Exchanging Third-Party Information in a Network

David J. Love[†], Bertrand M. Hochwald[‡], and Kamesh Krishnamurthy[†]
[†]School of Electrical and Computer Engineering, Purdue University
West Lafayette, IN 47907
[‡] Beceem Communications
Santa Clara, CA 94054
Email: djlove@ecn.purdue.edu, hochwald@beceem.com, kkrishna@purdue.edu

***Abstract*— We consider the problem of exchanging information in a network, where every node can communicate with every other node through a common channel. In our model, every node wishes to exchange some local information (perhaps about a third party) with every other node in the network through the common channel. We provide the rate region for this fully connected network. The rate region we compute can incorporate side knowledge of the exchanged information by the nodes.**

We demonstrate an application of the rate region to a third-party channel-information exchange and demonstrate a code that is optimal.

I. Introduction

Demand for high rate connectivity has made reliable networks a priority. Many network applications and networking algorithms often assume that each node in the network has some level of global network knowledge. However, the actual problem of teaching each network node global information has not been fully addressed. To reach some level of global knowledge, each node generally has to learn information that is local to other nodes but not to itself. This information can be called "third-party" because it is information outside its immediate neighborhood. It can usually be obtained only through some form of coding and/or cooperation involving its neighbors. We define the problem, present some preliminary results, and address a specific application in detail.

To provide an example, consider the three-node network shown in Fig.1. We say that two nodes are connected if the link between the two nodes can support a rate above some threshold and not connected if the link can not support this threshold rate. Suppose we wish every node to know which node-pairs are connected. The nodes are numbered 0, 1, and 2. Because there are three nodes, each node only has two possible connections. We assume that each node (through training or other means) knows its local connectivity to its neighbors. Node i therefore knows $\mathbf{x}_i = [g_{i,j_0}\ g_{i,j_1}]$ where $j_0, j_1 \neq i$ and $0 \leq j_0 < j_1 \leq 2$. (We assume that the links are symmetric so that $g_{i,j} = g_{j,i}$, and that $g_{i,j}$ is either a zero or one.) We wish node i to also learn the third-party information g_{j_0,j_1}. Clearly node i must learn this from either node j_0 or j_1. When the exchange of all third-party information is complete, all nodes learn $g_{0,1}$, $g_{0,2}$, and $g_{1,2}$.

The information that each node knows after training consists of the three binary vectors

$$\mathbf{x}_0 = [g_{0,1}\ g_{0,2}]\,, \quad \mathbf{x}_1 = [g_{1,2}\ g_{1,0}]\,, \quad \mathbf{x}_2 = [g_{2,0}\ g_{2,1}]\,.$$

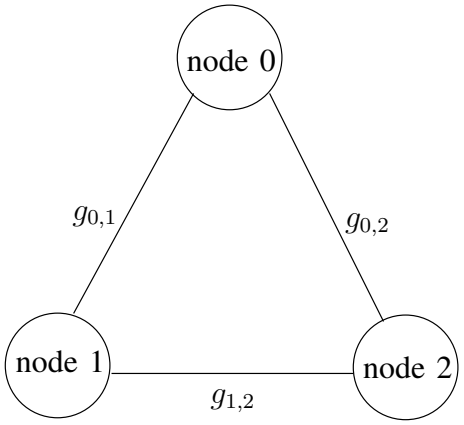

Fig. 1. Example of a three-node network connected by communication channels $g_{i,j} = g_{j,i}$. Each node i knows its local channel $g_{i,j}$ but does not know the remaining third-party channel.

Clearly there is some overlap in the information contained in the vectors. Each node has one item missing from its list.

Our network has a common control channel available to all three nodes. This control channel allows the reliable broadcast of one bit by any node to all the remaining nodes. This channel can be utilized by all nodes, but only by one at a time. One way to exchange information over the control channel would be for each node i to send $\mathbf{x}_i$ using two channel-uses for a total of six bits broadcast over six channel-uses. While this technique is very simple, it is clearly suboptimal because some information is sent twice. The correlation between the information known by the nodes is not exploited.

To exploit the correlation, we consider the following scheme. Node 0 sends the bit $c[0] = g_{0,1} \oplus g_{0,2}$ (we use $\oplus$ to denote modulo two addition) during one channel-use, node 1 sends $c[1] = g_{1,2} \oplus g_{1,0}$ during the second channel-use, and node 2 sends nothing. Therefore a total of only two bits have been transmitted over two channel-uses. Nevertheless, node i (for $i = 0, 1, 2$) learns $\mathbf{x}_j$ (for all $j \neq i$) from these two transmitted bits and its initial knowledge of $\mathbf{x}_i$. For example, node 0 starts initially with knowledge of the vector $\mathbf{x}_0$ and decodes the vectors as

$$\mathbf{x}_1 = [c[1] \oplus g_{0,1} \quad g_{0,1}] \quad \mathbf{x}_2 = [g_{0,2} \quad c[1] \oplus g_{0,1}]\,.$$

This shows that even a simple coding scheme can help

reduce the amount of data that must be transmitted. The correlation structure among the node sources in this example is the symmetry $g_{i,j} = g_{j,i}$. Clearly, other forms of correlation between the knowledge available at the various nodes are possible.

We now formulate the general third-party information exchange problem and derive a lower-bound on the number of bits that each node must transmit for every node to obtain knowledge of the other nodes' information. We then generalize the preceding network (to more than three nodes) and present a coding scheme that is within one channel-use of the bound.

II. Rate Region for Assuming a Common Control Channel Network

Consider an N-node network where each node has some information that must be exchanged with every other node. The local information for the ith node, $i = 0, 1, \ldots, N-1$, is a random vector $\mathbf{X}_i$ (we capitalize random vectors to distinguish them from their realizations), chosen from a finite alphabet $\mathcal{X}_i$, that must be conveyed to all the other nodes. We assume that all nodes have access to a common control channel that can carry one bit per channel-use. We also assume that when one node transmits on the control channel all other nodes listen. The goal is to convey every third-party information vector to every node using the minimum number of channel-uses.

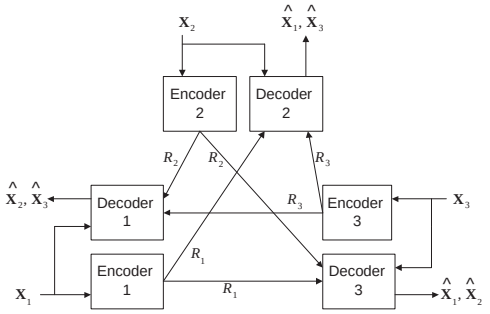

Fig. 2. Example of a three-node network, where the ith decoder has $\mathbf{X}_i$ as side information but wishes to learn (possibly correlated) $\mathbf{X}_j$ for $j \neq i$. The network is fully connected through a common one-bit-per-channel-use control channel that any node can use to convey information to all the remaining nodes simultaneously. Node i wishes to send R_i bits over the control channel.

The encoding and decoding framework we assume is shown in Fig. 2 for three nodes. The ith node uses an encoding function $f_i : \mathcal{X}_i^n \to \{1, 2, \ldots, 2^{nR_i}\}$ where n is the block length. The node then transmits the index corresponding to its source message. Each node uses a separate decoder that reconstructs the messages from their indices using the decoding function

$$\begin{aligned} h_i :&\{1, 2, \ldots, 2^{nR_0}\} \times \cdots \times \{1, 2, \ldots, 2^{nR_{i-1}}\} \times \\ &\mathcal{X}_i^n \times \{1, 2, \ldots, 2^{nR_{i+1}}\} \times \cdots \times \{1, 2, \ldots, 2^{nR_{N-1}}\} \\ &\longrightarrow \mathcal{X}_0^n \times \cdots \times \mathcal{X}_{i-1}^n \times \mathcal{X}_{i+1}^n \times \cdots \times \mathcal{X}_{N-1}^n. \end{aligned}$$

The maximum probability of error conditioned on a block length is given by

$$\begin{aligned} P_e^{(n)} = \max_{0 \le i \le N-1} Pr\Big(& h_i\big(f_0(\mathbf{X}_0^n), \ldots, f_{i-1}(\mathbf{X}_{i-1}^n), \\ & \mathbf{X}_i^n, f_{i+1}(\mathbf{X}_{i+1}^n), \ldots, f_{N-1}(\mathbf{X}_{N-1}^n)\big) \\ & \neq (\mathbf{X}_0^n, \ldots, \mathbf{X}_{i-1}^n, \mathbf{X}_{i+1}^n, \ldots, \mathbf{X}_{N-1}^n) \Big). \end{aligned}$$

We say that a rate-tuple $(R_0, R_1, \ldots, R_{N-1})$ is achievable if there exists a sequence of $(2^{nR_0}, 2^{nR_1}, \ldots, 2^{nR_{N-1}}, n)$ codes such that $P_e^{(n)} \to 0$ as $n \to \infty$. We define $\mathcal{R}_{3rd-p}$ to be the set of achievable rate-tuples, and the achievable rate region to be the closure of this set. For rates in this region, we are guaranteed that there exists a sequence of codes (as $n \to \infty$) such that all nodes learn $\mathbf{X}_0, \ldots, \mathbf{X}_{N-1}$.

Note that this is a different rate-region than the classic many-source Slepian-Wolf region [1], [2], [4], [6]. In the Slepian-Wolf set-up, a user i would be fixed as a receiver. This user has perfect knowledge of $\mathbf{X}_i$. For a subset $\mathcal{S} \subset \{0, 1, \ldots, N-1\}$, let

$$\begin{aligned} \mathcal{R}_i(\mathcal{S}) = \Big\{ & (R_0, R_1, \ldots, R_{N-1}) : \\ & R(\mathcal{S}) \ge H\left(\mathbf{X}_{\mathcal{S}} \mid \mathbf{X}_{\mathcal{S}^c}, \mathbf{X}_i\right) \Big\} \end{aligned}$$

where $H(\cdot \mid \cdot)$ is conditional entropy,

$$R(\mathcal{S}) = \sum_{j \in \mathcal{S}} R_j,$$

and

$$\mathbf{X}_{\mathcal{S}} = \{\mathbf{X}_j \mid j \in \mathcal{S}\}.$$

The rate-region for the Slepian-Wolf problem is then specified as

$$\mathcal{R}_{i,SW} = \bigcap_{\mathcal{S} \subseteq \mathcal{A}_i} \mathcal{R}_i(\mathcal{S}) \tag{1}$$

with $\mathcal{A}_i = \{0, 1, \ldots, i-1, i+1, \ldots, N-1\}$.

The achievable rate region for our third-party information exchange network is described in the following theorem.

Theorem 1: **Third-Party Slepian-Wolf.** In the third-party problem with $(\mathbf{X}_0, \mathbf{X}_1, \ldots, \mathbf{X}_{N-1})$ drawn from distribution $p(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1})$, the achievable rate region is given by the closure of the set

$$\mathcal{R}_{3rd-p} = \bigcap_{i=0}^{N-1} \mathcal{R}_{i,SW}. \tag{2}$$

Proof: To prove achievability we show that codes exist satisfying all of the Slepian-Wolf requirements that yield $P_e^{(n)} \to 0$ as $n \to \infty$. Let user j partition the set $\mathcal{X}_j^n$ into 2^{nR_j} bins. Each user then independently assigns each $\mathbf{x}_j \in \mathcal{X}_j^n$ (note that we abuse notation and do not add blocklength dependence on the source vectors in $\mathcal{X}_j^n$ to avoid confusion) to one of the 2^{nR_j} bins using a uniform distribution on $\{1, 2, \ldots, 2^{nR_j}\}$. The encoding function f_j sends the label of the bin to which $\mathbf{X}_j$ belongs. Let $J_j = f_j(\mathbf{X}_j)$ and $A_\epsilon^{(n)}$ denote the set of jointly typical

N-tuple source sequences. The decoder for user i decodes to $(\hat{\mathbf{x}}_0, \ldots, \hat{\mathbf{x}}_{i-1}, \hat{\mathbf{x}}_{i+1}, \ldots, \hat{\mathbf{x}}_{N-1})$ if there is one and only one N-tuple $(\hat{\mathbf{x}}_0, \ldots, \hat{\mathbf{x}}_{i-1}, \mathbf{x}_i, \hat{\mathbf{x}}_{i+1}, \ldots, \hat{\mathbf{x}}_{N-1}) \in A_\epsilon^{(n)}$ with $f_j(\hat{\mathbf{x}}_j) = J_j$ for $j \in \{0, \ldots, (i-1), (i+1), \ldots, N-1\}$.

Let $\mathcal{P}$ denote the power set of $\{0, 1, \ldots, N-1\}$ with the set $\{0, 1, \ldots, N-1\}$ removed and ϕ denote the null set. For $\mathcal{S} \in \mathcal{P} - \phi$, define

$$\begin{aligned} E_{\mathcal{S}} = &\{(\mathbf{X}_0, \ldots, \mathbf{X}_{N-1}) : \forall j \in \mathcal{S},\ \exists \mathbf{x}'_j \neq \mathbf{X}_j \text{ s.t.} \\ &f_j(\mathbf{x}'_j) = f_j(\mathbf{X}_j) \text{ and } (\tilde{\mathbf{X}}_0, \ldots, \tilde{\mathbf{X}}_{N-1}) \in A_\epsilon^{(n)}\}, \end{aligned}$$

with

$$\tilde{\mathbf{X}}_j = \begin{cases} \mathbf{x}'_j & \text{if } j \in \mathcal{S}, \\ \mathbf{X}_j & \text{if } j \notin \mathcal{S}. \end{cases}, \tag{3}$$

and

$$E_\phi = \{(\mathbf{X}_0, \ldots, \mathbf{X}_{N-1}) \notin A_\epsilon^{(n)}\}.$$

From these definitions,

$$P_e^{(n)} \leq \sum_{\mathcal{S} \in \mathcal{P}} Pr(E_{\mathcal{S}}).$$

It can easily be shown that $Pr(E_{\mathcal{S}}) \leq 2^{-nR(\mathcal{S})} 2^{n(H(X_{\mathcal{S}} | X_{\mathcal{S}^c}) + \epsilon)}$ for $\mathcal{S} \neq \phi$ and $Pr(E_\phi) \leq \epsilon$. Therefore, $P_e^{(n)}$ goes to 0 as n increases when $R(\mathcal{S}) \geq H(X_{\mathcal{S}} \mid X_{\mathcal{S}^c})$ for all $\mathcal{S} \in \mathcal{A}$.

To show the converse, we use proof techniques similar to those used to prove the Slepian-Wolf converse. Let $J_i = f_i(\mathbf{X}_i^n)$. For any set $\mathcal{S} \in \mathcal{P}$, Fano's Inequality tells us

$$H(\mathbf{X}_{\mathcal{S}}^n \mid J(\mathcal{S}), \mathbf{X}_{\mathcal{S}^c}^n) \leq P_e^{(n)} n R(\mathcal{S}) + 1 \leq n\epsilon_n$$

where

$$\mathbf{X}_{\mathcal{S}}^n = \{\mathbf{X}_j^n \mid j \in \mathcal{S}\}$$
$$J(\mathcal{S}) = \{J_i \mid i \in \mathcal{S}\}$$

and $\epsilon_n \to 0$ as $n \to \infty$.

Therefore,

$$\begin{aligned} nR(\mathcal{S}) &\geq H(J(\mathcal{S})) \\ &\geq I(\mathbf{X}_{\mathcal{S}}^n; J(\mathcal{S}) \mid \mathbf{X}_{\mathcal{S}^c}^n) \\ &= H(\mathbf{X}_{\mathcal{S}}^n \mid \mathbf{X}_{\mathcal{S}^c}^n) - H(\mathbf{X}_{\mathcal{S}}^n \mid J(\mathcal{S}), \mathbf{X}_{\mathcal{S}^c}^n) \\ &\geq nH(\mathbf{X}_{\mathcal{S}} \mid \mathbf{X}_{\mathcal{S}^c}) - n\epsilon_n. \end{aligned} \tag{4}$$

Dividing by n and letting $n \to \infty$ gives that

$$R(\mathcal{S}) \geq H(\mathbf{X}_{\mathcal{S}} \mid \mathbf{X}_{\mathcal{S}^c})$$

for all $\mathcal{S} \in \mathcal{P}$.

It then easily follows that.

$$\mathcal{R}_{3rd-p} = \bigcap_{i=0}^{N-1} \mathcal{R}_{i,SW}.$$

■

III. Exchanging Link Connectivity Information in a Network

We apply the third-party theorem to the problem outlined in Section I of sharing local connectivity information. Surprisingly, we show that the simple coding technique given in Section I is nearly optimal.

A. Problem Set-up and Learning Time

To generalize the example in Section I, consider an N-node network. There are a total of $\binom{N}{2}$ possible links in the network. We assume that through local training signals, each node knows the $N-1$ bits representing the presence or absence of a good connection (exceeding some threshold) between it and the other nodes. Therefore, there are a total of $\binom{N}{2}$ bits that must be learned at every node, of which each node knows some subset of $N-1$ bits (as side information).

We assume as in the Section I example that a single control channel exists that allows each node to convey one bit per channel-use to every other network node. The channel can be used only by one node at a time. Our goal is to minimize the number of channel-uses required for every node to obtain knowledge of all $\binom{N}{2}$ link connectivity bits. We refer to this number of channel-uses as the *learning time* of the network. Because of the control channel access structure, the learning time T is given by

$$T(R_0, R_1, \ldots, R_{N-1}) = \sum_{j=0}^{N-1} R_j. \tag{5}$$

The third-party information vectors are represented as bits of information $G_{i,j}$ about the link between nodes i and j for all $i \neq j$. By symmetry, $G_{i,j} = G_{j,i}$. We assume that $G_{i,j}$ takes values in $\{0, 1\}$ with equal probability. With this framework,

$$\mathbf{X}_i = \begin{bmatrix} G_{i,\text{mod}(i+1,N)} & \cdots & G_{i,\text{mod}(i+N-1,N)} \end{bmatrix}.$$

We have that

$$H(\mathbf{X}_{\mathcal{S}} \mid \mathbf{X}_{\mathcal{S}^c}) = \binom{N}{2} - \alpha(N-1) + \binom{\alpha}{2} \tag{6}$$

where

$$\alpha = card(\mathcal{S}^c) = N - card(\mathcal{S}).$$

The result in (6) follows because there are a total of $\binom{N}{2}$ bits of information in the entire network and $\alpha(N-1) - \binom{\alpha}{2}$ of these bits are known through training to the nodes in $\mathcal{S}^c$.

Define T_{min} to be the minimum over all rate-tuples $(R_0, \ldots, R_{N-1})$ of the achievable learning time $T(R_0, \ldots, R_{N-1})$ defined in (5). Using Theorem 1, we can find T_{min}.

Theorem 2: The minimum achievable learning time T_{min} in an N node orthogonal network is

$$T_{min} = \frac{N^2}{2} - N.$$

Proof: By definition,

$$T_{min} = \min_{(R_0, R_1, \ldots, R_{N-1}) \in \mathcal{R}_{3rd-p}} T(R_0, R_1, \ldots, R_{N-1}).$$

We can rewrite $T(R_0, R_1, \ldots, R_{N-1})$ as

$$\begin{aligned} &T(R_0, R_1, \ldots, R_{N-1}) \\ &= \frac{1}{N-1} \sum_{i=0}^{N-1} [R_0 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_{N-1}] \\ &= \frac{1}{N-1} \sum_{i=0}^{N-1} R\big(\{0, \ldots, (i-1), (i+1), \ldots, N-1\}\big). \end{aligned}$$

However, Theorem 1 gives the lower-bound

$$R\big(\{0, \ldots, (i-1), (i+1), \ldots, N-1\}\big) \geq H\left(\mathbf{X}_{\{0,\ldots,(i-1),(i+1),\ldots,N-1\}} \mid \mathbf{X}_i\right).$$

Using this and (6), we can therefore obtain that

$$T_{min} = \frac{1}{N-1} \sum_{i=0}^{N-1} \left(\binom{N}{2} - (N-1) \right) = \frac{N^2}{2} - N.$$

■

Compare this minimum sharing time with the naive retransmission scheme where each node transmits $N-1$ bits yielding a learning time of $N(N-1) = N^2 - N$ channel-uses. Thus, a savings of $N^2/2$ channel-uses is possible by using a better code.

B. Information Exchanging Code

We demonstrate a code that gives a near optimal learning time and has a block length of $n = 1$. It provides a learning time of $\lceil T_{min} \rceil$. Also the decoding complexity grows as $\mathcal{O}(N^3)$. This presents a significant improvement in the complexity of decoding.

To present our code's encoding/decoding, we assume that i) the nodes are numbered from 0 to $N-1$, ii) the control channel time slots are indexed as $1, 2, \ldots$, iii) some form of training has already been done to given node i knowledge of its $N-1$ link bits, and iv) the number of nodes is even. For the case of an even number of nodes, T_{min} is exactly achievable. We can extend this code to an odd number of nodes, but we will omit this for conciseness.

The encoding procedure is summarized below.

Encoding: *At transmission* t $(t = 1, 2, \ldots, \frac{N^2}{2} - N)$, *node* $i = mod(t-1, N)$ *transmits*

$$C[t] = G_{i,mod(i+1,N)} \oplus G_{i,mod\left(i+1+\lceil \frac{t}{N} \rceil, N\right)}$$

where $\oplus$ *is binary addition.*

In this code, each node only transmits the exclusive-or of two bits at each of its transmission instants. One of the two bits is kept constant for all transmissions. This gives a hint to the decoding operation: if $G_{i,\text{mod}(i+1,N)}$ can be determined all bits transmitted by node i can be uniquely recovered.

The encoding operation for each node can also be represented as a vector indexed in time. The vector that is transmitted by the ith source, which we denote as $\mathbf{C}_i$, is given by

$$\mathbf{C}_i = \left[C[i+1]\ C[i+1+N]\ \cdots\ C\left[i+1+\frac{N^2}{2} - 2N\right] \right].$$

This vector can also be written in terms of the channel elements as

$$\mathbf{C}_i = \Big[G_{i,\text{mod}(i+1,N)} \oplus G_{i,\text{mod}(i+2,N)}\ \cdots\ G_{i,\text{mod}(i+1,N)} \oplus G_{i,\text{mod}(i+\frac{N}{2},N)} \Big].$$

Transmissions end when all the sources have transmitted their vectors $\mathbf{C}_i$. At the end of all transmissions, an arbitrary node i has knowledge of $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_{N-1}$ in addition to its own bits.

One important point to make about this code is that every link bit is included in at least one $C[t]$. To show this, let $\mathcal{G}_i$ denote the set $\{G_{i,j}\}_{j \neq i}$ transmitted in linear combinations by node i or equivalently $\mathcal{G}_i = \left\{ G_{i,\text{mod}(i+k,N)} \mid k = 1, 2, \ldots, \frac{N}{2} \right\}$. Since

$$\max_{0 \leq i < j \leq (N-1)} \min\big(\text{mod}(i-j, N), \text{mod}(j-i, N)\big) = \frac{N}{2}$$

each $G_{i,j}$ is conveyed in a linear combination from at least one node. Therefore, all link bits are included in $\bigcup_{i=0}^{N-1} \mathcal{G}_i$.

Decoding: *To decode, node* i *uses its knowledge of i)* $C[0], C[1], \ldots, C\left[\frac{N^2}{2} - N\right]$ *and ii)* $G_{i,0}, \ldots, G_{i,i-1}, G_{i,i+1}, \ldots, G_{i,N-1}$ *to solve the resulting set of* $\frac{N^2}{2} - N$ *linear equations.*

A specific decoding algorithm is given in the next subsection. The encoding gives a property that we call the *Decoding Condition*.

Decoding Condition: A sufficient condition for a node to decode all elements in $\mathcal{G}_i$ *given* $\mathbf{C}_i$ *is knowledge of at least one* $G \in \mathcal{G}_i$.

This follows because knowledge of any $G \in \mathcal{G}_i$ allows us to determine $G_{i,\text{mod}(i+1,N)}$, and all elements of $\mathcal{G}_i$ are linear combinations with $G_{i,\text{mod}(i+1,N)}$. We can now prove that all link bits can be decoded.

Theorem 3: The proposed third-party code can be decoded so that every node knows $\bigcup_{j=0}^{N-1} \mathcal{G}_j$.

Proof: We have already shown the theorem is true for $N = 3$. Therefore, we assume $N \geq 4$ and N is even. We prove this theorem by showing that any arbitrary node i_0 (where $0 \leq i_0 \leq N-1$) can decode $\bigcup_{j=0}^{N-1} \mathcal{G}_j$.

Let

$$\mathcal{M}_{i_0} = \left\{ \text{mod}(i_0 - z, N) \mid z = 0, 1, 2, \ldots, \frac{N}{2} \right\}.$$

Because of the structure of the transmission strategy and the assumption that $N \geq 4$, every node $j \in \mathcal{M}_{i_0}$ transmits a linear combination that involves $G_{i_0,j}$ (i.e., a piece of information that node i_0 already knows). Since each node $j \in \mathcal{M}_{i_0}$ transmits a codeword involving $G_{j,\text{mod}(j+1,N)}$ during each transmission, node i_0 can determine all elements in $\mathcal{G}_j$ by the *Decoding Condition*.

We have now proven that an arbitrary node i_0 can determine all pieces of information in the set $\bigcup_{j\in\mathcal{M}_{i_o}}\mathcal{G}_j$. To show that a node i_0 can determine $\bigcup_{j=0}^{N-1}\mathcal{G}_j$, the *Decoding Condition* tells us that we only need that $\forall i\in\{0,1,\ldots,N-1\},\ \exists G\in\mathcal{G}_i$ such that $G\in\bigcup_{j\in\mathcal{M}_{i_o}}\mathcal{G}_j$.

Let $i\notin\mathcal{M}_{i_0}$. This means that

$$\text{mod}(i_0-i,N)>\frac{N}{2}.$$

Since each node transmits $\frac{N}{2}-1$ times, the last transmission of node i involves $G_{i,\text{mod}(i+\frac{N}{2},N)}$. Let $i_1=\text{mod}(i+\frac{N}{2},N)$. We must have that

$$\text{mod}(i_0-i_1,N)=\text{mod}\left(i_0-i-\frac{N}{2},N\right)\leq\frac{N}{2}-1,$$

meaning $i_1\in\mathcal{M}_{i_0}$.

As well, node i transmits $G_{i,\text{mod}(i+\frac{N}{2},N)}$ and

$$G_{i,\text{mod}(i+\frac{N}{2},N)}=G_{\text{mod}(i+\frac{N}{2},N),i}=G_{i_1,\text{mod}(i_1+\frac{N}{2},N)}.$$

Node i_1 transmits $G_{i_1,\text{mod}(i_1+\frac{N}{2},N)}$ in its last transmission, meaning

$$G_{i,\text{mod}(i+\frac{N}{2},N)}\in\bigcup_{j\in\mathcal{M}_{i_0}}\mathcal{G}_j.$$

By the *Decoding Condition*, this means node i_0 can determine $\mathcal{G}_i$.

We have now proven that the third-party information transmitted by an arbitrary node i (i.e., $\mathcal{G}_i$) can be determined at an arbitrary node i_0 for any value of N. This means node i_0 can determine $\bigcup_{j=0}^{N-1}\mathcal{G}_j$. Since this union is exhaustive, this completes the proof. ∎

C. Decoding Algorithm

We have shown that it is possible for each node to decode all the link connection bits. We now demonstrate the decoding procedure adopted by an arbitrary receiver for even N; the procedure for odd N follows along similar lines. Let us pick some arbitrary receiver node j. The receiver node begins decoding once all the codeword vectors have been transmitted. At the end of this time it has $C[0],C[1],\ldots,C\left[\frac{N^2}{2}-N\right]$ and $\mathbf{X}_j$ (and by default $\mathcal{G}_j$).

The jth decoder attempts to find $G_{i,j},\ \forall i\neq j$, and $0\leq i\leq N-1$. The decoding procedure for every receiver node has two phases. Let $C(i)_{\text{mod}(j-i,N)}$ denote the ith element of $\mathbf{C}_{\text{mod}(j-i,N)}$. Additionally, let

$$\text{vec}(\mathcal{G}_i)=\left[G_{i,\text{mod}(i+1,N)}\cdots G_{i,\text{mod}(i+N/2,N)}\right].$$

Phase I

Node j can recover all link connection bits in $\mathcal{G}_{\text{mod}(j-i,N)}$ for all $1\leq i\leq\frac{N}{2}$ by computing

$$\text{vec}\left(\mathcal{G}_{\text{mod}(j-i,N)}\right)=\left[0\ \mathbf{C}_{\text{mod}(j-i,N)}\right]\oplus\mathbf{a}_{\text{mod}(j-i,N)}$$

where

$$\mathbf{a}_{\text{mod}(j-i,N)}=\left(C(\max(i-1,1))_{\text{mod}(j-i,N)}\oplus G_{j,\text{mod}(j-i,N)}\right)\mathbf{1}_{N/2}$$

with $\mathbf{1}_{N/2}$ denoting an $N/2$-dimensional vector of ones. This follows because

$$C(\max(i-1,1))_{\text{mod}(j-i,N)}\oplus G_{j,\text{mod}(j-i,N)}=G_{\text{mod}(j-i,N),\text{mod}(j-i+1,N)}.$$

Additionally, it can be shown that at the end of this phase node j knows $G_{\text{mod}(j+i-\frac{N}{2},N),\text{mod}(j+i,N)}$ for any $1\leq i\leq\frac{N}{2}$. This fact implies that once node j has $\mathcal{G}_{\text{mod}(j-i,N)}$ for $1\leq i\leq\frac{N}{2}$, the second phase allows node j to find $\mathcal{G}_{\text{mod}(j+i,N)}$ for $1\leq i\leq\frac{N}{2}-1$, which means node j has all the information about the network.

Phase II

Node j can recover all link connection bits in $\mathcal{G}_{\text{mod}(j+i,N)}$ for all $1\leq i\leq\frac{N}{2}-1$ by computing

$$\text{vec}\left(\mathcal{G}_{\text{mod}(j+i,N)}\right)=\left[0\ \mathbf{C}_{\text{mod}(j+i,N)}\right]\oplus\mathbf{b}_{\text{mod}(j+i,N)}$$

where

$$\mathbf{b}_{\text{mod}(j+i,N)}=\left(C\left(\frac{N}{2}-1\right)_{\text{mod}(j+i,N)}\oplus G_{\text{mod}(j+i-\frac{N}{2},N),\text{mod}(j+i,N)}\right)\mathbf{1}_{N/2}.$$

This follows because

$$C\left(\frac{N}{2}-1\right)_{\text{mod}(j+i,N)}\oplus G_{\text{mod}(j+i-\frac{N}{2},N),\text{mod}(j+i,N)}=G_{\text{mod}(j+i,N),\text{mod}(j+i+1,N)}.$$

At the end of this phase the receiver node has $\mathcal{G}_{\text{mod}(j+i,N)}$ for $1\leq i\leq\frac{N}{2}-1$. This along with $\mathcal{G}_{\text{mod}(j-i,N)}$ for $1\leq i\leq\frac{N}{2}$ provides the jth receiver node with have all the information about the network since,

$$\bigcup_{j=0}^{N-1}\mathcal{G}_j=\bigcup_{i=0}^{N-1}\mathbf{X}_i.$$

D. Example

As an example of this code consider a four-node network, where the transmission strategy for this network is shown in Table I. Each row of the table represents a unit of time where the value in parentheses shows what is transmitted by the corresponding node (only one node can transmit at any time on the control channel). For example, at time instant 1, node 0 transmits $(G_{0,1}\oplus G_{0,2})$, at time instant 2 node 1 transmits $(G_{1,2}\oplus G_{1,3})$. The values not in parentheses are the bits that are learned by the nodes that are receiving the transmitted bit. The total number of transmissions required is $T_{min}=4$.

IV. Conclusions

We provided a model for sharing and exchanging third-party information in a network. We assumed that each node in the network has local information and that every node in the network would like to learn the local information through a common channel. We assumed the local information was correlated between nodes and showed how this correlation could reduce the burden of the information exchange.

TABLE I. Transmission strategy for a four-node network. Before transmission begins, we assume that node i has knowledge of $G_{i,j}$ for $i \neq j$. Each row of the table represents a unit of time and the value in parentheses shows what is transmitted by the corresponding node. The values not in parentheses show what is learned by the remaining nodes. At the end of the four transmissions, the nodes all know all of the $G_{i,j}$.

Node			
0	1	2	3
$(G_{0,1} \oplus G_{0,2})$	$G_{0,2}$	$G_{0,1}$	$G_{0,1} \oplus G_{0,2}$
$G_{1,2} \oplus G_{1,3}$	$(G_{1,2} \oplus G_{1,3})$	$G_{1,3}$	$G_{1,2}$
$G_{2,3}$	$G_{2,3}$	$(G_{0,2} \oplus G_{2,3})$	$G_{0,1}$, $G_{0,2}$
$G_{1,2}$, $G_{1,3}$	$G_{0,3}$	$G_{0,3}$	$(G_{0,3} \oplus G_{1,3})$

We determined the rate region for this problem assuming that a common control channel that can carry one bit per channel-use was available to all of the nodes. We also explored the specialized application of sharing connection-information in a network. In this application, every node had $N-1$ bits of information and the total amount of information is $\binom{N}{2}$ bits. We provided an encoding and decoding approach that was nearly optimal.

We believe that there is considerable room to design codes for correlation structures that we have not yet examined. It is also not clear how to effectively exchange information when the network does not have access to a reliable common channel. Perhaps multi-hop coding approaches might then be useful.

REFERENCES

[1] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, New York, 1992.

[2] T.M. Cover. A proof of the data compression theorem of Slepian and Wolf for ergodic sources. *IEEE Trans. Info. Th.*, 21:226–228, March 1975.

[3] S. S. Pradhan and K. Ramchandran. Distributed source coding using syndromes (DISCUS): Design and construction. *IEEE Trans. Info. Th.*, 49(3):626–643, March 2003.

[4] D. Slepian and J. K. Wolf. Noiseless coding of correlated information sources. *IEEE Trans. Info. Th.*, 19(4):471–480, July 1973.

[5] V. Stankovic, A. D. Liveris, Z. Xiong, and C. N. Georghiades. On code design for the Slepian-Wolf problem and lossless multiterminal networks. *IEEE Trans. Info. Th.*, 52(4):1495–1507, April 2006.

[6] A. Wyner. Recent results in the Shannon theory. *IEEE Trans. Info. Th.*, 20(1):2–10, Jan. 1974.