Gaussian diamond network with adversarial jammer

Soheil Mohajer and Suhas N. Diggavi
École Polytechnique Fédéral de Lausanne, Lausanne, Switzerland.
Email: {soheil.mohajer, suhas.diggavi}@epfl.ch

***Abstract*—In this paper we consider communication from a source to a destination over a wireless network with the help of a set of authenticated relays. We focus on a special "diamond" network, where there is no direct link between the source and the destination; however the relay nodes help to establish such a communication. There is a single adversarial node which injects signals to disrupt this communication. Like the source, it can only influence the destination through the relays. We develop an approximate characterization of the reliable transmission rate in the presence of such an adversary. This is done by developing an outer bound, and demonstrating an achievable strategy that is within a constant number of bits of the outer bound, regardless of the channel values. A deterministic version of the same problem is solved exactly, yielding insights which are used in the approximate characterization.**

I. Introduction

Wireless communication is inherently susceptible to malicious interference attempting to disrupt communications. An adversary can utilize the broadcast medium to insert disruptive signals. This problem has been well-studied for point-to-point communication, with early works in arbitrarily varying channels (AVC) [1]. This topic has not received significant attention in the context of wireless networks, where there are relay nodes to assist communication. In this paper we formulate and study coding strategies in this problem for a simple relay network.

The question of characterizing the capacity of wireless networks, even without the presence of malicious nodes, has been an open question for many decades. Recently there has been progress on this question by looking for an approximate characterization of the capacity [2]. Underlying this is an examination of the capacity of a deterministic model that focuses on the signal interaction rather than the noise [3]. Using this deterministic model, it was shown that an exact capacity characterization can be obtained in the form of an information-theoretic max-flow min-cut result; a first such result when there is both broadcast and multiple access interference in the signal interactions. This deterministic approach also gives insights that are used in obtaining the approximate characterization in noisy (Gaussian) wireless networks. In this paper we build on these ideas by first examining the impact of the adversarial node on a wireless network modeled using a linear deterministic signal interaction. In particular, we study both the deterministic and Gaussian versions of the diamond wireless network depicted in Figures 2 and 1, respectively.

The role of malicious jamming nodes in wired networks has received recent significant attention in network coded systems (see [4] and references therein). However, the problem in wireless networks is quite different due to the signal interactions caused by the broadcast nature of the channel. We will utilize the fact that the disrupting signal transmitted by the adversary (see Figure 1) cause the received signals at the authenticated relays to be related to each other. We use this in order to *neutralize* the adversarial signal without separating it from the legitimate transmitted signal. This technique is adapted from a coding technique, termed interference neutralization, developed for the the relay-interference network in [5], [6]. The idea is that we utilize the "correlation" in the received signal at the relays to cancel part of the undesired adversarial signal. A similar idea is used in [7] for an amplify-forward relaying strategy to reduce the interference at the receiver, and assuming a *sum power constraint* at the relays allows to utilize a beam-forming strategy.

The main contributions of this paper are the following. We formulate the problem of adversarial jamming for a wireless (diamond) network and provide an outer bound as well as achievable strategies for this network. In particular, we show an exact characterization of reliable transmission rate for a diamond network with linear deterministic model [3]. The coding strategy for this case crucially utilizes the interference neutralization technique developed in [5]. The deterministic version of this problem is studied for some regimes of parameters in a recent work [8]. However, here we generalize the deterministic characterization for arbitrary channel parameters. More importantly, we show that the achievable strategy inspired by the deterministic analysis is within a constant number of bits of the outer bound in the Gaussian case.

We describe the problem and main results in Section II. The analysis for linear deterministic networks is given in Section III. Section IV develops the outer bound and the achievable strategy for the Gaussian case. Due to lack of space, at times we only give the proof sketch. More details on the proof can be found in [9]. The results present in this paper lead to several natural questions on the generalizations to arbitrary networks, multiple adversaries etc. These are topics of future work.

II. Problem Statement and Main results

Consider the diamond network in Fig. 1, where the source S wishes to reliably send its message W to the destination D. It encodes the message and broadcasts x^n to the relays B_1 and B_2. However, the signal received at the relays are corrupted by the interference from an adversarial node A, who wishes

This work was supported in part by the Swiss National Science Foundation through NCCR-MICS under grant number 51NF40-111400 and by N-CRAVE under grant number FP7 ICT-2007-215252.

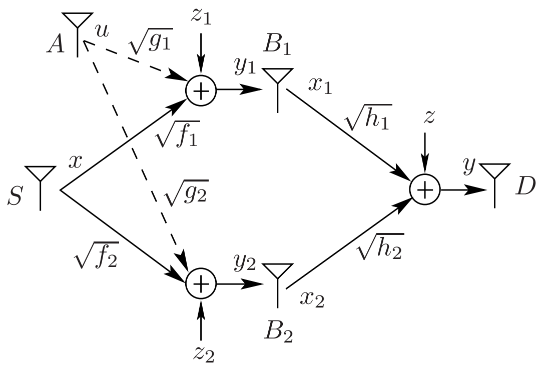

Fig. 1. Transmission model; Source node S wishes to communicate to D, while the system is jammed by the adversarial node A.

to jam the transmission by inserting disruptive signals to the system. Therefore, the relay B_i receives

$$y_i[t] = \sqrt{f_i}x[t] + \sqrt{g_i}u[t] + z_i[t], \qquad i = 1, 2,$$

where x is the transmitted signal by the source, u is the interfering signal inserted by the jammer, and z_i is an additive white Gaussian noise with unit variance, independent of x and u. The relay nodes perform any (causal) processing on their received signal sequences $\{y_1[t]\}$ and $\{y_2[t]\}$ respectively, to obtain their transmitting signal sequences, $\{x_1[t]\}$ and $\{x_2[t]\}$. The signal received at the destination D can be written as

$$y[t] = \sqrt{h_1}x_1[t] + \sqrt{h_2}x_2[t] + z[t],$$

over the Gaussian multiple access channel, and wishes to decode W based on its received signal. We also assume equal power constraints for the source, relays, and jammer, that is, $\mathbb{E}[x^2] \leq 1$, $\mathbb{E}[x_1^2] \leq 1$, $\mathbb{E}[x_2^2] \leq 1$, and $\mathbb{E}[u^2] \leq 1$.

The AVC problem in a point-to-point system is studied under two assumptions [1]: (a) there exists common randomness shared between the source and destination, unknown to adversary; This facilitates the use of *random* codebooks chosen using the common randomness; (b) if there is no such a common randomness, and a *fixed* codebook is used for transmission. Though we present the work for case (a), i.e., shared secret common randomness between source and the relays, these results can be easily extended to case (b) [9].

Our main result is the (approximate) capacity from S to D, in the presence of an adversarial jammer A.

Theorem 1. *The randomized capacity of the network in Figure 1 satisfies*

$$\mathcal{C} \leq \frac{1}{2}\log\left(1 + \frac{f_1 + f_2 + (\sqrt{f_1 g_2} - \sqrt{f_2 g_1})^2}{1 + g_1 + g_2}\right), \tag{1}$$

$$\mathcal{C} \leq \frac{1}{2}\log\left(1 + (\sqrt{h_1} + \sqrt{h_2})^2\right), \tag{2}$$

$$\mathcal{C} \leq \frac{1}{2}\log\left(1 + \frac{f_1}{1 + g_1}\right) + \frac{1}{2}\log(1 + h_2), \tag{3}$$

$$\mathcal{C} \leq \frac{1}{2}\log\left(1 + \frac{f_2}{1 + g_2}\right) + \frac{1}{2}\log(1 + h_1). \tag{4}$$

Moreover, for any $\mathcal{C}$ which satisfies (1)-(4)*, the rate $R = \mathcal{C} - 4$ is achievable.*

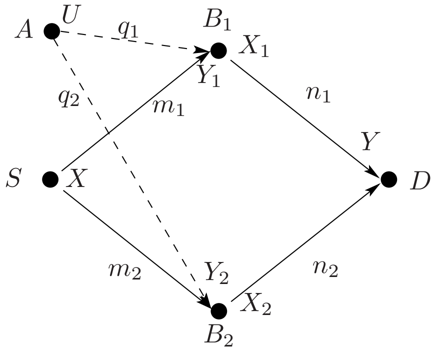

Fig. 2. The deterministic model of the problem.

A trivial sub-optimal scheme here is to treat the interference as independent noise, and follow the known schemes for noisy diamond relay network [2]. However, such noises are correlated since they are generated by the same jamming source, and can be utilized. However, the jammer is *not* limited to using just noise insertion strategies. It can use its knowledge of the channel parameters and the coding strategies to potentially further disrupt communication.

In the following section, we study the *deterministic* version of this problem, obtained by the linear deterministic model introduced in [3]. The bounding techniques and transmission strategies inspired by the deterministic network will be then translated for the Gaussian network in Section IV.

III. A Deterministic Approach

Consider the deterministic network shown in Figure 2, where source S wishes to communicate its message to the destination node D via the relays B_1 and B_2. Each transmitter can broadcast vectors of length p with elements from the binary[1] field $\mathbb{F}_2$. Such vectors get multiplied by the *channel matrix*, and the sum of all such vectors get received at the receiver over a multiple access channel. We denote the channel matrices from the source to the relays by *shift matrices* M_1 and M_2, from the jammer to the relays by Q_1 and Q_2, and from the relays to the destination by N_1 and N_2. These matrices are powers of the lower triangular matrix $\mathbf{J}$, where,

$$\mathbf{J} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}_{p \times p}. \tag{5}$$

Similar lowercase letters are used to denote the rank of the matrices (channel gains). Therefore, for example, $M_1 = \mathbf{J}^{p-m_1}$, and $\mathrm{rank}(M_1) = m_1$.

Using this model, the relay node B_i receives

$$Y_i[t] = M_i X[t] + Q_i U[t], \qquad i = 1, 2, \tag{6}$$

and the signal received at the destination D can be written as

$$Y[t] = N_1 X_1[t] + N_2 X_2[t]. \tag{7}$$

[1] Similar results holds for any arbitrary field, except that the capacity will be multiplied by $\log(q)$, where q is the field size.

The following theorem characterizes the capacity of this network.

Theorem 2. *The capacity of the deterministic diamond network with adversarial node is given by*

$$\mathcal{C} = \min\Big\{\Psi(m_1,m_2,q_1,q_2) - \max\{q_1,q_2\}, \max\{n_1,n_2\}, (m_1-q_1)^+ + n_2, (m_2-q_2)^+ + n_1\Big\}, \tag{8}$$

where

$$\Psi(m_1,m_2,q_1,q_2) \triangleq \begin{cases} \max\{m_1,m_2,q_1,q_2\} & \textit{if } m_1+q_2=m_2+q_1 \\ \max\{m_1+q_2, m_2+q_1\} & \textit{otherwise.}\end{cases} \tag{9}$$

Proof of Theorem 2:

a) The converse part: Assume we use code of length ℓ, and W can be decoded from Y^ℓ with error probability ϵ_ℓ, where $\epsilon_\ell \to 0$ as ℓ grows. Therefore, using Fano's inequality, we have

$$H(X^\ell|Y^\ell) \le H(W|Y^\ell) \le \ell\epsilon_\ell. \tag{10}$$

We use bold-face matrices, to denote ℓ copies of them, as the transfer matrix applied to a codeword of length ℓ, *e.g.*, $\mathbf{M}_1 = \mathbf{I}_\ell \otimes M_1$. Denote by G_X and G_U the transfer matrix from the adversarial node and the source to the relays, respectively. These matrices can be written as

$$G_X = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix}, \qquad G_U = \begin{bmatrix} Q_1 \\ Q_2 \end{bmatrix}. \tag{11}$$

Hence, we can write the signals received at the relays as

$$\begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} G_X \mid G_U \end{bmatrix} \begin{bmatrix} X \\ U \end{bmatrix} \tag{12}$$

Note that the Markov chain $X^\ell \leftrightarrow (Y_1^\ell, Y_2^\ell) \leftrightarrow Y^\ell$ implies that (Y_1^ℓ, Y_2^ℓ) are enough to decode the message. It is also clear that once B_1 and B_2 can decode X, they can also obtain $\mathbf{G}_U U^\ell$. Hence, $H(X^\ell, \mathbf{G}_U U^\ell | Y_1^\ell, Y_2^\ell) \le \ell\epsilon_\ell$. Therefore,

$$\begin{aligned} \ell R + H(\mathbf{G}_U U^\ell) &= H(X^\ell) + H(\mathbf{G}_U U^\ell) = H(X^\ell, \mathbf{G}_U U^\ell) \\ &\le I(X^\ell, \mathbf{G}_U U^\ell; Y_1^\ell, Y_2^\ell) + \ell\epsilon_\ell \\ &\le H(Y_1^\ell, Y_2^\ell) + \ell\epsilon_\ell = \operatorname{rank}(\mathbf{G}_{X,U}) + \ell\epsilon_\ell \\ &= \ell\operatorname{rank}(G_{X,U}) + \ell\epsilon_\ell \end{aligned} \tag{13}$$

It is clear that the adversary can choose U^ℓ such that $H(\mathbf{G}_U U^\ell) = \ell\operatorname{rank}(G_U) = \ell\max\{q_1,q_2\}$. Therefore, we have $R \le \operatorname{rank}(G_{X,U}) - \max\{q_1,q_2\} + \epsilon_\ell$. It only remains to show that $\operatorname{rank}(G_{X,U}) = \Psi(m_1,m_2,q_1,q_2)$, which is a known fact from linear algebra, and the details can be found in [9]. This proves the first upper bound on R. Note that this bound captures the maximum flow of information through the cut $\Omega_1 = \{S, A\}$.

The proof of the second bound is straight-forward.

$$\begin{aligned} \ell R &\le H(X^\ell) \le I(X^\ell; Y^\ell) + \ell\epsilon_\ell \\ &\le H(Y^\ell) + \ell\epsilon_\ell \le \ell\max\{n_1,n_2\} + \ell\epsilon_\ell. \end{aligned} \tag{14}$$

In order to show $R \le (m_1-q_1)^+ + n_2$, we first recall that decodability of W from Y^ℓ implies

$$\begin{aligned} H(X^\ell, \mathbf{Q}_1U^\ell|Y_1^\ell, Y^\ell) &= H(X^\ell|Y_1^\ell, Y^\ell) + H(\mathbf{Q}_1U^\ell|X^\ell, Y_1^\ell, Y^\ell) \\ &\le H(W|Y_1^\ell, Y^\ell) + H(Y_1^\ell - \mathbf{M}_1X^\ell|X^\ell, Y_1^\ell, Y^\ell) \le \ell\epsilon_\ell. \end{aligned}$$

Hence,

$$\begin{aligned} \ell R + H(\mathbf{Q}_1U^\ell) &= H(X^\ell) + H(\mathbf{Q}_1U^\ell) \\ &\overset{(a)}{=} H(X^\ell, \mathbf{Q}_1U^\ell) \le I(X^\ell, \mathbf{Q}_1U^\ell; Y_1^\ell, Y^\ell) + \ell\epsilon_\ell \\ &\le H(Y_1^\ell, Y^\ell) + \ell\epsilon_\ell) = H(Y_1^\ell) + H(Y^\ell|Y_1^\ell) + \ell\epsilon_\ell \\ &\overset{(b)}{\le} H(Y_1^\ell) + H(\mathbf{N}_2X_2^\ell|Y_1^\ell) + \ell\epsilon_\ell \\ &\le \ell\max\{m_1,q_1\} + \ell n_2 + \ell\epsilon_\ell. \end{aligned} \tag{15}$$

where in (a) we used the assumption that the adversary does not know the message, and therefore, its interfering signal is independent of X^ℓ, and (b) holds since X_1^ℓ is a function of Y_1^ℓ. Combining (15) with the fact that the adversarial node can make $H(\mathbf{Q}_1U^\ell)$ as large as ℓq_1, gives us the third bound. It is worth mentioning that this bound essentially captures the maximum flow of information through the cut $\Omega = \{S, A, B_1\}$. The proof of the last bound is just repeating the same argument for a symmetric situation in cut $\Omega = \{S, A, B_2\}$.

b) The achievability part (proof sketch): The basic idea is to provide D with R interference-free linearly independent equations about the message. Note that some of sub-nodes in B_1 and B_2 receive the same interfering bit from A, and therefore this interference can be neutralized [5], if they get forwarded and received on the same sub-node of D. We will identify $R^{(N)}$, the maximum number of linearly independent equations can be neutralized using this technique.

There are also possibly a subset of message bits received at the relays above the interference level, and therefore not corrupted by interference. These *pure* bits can be directly forwarded to the destination. We denote the number of such *pure* linear equations by $R^{(P)}$.

We denote the levels of B_1 at the receiver side by $Y_{1,1}$ (for the highest) to $Y_{1,p}$ (for the lowest), and similarly for B_2. Define

$$\delta \triangleq \min\{q_1, q_2\} - \min\{(q_1-m_1)^+, (q_2-m_2)^+\}.$$

It is easy to show that $Y_{1,(p-(q_1-q_2)^++\kappa)}$ and $Y_{2,(p-(q_2-q_1)^++\kappa)}$ are corrupted by the same bit from A, for $\kappa = 0, \ldots, \delta - 1$. Moreover, at least one of $Y_{1,(p-(q_1-q_2)^++\kappa)}$ and $Y_{2,(p-(q_2-q_1)^++\kappa)}$ receive a bit from the source. Therefore, for each κ, if $Y_{1,(p-(q_1-q_2)^++\kappa)}$ and $Y_{2,(p-(q_2-q_1)^++\kappa)}$ can get forwarded on the same destination sub-node, the destination receives an equation about the source whose interference is neutralized. It is worth mentioning that if $m_1 + q_2 = m_2 + q_1$, then the neutralized equations received at D are zero, since the message bits would be also neutralized. On the other hand, the condition $m_1 + q_2 \neq m_2 + q_1$ guarantees that such received legitimate bits are different.

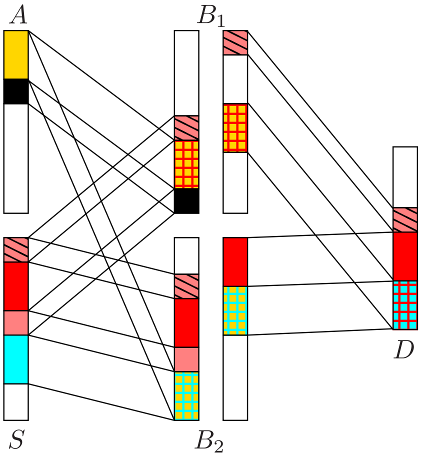

Fig. 3. Transmission strategy to provide interference neutralization.

Each bit neutralization utilizes one sub-link for B_1 to D, and one sub-link from B_2 to D. Hence, we can send up to

$$R^{(N)} = \nu \triangleq \begin{cases} 0 & \text{if } m_1 + q_2 = m_2 + q_1 \\ \min\{\delta, n_1, n_2\} & \text{otherwise.} \end{cases} \tag{16}$$

neutralized equations to the destination.

On the other hand, nodes B_1 and B_2, respectively, receive $(m_1 - q_1)^+$ and $(m_2 - q_2)^+$ bits from the source which are above the interference level, and therefore not corrupted. These bits can be forwarded to D through the remaining $(n_1 - \nu)$ and $(n_2 - \nu)$ links in the second layer of the network. However, these two set of bits have overlap, since they are both the upper level bits sent by S. Analysis of the number of pure bits can be sent to the destination node, is equivalent to a study of a linear shift deterministic diamond network without adversary, where there are $(m_1 - q_1)^+$ and $(m_2 - q_2)^+$ links from S to the relays, and $(n_1 - \nu)$ and $(n_2 - \nu)$ links from the relays to the destination. The capacity of this network is easy to compute as in [3]. That is,

$$\begin{aligned} R^{(P)} = \min\Big\{ & \max\{(m_1 - q_1)^+, (m_2 - q_2)^+\}, \\ & (m_1 - q_1)^+ + (n_2 - \nu), (m_2 - q_2)^+ + (n_1 - \nu), \\ & \max\{n_2 - \nu, n_2 - \nu\}\Big\}. \end{aligned} \tag{17}$$

One can show that the received equations using two methods are linearly independent [9], and therefore any rate $R \leq R^{(N)} + R^{(P)}$ is achievable. Using some algebra and manipulations, one can show that adding the RHS's of (16) and (17) gives us the same bound claimed in the theorem. ■

In the following example we illustrate in details the two methods to achieve the capacity of the network.

Example 1. *Consider a diamond network with parameters* $m_1 = 4$, $m_2 = 6$, $q_1 = 3$, $q_2 = 2$, $n_1 = 5$, *and* $n_2 = 4$. *Also assume* $p = 7$. *Theorem 2 implies that* $\mathcal{C} = 5$. *In the following we show how the destination can get* 5 *linearly independent equations about the bits transmitted by the source node. Denoting the source and interference bits by* X_i *and* U_j, *for* $i = 1, \ldots, p$, *and* $j = 1, \ldots, p$, *we have*

$$\begin{aligned} Y_1 &= \begin{bmatrix} Y_{1,1} & Y_{1,2} & Y_{1,3} & Y_{1,4} & Y_{1,5} & Y_{1,6} & Y_{1,7} \end{bmatrix}^T \\ &= \begin{bmatrix} 0 & 0 & 0 & X_1 & X_2 + U_1 & X_3 + U_2 & X_4 + U_3 \end{bmatrix}^T \end{aligned}$$

and

$$\begin{aligned} Y_2 &= \begin{bmatrix} Y_{2,1} & Y_{2,2} & Y_{2,3} & Y_{2,4} & Y_{2,5} & Y_{2,6} & Y_{2,7} \end{bmatrix}^T \\ &= \begin{bmatrix} 0 & X_1 & X_2 & X_3 & X_4 & X_5 + U_1 & X_6 + U_2 \end{bmatrix}^T. \end{aligned}$$

Recall that we can neutralize up to $\nu = \min\{\delta, n_1, n_2\} = 2$ *bits. This will be done by forwarding* $Y_{1,5}$ *and* $Y_{1,6}$ *by* B_1 *and* $-Y_{2,6}$ *and* $-Y_{2,7}$ *by* B_2 *over their lowest two links to* D. *The destination node will receive* $Y_6 = Y_{1,5} - Y_{2,6} = X_2 - X_5$ *and* $Y_7 = Y_{1,6} - Y_{2,7} = X_3 - X_6$ *on its lowest levels.*

The relay node B_1 *has only one bit of non-corrupted signal,* X_1 *and node* B_2 *has four of them,* X_1, X_2, X_3, *and* X_4. *In order to send these bits,* B_1 *send* X_1 *on its highest level, and* B_2 *forwards* X_2 *and* X_3 *on its highest levels. This provides* D *with* $Y_3 = X_1$, $Y_4 = X_2$, *and* $Y_5 = X_3$. *Note that, we cannot decode all the six bits, but we obtain five linearly independently equations describing* $X_1, \ldots, X_6$. *This transmission scheme is illustrated in Figure 3.*

IV. The Gaussian Network: proof of Theorem 1

The upper bound: We imitate the same bounding techniques used to prove Theorem 2. Let R be an achievable rate using a code of length ℓ. Note that the Markov chain

$$y^\ell \leftrightarrow (x_1^\ell, x_2^\ell) \leftrightarrow (y_1^\ell, y_2^\ell) \leftrightarrow x^\ell \tag{18}$$

is induced by the network structure. We first start with

$$\begin{aligned} \ell R &\leq I(y^\ell; x^\ell) + \ell\epsilon_\ell \overset{(a)}{\leq} I(y_1^\ell, y_2^\ell; x^\ell) + \ell\epsilon_\ell + \ell\epsilon_\ell \\ &\overset{(b)}{\leq} \frac{\ell}{2}\log\left(1 + \frac{f_1 + f_2 + (\sqrt{f_1 g_2} - \sqrt{f_2 g_1})^2}{1 + g_1 + g_2}\right) + \ell\epsilon_\ell. \end{aligned}$$

where in (a) we used the data-processing inequality for the Markov chain in (18). Note that (b) follows from the fact that the adversary wishes to minimize the mutual information, and in particular, it can reduce it to the expression in RHS by sending random Gaussian noise. This proves the first bound.

Similarly, the second bound holds since

$$\begin{aligned} \ell R &\leq I(y^\ell; x^\ell) + \ell\epsilon_\ell \overset{(c)}{\leq} I(y^\ell; x_1^\ell x_2^\ell) + \ell\epsilon_\ell \\ &\leq \frac{\ell}{2}\log\left(1 + (\sqrt{h_1} + \sqrt{h_2})^2\right). \end{aligned}$$

We again used the data-processing inequality in (c).

In order to show the third upper bound, we can write

$$\begin{aligned} \ell R &\leq I(y_1^\ell, y^\ell; x^\ell) + \ell\epsilon_\ell = I(y_1^\ell; x^\ell) + I(y^\ell; x^\ell | y_1^\ell) + \ell\epsilon_\ell \\ &\overset{(d)}{\leq} \frac{1}{2}\log\left(1 + \frac{f_1}{1 + g_1}\right) + I(y^\ell; x^\ell | y_1^\ell) + \ell\epsilon_\ell \end{aligned} \tag{19}$$

where (d) holds due to the same argument we used in (b).The second term in (19) can be upper bounded by

$$\begin{aligned} I(y^\ell; x^\ell|y_1^\ell) &= h(y^\ell|y_1^\ell) - h(y^\ell|x^\ell, y_1^\ell) \\ &\overset{(e)}{\leq} h(y^\ell|x_1^\ell) - h(y^\ell|x_1^\ell, x_2^\ell) \\ &= h(\sqrt{h_2}x_2^\ell + z^\ell|x_1^\ell) - h(y^\ell|x_1^\ell, x_2^\ell) \\ &\leq h(\sqrt{h_2}x_2^\ell + z^\ell) - h(y^\ell|x_1^\ell, x_2^\ell) \leq \frac{\ell}{2}\log(1+h_2). \end{aligned}$$

Note that in (e), we used the fact that x_1^ℓ is a function of y_1^ℓ, as well as the data-processing inequality for the Markov chain in (18). This proves the third inequality in (3). The last bound can be proved by repeating the same argument for $I(y_2^\ell, y^\ell; x^\ell)$.

The proof sketch for the inner bound: The achievability is based on *message splitting* and *superposition coding*. The power allocation should be performed such that the part of the message which is not corrupted by interference can be decoded at the relays. Moreover, the interfered part get forwarded to the destination such that the effective interference at the destination be small enough such that this part of the message can be decoded at the destination. In the following we only explain this idea without specifying the exact power allocation coefficients which involves considering different cases of channel parameters. We also focus on the randomized capacity [1], though these ideas extend to fixed codebooks [9].

Without loss of generality, we assume that the relay B_1 is stronger than B_2, *i.e.*, $\mathsf{SINR}_1 \geq \mathsf{SINR}_2$, where $\mathsf{SINR}_i = f_i/(1+g_i)$. We first split the message W into three parts, namely, W_c, W_p, W_n, with rates R_c, R_p, and R_n. Our encoding and decoding strategy guarantees that the common message, W_c, can be decoded at both relays, while the private sub-message, W_p, can be only decoded at B_1. However, neither of the relays can decode the neutralization sub-message, W_n, and it can be only decoded at the destination, once the interference is neutralized.

We use three random codebooks of rates R_c, R_p, and R_n, generated according to the Gaussian distribution with unit variance. The source maps its sub-messages to the codewords from corresponding codebooks, and obtains $\mathbf{x}_c$, $\mathbf{x}_p$, and $\mathbf{x}_n$. Then the signal transmitted by the source is formed as a super position of the three codewords, using a proper power allocation,

$$\mathbf{x} = \sqrt{\alpha_c}\mathbf{x}_c + \sqrt{\alpha_p}\mathbf{x}_p + \sqrt{\alpha_n}\mathbf{x}_n, \qquad (20)$$

where $\alpha_n = \min(1, 1/\mathsf{SINR}_1)$, $\alpha_p = \min(1, 1/\mathsf{SINR}_2) - \alpha_n$, and $\alpha_c = 1 - \alpha_n - \alpha_p$ are the power allocation coefficients. The relay node i receives

$$\mathbf{y}_i = \sqrt{f_i\alpha_c}\mathbf{x}_c + \sqrt{f_i\alpha_p}\mathbf{x}_p + \sqrt{f_i\alpha_n}\mathbf{x}_n + \sqrt{g_i}\mathbf{u} + \mathbf{z}_i$$

Both nodes B_1 and B_2, first decodes $\mathbf{x}_c$ treating everything else as noise. Once $\mathbf{x}_c$ is decoded, B_1 can cancel it from its received signal, and decode $\mathbf{x}_p$. This can be done as long as

$$R_c \leq \frac{1}{2}\log\left(1+\mathsf{SINR}_2\right) - \frac{1}{2}.$$

and

$$R_c + R_p \leq \frac{1}{2}\log\left(1+\mathsf{SINR}_1\right) - \frac{1}{2}.$$

It is worth mentioning that in the case of *fixed code capacity* [10], we have $R_c = 0$ if $g_1 \geq f_1$, and similarly for $R_c + R_p$. The remaining parts of the signals will be still used for forming the transmitting signal and so this scheme can be extended for fixed codes (see [9] for details). The signal transmitted by the relays are again formed by superposition of what they have decoded, and their residual signals.

$$\begin{aligned} \mathbf{x}_1 &= \sqrt{\beta_c}\mathbf{x}_c + \sqrt{\beta_p}\mathbf{x}_p + \sqrt{\beta_n}\frac{\mathbf{y}_1 - \sqrt{f_1\alpha_c}\mathbf{x}_c - \sqrt{f_1\alpha_p}\mathbf{x}_p}{\sqrt{f_1\alpha_n + g_1 + 1}} \\ \mathbf{x}_2 &= \sqrt{\gamma_c}\mathbf{x}_c - \sqrt{\gamma_n}\frac{\mathbf{y}_2 - \sqrt{f_2\alpha_c}\mathbf{x}_c}{\sqrt{f_2\alpha_p + f_2\alpha_n + g_2 + 1}}, \qquad (21) \end{aligned}$$

where the power allocation coefficients satisfy $\beta_c+\beta_p+\beta_n \leq 1$ and $\gamma_c + \gamma_n \leq 1$.

Finally the decoder receivers a noisy linear combination of $\mathbf{x}_1$ and $\mathbf{x}_2$ over the multiple access channel. It should first jointly decode W_c and W_p, and then remove corresponding codewords from its received signal. Then, it can decode W_n. Note that the power allocations coefficients can be chosen such that the effective interference received at the destination is zero[2]. In order to that, they should satisfy

$$\frac{h_1 g_1 \beta_n}{f_1\alpha_n + g_1 + 1} = \frac{h_2 g_2 \gamma_n}{f_2(\alpha_p + \alpha_n) + g_2 + 1}. \qquad (22)$$

■

References

[1] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie Verw. Gebiete*, vol. 44, pp. 159–175, 1978.

[2] A. S. Avestimehr, S. N. Diggavi, and D. N. C. Tse, "Wireless network information flow: A deterministic approach," 2009, submitted to IEEE Trans. Inform. Theory, Available from http://arxiv.org/pdf/0906.5394.

[3] A. Avestimehr, S. Diggavi, and D. Tse, "A deterministic approach to wireless relay networks," in *Proceedings of Allerton Conference on Communication, Control, and Computing*, Illinois, USA, Sept. 2007.

[4] R. Koetter and F. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, pp. 3579–3591, Aug. 2008.

[5] S. Mohajer, S. N. Diggavi, C. Fragouli, and D. Tse, "Transmission techniques for relay-interference networks," in *Proceedings of Allerton Conference on Communication, Control, and Computing*, Illinois, USA, Sept. 2008.

[6] S. Mohajer, S. N. Diggavi, , and D. Tse, "Approximate capacity of a class of gaussian relay-interference networks," in *Proceedings of IEEE Int. Symp. Inform. Theory*, Seoul, Korea, July 2009.

[7] K. Gomadam and S. A. Jafar, "The effect of noise correlation in amplifyand-forward relay networks," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 731–745, Feb. 2009.

[8] S. M. H. T. Yazdi and M. R. Aref, "The capacity of a class of linear deterministic networks," 2010, available from http://arxiv.org/pdf/1001.2164.

[9] S. Mohajer and S. N. Diggavi, "Gaussian diamond network with adversarial jammer," tech. Rep., EPFL, Apr. 2010, Available at http://infoscience.epfl.ch.

[10] I. Csiszár and P. Narayan, "Capacity of the gaussian arbitrarily varying channel," *IEEE Trans. Inform. Theory*, vol. 37, pp. 18–26, Jan. 1991.

[2] In fact, we do not need to completely neutralize the interference. As long as the effective interference is below of the Gaussian noise power, a total rate with constant bit away from the upper bound can be achieved.