ISIT'2013 1569716831

Linear Network Coding Capacity for Broadcast Erasure Channels With Feedback, Receiver Coordination, and Arbitrary Security Requirement

Chih-Chun Wang, Email: chihw@purdue.edu
Center for Wireless Systems and Applications
School of Electrical and Computer Engineering, Purdue University, USA

***Abstract*—This work considers a commonly encountered wireless transmission scenario. The base station s would like to send two independent packet streams to clients d_1 and d_2, respectively. For each time slot, only one of the three nodes $\{s, d_1, d_2\}$ can transmit a packet and the packet will be heard by a random subset of the other two nodes. We are interested in the corresponding capacity region (R_1^*, R_2^*). Such a setting can also be viewed as allowing *receiver coordination* for the s-to-$\{d_1, d_2\}$ broadcast erasure channel with a critical feature that any coordination/transmission between d_1 and d_2 also takes away the precious time resources from s.**

With the exclusive focus on linear network coding (LNC) with causal packet acknowledgement feedback, this work characterizes the exact LNC capacity region with arbitrary security requirement, i.e, the system designer can decide for each d_i, respectively, whether the corresponding (s, d_i)-flow needs to be secure or not. The results show that for any channel parameters and any security requirement, the LNC capacity can always be achieved either by the XOR-in-the-air LNC scheme, or by random LNC, or by time-sharing between the two.

I. Introduction

The seminal paper [1] has proven that under a theoretic model, linear network coding (LNC) can achieve the network capacity of the single multicast traffic, previously not attainable by any non-coding solutions. On the system side, recent testbed implementation of wireless LNC in a local neighborhood [2]–[5] has also demonstrated substantial throughput gain over the traditional 802.11 protocols. Despite the above promising results, there are several issues that hamper the transition of LNC from a theoretical technique to a full-fledged practical wireless networking solution.

Issue 1: Many theoretic results consider only one multicast flow in the network, while in practice that there are often multiple coexisting unicast flows. Issue 2: a widely used channel model is the point-to-point noiseless channel, while a more realistic/practical wireless setting is the broadcast packet erasure channel (PEC) for which a packet may be heard simultaneously by multiple nodes but sometimes may also get lost (erased). Issue 3: Causal feedback is often not considered in the theory side since it further complicates the analysis. For the system side, causal packet ACKnowledgement (ACK) has always been one of the most basic mechanisms of communication networks. In fact, all the wireless LNC testbed implementations [2]–[5] are based on ingenious use of ACK to capture the diversity of the wireless channels.

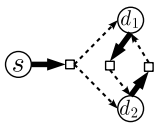
There are many works that address these issues. E.g., [6] characterizes the single-multicast capacity of erasure networks with or without ACK, which effectively solves issues 2 and 3. The first capacity result that takes into account all three issues is [7], which characterizes the broadcast PEC capacity region with ACK. Some subsequent results consider the settings of $K > 2$ receivers [8], [9], degraded messages [10], concurrently secure capacity [11], multi-input broadcast PECs [12], and the generalizations to the XOR-in-the-air principle [13], line networks [14], and the symmetric proximity networks [15].

Along a similar line of the above results, this work considers the following new setting. Source s would like to send two independent packet streams to destinations d_1 and d_2, respectively. For each time slot, only one of the three nodes $\{s, d_1, d_2\}$ can transmit a packet and the packet will be heard by a random subset of the other two nodes, which is modeled by a broadcast PEC. Such a setting can also be viewed as allowing *receiver coordination* for the s-to-$\{d_1, d_2\}$ broadcast PEC with a critical feature that any coordination/transmission between d_1 and d_2 also takes away the precious time resources from s. This setting closely models the scenario in which two Wi-Fi clients are downloading different files from a common Wi-Fi router. The clients can communicate with each other if desired, but any client-to-client communication will disrupt the router-to-client communication due to the half-duplex and the Carrier-Sensing Multiple Access (CSMA) constraints. The question to be answered in this work is *what is the optimal way of exploiting the ability of client-to-client Wi-Fi communications.*

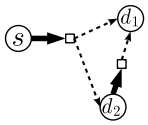
With the exclusive focus on linear network coding (LNC) with causal ACK, this work characterizes the exact LNC capacity region with arbitrary security requirement, i.e, the system designer can decide for each d_i, respectively, whether the corresponding (s, d_i)-flow needs to be secure or not. Our main results can be summarized as follows. For any arbitrary broadcast PEC parameters and arbitrary security requirement, the LNC capacity can be achieved either by the XOR-in-the-air scheme [7], [11], or by random LNC (RLNC) [6], or by time-sharing between the two.

II. Problem Formulation

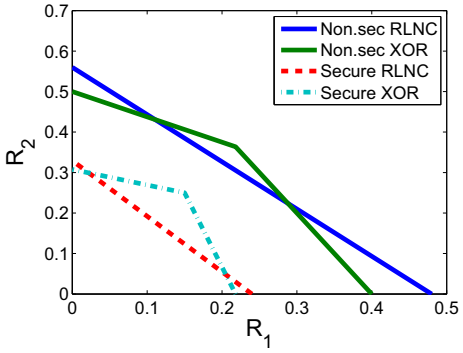
Consider a network of 3 nodes s, d_1, and d_2, see Fig. 1(a), and assume slotted transmission. Within a total time budget



(a) This work.



(b) Erasure relay channel.



(c) Relative positions of the existing results with $(p_1, p_2, p_{1\vee 2}, p_{1\to 2}, p_{2\to 1}) = (0.4, 0.5, 0.8, 0.7, 0.6)$.

Fig. 1. Erasure network models and illustration of the existing capacity results.

of n time slots, s would like to send $n \cdot R_i$ packets $\mathbf{W}_i \triangleq (W_{i,1}, \cdots, W_{i,nR_i})$ to d_i for $i \in \{1,2\}$. Each packet $W_{i,l}$, $l = 1, \cdots, nR_i$, is chosen independently and uniformly randomly from a finite field $\mathsf{GF}(q)$.

For any time slot $t \in [n] \triangleq \{1, \cdots, n\}$, consider a random 4-dimensional *channel state information (CSI) vector*:

$$\mathbf{Z}(t) = (Z_{s\to d_1}(t), Z_{s\to d_2}(t), Z_{d_1\to d_2}(t), Z_{d_2\to d_1}(t)) \in \{*, 1\}^4$$

where "$*$" and "1" represent erasure and successful reception, respectively. That is, $Z_{s\to d_i}(t) = 1$ means that d_i will receive $Y_{s\to d_i}(t) = X_s(t)$, where $X_s(t) \in \mathsf{GF}(q)$ is the packet sent by s at time t. The other case $Z_{s\to d_i}(t) = *$ means that d_i will receive $Y_{s\to d_i}(t) = *$, an erasure. Since we allow receiver coordination, we use $Z_{d_i\to d_j}(t)$ to denote whether the packet $X_{d_i}(t) \in \mathsf{GF}(q)$ sent by d_i can be heard by d_j. For simplicity, for any distinct nodes $u \in \{s, d_1, d_2\}$ and[1] $v \in \{d_1, d_2\}$, we use $Y_{u\to v}(t) = X_u(t) \circ Z_{u\to v}(t)$ as shorthand. We also assume $\mathbf{Z}(t)$ being independent of $\mathbf{W}_1$ and $\mathbf{W}_2$.

For any time t, we assume that only one of $\{s, d_1, d_2\}$ can transmit. We use $\sigma(t) \in \{s, d_1, d_2\}$ to denote the *scheduling decision* at time t. For convenience, when a node u is not scheduled at time t, we simply set $Y_{u\to v}(t) = *$ for any possible receiver v. As a result, the $\sigma(t)$ can be incorporated into the following expression of $Y_{u\to v}(t)$:

$$Y_{u\to v}(t) = X_u(t) \circ Z_{u\to v}(t) \circ 1_{\{\sigma(t)=u\}}.$$

We assume that the PECs in the network (Fig. 1(a)) are memoryless and stationary. We use $p_i \triangleq \mathsf{Prob}(Z_{s\to d_i}(t) = 1)$ to denote the probability that $X_s(t)$ is heard by d_i and use $p_{1\vee 2} \triangleq \mathsf{Prob}(\exists i \in \{1,2\}, Z_{s\to d_i}(t) = 1)$ to denote the probability that $X_s(t)$ is heard by at least one of $\{d_1, d_2\}$. If the broadcast PEC is *spatially independent* (see [9] for discussion), then $p_{1\vee 2} = 1 - (1-p_1)(1-p_2)$. Throughout this paper, we do not assume spatial independence. We only require "$\max(p_1, p_2) \le p_{1\vee 2} \le p_1 + p_2$" for consistence. For the d_i-to-d_j channel, we define $p_{i\to j} \triangleq \mathsf{Prob}(Z_{d_i\to d_j} = 1)$. We use brackets $[\cdot]_1^t$ to denote the collection from time 1 to t. For example, $[\mathbf{Z}, Y_{s\to d_2}]_1^t \triangleq \{\mathbf{Z}(\tau), Y_{s\to d_2}(\tau) : \forall \tau \in [1,t]\}$.

Given the traffic load (R_1, R_2), a network code is defined by n scheduling decision functions

$$\forall t \in [n],\ \sigma(t) = f_{\sigma,t}([\mathbf{Z}]_1^{t-1}), \tag{1}$$

$3n$ encoding functions at s, d_1, and d_2, respectively: For all $t \in [n]$, $i \in \{1,2\}$, and $j \in \{1,2\}\backslash i$,

$$X_s(t) = f_{s,t}(\sigma(t), \mathbf{W}_1, \mathbf{W}_2, [\mathbf{Z}]_1^{t-1}) \tag{2}$$

$$X_{d_i}(t) = f_{d_i,t}(\sigma(t), [Y_{s\to d_i}, Y_{d_j\to d_i}, \mathbf{Z}]_1^{t-1}), \tag{3}$$

and 2 decoding functions at d_1 and d_2, respectively:

$$\hat{\mathbf{W}}_i = f_{d_i}([\sigma, Y_{s\to d_i}, Y_{d_j\to d_i}, \mathbf{Z}]_1^n) \text{ for all distinct } i, j. \tag{4}$$

Eq. (1) implies that the scheduling decision at time t is based on the network-wide CSI in time 1 to $(t-1)$. A network code is linear if (2) and (3) can be written as

$$X_s(t) = (\mathbf{W}_1, \mathbf{W}_2, \mathbf{V}) \cdot \mathbf{c}_{s,t}^{\mathrm{T}}$$
$$\text{and } X_{d_i}(t) = (\mathbf{W}_1, \mathbf{W}_2, \mathbf{V}) \cdot \mathbf{c}_{d_i,t}^{\mathrm{T}},$$

where $\mathbf{V}$ is an n_{seed}-dimensional row vector in $\mathsf{GF}(q)$ of which each coordinate is a "seed" independently and uniformly randomly generated at source s that is unknown to d_1 and d_2 unless being communicated. $\mathbf{c}_{s,t}$ and $\mathbf{c}_{d_i,t}$ are $(nR_1 + nR_2 + n_{\text{seed}})$-dimensional row vectors in $\mathsf{GF}(q)$, also termed the global coding vectors (GCVs), and $\mathbf{c}_{s,t}^{\mathrm{T}}$ and $\mathbf{c}_{d_i,t}^{\mathrm{T}}$ are the corresponding transpose. For the input/output consistence, we require $\mathbf{c}_{d_i,t}$ being in the linear span of the GCVs of the received packets $[Y_{s\to d_i}, Y_{d_j\to d_i}]_1^{t-1}$. The LNC designer can choose the GCVs $\mathbf{c}_{s,t}$ and $\mathbf{c}_{d_i,t}$ based on the current scheduling $\sigma(t)$ and the past CSI $[\mathbf{Z}]_1^{t-1}$. The introduction of the random seed packets in $\mathbf{V}$ is to encompass the design of any *one-time pad encryption* under the general umbrella of LNC designs. The value of n_{seed} can be chosen arbitrarily by the LNC designer. Decoding of LNC (cf. (4)) can be easily implemented [5] by Gaussian elimination.

A *security requirement* is denoted by $\mathsf{sr} \in \{0,1\}^2$. For any $\theta_1, \theta_2 \in \{0,1\}$, $\mathsf{sr} = (\theta_1, \theta_2)$ represents the following *information-theoretic security* requirement: "For any i satisfying $\theta_i = 1$, we must have $I(\mathbf{W}_i; [Y_{s\to d_j}, Y_{d_i\to d_j}]) = 0$ where $j \in \{1,2\}\backslash i$ and $I(\cdot;\cdot)$ is the mutual information." Namely, the (s, d_i)-flow needs to be secure if $\theta_i = 1$. For example, $\mathsf{sr} = (0,1)$ means that only the (s, d_2)-flow needs to be secure while there is no security constraint on the (s, d_1)-flow.

Definition 1: Fix the p_1, p_2, $p_{1\vee 2}$, $p_{1\to 2}$, $p_{2\to 1}$, and sr values. A rate vector (R_1, R_2) is LNC-achievable if for any $\epsilon > 0$, there exists a linear network code with sufficiently large n, n_{seed}, and $\mathsf{GF}(q)$ such that $\max_{\forall i\in\{1,2\}} \mathsf{Prob}(\mathbf{W}_i \neq \hat{\mathbf{W}}_i) < \epsilon$ and the security requirement sr is satisfied. The LNC-capacity region is the closure of all LNC-achievable (R_1, R_2).

III. Degenerate Cases

If we choose $p_{1\to 2} = p_{2\to 1} = 0$, then our setting collapses to [7] when $\mathsf{sr} = (0,0)$ and collpases to [11] when $\mathsf{sr} = (1,1)$.

[1] We implicitly assume that a packet sent by d_i will never arrive at s. The reason is that since source s has all the packets to begin with, even if s receives some packets from d_i, s can simply discard those packets without affecting the overall throughput.

The following is a restatement of the results in [7], [11] for these degenerate cases.

Proposition 1 ([7], [11]): Suppose $p_{1\to 2} = p_{2\to 1} = 0$ (no receiver coordination). The $\mathsf{sr} = (0,0)$ capacity region is the convex hull of $(0,0)$ and the following three rate vectors:

$$(p_1, 0), \quad (0, p_2), \quad \text{and} \quad (R_{1,\text{XOR}}^{\text{non.sec}}, R_{2,\text{XOR}}^{\text{non.sec}}) \triangleq \left(\frac{p_1 p_{1\vee 2}(p_{1\vee 2} - p_2)}{{p_{1\vee 2}}^2 - p_1 p_2}, \frac{p_2 p_{1\vee 2}(p_{1\vee 2} - p_1)}{{p_{1\vee 2}}^2 - p_1 p_2} \right).$$

The $\mathsf{sr} = (1,1)$ capacity region is the convex hull of $(0,0)$ and the following three rate vectors:

$$\left(\frac{p_1(p_{1\vee 2} - p_2)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_2)}, 0 \right),$$
$$\left(0, \frac{p_2(p_{1\vee 2} - p_1)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_1)} \right), \text{ and}$$
$$(R_{1,\text{XOR}}^{\text{secure}}, R_{2,\text{XOR}}^{\text{secure}}) \triangleq \left(\frac{p_1(p_{1\vee 2} - p_2)}{p_{1\vee 2}}, \frac{p_2(p_{1\vee 2} - p_1)}{p_{1\vee 2}} \right).$$

The subscript "XOR" denotes that those rates can be achieved by the XOR-in-the-air principle, which are provably optimal [7], [11] when receiver coordination is prohibited.

The following is a combination of [6] and some new findings on the secure unicast capacity of erasure relay channels.

Proposition 2: The *unicast capacity points* of the $\mathsf{sr} = (0,0)$ capacity region (the farthest points along the x- and y-axes) are $(R_{1,\text{RLNC}}^{\text{non.sec}}, 0)$ and $(0, R_{2,\text{RLNC}}^{\text{non.sec}})$, respectively, where

$$R_{1,\text{RLNC}}^{\text{non.sec}} \triangleq \max\left(p_1, \frac{p_{2\to 1} p_{1\vee 2}}{p_{2\to 1} + p_{1\vee 2} - p_1} \right) \tag{5}$$

$$R_{2,\text{RLNC}}^{\text{non.sec}} \triangleq \max\left(p_2, \frac{p_{1\to 2} p_{1\vee 2}}{p_{1\to 2} + p_{1\vee 2} - p_2} \right). \tag{6}$$

The unicast capacity points of the $\mathsf{sr} = (1,1)$ LNC-capacity region are $(R_{1,\text{RLNC}}^{\text{secure}}, 0)$ and $(0, R_{2,\text{RLNC}}^{\text{secure}})$, respectively, where

$$R_{1,\text{RLNC}}^{\text{secure}} \triangleq \max\left(\frac{p_1(p_{1\vee 2} - p_2)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_2)}, \frac{p_{2\to 1}(p_{1\vee 2} - p_2)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_2 + p_{2\to 1} - p_1)} \right) \tag{7}$$

$$R_{2,\text{RLNC}}^{\text{secure}} \triangleq \max\left(\frac{p_2(p_{1\vee 2} - p_1)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_1)}, \frac{p_{1\to 2}(p_{1\vee 2} - p_1)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_1 + p_{1\to 2} - p_2)} \right). \tag{8}$$

The subscript "RLNC" denotes that the two unicast capacity points can be achieved by RLNC [3], [4], [6]. The proof of this proposition is relegated to Section V.

Fig. 1(c) illustrates the relative positions of the rate vectors in Propositions 1 and 2. The triangular regions correspond to the rates achievable by time-sharing the unicast capacity points described in Proposition 2.

IV. Main Result

Proposition 3: Consider arbitrary p_1, p_2, $p_{1\vee 2}$, $p_{1\to 2}$, and $p_{2\to 1}$ values. We then have

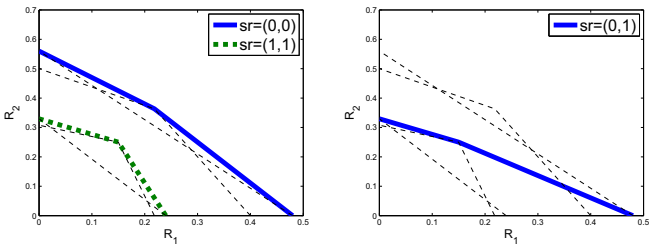


Fig. 2. The LNC-capacity regions for $\mathsf{sr} = (0,0)$, $(1,1)$, and $(0,1)$, respectively, with $(p_1, p_2, p_{1\vee 2}, p_{1\to 2}, p_{2\to 1}) = (0.4, 0.5, 0.8, 0.7, 0.6)$.

- If $\mathsf{sr} = (0,0)$, the LNC-capacity is the convex hull of $(0,0)$ and the following three rate vectors: $(R_{1,\text{XOR}}^{\text{non.sec}}, R_{2,\text{XOR}}^{\text{non.sec}})$, $(R_{1,\text{RLNC}}^{\text{non.sec}}, 0)$, and $(0, R_{2,\text{RLNC}}^{\text{non.sec}})$.
- If $\mathsf{sr} = (0,1)$, the LNC-capacity is the convex hull of $(0,0)$ and the following three rate vectors: $(R_{1,\text{XOR}}^{\text{secure}}, R_{2,\text{XOR}}^{\text{secure}})$, $(R_{1,\text{RLNC}}^{\text{non.sec}}, 0)$, and $(0, R_{2,\text{RLNC}}^{\text{secure}})$.
- If $\mathsf{sr} = (1,1)$, the LNC-capacity is the convex hull of $(0,0)$ and the following three rate vectors: $(R_{1,\text{XOR}}^{\text{secure}}, R_{2,\text{XOR}}^{\text{secure}})$, $(R_{1,\text{RLNC}}^{\text{secure}}, 0)$, and $(0, R_{2,\text{RLNC}}^{\text{secure}})$.
- The case $\mathsf{sr} = (1,0)$ is symmetric to the case $\mathsf{sr} = (0,1)$.

If we use dashed lines to represent the existing "regions" first plotted in Fig. 1(c), then the LNC capacity regions for different security requirements are plotted in Fig. 2. It is worth noting that in this example, the point $(R_{1,\text{XOR}}^{\text{non.sec}}, R_{2,\text{XOR}}^{\text{non.sec}})$ is outside the convex hull of $(0,0)$, $(R_{1,\text{RLNC}}^{\text{non.sec}}, 0)$ and $(0, R_{2,\text{RLNC}}^{\text{non.sec}})$. This means that XOR-in-the-air strictly outperforms time-sharing plus random LNC. However, for certain $(p_1, p_2, p_{1\vee 2}, p_{1\to 2}, p_{2\to 1})$ values, we may have $(R_{1,\text{XOR}}^{\text{non.sec}}, R_{2,\text{XOR}}^{\text{non.sec}})$ being strictly within the convex hull of $(0,0)$, $(R_{1,\text{RLNC}}^{\text{non.sec}}, 0)$ and $(0, R_{2,\text{RLNC}}^{\text{non.sec}})$. In those cases, time-sharing plus RLNC is LNC-capacity-achieving.

V. An Outline Of The Proof

A. Achievability

Consider the security requirement $\mathsf{sr} = (0,0)$. By [7], the rate vector $(R_{1,\text{XOR}}^{\text{non.sec}}, R_{2,\text{XOR}}^{\text{non.sec}})$ is achievable. Since the unicast capacity point corresponds to an erasure relay channel Fig. 1(b), the results in [6], [13] can be used to prove directly that $(R_{1,\text{RLNC}}^{\text{non.sec}}, 0)$ is achievable. Symmetrically, $(0, R_{2,\text{RLNC}}^{\text{non.sec}})$ is achievable. The achievability proof for $\mathsf{sr} = (0,0)$ is complete.

We now focus on the more interesting case: $\mathsf{sr} = (1,1)$. By [11], the rate vector $(R_{1,\text{XOR}}^{\text{secure}}, R_{2,\text{XOR}}^{\text{secure}})$ is achievable. We now prove that $(R_{1,\text{RLNC}}^{\text{secure}}, 0)$ is achievable. Without loss of generality, assume $p_{2\to 1} \geq p_1$, in which case $R_{1,\text{RLNC}}^{\text{secure}} = \frac{p_{2\to 1}(p_{1\vee 2} - p_2)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_2 + p_{2\to 1} - p_1)}$ by (7). Otherwise, we have $R_{1,\text{RLNC}}^{\text{secure}} = \frac{p_1(p_{1\vee 2} - p_2)p_{1\vee 2}}{p_1 p_2 + p_{1\vee 2}(p_{1\vee 2} - p_2)}$, which is achievable even without receiver coordination, see Proposition 1 and [11].

We borrow the ideas in [11] and develop the following 3-staged scheme sending $nR_{1,\text{RLNC}}^{\text{secure}}$ packets from s to d_1 within n time slots while respecting the security requirement.

Stage 1: For each time slot, s sends an independently and uniformly randomly generated "seed" packet. We continue Stage 1 for $t_1 \triangleq \frac{nR_{1,\text{RLNC}}^{\text{secure}} \cdot p_2}{p_{1\vee 2}(p_{1\vee 2} - p_2)}$ time slots. After Stage 1, d_1

will receive $t_1 \cdot (p_{1\vee 2} - p_2)$ number[2] of seeds that are shared *only* between s and d_1, i.e., completely unknown to d_2. We use V_1 to $V_{t_1(p_{1\vee 2}-p_2)}$ to denote the shared seeds. Obviously, d_2 cannot extract any information of $\mathbf{W}_1$ in Stage 1 since all seeds are generated randomly.

Stage 2: For each time slot, s sends a linear sum $X_s(t) = V_h + W_{1,l}$ where the indices h and l are initialized to 1. Whenever d_2 receives $X_s(t)$, we update $h \leftarrow h+1$. Whenever at least one of $\{d_1, d_2\}$ receives $X_s(t)$, we update $l \leftarrow l+1$. We continue Stage 2 for $t_2 \triangleq \frac{nR^{\text{secure}}_{1,\text{RLNC}}}{p_{1\vee 2}}$ time slots. We first observe that $t_2 p_2 = t_1(p_{1\vee 2} - p_2)$. Therefore, the h value reaches $t_1(p_{1\vee 2} - p_2)$ in the end of Stage 2. This means that every packet received by d_2 is a linear sum with a distinct random seed V_h as one of its summands. Therefore, d_2 cannot extract any information of $\mathbf{W}_1$ in Stage 2. From d_1's perspective, d_1 knows all V_h in Stage 1. Therefore, whenever d_1 receives a linear sum $X_s(t)$, it can decode its desired $W_{1,l}$ by subtracting V_h. Since $t_2 p_{1\vee 2} = nR^{\text{secure}}_{1,\text{RLNC}}$, the l value reaches $nR^{\text{secure}}_{1,\text{RLNC}}$ in the end of Stage 2. This means that every information packet $W_{1,1}$ to $W_{1,nR^{\text{secure}}_{1,\text{RLNC}}}$ is either decoded by d_1, or participates in one of the linear sums received by d_2. If we count those linear sums that contains a $W_{1,l}$ that has not been decoded by d_1, we will have $t_2(p_{1\vee 2} - p_1)$ such linear sums. We denote them by U_1 to $U_{t_2(p_{1\vee 2}-p_1)}$.

Stage 3: For each time slot, d_2 sends $X_{d_2}(t) = U_m$ where the index m is initialized to 1. Whenever d_1 receives $X_{d_2}(t)$, we update $m \leftarrow m+1$. We continue Stage 3 for $t_3 \triangleq \frac{t_2(p_{1\vee 2}-p_1)}{p_{2\to 1}}$ time slots. Since neither s nor d_1 transmits in Stage 3, d_2 cannot extract any further information of $\mathbf{W}_1$ in Stage 3. We also observe that $t_3 p_{2\to 1} = t_2(p_{1\vee 2} - p_1)$. Therefore, the m value reaches $t_2(p_{1\vee 2} - p_1)$ in the end of Stage 3. This means that every U_m packet has been sent to d_1. Since each U_m is a linear sum of a V_h and a $W_{1,l}$, d_1 can decode in Stage 3 all the $W_{1,l}$ that have not already been decoded (by d_1) in Stage 2. The above arguments show that after 3 stages, d_2 cannot extract any information of $\mathbf{W}_1$ while d_1 can decode all $\mathbf{W}_1$ packets. One can easily verify by (7) that $t_1 + t_2 + t_3 = n$ in our construction. We have thus shown that rate vector $(R^{\text{secure}}_{1,\text{RLNC}}, 0)$ is achievable under $\mathsf{sr} = (1,1)$. Symmetrically, $(0, R^{\text{secure}}_{2,\text{RLNC}})$ is achievable. The achievability proof for $\mathsf{sr} = (1,1)$ is complete.

Consider $\mathsf{sr} = (0,1)$. Since there is no security requirement on flow-1, rate $(R^{\text{non.sec}}_{1,\text{RLNC}}, 0)$ is achievable. Since $\mathsf{sr} = (0,1)$ is a less demanding requirement than $\mathsf{sr} = (1,1)$, any achievable rate for $\mathsf{sr} = (1,1)$ is also achievable for $\mathsf{sr} = (0,1)$. As a result, both $(R^{\text{secure}}_{1,\text{XOR}}, R^{\text{secure}}_{2,\text{XOR}})$ and $(0, R^{\text{secure}}_{2,\text{RLNC}})$ are achievable by our previous analysis. The achievability proof for $\mathsf{sr} = (0,1)$ is complete.

B. The Converse

For the following, we only outline the proof for the hybrid security requirement $\mathsf{sr} = (0,1)$. The proofs for other sr values are similar and are thus omitted due to the space constraint.

[2]We only use the first-order analysis ($n \to \infty$) based on the laws of large numbers and omit the technical discussion of the ϵ terms when n is finite.

The main structure of the proof is as follows. Given any $(p_1, p_2, p_{1\vee 2}, p_{1\to 2}, p_{2\to 1})$ and any (R_1, R_2) values, we first construct a linear programming (LP) problem and prove that if (R_1, R_2) is LNC-achievable, then the LP problem is feasible. Then for any fixed $\hat{R}_1$ value, we can maximize R_2 subject to the LP formulation that captures all feasible (R_1, R_2). This leads to an outer bound on the achievable $(\hat{R}_1, R_2)$ for the given $\hat{R}_1$. Finally, we convert the maximization problem into its dual and derive the converse part of Proposition 3 that holds for *any arbitrary* (R_1, R_2).

Consider $\mathsf{sr} = (0,1)$ and assume $p_{1\to 2} \geq p_2$ and $p_{2\to 1} \geq p_1$. The other case (either $p_{1\to 2} < p_2$ or $p_{2\to 1} < p_1$) is actually a degenerate case and is less interesting. For any time t, we define the *knowledge space* S_i as the linear span of all the GCVs of the packets $[Y_{s\to d_i}, Y_{d_j\to d_i}]_1^{t-1}$ that d_i has received until time $t-1$. The *message space* Ω_i is the linear span of the GCVs corresponding to sending uncoded $W_{i,l}$ packets (the delta vectors). For two linear spaces, T_1 and T_2, we define the sum-space operator $\oplus$ by $T_1 \oplus T_2 = \mathsf{span}(\mathbf{v} : \forall \mathbf{v} \in T_1 \cup T_2)$. We define the following 8 linear subspaces

$$\begin{aligned} &A_1 \triangleq S_1; \quad A_2 \triangleq S_2; \quad A_3 \triangleq S_1 \oplus \Omega_1; \quad A_4 \triangleq S_2 \oplus \Omega_2; \\ &A_5 \triangleq S_1 \oplus S_2; \quad A_6 \triangleq S_1 \oplus S_2 \oplus \Omega_1; \\ &A_7 = S_1 \oplus S_2 \oplus \Omega_2; \quad A_8 \triangleq S_1 \oplus \Omega_2. \end{aligned} \tag{9}$$

Using A_1 to A_8, we can now partition the overall message space Ω into $2^8 = 256$ disjoint subsets depending on whether a GCV $\mathbf{c}$ is in A_k or not, for $k = 1, \cdots, 8$. Each subset is termed a *coding type* and can be indexed by an 8-bit string $\mathbf{b} = b_1 b_2 \cdots b_8$ where each b_k indicates whether $\mathbf{c}$ belongs to A_k or not. See [12] for the discussion of coding types.

Given any scheme that can achieve rate (R_1, R_2) with $\mathsf{sr} = (0,1)$, we claim that the source s must never send a GCV $\mathbf{c}$ of type-00000011 during the course of executing this scheme. The reason is that type-00000011 corresponds to $(A_7 \cap A_8) \backslash \left(\bigcup_{k=1}^{6} A_k\right)$. Suppose the scheme sends a GCV in $A_8 = S_1 \oplus \Omega_2$ but not in $A_1 = S_1$. This means that whenever d_1 receives such a packet, the "collective" space $S_1 \oplus \Omega_2$ will remain the same, but the individual space S_1 will increase. Therefore, *the overlap $S_1 \cap \Omega_2$ will increase, which implies that S_1 can now derive some information of* $\mathbf{W}_2$. This violates the requirement $\mathsf{sr} = (0,1)$. By applying such a security-based observation, we can follow the steps in [12] and derive the corresponding LP problem. Due to space constraints, we directly present the final result.

Define the following finite index sets S, $\mathsf{D1}$, and $\mathsf{D2}$:

$$\begin{aligned} \mathsf{S} \triangleq \{&0, 2, 4, 6, 14, 18, 22, 30, \\ &36, 38, 46, 54, 62, 94, 126, 175, 191, 255\}, \end{aligned}$$

$$\mathsf{D1} \triangleq \{175, 191, 255\}, \text{ and } \mathsf{D2} \triangleq \{94, 126, 255\}.$$

For any 8-bit coding type $\mathbf{b} = b_1 b_2 \cdots b_8$, we can view $\mathbf{b}$ as a base-2 expression with the leftmost bit being the most significant bit (MSB). For example, the statement "$\mathbf{b} = 38$" is equivalent to "$\mathbf{b} = 00100110$" and the statement "$\mathbf{b} \in \mathsf{S}$ and $b_7 = 0$" is equivalent to "$\mathbf{b} \in \{0, 4, 36\}$". For simplicity,

we use $\mathbf{b}_s$, $\mathbf{b}_{d_1}$, and $\mathbf{b}_{d_2}$ to denote the strings in S, D1, and D2, respectively. $b_{s,i}$ denotes the i-th coordinate of the given string $\mathbf{b}_s$. Similarly, we define $b_{d_1,i}$ and $b_{d_2,i}$.

Claim: A rate vector (R_1, R_2) is in the $\mathsf{sr} = (0,1)$ LNC-capacity region only if there exist $18+3+3$ non-negative variables $x_{s,\mathbf{b}_s}$, $x_{d_1,\mathbf{b}_{d_1}}$, and $x_{d_2,\mathbf{b}_{d_2}}$ for all $\mathbf{b}_s$, $\mathbf{b}_{d_1}$ and $\mathbf{b}_{d_2}$; 8 non-negative variables y_1 to y_8 such that jointly they satisfy 4 groups of linear conditions:

- Group 1, termed the *time-sharing condition*:

$$\sum_{\forall \mathbf{b}_s} x_{s,\mathbf{b}_s} + \sum_{\forall \mathbf{b}_{d_1}} x_{d_1,\mathbf{b}_{d_1}} + \sum_{\forall \mathbf{b}_{d_2}} x_{d_2,\mathbf{b}_{d_2}} \le 1. \qquad (10)$$

- Group 2, termed the *rank-conversion conditions*:

$$y_1 = \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,1}=0} x_{s,\mathbf{b}_s} p_1 + \sum_{\forall \mathbf{b}_{d_2} \text{ w. } b_{d_2,1}=0} x_{d_2,\mathbf{b}_{d_2}} p_{2\to 1}$$

$$y_2 = \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,2}=0} x_{s,\mathbf{b}_s} p_2 + \sum_{\forall \mathbf{b}_{d_1} \text{ w. } b_{d_1,2}=0} x_{d_1,\mathbf{b}_{d_1}} p_{1\to 2}$$

$$y_3 = R_1 + \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,3}=0} x_{s,\mathbf{b}_s} p_1 + \sum_{\forall \mathbf{b}_{d_2} \text{ w. } b_{d_2,3}=0} x_{d_2,\mathbf{b}_{d_2}} p_{2\to 1}$$

$$y_4 = R_2 + \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,4}=0} x_{s,\mathbf{b}_s} p_2 + \sum_{\forall \mathbf{b}_{d_1} \text{ w. } b_{d_1,4}=0} x_{d_1,\mathbf{b}_{d_1}} p_{1\to 2}$$

$$y_5 = \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,5}=0} x_{s,\mathbf{b}_s} p_{1\vee 2}$$

$$y_6 = R_1 + \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,6}=0} x_{s,\mathbf{b}_s} p_{1\vee 2}$$

$$y_7 = R_2 + \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,7}=0} x_{s,\mathbf{b}_s} p_{1\vee 2}$$

$$y_8 = R_2 + \sum_{\forall \mathbf{b}_s \text{ w. } b_{s,8}=0} x_{s,\mathbf{b}_s} p_1 + \sum_{\forall \mathbf{b}_{d_2} \text{ w. } b_{d_2,8}=0} x_{d_2,\mathbf{b}_{d_2}} p_{2\to 1}$$

- Group 3, termed the *rank-comparison conditions*:

$$y_5 \le y_6, \quad y_8 \le y_7, \quad \text{and} \quad y_4 + y_5 - y_7 \ge y_2.$$

- Group 4, termed the *decodability conditions*:

$$y_3 = y_1 \quad \text{and} \quad y_4 = y_2.$$

The intuition behind the above LP formulation is as follows. Fix any scheme that achieves rate (R_1, R_2) and satisfies $\mathsf{sr} = (0,1)$. We define for any $u \in \{s, d_1, d_2\}$

$$x_{u,\mathbf{b}_u} \triangleq \frac{\mathsf{E}\left\{\sum_{t=1}^{n} 1_{\{u \text{ is scheduled and transmits a } \mathbf{c}_{u,t} \in \mathsf{TYPE}_{\mathbf{b}_u}\}}\right\}}{n}.$$

That is, $x_{u,\mathbf{b}_u}$ is the normalized time allocation for which the scheme lets node u send coding type $\mathbf{b}_u$. As a result, they satisfy (10) naturally. Define $y_k \triangleq \frac{1}{n}\mathsf{E}\{\mathrm{Rank}(A_k)\}$ as the normalized rank of space A_k in the end of time n. The rank conversion equalities establish the relationship between "how frequently we send a packet of type-$\mathbf{b}$" and "how fast the rank of A_k grows over time". By definition (9),

$$A_5 = (S_1 \oplus S_2) \subseteq A_6 = (S_1 \oplus S_2 \oplus \Omega_1). \qquad (11)$$

Taking the normalized expected rank of (11), we immediately have the rank comparison inequality $y_5 \le y_6$. The decodability condition ensures that destination d_i can successfully decode $\mathbf{W}_i$. See [12] for detailed discussion. From the above arguments, given any achievable scheme, we can explicitly construct the x and y variables satisfying the above LP problem. The existence of an achievable scheme thus implies the feasibility of the LP problem.

The final step is to convert the above LP problem to its dual and prove the converse of the $\mathsf{sr} = (0,1)$ LNC-capacity.

VI. Conclusion

This work considers the 1-to-2 broadcast PEC with causal feedback, receiver coordination, and arbitrary security requirement. We have proven that the LNC capacity can be achieved either by the XOR-in-the-air scheme, or by RLNC, or by time-sharing between the two. The results imply that to design an optimal Wi-Fi receiver coordination scheme, a system designer only needs to focus the efforts on optimally combining the existing RLNC solutions [4] and XOR-in-the-air [5] solutions without the need to explore any other forms of LNC.

This work was supported in part by NSF grants CCF-0845968 and CNS-0905331.

References

[1] S.-Y. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, February 2003.

[2] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Médard, and J. Crowcroft, "XORs in the air: Practical wireless network," in *Proc. ACM Special Interest Group on Data Commun. (SIGCOMM)*, 2006.

[3] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in *Proc. ACM Special Interest Group on Data Commun. (SIGCOMM)*. Kyoto, Japan, August 2007.

[4] D. Koutsonikolas, C.-C. Wang, and Y. Hu, "Efficient network coding based opportunistic routing through cumulative coded acknowledgment," *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1368–1381, October 2011.

[5] D. Koutsonikolas, C.-C. Wang, Y. Hu, and N. Shroff, "FEC-based AP downlink transmission schemes for multiple flows: Combining the reliability and throughput enhancement of intra- and inter-flow coding," *Elsevier Performance Evaluation (PEVA)*, vol. 68, no. 11, November 2011.

[6] A. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 789–804, March 2006.

[7] L. Georgiadis and L. Tassiulas, "Broadcast erasure channel with feedback — capacity and algorithms," in *Proc. 5th Workshop on Network Coding, Theory, & Applications (NetCod)*. Lausanne, Switzerland, June 2009, pp. 54–61.

[8] M. Gatzianas, L. Georgiadis, and L. Tassiulas, "Multiuser broadcast erasure channel with feedback — capacity and algorithms," in *Proc. NetCoop*, 2010.

[9] C.-C. Wang, "Capacity of 1-to-K broadcast packet erasure channels with channel output feedback," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 957–988, February 2012.

[10] M. Gatzianas, S. Bidokhti, and C. Fragouli, "Feedback-based coding algorithms for broadcast erasure channels with degraded message sets," in *Proc. 8th Workshop on Network Coding, Theory, & Applications (NetCod)*. Cambridge, USA, June 2012.

[11] L. Czap, V. Prabhakaran, S. Diggavi, and C. Fragouli, "Broadcasting private messages securely," in *Proc. IEEE Int'l Symp. Inform. Theory*. Cambridge, USA, July 2012, pp. 428–432.

[12] C.-C. Wang and D. Love, "Linear network coding capacity region of 2-receiver MIMO broadcast packet erasure channels with feedback," in *Proc. IEEE Int'l Symp. Inform. Theory*. Boston, USA, July 2012.

[13] W. Kuo and C.-C. Wang, "On the capacity of 2-user 1-hop relay erasure networks — the union of feedback, scheduling, opportunistic routing, and network coding," in *Proc. IEEE Int'l Symp. Inform. Theory*. Saint Petersburg, Russia, August 2011.

[14] G. Kramer, "Communication on line networks with deterministic or erasure broadcast channels," in *Proc. IEEE Inform. Theory Workshop*. Taormina, Italy, October 2009, pp. 404–405.

[15] C.-C. Wang, "Capacity region of two symmetric nearby erasure channels with channel state feedback," in *Proc. IEEE Inform. Theory Workshop*. Lausanne, Switzerland, September 2012.