An Efficient Network Coding based Broadcast Scheme with Reliability Guarantee

Peng Wang*, Guoqiang Mao†‡, Zihuai Lin*, Xiaohu Ge$^\&$
*School of Electrical and Information Engineering, The University of Sydney
†School of Computing and Communications, The University of Technology Sydney
‡National ICT Australia (NICTA), Australia $^\&$Huazhong University of Science and Technology
Email: g.mao@iee.org, {thomaspeng.wang, zihuai.lin}@sydney.edu.au, xhgeg@mail.hust.edu.cn

***Abstract*—There is an increasing demand for broadcasting information of common interest to a large number of users. The unreliable nature of wireless links and the difficulty of acknowledging the correct reception of every broadcast packet by every user when the number of users becomes large are two major challenges for wireless network broadcasting. In this paper we investigate the problem that a base station broadcasts a given number of packets to a given number of users, without user acknowledgment, while being able to provide a guarantee on the probability of successful delivery. Network coding technique is employed to improve both the efficiency and the reliability of the broadcast. Performance analysis is conducted. Based on the analysis, an upper and a lower bound on the number of packet transmissions required to meet the reliability guarantee are obtained. Simulations are conducted to validate the accuracy of the theoretical analysis. The technique and analysis developed in this paper can be useful for designing strategies to deliver information of common interest to a large number of users efficiently and reliably.**

***Index Terms*—Network coding, wireless broadcast, reliability**

I. Introduction

There is an increasing demand for using wireless broadcast to deliver information of common interest, e.g. safety warning messages, emergency information and weather information, to a large number of users. The unreliable nature of wireless communications forms a major challenge in wireless broadcast. Further, qualities of wireless links often vary. A common solution to combat the challenge of unreliable wireless communications is using Automatic Repeat reQuest (ARQ). With ARQ, users provide feedback to the transmitter, e.g. a base station (BS), using either acknowledgements (ACKs) if the packets are correctly received or negative acknowledgements (NACKs) if the packets are deemed erroneous. If NACKs are received or ACKs are not received within a predesignated amount of time, the BS will retransmit the packets. There are several drawbacks of using packet acknowledgment. First, the overhead incurred when gathering acknowledgment information from multiple users increases with the number of users. Therefore, using ARQ for wireless broadcast is not scalable [1]. Second, when the number of rusers is large, packet acknowledgement may cause significant delay and bandwidth consumption [2]. This is particularly true for highly dynamic networks where the user population and the users' locations change dramatically with time. Thus, it is highly desirable to design a wireless broadcast scheme that a) can deliver information to a large number of users, b) without relying on user acknowledgment, and c) is able to provide a guaranteed performance on the probability of successful delivery.

In this paper we tackle the above challenges using the network coding(NC) technique. Recent work has shown that NC can significantly improve both the transmission efficiency and the reliability of transmission [3]. Particularly, in [3] Dong *et al.* proposed several NC based broadcast schemes [3]. It was shown that NC based retransmission scheme performs better than its counterpart using ARQ only. However, their NC based retransmission strategy relies on the use of feedback information from receivers. In [4], Shokrollahi developed rateless codes (RCs) for network coding to improve the transmission efficiency. RCs are a special class of forward error correcting codes, which can automatically adapt to the channel conditions and avoid the need for a feedback channel [4], [5]. Due to these salient advantages of RCs, in this paper we choose RCs for use in our broadcast strategy design. It is worth noting that in [6], a decoding algorithm called full-rank decoding was presented and on that basis theoretical analysis was conducted on the decoding success probability of the proposed algorithm. However the analysis in [6] was incomplete to the extent that no rigorous analysis was presented to support some results presented in the paper and the analytical result presented on the decoding success probability was in fact an approximation only, which will be shown in the analysis of Section III.

In this paper, we consider that a BS broadcasts a given number of packets to a given number of receivers, without requiring the receivers to acknowledge the correct receipt of broadcast packets. NC technique, particularly RCs, is used to reduce the number of transmissions while providing a guaranteed performance on the probability of successful delivery. The performance of the proposed NC based broadcast scheme is validated both analytically and via simulations. The following is a detailed summary of our contributions:

1) A RCs based broadcast scheme is proposed, which broadcasts a given number of packets from a BS to a given number of users. The scheme does not need user acknowledgment.
2) The performance of the proposed scheme is analyzed.

This work is funded by Australian Research Council Discovery projects DP110100538 and DP120102030.

An upper and a lower bound are obtained on the probability that all receivers successfully receive all broadcast packets from the BS.

3) On the basis of the above result, the minimum number of transmissions required for a guaranteed performance on the probability of successful delivery is obtained.
4) Simulations are conducted which validate both the accuracy of the analysis and the performance improvement of the proposed scheme.

The technique and analysis presented in this paper can be useful for designing strategies to deliver information of common interest to a large number of users efficiently and reliably.

The rest of the paper is organized as follows. Section II describes the system model and problem formulation. In Section III, we carry out performance analysis of the proposed NC based broadcast scheme and present a technique to estimate the number of transmissions required to meet the performance objective on the probability of successful delivery. In Section IV, we validate our analytical results using simulations. Section V concludes the paper.

II. System model and Problem Formulation

In this paper, a network with one base station(BS) and a known number of receivers is used. Let N denote the number of receivers. We assume that the channels between the BS and the receivers are independent[1] and the packet transmission success probabilities are known, denoted by $P_1, P_2, \ldots, P_N$ respectively. Further, for each receiver, the event that a (coded) packet is successfully received and the event that another (coded) packet is received are independent. Therefore $P_1, P_2, \ldots, P_N$ correspond to the long-term average packet transmission success probabilities. As mentioned in the introduction, it is assumed that the BS cannot gather feedback information from receivers on whether or not a particular packet transmission is successful. However, the BS may still be able to obtain feedback from receivers infrequently to estimate the long-term average channel conditions [2] required for estimating $P_1, P_2, \ldots, P_N$.

The BS has k source packets of equal length to broadcast to all N receivers. Either the source packets or coded copies of the source packets can be transmitted. As mentioned in Section I, RCs are used for packet encoding. Denote by η_j the event that all receivers have received, i.e. successfully decoded, the j^{th} source packet. Let $\eta = \bigcap_{j\in\Gamma_s} \eta_j$, where Γ_s denotes the set of indices of all source packets. Denote by ϵ a pre-determined small positive constant. The objective of the network coded broadcast scheme is to determine the number of (coded) packets that the BS needs to transmit to guarantee that $\Pr(\eta) \geq 1{-}\epsilon$. By comparing the number of packet transmissions required for the BS to reach the objective $\Pr(\eta) \geq 1{-}\epsilon$ with and without using NC respectively, we shall also establish the performance benefit of using NC in packet broadcast. Fig. 1 illustrates the system model.

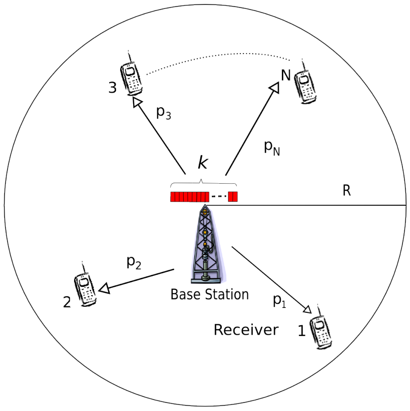

Figure 1. An illustration of the system model.

III. Analysis of Rateless Codes based Broadcast Scheme

In this section, the decoding success probability using RCs is analyzed first. On that basis, the number of transmissions required to meet the objective $\Pr(\eta) \geq 1{-}\epsilon$ is obtained.

When RCs are used by the BS to broadcast k source packets, the following encoding rule is utilized to produce each coded packet: firstly draw a positive integer d (often referred to as the "degree" [5] of coded packets) from the set of integers $\{1, ..., k\}$ according to a probability distribution $\mathbf{\Omega} = (\Omega_1, ..., \Omega_k)$ where Ω_d is the probability that d is picked and $\sum_{d=1}^{k} \Omega_d = 1$. Then, select d distinct source packets randomly and independently from the k source packets, where each source packet is selected with equal probability, and XOR them to generate the corresponding coded packet [4], [5]. Finally, these coded packets will be broadcast to all receivers.

A typically used decoding process for RCs is the so-called "LT process" [5], but it is well known that the LT process is not able to decode all decodable source packets from the successfully received coded packets. Therefore in this paper, we use a different decoding algorithm called the full-rank decoding [6] to decode the source packets. More specifically, let n $(n \geq k)$ be the number of coded packets that have already been successfully received by a receiver. We use a $1 \times k$ row vector to represent a coded packet, where the j^{th} entry of the row vector is 1 if the corresponding coded packet is a result of XOR operation on the j^{th} source packet (and other source packets); otherwise the j^{th} entry equals to 0. Thus, a random row vector in this paper refers to the row vector of a randomly chosen coded packet where the coded packet is generated using the RCs encoding process. In this way, the information contained in the n coded packets can be represented by a $n \times k$ matrix, denoted by $\mathbf{G}_{n\times k}$. We say that the receiver can recover all k source packets from the n coded packets if and only if $\mathbf{G}_{n\times k}$ is a full rank matrix, i.e. its rank equals to k. Note that in this paper, all algebraic operations and the associated analysis are conducted in a binary field.

A. Analysis of the rank of a random matrix

In this subsection, we give procedure on computing the probability that $\mathbf{G}_{n\times k}$ is a full rank matrix, where $n \geq k$.

[1] The assumption of channel independence has been widely used and is also supported by some measurement studies although we acknowledge that in some environment channel correlations can be a major concern. For example, In a recent work it was shown [7] that if a pair of receivers are separated by more than λ, their received signals from a common transmitter can seen as independent (with a correlation coefficient less than 0.15).

Let R^r_n be the event that the rank of the encoding coefficient matrix $\mathbf{G}_{n\times k}$ is r and let $\Pr[R^r_n]$ be its probability. Define the rank profile of $\mathbf{G}_{n\times k}$ to be a vector $\mathbf{R}(n) = (\Pr[R^1_n], \Pr[R^2_n], \ldots, \Pr[R^k_n])^T$. Noting that the decoding success probability is equal to the probability that the rank of the encoding coefficient matrix $\mathbf{G}_{n\times k}$ equals k, i.e. $\Pr[R^k_n]$, our analysis on the decoding success probability relies on a recursive computation of $\mathbf{R}(n)$ as n increases.

When $n = 1$, it can be readily shown that $\mathbf{R}(1) = (1, 0, \ldots, 0)^T$. For $n > 1$, the rank profile of $\mathbf{G}_{n\times k}$ can be obtained from the rank profile of $\mathbf{G}_{(n-1)\times k}$ recursively. Particularly, $\mathbf{G}_{n\times k}$ can be considered as $\mathbf{G}_{(n-1)\times k}$ with an additional row $\mathbf{x}$ added into $\mathbf{G}_{(n-1)\times k}$. The degree of $\mathbf{x}$, i.e. the number of non-zero elements of $\mathbf{x}$, is chosen according to the pre-defined degree distribution $\mathbf{\Omega} = (\Omega_1, ..., \Omega_k)$ and each non-zero element is then placed randomly and uniformly into $\mathbf{x}$. Let $rk(\mathbf{G})$ be the rank of the matrix and let $Im(\mathbf{G})$ be the row vector space generated by a matrix $\mathbf{G}$. That is, $Im(\mathbf{G})$ is the vector space formed by all linear combinations of the rows of $\mathbf{G}$. Note that it may possibly occur that $Im(\mathbf{G}_{n\times k}) = Im(\mathbf{G}_{m\times k})$ where $m \neq n$. If a row vector $\mathbf{x}$ can be expressed as a linear combination of the row vectors of $\mathbf{G}$, we say that $\mathbf{x} \in Im(\mathbf{G})$; otherwise $\mathbf{x} \notin Im(\mathbf{G})$. For $k \geq r \geq 2$, it can be shown that

$$\begin{aligned}
&\Pr\left[rk(\mathbf{G}_{n\times k}) = r\right] \\
=&\Pr\left[rk(\mathbf{G}_{(n-1)\times k}) = r\right] \times \\
&\Pr\left[\mathbf{x} \in Im(\mathbf{G}_{(n-1)\times k}) \mid rk(\mathbf{G}_{(n-1)\times k}) = r\right] \\
&+ \Pr\left[rk(\mathbf{G}_{(n-1)\times k}) = r-1\right] \times \\
&\Pr\left[\mathbf{x} \notin Im(\mathbf{G}_{(n-1)\times k}) \mid rk(\mathbf{G}_{(n-1)\times k}) = r-1\right] \qquad (1)
\end{aligned}$$

Let $O^{r-1}_{n-1} = \Pr\left[\mathbf{x} \notin Im(\mathbf{G}_{(n-1)\times k}) \mid R^{r-1}_{n-1}\right]$. It follows from the equation (1) that:

$$\Pr\left[R^r_n\right] = \Pr\left[R^r_{n-1}\right](1 - O^r_{n-1}) + \Pr\left[R^{r-1}_{n-1}\right] O^{r-1}_{n-1} \qquad (2)$$

Based on (2), the following equation can be obtained by recursion: $\mathbf{R}(n) = (\prod_{m=1}^{n-1} \mathbf{X}_m)\mathbf{R}(1)$, where

$$\mathbf{X}_m = \begin{pmatrix} 1 - O^1_m & 0 & \cdots & 0 & 0 \\ O^1_m & 1 - O^2_m & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & O^{k-1}_m & 1 - O^k_m \end{pmatrix}$$

The probability that $\mathbf{G}_{n\times k}$ is of full rank, hence all source packets can be successfully decoded, can be calculated by:

$$\Pr\left[R^k_n\right] = \mathbf{e}_k \cdot \mathbf{R}(n) = \mathbf{e}_k(\prod_{m=1}^{n-1} \mathbf{X}_m)\mathbf{R}(1) \qquad (3)$$

where $\mathbf{e}_i$, $1 \leq i \leq k$, is a $1 \times k$ row vector with the i^{th} entry equal to 1 and all other entries equal to 0.

The above recursive way of computing the rank profile of $\mathbf{G}_{n\times k}$ and the probability that $\mathbf{G}_{n\times k}$ is a full rank matrix relies on the knowledge of the parameters $O^z_{n-1} = \Pr\left[\mathbf{x} \notin Im(\mathbf{G}_{(n-1)\times k}) \mid R^z_{n-1}\right], 1 \leq z \leq k$. In the following paragraphs, we give analysis on the computation of $\Pr\left[\mathbf{x} \in Im(\mathbf{G}_{(n-1)\times k}) \mid R^z_{n-1}\right]$.

For convenience let A_{n-1} be the event that $\mathbf{x} \notin Im(\mathbf{G}_{(n-1)\times k})$ and $\overline{A_{n-1}}$ be the complement of event A_{n-1}. Temporarily assuming that $rk(\mathbf{G}_{(n-1)\times k}) = z, 1 \leq z \leq k$ and noting that $\mathbf{G}_{(n-1)\times k}$ is a random matrix, under the above two conditions, let V^z be a row vector space formed by all linear combinations of the rows of *an instance* of $\mathbf{G}_{(n-1)\times k}$. Of course the dimension of V^z equals to z, hence the superscript. Further, let $\mathcal{E}^z$ be the set of *all possible* and *distinct* V^zs: $\mathcal{E}^z \triangleq \{V^z\}$. When $z = k$, the row vector space whose dimension is k is unique. However when $1 \leq z < k$, there are multiple row vector spaces with dimension z. For convenience, we number the elements of $\mathcal{E}^z$ sequentially and denote by Γ^z_v be the set of indices of all $V^z \in \mathcal{E}^z$. Denote by V^z_i the i^{th} element of $\mathcal{E}^z$. As noted in the last paragraph, the coding coefficient matrix $\mathbf{G}$ and the vector space formed by the row vectors of matrix $\mathbf{G}$ have independent significance in the sense that for two positive integers $m, n \geq z$ and $m \neq n$, it may happen that $V^z_i = Im(\mathbf{G}_{n\times k}) = Im(\mathbf{G}_{m\times k})$. That is, the vector space and its existence does not depend on some details of the matrix $\mathbf{G}$, e.g. number of rows in the matrix and a particular instance of the matrix.

Let $F^z_{i,n-1}$ be the event $Im(\mathbf{G}_{(n-1)\times k}) = V^z_i$. It can be readily shown that: 1) $R^z_{n-1} = \cup_{i\in\Gamma^z_v} F^z_{i,n-1}$, i.e. event that the rank of the matrix $\mathbf{G}_{n\times k}$ is z equals to the joint events that $Im(\mathbf{G}_{(n-1)\times k}) = V^z_i$ for all $i, i \in \Gamma^z_v$; 2) $F^z_{i,n-1} \cap F^z_{j,n-1} = \emptyset$ for $i \neq j$. Considering the definitions of the two events R^z_n and $F^z_{i,n-1}$, Bayes' formula and the two results, we have

$$\begin{aligned}
&\Pr\left[\mathbf{x} \in Im(\mathbf{G}_{(n-1)\times k}) \mid rk(\mathbf{G}_{(n-1)\times k}) = z\right] \\
=&\Pr\left[\overline{A_{n-1}} \mid R^z_{n-1}\right] = \frac{\Pr\left[\overline{A_{n-1}} \cap (\cup_{i\in\Gamma^z_v} F^z_{i,n-1})\right]}{\Pr\left[\cup_{i\in\Gamma^z_v} F^z_{i,n-1}\right]} \\
=&\frac{\sum_{i\in\Gamma^z_v} \Pr\left[\overline{A_{n-1}} \mid F^z_{i,n-1}\right] \Pr\left[F^z_{i,n-1}\right]}{\sum_{i\in\Gamma^z_v} \Pr\left[F^z_{i,n-1}\right]} \qquad (4)
\end{aligned}$$

Let $\overline{B^z_i}$ be the event that $\mathbf{x} \in V^z_i$. Conditioned on the event $F^z_{i,n-1}$ and noting that $\mathbf{x}$ is drawn randomly and independently of the row vectors of $\mathbf{G}_{(n-1)\times k}$, we have

$$\overline{A_{n-1}} \mid F^z_{i,n-1} \Leftrightarrow \overline{B^z_i} \mid F^z_{i,n-1} \qquad (5)$$

Because each row vector is drawn *independently* of other row vectors, the two events $\mathbf{x} \in V^z_i$ and $Im(\mathbf{G}_{(n-1)\times k}) = V^z_i$ are independent. It follows using the definitions of $\overline{B^z_i}$ and $F^z_{i,n-1}$ that $\Pr\left[\overline{B^z_i} \mid F^z_{i,n-1}\right] = \Pr\left[\overline{B^z_i}\right] = \Pr\left[\mathbf{x} \in V^z_i\right]$.

For the other term $\Pr\left[F^z_{i,n-1}\right]$ in (4), we recall that $F^z_{i,n-1}$ is the event $Im(\mathbf{G}_{(n-1)\times k}) = V^z_i$. Let $E^z_{i,n-1}$ be the event $V^z_i \subseteq Im(\mathbf{G}_{(n-1)\times k})$ and obviously $F^z_{i,n-1} \subseteq E^z_{i,n-1}$. Conditioned on the event $E^z_{i,n-1}$, without loss of generality, let $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_z\}$ be the row vectors of $\mathbf{G}_{(n-1)\times k}$ that forms a basis of V^z_i, which may not be unique. Let $\{\mathbf{w}_1, \mathbf{w}_1, ..., \mathbf{w}_{n-z-1}\}$ be the remaining row vectors of $\mathbf{G}_{(n-1)\times k}$. Further note that each row vector of $\mathbf{G}_{(n-1)\times k}$ is formed *independently* of other row vectors. Noting that $F^z_{i,n-1} \subseteq E^z_{i,n-1}$, it can be shown that

$$\begin{aligned}
\Pr\left[F^z_{i,n-1}\right] &= \Pr\left[F^z_{i,n-1} | E^z_{i,n-1}\right] \Pr\left[E^z_{i,n-1}\right] \\
&= \left(\Pr\left[\mathbf{w}_1 \in V^z_i | E^z_{i,n-1}\right]\right)^{n-z-1} \Pr\left[E^z_{i,n-1}\right] \\
&= \left(\Pr\left[\overline{B^z_i}\right]\right)^{n-z-1} \Pr\left[E^z_{i,n-1}\right] \qquad (6)
\end{aligned}$$

where the last step results because the two events $\mathbf{w}_1 \in V_i^z$ and $E_{i,n-1}^z$ are independent. Combining the three equations (4), (5), and (6), conclusion follows that

$$\begin{aligned}\Pr\left[\overline{A_{n-1}} \mid R_{n-1}^z\right] &= \frac{\sum_{i\in\Gamma_v^z} \Pr\left[\overline{A_{n-1}} \mid F_{i,n-1}^z\right] \Pr\left[F_{i,n-1}^z\right]}{\sum_{i\in\Gamma_v^z} \Pr\left[F_{i,n-1}^z\right]} \\ &= \frac{\sum_{i\in\Gamma_v^z} \left(\Pr\left[\overline{B_i^z}\right]\right)^{n-z} \Pr\left[E_{i,n-1}^z\right]}{\sum_{i\in\Gamma_v^z} \left(\Pr\left[\overline{B_i^z}\right]\right)^{n-z-1} \Pr\left[E_{i,n-1}^z\right]} \quad (7)\end{aligned}$$

As manifested in the equation (7), the computation of $\Pr\left[\overline{A_{n-1}} \mid R_{n-1}^z\right]$, which is required for computing the rank profile of $\mathbf{G}_{n\times k}$ and the probability that $\mathbf{G}_{n\times k}$ is a full rank matrix, relies on the knowledge of $\Pr\left[\overline{B_i^z}\right]$ and $\Pr\left[E_{i,n-1}^z\right]$. These parameters can be difficult to obtain when k is large. In the rest of this section, we devote our efforts to finding an upper and a lower bound of $\Pr\left[\overline{A_{n-1}} \mid R_{n-1}^z\right]$, which will be shown later using simulations to be reasonably tight.

1) Derivation of An Upper Bound of $\Pr\left[R_n^k\right]$*:* Let $a_{i,n-1} = \Pr\left[E_{i,n-1}^z\right]$ and $b_{i,z} = \Pr\left[\overline{B_i^z}\right]$ for notational convenience. Equation (7) can be rewritten as:

$$\Pr[\overline{A_{n-1}} \mid R_{n-1}^z] \quad = \textstyle\sum_{i\in\Gamma_v^z} a_{i,n-1} b_{i,z}^{(n-z)} / \sum_{i\in\Gamma_v^z} a_{i,n-1} b_{i,z}^{(n-z-1)}$$

Next we shall evaluate the monoticity of $\Pr\left[\overline{A_{n-1}} \mid R_{n-1}^{r-1}\right]$ as a function of n. It can be shown that:

$$\begin{aligned}&\Pr\left[\overline{A_n} \mid R_n^z\right] - \Pr\left[\overline{A_{n-1}} \mid R_{n-1}^z\right] \\ &= \frac{\sum_{i\in\Gamma_v^z} a_{i,n} b_{i,z}^{n-z+1}}{\sum_{i\in\Gamma_v^z} a_{i,n} b_{i,z}^{n-z}} - \frac{\sum_{i\in\Gamma_v^z} a_{i,n-1} b_{i,z}^{n-z}}{\sum_{i\in\Gamma_v^z} a_{i,n-1} b_{i,z}^{n-z-1}} \\ &= \frac{\sum_{j\in\Gamma_v^z}\sum_{i\in\Gamma_v^z} a_{i,n} a_{j,n-1} b_{i,z}^{n-z-1} b_{j,z}^{n-z-1} (b_{i,z} - b_{j,z})^2}{\sum_{i\in\Gamma_v^z} a_{i,n} b_i^{n-z} \sum_{i\in\Gamma_v^z} a_{i,n-1} b_i^{n-z-1}} \geq 0\end{aligned}$$

As a result of the above analysis, we can conclude that the conditional probability $\Pr\left[\overline{A_{n-1}} \mid R_n^z\right]$ is a monotonically increasing function of n and $\Pr\left[\overline{A_n} \mid R_n^z\right] \geq \Pr\left[\overline{A_{n-1}} \mid R_{n-1}^z\right] \geq \cdots \geq \Pr\left[\overline{A_z} \mid R_z^z\right]$.

We can then obtain that

$$\Pr\left[R_n^k\right] = \mathbf{e}_k\left(\prod_{m=1}^{n-1} \mathbf{X}_m\right)\mathbf{R}(1) \quad \leq \quad \mathbf{e}_k(\mathbf{X})^{n-1}\mathbf{R}(1) \quad (8)$$

where

$$\mathbf{X} = \begin{pmatrix} 1-O_1^1 & 0 & \cdots & 0 & 0 \\ O_1^1 & 1-O_2^2 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & O_{k-1}^{k-1} & 1-O_k^k \end{pmatrix}$$

Now an upper bound of the decoding success probability is derived and this relies on the knowledge of $O_z^z, 1 \leq z \leq k$. In the following paragraphs, we present analysis leading to the computation of $O_z^z, 1 \leq z \leq k$. Noting that when $1 \leq z \leq k$, $\mathbf{x} \notin Im(\mathbf{G}_{z\times k}) \cap rk(\mathbf{G}_{z\times k}) = z \Leftrightarrow rk(\mathbf{G}_{(z+1)\times k}) = z+1$, it can be shown that

$$O_z^z = \Pr\left[\mathbf{x} \notin Im(\mathbf{G}_{z\times k}) \mid rk(\mathbf{G}_{z\times k}) = z\right] = \frac{\Pr\left[R_{z+1}^{z+1}\right]}{\Pr\left[R_z^z\right]} \quad (9)$$

where $\Pr\left[R_z^z\right]$ represents the probability that a random (encoding coefficient) matrix $\mathbf{G}_{z\times k}$, $z \leq k$, is of full rank. The method to calculate $\Pr\left[R_z^z\right]$ is provided in the following lemma.

Lemma 1. *Let $\mathbf{v}_i$ be the i^{th} row vector of $\mathbf{G}_{z\times k}$. Denote by I_q (whose value will be determined later in Lemma 2) the probability of the event that $\sum_{i=1}^q \mathbf{v}_i = \mathbf{0}$, conditioned on that the summation of any w row vectors of $\mathbf{G}_{z\times k}$ is not equal to $\mathbf{0}$, where $\mathbf{0}$ is a $1\times k$ row vector with all elements equal to 0, $w \in \mathbb{Z}^+,\ 1 < w < q$. $F(z)$ can be determined by:*

$$\Pr\left[R_z^z\right] \quad = \quad \prod_{q=2}^{z}\left[(1-I_q)^{\binom{z}{q}}\right]$$

Proof: We observe that $\mathbf{G}_{z\times k}$ being full rank implies that there does *not* exist a set of coefficients $c_1,\ldots,c_r$ such that $\sum_{i=1}^r c_i\mathbf{v}_i = 0$. Further, since we are working in a binary field, c_i can be either 1 or 0. It follows that $\mathbf{G}_{z\times k}$ being full rank is a sufficient and necessary condition for that for every integer $2 \leq q \leq r$, the summation of any q row vectors of $\mathbf{G}_{z\times k}$ is not equal to $\mathbf{0}$. This observation forms the basis of the proof.

Let $NZ(q)$ be the event that the summation of any q row vectors in $\mathbf{G}_{z\times k}$ are not equal to $\mathbf{0}$. The probability of $NZ(2)$ can be expressed as $\Pr[NZ(2)] = (1-I_2)^{\binom{r}{2}}$. Further, for every integer q satisfying $3 \leq q \leq r$,

$$\Pr\left[\cap_{i=2}^q NZ(i)\right] = \Pr\left[NZ(q) \mid \cap_{i=2}^{q-1} NZ(i)\right] \Pr\left[\cap_{i=2}^{q-1} NZ(i)\right] \quad (10)$$

With the recursive application of equation (10), we can calculate the probability that $\mathbf{G}_{z\times k}$, $z \leq k$, is of full rank as $\Pr\left[R_z^z\right] = \Pr(\cap_{i=2}^z NZ(i)) = \prod_{q=2}^z \left[(1-I_q)^{\binom{z}{q}}\right]$ ■

Now we shall derive I_q which is required in Lemma 1. To obtain I_q which is required in Lemma 1. , we must first evaluate the degree transition probability Q_{ij}, i.e. the probability that the row vector $\mathbf{S}_q$ produced by summing q row vectors has degree j given that the row vector $\mathbf{S}_{q-1}$ generated by summing the first $q-1$ row vectors of the above q row vectors has degree i. We can derive Q_{ij} [6] as:

$$Q_{ij} = \begin{cases} \displaystyle\sum_{\substack{0\leq a\leq\min(k-j,i) \\ b=j-i+a}} \Omega_{a+b}\frac{\binom{i}{a}\binom{k-i}{b}}{\binom{k}{a+b}}, & i \leq j \\ \displaystyle\sum_{\substack{i-j\leq a\leq\min(k-j,i) \\ b=j-i+a}} \Omega_{a+b}\frac{\binom{i}{a}\binom{k-i}{b}}{\binom{k}{a+b}}, & i > j \end{cases}$$

where Ω_d, $1 \leq d \leq k$ is the degree distribution of RCs, which is defined in Section III. Now we are ready to analyze I_q.

Lemma 2. *Let $\mathbf{Tr}$ be a $k\times k$ transition matrix with dimension $k\times k$ whose $(j,i)^{th}$ element equal to Q_{ij}. The matrix $\mathbf{Tr}$ can be expressed as:*

$$\mathbf{Tr} = \begin{pmatrix} Q_{11} & \cdots & Q_{(k-1)1} & Q_{k1} \\ \vdots & \ddots & \vdots & \vdots \\ Q_{1k} & \cdots & Q_{(k-1)k} & Q_{kk} \end{pmatrix}$$

the probability I_q is given by:

$$I_{q,\ q\geq 2.} = (Q_{10}, Q_{20}, \ldots, Q_{k0})\mathbf{Tr}^{q-2} \cdot (\Omega_1, \Omega_2, \ldots, \Omega_k)^T$$

Proof: To obtain I_q, we analyze the degree distribution of row vector $\mathbf{S}_w$ which is the sum of w row vectors. Note that the degree of $\mathbf{S}_w$ should not equal to 0. Let $\mathbf{D}^w = (D_1^w, \ldots, D_k^w)^T$ be the degree distribution of the sum of w (random) row vectors and $w \geq 1$, where D_i^w is the probability that the degree of the row vector $\mathbf{S}_w$ is i, $1 \leq i \leq k$. When $w = 1$, the degree distribution $\mathbf{D}^1$ is obviously $(\Omega_1, \Omega_2, \ldots, \Omega_k)^T$. For $w \geq 2$, the relationship can be analytically described as :

$$D_m^w = (Q_{1m}, Q_{2m}, \ldots, Q_{km})(D_1^{w-1}, \ldots, D_k^{w-1})^T \quad (11)$$

From the equation (11), it follows that:

$$\mathbf{D}^w = (D_1^w, \ldots, D_k^w)^T = \mathbf{Tr}^{w-1} \cdot (\Omega_1, \Omega_2, \ldots, \Omega_k)^T \quad (12)$$

As an easy consequence of equation (12), I_q can be obtained:

$$I_q = D_0^q = (Q_{10}, Q_{20}, \ldots, Q_{k0})\mathbf{Tr}^{q-2} \cdot (\Omega_1, \Omega_2, \ldots, \Omega_k)^T$$

■

Using (8), (9) and Lemmas 1 and 2, an upper bound on $\Pr\left[R_n^k\right]$ can be computed.

2) Derivation of A Lower Bound of $\Pr\left[R_n^k\right]$*:* In addition to the upper bound derived earlier in the section, a lower bound on the decoding success probability can also be obtained:

$$\Pr\left[\overline{A_n} \mid R_n^z\right] = \frac{\sum_{i\in\Gamma_v^z} a_{i,n} b_{i,z}^{n-z+1}}{\sum_{i\in\Gamma_v^z} a_{i,n} b_{i,z}^{n-z}} \leq \max_{i\in\Gamma_v^z}\{b_{i,z}\}$$

Thus we can obtain that

$$\Pr\left[R_n^k\right] = \mathbf{e}_k\Big(\prod_{m=1}^{n-1} \mathbf{X}_m\Big)\mathbf{R}(1) \geq \mathbf{e}_k(\mathbf{X}_{min})^{n-1}\mathbf{R}(1) \quad (13)$$

where

$$\mathbf{X}_{min} = \begin{pmatrix} 1 - \max_{i\in\Gamma_v^1}\{b_{i,1}\} & \cdots & 0 \\ \max_{i\in\Gamma_v^1}\{b_{i,1}\} & \ddots & 0 \\ 0 & \cdots & 1 - \max_{i\in\Gamma_v^k}\{b_{i,k}\} \end{pmatrix}$$

The above lower bound relies on the knowledge of $\max_{i\in\Gamma_v^z}\{b_{i,z}\}$, i.e., $\max_{i\in\Gamma_v^z}\{\Pr\left[\overline{B_i^z}\right]\}, 1 \leq z \leq k$. In the following analysis, we give analysis that leads to the computation of $\max_{i\in\Gamma_v^z}\{\Pr\left[\overline{B_i^z}\right]\}$.

Note that a particular row vector with degree d occurs with probability $P_g(d) = \Omega_d/\binom{k}{d}$ where Ω_d is the probability that a (any) row vector with degree d is chosen and $\binom{k}{d}$ is the total number of degree d vectors among all $1 \times k$ binary vectors. Recall that the degree of a vector is the number of non-zero elements in it. Recall that $\mathbf{e}_i$ is a $1 \times k$ row vector with the i^{th} entry equal to 1 and all other entries equal to 0. Obviously $\{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ forms a set of orthogonal basis vectors where *any row vector,* hence a row vector in any V_i^z, $i \in \Gamma_v^z$, in the matrix can be represented as a linear combination of these basis vectors. Let us focus now on a z dimensional subspace formed by $\{\mathbf{e}_1, \ldots, \mathbf{e}_z\}$, denoted by $V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_z\}}$. Using a straightforward combinatorial argument and further noting that we are working in a binary field, it can be shown that the number of degree d, $d \leq z$, vectors in $V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_z\}}$ is given by $\binom{z}{d}$. Therefore $\Pr[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_z\}}] = \sum_{d=1}^{z}[\binom{z}{d}P_g(d)]$. Denote by Ω_i^z any other z dimensional vector space whose basis vectors are the row vectors of a matrix obtainable by reshuffling the columns of the matrix $\{\mathbf{e}_1, \ldots, \mathbf{e}_z\}^T$ (or equivalently any other z dimensional vector space whose basis vectors are obtained by randomly choosing z vectors from $\{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$). Because the number of non-zero elements are uniformly and independently distributed in a row vector, it follows that $\Pr[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_z\}}] = \Pr\left[\mathbf{x} \in \Omega_i^z\right]$.

Now let us consider a z dimensional vector space formed by the basis vectors $\{\mathbf{e}_1, \ldots, \mathbf{e}_{z-1}, \mathbf{e}_z + \mathbf{e}_{z+1}\}$. Except for the last basis vector which has degree 2, all other basis vectors have degree 1 only. Using some straightforward combinatorial argument, the number of vectors in $V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\mathbf{e}_{z+1}\}}$ containing $\mathbf{e}_z + \mathbf{e}_{z+1}$ and having a degree $d + 2$ is given by $\binom{z-1}{d}$; the number of vectors in $V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\mathbf{e}_{z+1}\}}$ *not* containing $\mathbf{e}_z + \mathbf{e}_{z+1}$ and having a degree d is given by $\binom{z-1}{d}$. Therefore $\Pr[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\mathbf{e}_{z+1}\}}] = \sum_{d=0}^{z-1}[\binom{z-1}{d}P_g(d+2)] + \sum_{d=1}^{z-1}[\binom{z-1}{d}P_g(d)]$. Similarly, denote by Ω_i^z any other z dimensional vector space whose basis vectors are the row vectors of a matrix obtainable by reshuffling the columns of the matrix $\{\mathbf{e}_1, \ldots, \mathbf{e}_{z-1}, \mathbf{e}_z + \mathbf{e}_{z+1}\}^T$. It can be shown that $\Pr\left[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\mathbf{e}_{z+1}\}}\right] = \Pr\left[\mathbf{x} \in \Omega_i^z\right]$. Continue with the above discussion for $V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\mathbf{e}_{z+1}+\mathbf{e}_{z+2}\}}$,...,$V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\cdots+\mathbf{e}_k\}}$, it can be shown that

$$\begin{aligned} &\Pr\left[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\cdots+\mathbf{e}_i\}}\right] \\ &= \sum_{d=0}^{z-1}[\binom{z-1}{d}P_g(d+i-z+1)] + \sum_{d=1}^{z-1}[\binom{z-1}{d}P_g(d)] \end{aligned} \quad (14)$$

where $0 \leq i \leq k - z$. Because we are working in the binary field, it can be shown that the above discussion covers all occurrences of z dimensional spaces. Summarizing the above discussion, it follows that $\max_i\{\Pr\left[\overline{B_i^z}\right]\} = \max_{0\leq i\leq k-z}\Pr\left[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\cdots+\mathbf{e}_{z+i}\}}\right]$, where the values of $\Pr\left[\mathbf{x} \in V_{\{\mathbf{e}_1,\ldots,\mathbf{e}_{z-1},\mathbf{e}_z+\cdots+\mathbf{e}_{z+i}\}}\right]$ is given by (14).

B. Analysis of the minimum number of transmissions

Let $\rho_{lower}(n)$ and $\rho_{upper}(n)$ be the upper and lower bound of the decoding success probability of a receiver who have already successfully receive n, $n \geq k$, packets respectively. According to (13) and (8), $\rho_{lower}(n) = \mathbf{e}_k(\mathbf{X}_{min})^{(n-1)}\mathbf{R}(1)$ and $\rho_{upper}(n) = \mathbf{e}_k(\mathbf{X})^{(n-1)}\mathbf{R}(1)$. Denote by $\overline{C}$ the total number of transmissions the BS needs to perform in order to meet the objective $\Pr(\eta) \geq 1-\epsilon$. The probability that all the k source packets can be successfully received by all N receivers after $\overline{C}$ transmissions by the BS can be expressed as:$\Pr(\eta_{k,\overline{C}}) = \prod_{i=1}^{N}\Pr(\eta_{k,\overline{C},i})$ where $\Pr(\eta_{k,\overline{C},i}) = \sum_{n=k}^{\overline{C}}\binom{\overline{C}}{n}P_i^n(1-P_i)^{\overline{C}-n}\rho(n)$. Therefore

$$\Pr(\eta_{k,\overline{C}}) = \prod_{i=1}^{N}\{\sum_{n=k}^{\overline{C}}\binom{\overline{C}}{n}P_i^n(1-P_i)^{\overline{C}-n}\rho(n)\} \quad (15)$$

To provide a guaranteed performance on the probability of successful delivery, the following inequality needs to be met:

$$\prod_{i=1}^{N}\{\sum_{n=k}^{\overline{C}}\binom{\overline{C}}{n}P_i^n(1-P_i)^{\overline{C}-n}\rho(n)\} \geq 1-\epsilon \quad (16)$$

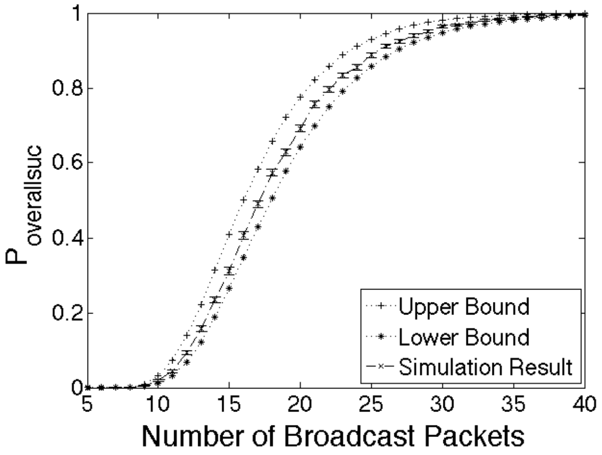

Figure 2. The probability of successfully decoding all 5 source packets by all 6 receivers versus the number of broadcast packets.

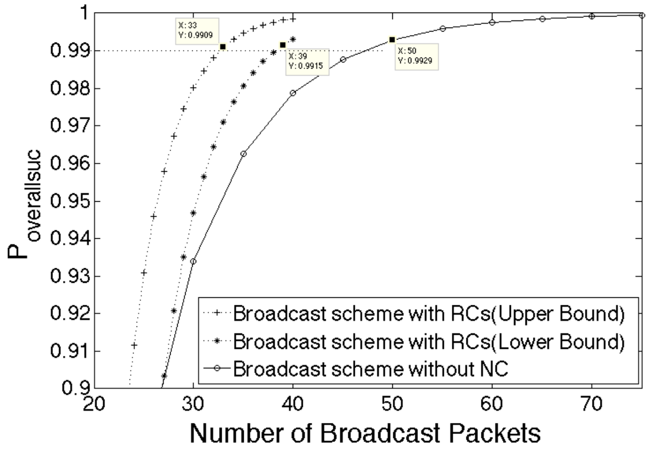

Figure 3. The probabilities of successfully decoding all 5 source packets by all 6 receivers for broadcast scheme using RCs and that without NC as a function of the number of broadcast packets.

Using equations (16), (13) and (8), a lower and an upper bound of the minimum number of transmissions required by the BS to meet $\Pr(\eta) \geq 1{-}\epsilon$ can be computed numerically.

IV. Simulation Results

In this section, we validate our analytical results and the accuracy of the upper and the lower bound using simulations.

We set the number of source packets to be 5 and the number of receivers to be 6. Packet transmission successful probabilities of the 6 receivers are 0.4, 0.5, 0.6, 0.7, 0.8 and 0.9 respectively. Simulations using other packet transmission successful probabilities showed the same match between the analytical and simulation results. The degree distribution of the RCs follows the widely used Luby's Ideal Soliton distribution [5]. Analytical and simulation results are presented on the probability that all receivers successfully receive all 5 source packets as a function of the number of transmissions using RCs by the BS. Each simulation is repeated 100000 number of times and the average result is presented in the figures, together with the 95% confidence interval. As shown in Fig. 2, our analytical results match the simulation results very well, which validate the accuracy of the analysis.

In Fig. 3, we further compare the success probabilities of broadcast using RCs and that without using network coding(NC). As shown in Fig. 3, it can be seen that the use of RCs yields much better performance in terms of the number of transmitted packets required to meet the same reliability constraint. In comparison, when NC is not used, the BS needs to transmit more packets to meet the reliability constraint. For example, when the reliability constraint is set to be 0.99, 39 transmissions are needed when RCs are used, while 50 broadcasts are required when NC is not used, i.e. a saving of 28% transmissions is obtained when using RCs.

V. Conclusion

In this paper we studied reliable broadcast in a wireless network with a BS and a number of receivers. More specifically, assuming that the number of receivers, their channel conditions measured by the packet transmission successful probability, and the number of broadcast packets are known, we investigated the number of required transmissions from the transmitter to meet the reliability guarantee without using acknowledgement/feedback from the receivers. The reliability guarantee is given by that the probability that all receivers successfully receive all broadcast packets is above a predefined threshold. Theoretical analysis has been conducted on the performance of the broadcast using RCs. On the basis of the analysis, an upper and a lower bound of the number of transmissions required by the BS to meet the reliability guarantee is obtained. It was shown that the use of RCs can significantly reduce the number of transmissions required to meet the same reliability guarantee, compared with that without using NC. Simulations were conducted which indicated a good accuracy of the analytical results.

Our future will expand the analysis to incorporate the situation that the exact channel conditions of users are not known, instead one only has a statistical knowledge of the users, e.g. user distribution and channel model in the environment.

References

[1] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "Xors in the air: practical wireless network coding," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 497–510, 2008.

[2] I.-H. Hou and P. R. Kumar, "Broadcasting delay-constrained traffic over unreliable wireless links with network coding," in *Proceedings of the 12th ACM MobiHoc*, 2011, pp. 1–10.

[3] N. Dong, T. Tuan, N. Thinh, and B. Bose, "Wireless broadcast using network coding," *IEEE Trans. Vehicular Technology*, vol. 58, no. 2, pp. 914–925, 2009.

[4] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, 2006.

[5] M. Luby, "LT codes," in *Proceedings of the 43rd IEEE FOCS*, 2002, pp. 271–280.

[6] L. Feng, F. Chuan Heng, C. Jianfei, and C. Liang-Tien, "LT codes decoding: Design and analysis," in *Proceedings of IEEE ISIT*, 2009, pp. 2492–2496.

[7] S. Rajabi, M. Shahabadi, and M. ArdebiliPoor, "Modeling of the correlation coefficients of a receive antenna array in a MIMO multipath channel," in *Proceedings of 2nd IEEE/IFIP ICI*, 2006, pp. 1–4.