel is a Gaussian channel where the gains to the intended receiver and the eavesdropper are fixed. We have the following claim:

Claim 1: For the channel model (1) with perfect CSI (H, H_e) at all the nodes, for an optimal coding scheme (i) transmit only on sub-channels where $|H|^2 > |H_e|^2$ (ii) use an independent Gaussian wiretap codeword on each of the sub-channel (iii) maximize the power allocation across the sub-channels.

Proof: See the Appendix.

With the above claim, we get the following expression for the secrecy capacity of the genie aided channel:

$$\begin{aligned} C^{\text{full}}(P) &= \Pr(|H|^2 \geq |H_e|^2) \times \\ &\sup_{P_{H,He}:E[P_{H,He}]\leq P} E\left[\log\frac{(1+|H|^2 P_{H,H_e})}{(1+|H_e|^2 P_{H,H_e})} \,\middle|\, |H|^2 \geq |H_e|^2\right] \end{aligned} \tag{9}$$

It can be verified that the objective function in (9) is concave and hence the KKT conditions are both necessary and sufficient to specify the optimal P_{H,H_e} function. To get some insight, we provide the following numerical upper bound which is tight in the high SNR limit.

Corollary 1: For any $P > 0$

$$C^{\text{full}}(P) \leq 1 \text{ bits/symbol} \tag{10}$$

Proof: We note that for $|h| \geq |h_e|$, the term $\log \frac{(1+|h|^2 P)}{(1+|h_e|^2 P)}$ is monotonically increasing in P, and the supremum is given by $\log\left(\frac{|h|^2}{|h_e|^2}\right)$ in the limit $P \to \infty$. Thus from (9)

$$\begin{aligned} C^{\text{full}}(P) &\leq \Pr(|H|^2 \geq |H_e|^2) E\left[\log\frac{|H|^2}{|H_e|^2} \,\middle|\, |H|^2 \geq |H_e|^2\right] \\ &= \log_e(2) = 1 \text{ bits/symbol} \end{aligned} \tag{11}$$

■

We note that there is a significant gap between our upper and lower bounds for the single user case (see (8) and (11)). This gap however vanishes as the number of users becomes large as we will see next.

IV. Multiple Receivers: Independent Messages

As in Section II we assume that there are K receivers and each is interested in an independent message.

Our achievable scheme is simply a time division multiplexing scheme that selects the best user at each time and uses independent single user codebooks discussed in Section III. An expression for the achievable sum-rate is:

$$R^J_{\text{sum,K}}(P) = \sup_{\{P_v\}:P_v\geq 0, E[P_v]\leq P} \int_{v=0}^{\infty} R^J(v,P_v) f_K(v)dv, \quad J \in \{I, II\}, \tag{12}$$

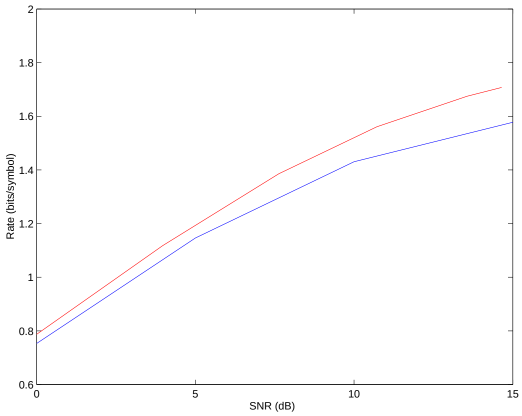

Fig. 2. Upper and lower bounds on the sum rate for a system with K=5 users. The lower bound is computed by the two step power allocation rule in (13) while the upper bound is computed using the optimal water-filling rule. Note that the bounds are quite close over a wide range of SNR.

where $f_K(v) = K\exp(-v)(1-\exp(-v))^{K-1}$ is the probability distribution of the maximum of K independent, unit mean, exponential random variables.

The power allocation in (12), is difficult to compute analytically. We consider a simpler two step power allocation, which provides several insights. Furthermore, we will only consider the achievability scheme R^I, since the rate R^{II} is better only when the channel gain (of the best user) is less than 1 an even that will happen only rarely if there are enough users. Let us denote, the channel gain of the best user as $|h_{\max}|^2 \overset{\Delta}{=} \max_{1\le i\le K}\{|h_i|^2\}$. For a given power P, we select a threshold $T(P)$ and transmit with a constant power P_0 only if $|h_{\max}|^2 \ge T(P)$. Naturally, $P_0 = P/\Pr(|h_{\max}|^2 > T(P))$. An achievable sum rate can be obtained by maximizing over the threshold:

$$R^T_{\text{sum},K}(P) = \max_{T\ge 0}\left\{\Pr(|H_{\max}|^2 \ge T)\times \left(E\left[\log(1+|H_{\max}|^2P_0) \mid |H_{\max}|^2 \ge T\right] - F(P_0)\right)\right\}, \tag{13}$$

where $F(t) \overset{\Delta}{=} E[\log(1+|H_e|^2 t)] = \exp\left(\frac{1}{t}\right)\int_{\frac{1}{t}}^{\infty}\frac{\exp(-x)}{x}dx$, denotes the mutual information of the eavesdropper.

An achievable rate for the two-step power allocation scheme (13) with 5 users is shown in Fig. 2 as a function of the SNR. We note that the corresponding rate is close to an upper bound, derived next, over a large range of SNR. Note that, we expect the two bounds to be close particularly in the low SNR regime. As the SNR decreases our proposed scheme transmits only if any user has an unusually large channel gain. Since the eavesdropper's channel will not be equally large, the loss in capacity due to the secrecy constraint vanishes in the low SNR limit. The fact that the bounds are quite close in the medium SNR limit is somewhat surprising. It demonstrates that the gains from exhaustive waterfilling over the two step power allocation scheme are not significant even at moderate values of SNR.

To establish the upper bound, we consider a genie aided channel, where the eavesdropper's channel is known to the transmitter and the intended receivers.

Claim 2: If the channel coefficients of all the intended receivers and the eavesdropper are known to all the nodes in the system, then the sum capacity of the K user, single eavesdropper channel, can be obtained by a scheme which: (a) only transmits to the best user at each time, (b) uses an independent Gaussian codebook for each fading state (c) optimizes power allocation across the codebooks via waterfilling.

Note that Claim 2 is an extension of the opportunistic transmission result [19] to the case of a secrecy constraint. We can basically decompose the system into a set of parallel channels indexed by the channel gain vector $(H_1, H_2, \dots, H_K, H_e)$ and show that it suffices to use an independent code for each state and transmit to the best user on each state.

In what follows, we show the result for two users and two parallel channels. The extension to the case of K receivers and M parallel channels is straightforward.

Consider two parallel Gaussian channels, as shown in Fig. 3(a), of the form [1]

$$\begin{aligned} Y_{11} &= X_1 + N_{11}, \qquad & Y_{12} &= Y_{11} + N_{12} \\ Y_{21} &= Y_{22} + N_{21}, \qquad & Y_{22} &= X_2 + N_{22} \end{aligned} \tag{14}$$

User 2 is degraded user on the first channel, while user 1 is the degraded user on the second channel. Assume that there is an eavesdropper who receives $Y_{e1} = Y_{12} + E_1$ and $Y_{e2} = Y_{21} + E_2$. The eavesdropper is degraded with respect to both the receivers. Assume the noise distribution is given by $N_{ij} \sim \mathcal{CN}(0, \sigma_{ij}^2)$ and $E_i \sim \mathcal{CN}(0, \mu_i)$.

Claim 3: The sum capacity of the parallel Gaussian wiretap channel is

$$\begin{aligned} C_{\text{sum}} = \max_{\beta\in[0,1]} &\log\left(1+\frac{\beta P}{\sigma_{11}^2}\right) - \log\left(1+\frac{\beta P}{\sigma_{11}^2+\sigma_{12}^2+\mu_1}\right) \\ &+ \log\left(1+\frac{(1-\beta)P}{\sigma_{22}^2}\right) - \log\left(1+\frac{(1-\beta)P}{\sigma_{22}^2+\sigma_{21}^2+\mu_2}\right) \end{aligned} \tag{15}$$

The sum-capacity is obtained by transmitting to user 1 on the first channel and to user 2 on the second channel with a Gaussian wiretap codebook.

To prove the above claim, we first make a simple observation. Consider a modified channel as shown in Fig. 3(b). For this channel, user 2 is always degraded with respect to user 1. The channel model is given by:

$$\begin{aligned} Y_{11} &= X_1 + N_{11}, \qquad & Y_{12} &= Y_{11} + N_{12} \\ Y_{21}' &= X_2 + N_{21}, \qquad & Y_{22}' &= Y_{21}' + N_{22} \end{aligned} \tag{16}$$

We will refer to the model (14) as the reversely degraded channel model and to (16) as the degraded channel model.

Lemma 1: The sum capacity of the reversely degraded parallel channels (14) is upper bounded by the sum capacity of the degraded parallel channels in (16).

[1] The physical degradedness condition here can be replaced with the stochastic degradedness condition, since only the marginal distribution of the noise affects the capacity of the broadcast channels.

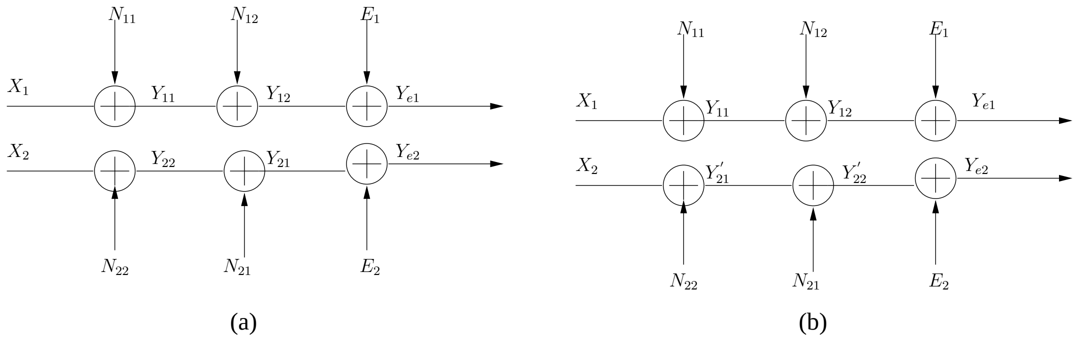

Fig. 3. Parallel Gaussian broadcast channels with a degraded eavesdropper. In (a) the channels are reversely degraded while in (b) user 2 is degraded with respect to user 1.

To verify the above Lemma, it suffices to show that if (R_1, R_2) is achievable for the reversely degraded channel (14), then $(R_1 + R_2, 0)$ is achievable for the degraded channel (16). This follows since user 1 in the degraded channel model can always simulate user 2 in the reversely degraded channel model and so any rate achievable for user 2 in the reversely degraded model is also additionally achievable to user 1 in the degraded model.

Lemma 2: The sum capacity of the degraded parallel broadcast channel is equal to (15).

To verify lemma 2, first note that it suffices to transmit only to user 1. Since user 1 can simulate user 2, any rate achievable to user 2 is additionally achievable to user 1. Thus the problem reduces to the case of Gaussian parallel channels with one receiver and one eavesdropper. We now invoke the single user result for parallel channels in Claim 1 to observe that it suffices to use independent Gaussian codebooks on each of the channels. Finally, any achievable rate with independent Gaussian codebooks is also achievable on the original reversely degraded channel and this completes our proof.

It follows that the capacity expression with global channel knowledge of the eavesdropper is given by

$$C_K^{\text{full}}(P) = \Pr(|H_{\max}|^2 \geq |H_e|^2) \max_{P_{H_{\max},H_e}: E[P_{H_{\max},H_e}] \leq P} E\left[\log \frac{(1+|H|^2 P_{H_{\max},H_e})}{(1+|H_e|^2 P_{H_{\max},H_e})} \,\middle|\, |H_{\max}|^2 \geq |H_e|^2\right] \tag{17}$$

Following a derivation analogous to (9), we compute the following upper bound, which is tight in the high SNR limit.

$$C_K^{\text{full}}(P) \leq \Pr(|H_{\max}|^2 \geq |H_e|^2) E\left[\log \frac{|H_{\max}|^2}{|H_e|^2} \,\middle|\, |H_{\max}|^2 \geq |H_e|^2\right] \tag{18}$$

We compute the achievable rate and upper bound from (13) and (18) in Fig. 4. For analytical tractability, the rate is calculated by taking the limit SNR $\to \infty$ for a fixed K. We note that the upper and lower bounds are furthest for the case of single user and, as the user population increases, the bounds get closer. Asymptotically the bounds coincide and we have the following expression for the sum capacity.

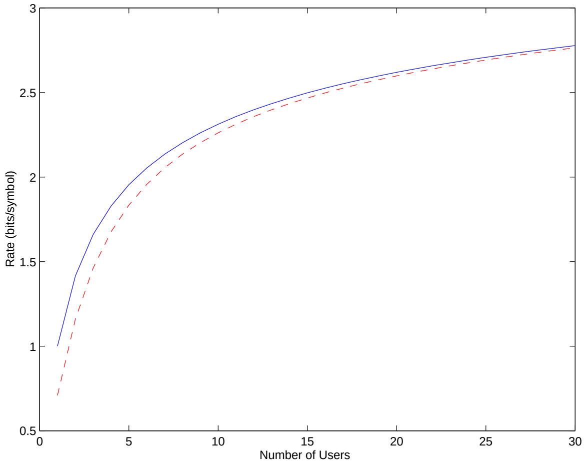

Fig. 4. Upper and lower bounds on the sum rate for fading channels with perfect secrecy constraint. The sum rate is evaluated in the limit SNR $\to \infty$, but is close for practical values of SNR, see Fig. 2.

Theorem 1: The sum capacity of the fading broadcast channel with K independent receivers and a total power P with perfect secrecy constraint satisfies $\lim_{P\to\infty} C(P) = \log\log K + \gamma + o(1)$, where $\gamma = 0.5772$ is the Euler-Gamma constant and $o(1) \to 0$ as $K \to \infty$.

Thus even though our proposed achievable scheme is suboptimal for the case of a single receiver, it is asymptotically optimal as the user population grows.

Remarks:

- The double logarithmic scaling of sum rate with the number of receivers is a consequence of the multiuser diversity (see e.g. [19]). We note that the secrecy constraint preserves the multiuser diversity gain, but the power gain is lost as in the AWGN wiretap channel [3].
- The two-step power allocation strategy provides a natural architectural solution. In particular, scheduling algorithms optimized for conventional multiuser diversity systems can still be used with the secrecy constraint. The modification required at the scheduling layer is that transmission must be done only if the channel of the selected user is sufficiently strong. Moreover, the transmitted information must be protected via a wiretap

code instead of a conventional channel code.

- Our analysis has focussed on the case of statistically equivalent users and eavesdroppers. Generalizations to the case when some receivers are stronger than others are straightforward. Both our upper and lower bounds can be generalized to this situation.

V. Multiple Users: Common Information

In this section, we consider a scenario when each of the K receivers is interested in a common confidential message. The problem of multicasting common information has received less attention than the problem of broadcasting independent messages in systems without a secrecy constraint. Transmitter CSI in general does not appear to significantly improve the common message rate over a flat power allocation based scheme (that does not require transmitter CSI). In contrast, when we have to multicast confidential information, it is necessary that the knowledge of channel coefficients be taken into account so as to selectively serve the intended users. A scheme based on flat power allocation will naturally reveal the message to the eavesdroppers. How can the transmitter CSI be taken into account efficiently? One ad-hoc solution is to transmit only when the channel gains of *all* the users are sufficiently large. With independent fading however, it will be only rarely (with sufficiently many receivers) that all the users simultaneously experience a strong channel. The achievable rate will decay exponentially with the number of users.

One might naturally wonder how the multicasting secrecy capacity scales with the number of intended receivers. Since we are limited by the single user upper bound (9), the capacity cannot increase with the number of receivers. The best we can hope for is that the capacity is a constant, independent of the number of receivers. In what follows we propose a scheme that also achieves a rate independent of the number of intended receivers. This establishes that the capacity does not decay with the number of receivers.

A. Case of two receivers

We first present the scheme for the case of two receivers. The generalization to multiple receivers will be presented subsequently.

We first define a few parameters.

- $R \stackrel{\Delta}{=} E[\log(1+|H|^2P)||H|^2 > T] - E[\log(1+|H_e|^2P)]$
- $R_w \stackrel{\Delta}{=} E[\log(1+|H_e|^2P)]$
- T: threshold for transmission.
- $p \stackrel{\Delta}{=} \Pr(|H|^2 \geq T)$
- $n_0 \stackrel{\Delta}{=} p^2 n$, $n_1 \stackrel{\Delta}{=} p(1-p)n$

Codebook Generation: We use two independent Gaussian codebooks $\mathscr{C}_0, \mathscr{C}_1$ as shown in Fig. 5. The codebook $\mathscr{C}_0$ is a $(n_0, 2^{n_0 R})$ code constructed as follows. We generate $2^{n_0(R+R_w)}$ codewords i.i.d. $\mathscr{CN}(0,P)$ and randomly partition them into $2^{n_0 R}$ bins. There are $2^{n_0 R_w}$ codewords per bin. The codebook $\mathscr{C}_1$ is a $(n_1, 2^{n_1 R})$ code, with $2^{n_1(R+R_w)}$ i.i.d. $\mathscr{CN}(0,P)$ codewords randomly partitioned into $2^{n_1 R}$ bins.

Our common message is of the form (W_0, W_1). The message W_0 is uniformly distributed over the indices $\{1, 2, \ldots 2^{n_0 R}\}$ while the message W_1 is uniformly distributed over the indices $\{1, 2, \ldots 2^{n_1 R}\}$. Accordingly, the overall rate is:

$$\frac{n_0}{n}R + \frac{n_1}{n}R = pR. \tag{19}$$

We note that our construction for $\mathscr{C}_0$ and $\mathscr{C}_1$ is analogous to the Gaussian wiretap codebook construction [3].

Encoding: We select randomly a codeword $U_0^{n_0}$ for message W_0 from the set of all codewords associated with this message. For message W_1 we select two codewords $U_1^{n_1}$ and $U_2^{n_1}$ uniformly and independently of one another as shown in Fig. 5 (potentially these codewords might be the same). At each time depending on the state of the channel, we select one of the codewords according to the table below and transmit its subsequent symbol.

	Channel State	Selected Codeword
(a)	$\lvert H_1\rvert^2 \geq T$ & $\lvert H_2\rvert^2 \geq T$	$U_0^{n_0}$
(b)	$\lvert H_1\rvert^2 \geq T$ & $\lvert H_2\rvert^2 \leq T$	$U_1^{n_1}$
(c)	$\lvert H_1\rvert^2 \leq T$ & $\lvert H_2\rvert^2 \geq T$	$U_2^{n_1}$
(d)	$\lvert H_1\rvert^2 \leq T$ & $\lvert H_2\rvert^2 \leq T$	$\emptyset$

The transmission stops when the we have transmitted exactly n_0 symbols of $U_0^{n_0}$ and n_1 symbols each of $U_1^{n_1}$ and [2] $U_2^{n_1}$. Because of global CSI of the state, all the receivers know the current state of the system and accordingly know which codeword the transmitted symbol belongs to.

Decoding: Decoder 1 observes $(Y_{r0}^{n_0}, Y_{r1}^{n_1}, Y_{r2}^{n_1})$ corresponding to the codewords $(U_0^{n_0}, U_1^{n_1}, U_2^{n_1})$. Since the codewords $U_0^{n_0}$ and $U_1^{n_1}$ are transmitted whenever $|H_1|^2 \geq T$, user 1 is able to decode these codewords with high probability. Thus user 1 recovers the message (W_0, W_1). User 2 is able to recover the codewords $U_0^{n_0}$ and $U_2^{n_0}$ and therefore the message (W_0, W_1).

Secrecy Analysis: Let us denote the observed sequence at the eavesdropper as $(Y_{e,0}^{n_0}, Y_{e,1}^{n_1}, Y_{e,2}^{n_1})$, where $Y_{e,0}^{n_0}$ is the eavesdroppers observation of codeword $U_0^{n_0}$, and $Y_{e,i}^{n_1}$, for $i = 1, 2$ are the eavesdroppers observations of codewords $U_i^{n_1}$. We first note that form our construction of codebooks $\mathscr{C}_0$ and $\mathscr{C}_1$, we have that for any fixed $\varepsilon > 0$ and sufficiently large n_0 and n_1 that

$$I(W_0, Y_{e,0}^{n_0}) \leq n_0\varepsilon \quad I(W_1; Y_{e,1}^{n_1}) \leq n_1\varepsilon \quad I(W_1; Y_{e,2}^{n_1}) \leq n_1\varepsilon, \tag{20}$$

To establish the condition of perfect secrecy we wish to upper bound the following quantity $I(W_0, W_1; Y_{e,0}^{n_0}, Y_{e,1}^{n_1}, Y_{e,2}^{n_1})$.

$$\begin{aligned} I(W_0, W_1; Y_{e,0}^{n_0}, Y_{e,1}^{n_1}, Y_{e,2}^{n_1}) &= I(W_0; Y_{e,0}^{n_0}) + I(W_1; Y_{e,1}^{n_1}, Y_{e,2}^{n_1}) \\ &\leq I(W_1; Y_{e,1}^{n_1}, Y_{e,2}^{n_1}) + n_0\varepsilon \end{aligned} \tag{21}$$

The first equality above holds from the fact that W_0 and W_1 are mutually independent and the codebooks $\mathscr{C}_0$ and $\mathscr{C}_1$

[2] It may be necessary to skip transmission in a few time-slots in this process before all the states have occurred the desired number of times. This will incur a small overhead in rate, but this loss vanishes as the block length becomes large. This will be discussed in more detail in the full paper.

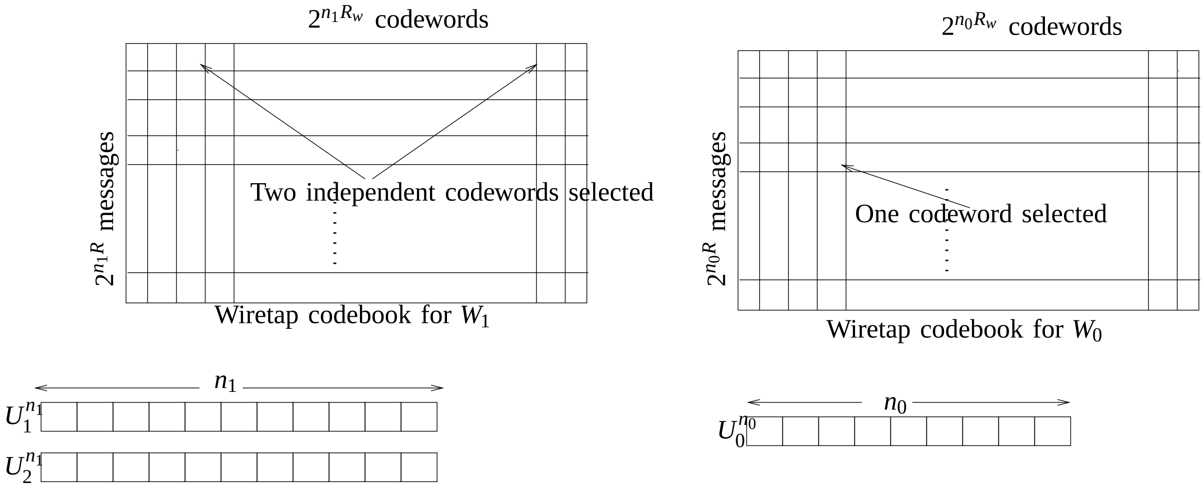

Fig. 5. Coding scheme for the two user multicasting case. Two independent Gaussian codebooks are generated, one for message W_0 and one for message W_1. The length of the codewords are n_0 and n_1 respectively. We generate $2^{n_i(R+R_w)}$ codewords i.i.d. $\mathscr{C}\mathscr{N}(0,P)$ and partition into 2^{n_iR} bins. For message W_0, we select one codeword $U_0^{n_0}$ from the bin of W_0. For W_1, we select two codewords $U_1^{n_1}$ and $U_2^{n_1}$, independently and uniformly from the bin of W_1. A symbol of $U_0^{n_0}$ is transmitted whenever $|H_1|^2 \geq T$ and $|H_2|^2 \geq T$. A symbol of $U_1^{n_1}$ is transmitted whenever $|H_1|^2 \geq T$ and $|H_2|^2 < T$, while a symbol of $U_2^{n_1}$ is transmitted whenever $|H_1|^2 < T$ and $|H_2|^2 \geq T$.

are generated independent of one another. It remains to upper bound $I(W_1;Y_{e,1}^{n_1},Y_{e,2}^{n_1})$.

$$\begin{aligned}
I(W_1;Y_{e,1}^{n_1},Y_{e,2}^{n_1}) &= h(Y_{e,1}^{n_1},Y_{e,2}^{n_1}) - h(Y_{e,1}^{n_1},Y_{e,2}^{n_1}|W_1)\\
&= h(Y_{e,1}^{n_1},Y_{e,2}^{n_1}) - h(Y_{e,1}^{n_1}|W_1) - h(Y_{e,2}^{n_1}|W_1) \tag{22}\\
&\leq h(Y_{e,1}^{n_1}) + h(Y_{e,2}^{n_1}) - h(Y_{e,1}^{n_1}|W_1) - h(Y_{e,2}^{n_1}|W_1)\\
&\leq I(W_1;Y_{e,1}^{n_1}) + I(W_1;Y_{e,2}^{n_1}) \leq 2n_1\varepsilon
\end{aligned}$$

Here (22) follows from the fact that the codewords $U_1^{n_1}$ and $U_2^{n_1}$ are chosen conditionally independent given W_1 hence $Y_{e,1}^{n_1}$ and $Y_{e,2}^{n_1}$ are conditionally independent given W_1.

Thus we have shown that by choosing a sufficiently large block length, we can keep the eavesdropper in almost perfect equivocation, while the rate of the common message is given by (19). We summarize our result below.

Claim 4: An achievable rate for the two user multicasting system is given by

$$\begin{aligned}
R_{\text{common},2}(P) = \max_{T\geq 0}\big\{&\Pr(|H|^2 \geq T)\times\\
&\big(E\left[\log(1+|H|^2P) \mid |H|^2 \geq T\right] - F(P)\big)\big\}, \tag{23}
\end{aligned}$$

where $F(t) \triangleq E[\log(1+|H_e|^2t)] = \exp\left(\frac{1}{t}\right)\int_{\frac{1}{t}}^{\infty}\frac{\exp(-x)}{x}dx$, denotes the mutual information of the eavesdropper.

We next show that this rate is achievable for any number of receivers.

B. Many Receivers

Our extension of the multicasting scheme to the case of K intended receivers requires us to deal with many more states. Accordingly, we introduce the following additional definitions:

- The channel is said to be in *state* S_i, $i = 0,1,\dots K$, if exactly i of the K users have channel gains above the threshold T.
- A *configuration* Q_{ki} in state S_i, for $k = 1,2,\dots D_i$ denotes the labelling of which users have channel above the threshold when in state S_i. Note that there are $D_i = \binom{K}{i}$ total configurations when in state S_i.
- A user is said to be *active* if his channel exceeds the threshold. When in state S_i, a user is active in A_i=$\binom{K-1}{i-1}$ different configurations.
- The probability of being in configuration Q_{ki} of state i is given by $q_i \triangleq p^i(1-p)^{K-i}$, where $p \triangleq \Pr(|H|^2 \geq T)$. Also let $n_i = q_in$, be the expected fraction of time configuration Q_{ki} occurs.

We will transmit a separate message in each such state S_i. Let the message be W_i. Thus our common message is of the form $(W_1,W_2,\dots,W_K)$. For the rest of this section we focus on transmission of message W_i.

Codebook Generation:

We propose to use a concatenated codebook as shown in Figure 6.

- For each of the configuration Q_{ki} we generate a Gaussian wiretap codebook $\mathscr{C}_{ki}$ which is a $(n_i,2^{n_iR})$ code. Each codebook is generated via random partitioning as in the two user case (c.f. Fig. 5). This constitutes our inner code.
- We select a maximum distance separable (MDS) code over a field $\mathbb{F}_{2^{nq_iR}}$ with parameters (A_i,D_i). This forms our outer code.

Encoding

- The message W_i is split into A_i sub-messages $(W_{i1},\dots W_{iA_i})$. Each of the sub-messages W_{ij} is an independent binary information sequence of length nq_iR.
- We view each W_{ij} as a symbol over this field $\mathbb{F}_{2^{nq_iR}}$ and map the tuple $(W_{1i},\dots W_{A_ii})$ to a $(V_{1i},\dots,V_{D_ii})$ using the outer erasure code.
- Each sequence V_{ki} is mapped to a codeword $U_{ki}^{n_i}$ via the inner wiretap code $\mathscr{C}_{ki}$. A symbol of $U_{ki}^{n_i}$ is transmitted

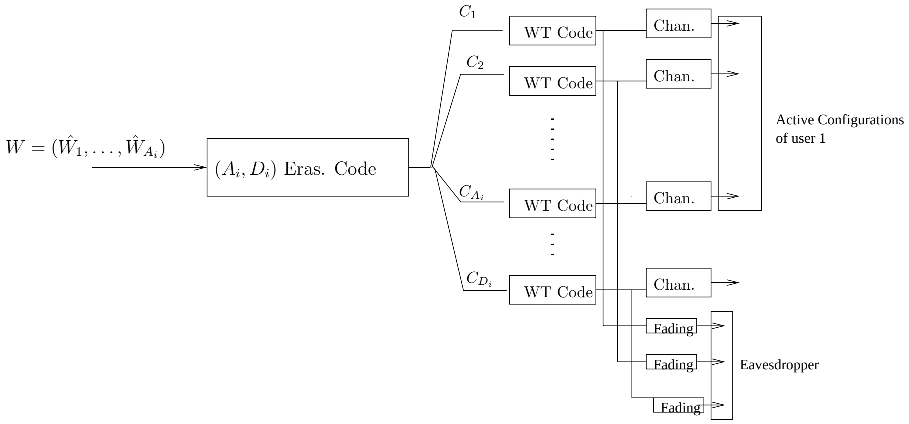

Fig. 6. A concatenated coding scheme for multicasting confidential messages in state S_i. The message is broken down into A_i bit sequences of length nq_iR. By treating these as elements of $\mathbb{F}_{2^{nq_iR}}$, a (A_i, D_i) erasure code is applied. Each of the resulting output symbol is then mapped to a wiretap codeword, as shown and then output during a specific configuration. Each channel above represents one such configuration. Each receiver can decode A_i different codewords in the configurations he is active. Then using the outer erasure code, the original message can be recovered. An eavesdropper observes all the D_i codewords over fading channels, but still has almost perfect equivocation.

whenever we are in configuration Q_{ki}.

Decoding Let us denote the observations at receiver j to be $(Y^{n_i}_{rj1}, \ldots, Y^{n_i}_{rjD_i})$ corresponding to the codewords $(U^{n_i}_{1i}, \ldots, U^{n_i}_{D_i i})$. With high probability, user j can recover all the A_i the codewords which are transmitted in configurations where he is active. Using the outer MDS erasure code, the message W_i can thus be recovered.

Secrecy Analysis: The eavesdropper observes all the codewords over a fading channel. Let $(Y^{nq_i}_{jie}$ be the output sequence at the eavesdropper when codeword $U^{n_i}_{ji}$ corresponding to V_{ji} is transmitted. From the wiretap code construction, it follows that $I(V_{ij}; Y^{nq_i}_{ije}) \leq nq_i\varepsilon$. We wish to show that for sufficiently large n, $I(W_i; \bigcup_j Y^{nq_i}_{ije}) \leq \varepsilon'$ for any given ε'.

$$I(W_i; \bigcup_j Y^{nq_i}_{ije}) = I(V_{i1}, V_{i2}, \ldots, V_{iD_i}; Y^{nq_i}_{i1e}, \ldots, Y^{nq_i}_{iD_ie}) \tag{24}$$

$$= h(Y^{nq_i}_{i1e}, \ldots, Y^{nq_i}_{iD_ie}) - h(Y^{nq_i}_{i1e}, \ldots, Y^{nq_i}_{iD_ie} | V_{i1}, V_{i2}, \ldots, V_{iD_i})$$

$$= h(Y^{nq_i}_{i1e}, \ldots, Y^{nq_i}_{iD_ie}) - \sum_j h(Y^{n}_{ije} | V_{ij}) \tag{25}$$

$$\leq \sum_j I(Y^{nq_i}_{i1e}; V_{ij}) \leq D_i nq_i \varepsilon$$

Here (24) follows from the fact that the $V_{i1} \ldots V_{iD_i}$ is a one to one function of W_i and (25) from the fact that $\{Y^n_{ije}\}_j$ are conditionally independent given $\{V_{ij}\}_j$. Finally, observe that the common message rate for the proposed scheme is given by:

$$R_{\text{common}} = \sum_{i=1}^{K} A_i q_i R \tag{26}$$

$$= \sum_{i=1}^{K} \binom{K-1}{i-1} p^i (1-p)^{K-i} R = pR, \tag{27}$$

which is the same rate in (23).

Theorem 2: An achievable rate for multicasting a confidential common message to K receivers is given by (23). The achievable rate is constant, independent of the number of intended receivers.

Note on the overhead information

Note that each active user at a given time, has to know the state and the configuration of the system at that time. In our model, we have assumed global CSI knowledge, so that each receiver knows this information for free. In practice, the transmitter has to send the configuration information explicitly. If there are K users in the system, there are $K+1$ possible states and at-most $\binom{K}{\frac{K}{2}}$ configurations. The amount of overhead is of the order of $\log\binom{K}{\frac{K}{2}}$, which increases linearly in the number of users.

The significance of this overhead depends on how quickly the underlying channel changes. If the channel is changing every symbol, then this overhead could be huge, since we need to transmit K bits per symbol. In practice however, if one uses a slow frequency hopping scheme, then the transmitter will spend a certain fraction of time in each narrow-band sub-channel. During this period, the configuration information will be broadcasted first. Thereafter the wire-tap codeword of the corresponding configuration will be transmitted.

We believe that at least in the high SNR situations, the overhead information may not be the bottleneck. The main justification for this is that this information does not have to be secure. So unlike the secrecy rate, its rate increases with the power. Hence it can be broadcasted at a much higher rate than confidential messages.

VI. Conclusion

The problem of secure broadcasting in an i.i.d. Rayleigh fading environment is investigated. Throughout we assume that the channel state of the intended receivers are known globally to all the nodes, including the eavesdroppers. On the other hand the channel state information of the eavesdropping nodes are only known to the eavesdroppers and not revealed to the transmitter or receivers. Upper and lower bounds have been derived for the case of one sender and one receiver. For the case of independent messages, a coding scheme which is asymptotically optimal in the sum rate as the number of receivers grows is presented. For the case of a common message, a concatenated coding scheme is presented that has an achievable rate that is independent of the number of receivers interested in the message.

APPENDIX

We consider two parallel Gaussian channels; the generalization to M parallel channels is straightforward. Also for simplicity we only consider real channels. The generalization to complex channels is immediate.

We wish to show that it suffices to use an independent Gaussian codebook on each parallel channel where the eavesdropper is degraded with respect to the intended receiver and transmit nothing if the eavesdropper is stronger than the intended receiver. We first consider the case where the intended receiver is stronger than the eavesdropper on both the channels. Recall that it suffices to use a physically degraded model as below.

$$\begin{aligned} Y_1 &= X_1 + Z_1, \quad Y_{e1} = Y_1 + Z_{e1} \\ Y_2 &= X_2 + Z_2, \quad Y_{e2} = Y_2 + Z_{e2} \end{aligned} \tag{28}$$

where $Z_1 \sim \mathcal{N}(0,\sigma_1^2)$, $Z_2 \sim \mathcal{N}(0,\sigma_2^2)$, $Z_{e1} \sim \mathcal{N}(0,\sigma_{e1}^2)$ and $Z_{e2} \sim \mathcal{N}(0,\sigma_{e2}^2)$.

Claim 5: The secrecy capacity of the above channel with two parallel sub-channels is

$$\begin{aligned} C = \sup_{\beta\in[0,1]} &\left\{ \frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_{11}^2}\right) - \frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_{11}^2+\sigma_{e1}^2}\right) \right. \\ &\left. + \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_2^2+\sigma_{e2}^2}\right) \right\} \end{aligned} \tag{29}$$

Note that the achievability scheme is to use independent Gaussian codebooks on the two parallel channels. We only have to show the converse. Let W be the transmitted message. Assume that there exists a length n block code with 2^{nR} messages. From the secrecy constraint, we have that $I(W;Y_{e1}^n,Y_{e2}^n) \le n\varepsilon_n$ for some sequence $\varepsilon_n \to 0$ as $n \to \infty$. Let $nR = H(W)$ By Fano's inequality, we have

$$\begin{aligned} nR &\le I(W;Y_1^n,Y_2^n) + n\varepsilon_n \\ &\le I(W;Y_1^n,Y_2^n) - I(W;Y_{e1}^n,Y_{e2}^n) + 2n\varepsilon_n \\ &\le I(W;Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n) + 2n\varepsilon_n \end{aligned} \tag{30}$$

Now let X_1^n and X_2^n denote the transmitted sequences on the two channels. Due to the sum power constraint, there exists a $\beta \in [0,1]$ such that $\sum_{i=1}^n E[X_{1i}^2] \le n\beta P$ and $\sum_{i=1}^n E[X_{2i}^2] \le n(1-\beta)P$. We use this to further simplify (30).

$$\begin{aligned} nR &\le I(W;Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n) + 2n\varepsilon_n \\ &= h(Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n) - h(Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n,W) + 2n\varepsilon_n \\ &\le h(Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n) - h(Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n,W,X_1^n,X_2^n) + 2n\varepsilon_n \\ &= h(Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n) - h(Z_1^n,Z_2^n|Z_1^n+Z_{e1}^n,Z_2^n+Z_{e2}^n) + 2n\varepsilon_n \qquad (31) \\ &= h(Y_1^n,Y_2^n|Y_{e1}^n,Y_{e2}^n) - h(Z_1^n|Z_1^n+Z_{e1}^n) - h(Z_2^n|Z_2^n+Z_{e2}^n) + 2n\varepsilon_n \qquad (32) \\ &\le h(Y_1^n|Y_{e1}^n) + h(Y_2^n|Y_{e2}^n) \\ &\qquad - h(Z_1^n|Z_1^n+Z_{e1}^n) - h(Z_2^n|Z_2^n+Z_{e2}^n) + 2n\varepsilon_n \\ &= h(Y_1^n|Y_{e1}^n) - h(Z_1^n|Z_1^n+Z_{e1}^n) \\ &\qquad + h(Y_2^n|Y_{e2}^n) - h(Z_2^n|Z_2^n+Z_{e2}^n) + 2n\varepsilon_n \end{aligned}$$

Here (31) follows from the channel model (28) and (32) from the independence of the noise process across the channels. We will provide an upper bound for $h(Y_1^n|Y_{e1}^n) - h(Z_1^n|Z_1^n+Z_{e1}^n)$. The derivation of the upper bound for $h(Y_2^n|Y_{e2}^n) - h(Z_2^n|Z_2^n+Z_{e2}^n)$ is analogous. Together, these bounds will yield the claim.

$$\begin{aligned} h(Y_1^n|Y_{e1}^n) - h(Z_1^n|Z_1^n+Z_{e1}^n) \le{}& \frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_1^2}\right) \\ &- \frac{1}{2}\log\left(1+\frac{\beta P}{\sigma_1^2+\sigma_{e1}^2}\right). \end{aligned} \tag{33}$$

We first note that since Z_1^n and Z_{e1}^n are i.i.d. and independent, we have

$$\begin{aligned} h(Z_1^n|Z_1^n+Z_{e1}^n) &= h(Z_1^n) + h(Z_{e1}^n) - h(Z_1^n+Z_{e1}^n) \\ &= n\log 2\pi e \frac{\sigma_1^2\sigma_{e1}^2}{\sigma_1^2+\sigma_{e1}^2} \end{aligned} \tag{34}$$

We now upper bound $h(Y_1^n|Y_{e1}^n)$ as follows:

$$\begin{aligned} h(Y_1^n|Y_{e1}^n) &\le \sum_{i=1}^n h(Y_{1i}|Y_{e1i}) \\ &= \sum_{i=1}^n h(Y_{1i}|Y_{1i}+Z_{e1i}) \\ &\le \sum_{i=1}^n h(Y_{1i} - \alpha_{\text{MMSE,i}}(Y_{1i}+Z_{e1i})) \qquad (35) \\ &\le \sum_{i=1}^n \log 2\pi e\left(\frac{(P_{1i}+\sigma_{11}^2)\sigma_{e1}^2}{P_{1i}+\sigma_{11}^2+\sigma_{e1}^2}\right) \\ &\le n\log 2\pi e\left(\frac{(\frac{1}{n}\sum_{i=1}^n P_{1i}+\sigma_1^2)\sigma_{e1}^2}{\frac{1}{n}\sum_{i=1}^n P_{1i}+\sigma_1^2+\sigma_{e1}^2}\right) \qquad (36) \\ &\le n\log 2\pi e\left(\frac{(\beta P_1+\sigma_1^2)\sigma_{e1}^2}{\beta P_1+\sigma_1^2+\sigma_{e1}^2}\right) \qquad (37) \end{aligned}$$

Here $\alpha_{\text{MMSE,i}}$ in (35) is the constant in the linear MMSE estimation of Y_{1i} from $Y_{1i}+Z_{e1i}$. Finally combining (37) with (34) gives (38). In an analogous fashion, it can be shown that

$$\begin{aligned} h(Y_2^n|Y_{e2}^n) - h(Z_2^n|Z_2^n+Z_{e2}^n) \le{}& \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_2^2}\right) \\ &- \frac{1}{2}\log\left(1+\frac{(1-\beta)P}{\sigma_2^2+\sigma_{e2}^2}\right), \end{aligned} \tag{38}$$

and this completes the proof of Claim 5.

It remains to show that if the eavesdropper is stronger on any sub-channel then the transmitter should not transmit on such sub-channels and use independent codewords on those channels where the intended receiver is stronger than eavesdropper. To see this, suppose we make the intended receiver as strong as the eavesdropper on any sub-channel where he is originally weaker. Clearly, the capacity of this channel can only be larger than the original channel. But on this new channel, the eavesdropper is degraded with respect to the intended receiver on every sub-channel. So by Claim 5, it suffices to use independent code-books on each parallel channel. However, on any parallel channel where the eavesdropper is as strong as the intended receiver, the secrecy capacity is zero. So it suffices to only transmit on sub-channels where the intended receiver is stronger than the eavesdropper. But this scheme can also, be used on the original channel, thus establishing its optimality.

References

[1] A. D. Wyner, “The Wiretap Channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–87, 1975.

[2] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–56, 1978.

[4] H. Yamamoto, “On secret sharing communication systems with two or three channels,” *IEEE Trans. Inform. Theory*, vol. 32, pp. 387–393, May 1986.

[5] ——, “A coding theorem for secret sharing communication systems with two Gaussian wiretap channels,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 634–638, May 1991.

[6] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography – Part I: Secret sharing,” *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.

[7] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, Mar. 1993.

[8] E. Tekin and A. Yener, “The Gaussian multiple access wire-tap channel with collective secrecy constraints,” in *Proc. Int. Symp. Inform. Theory*, 2006.

[9] Y. Liang and H. V. Poor, “Generalized multiple access channels with confidential messages.” in *Proc. Int. Symp. Inform. Theory*, 2006.

[10] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, “The discrete memoryless multiple access channel with confidential messages,” in *Proc. Int. Symp. Inform. Theory*, 2006.

[11] A. Fiat and M. Naor, “Broadcast encryption,” in *Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, Santa Barbara, CA, 1994, pp. 480–491.

[12] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. Int. Symp. Inform. Theory*, Seattle, July 2006.

[13] A. O. Hero, “Secure space-time communication,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 1–16, Dec. 2003.

[14] X. Li and E. P. Ratazzi, “MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks,” in *IEEE Military Communications Conference (MILCOM’2005)*, 2005.

[15] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in *Proc. Int. Symp. Inform. Theory*, 2005.

[16] R. Negi and S. Goel, “Secret communication using artificial noise,” in *Proc. IEEE Vehicular Tech. Conf*, 2005.

[17] Y. Liang and H. V. Poor, “Secure communication over fading channels,” in *Proc. 44th Allerton Conf. on Communication, Control and Computing*, 2006.

[18] Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” in *Proc. 44th Allerton Conf. on Communication, Control and Computing*, 2006.

[19] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[20] I. Csiszár, “Almost independence and secrecy capacity (in russian),” *Problems of Information Transmission (PPI)*, vol. 32, pp. 48–57, 1996.

[21] U. M. Maurer and S. Wolf, “Information-theoretic key agreement: from weak to strong secrecy for free,” in *EUROCRYPT*, 2000.

[22] G. Caire and S. Shamai, “On achievable rates in a multi-antenna Gaussian broadcast channel,” in *Proc. Int. Symp. Inform. Theory*, Washington, DC, June 2001, p. 147.