Reliability-Constrained Broadcast using Network Coding without Feedback

Peng Wang*‡, Guoqiang Mao†‡, and Zihuai Lin*
*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
Email: thomaspeng.wang@sydney.edu.au, g.mao@ieee.org, zihuai.lin@sydney.edu.au

***Abstract*—Wireless broadcast has been widely utilized to deliver information of common interest to a large number of users. A major challenge for wireless broadcast is that wireless links are often unreliable. Further, it is not feasible for every receiver to acknowledge the correct reception of broadcasted packets. In this paper we investigate the use of wireless broadcast to deliver a given number of packets by a common transmitter to a given number of receivers, without feedback from the receivers, while meeting the reliability constraint, i.e. the probability that all receivers successfully receive all broadcasted packets is above a certain threshold. Rateless codes(RCs) technology is used to assist the broadcast. Performance analysis with the use of RCs is conducted. Simulations are conducted to validate the accuracy of the theoretical analysis. It is shown that the use of RCs can significantly reduce the number of transmissions required to meet the reliability constraint.**

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

I. Introduction

Wireless broadcast has been widely used to deliver information of common interest, e.g. safety warning messages, emergency information, to a colossal number of users. A major challenge for broadcast in wireless networks is that wireless links are often unreliable. Further, qualities of wireless links vary from node to node. To guarantee reliable packet transmissions over unreliable links, Automatic Repeat reQuest (ARQ) is often utilized. With ARQ, receivers afford feedback to the common transmitter, e.g. Base Station (BS), using either acknowledgements (ACKs) if the packets are correctly received or negative acknowledgements (NACKs) if the packets are deemed to be erroneous. If NACKs are received or ACKs are not received within a pre-designated amount of time, the BS will retransmit these packets. There are several drawbacks of packet acknowledgment. First of all, the overhead of gathering acknowledgments from multiple receivers increases with the number of receivers. Therefore, using ARQ for wireless broadcast is not scalable [1]. Moreover, when the number of receivers 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, a solution for reliable wireless broadcast that does not necessitate feedback information is highly desirable in many circumstances.

Recent work has shown that the transmission efficiency and reliability of wireless broadcast can be enhanced by employing network coding [3], [4]. More specifically, in [3], Dong et al. presented several broadcast protocols based on the use of network coding. It was observed that the network coding based retransmission scheme performs better than ARQ without using network coding, particularly when the channel conditions are good and there are only a small number of receivers. However, their network coding-based retransmission strategy still requires feedback information from receivers. Techniques were also reported to improve the transmission efficiency of wireless broadcast, based on the utilization of rateless codes [5]. Rateless codes are a special class of forward error correcting codes, which can automatically adapt to any channel conditions and avoid the need for feedback channels [5], [6]. Rateless codes can generate a potentially limitless stream of coded packets. A sufficient number of successfully received coded packets, regardless of which coded packets are received, can lead to successful decoding of all source packets.

In this paper, we present a network coding based wireless broadcast scheme without relying on feedback information from receivers. The scheme tries to minimize the number of transmissions by a common transmitter while ensuring that the probability that all receivers correctly receive all broadcast packets from the transmitter, e.g. a BS, is higher than a pre-designated objective. The performance of the proposed scheme is validated both analytically and via simulations. The following is a detailed summary of our contributions:

1) We propose a rateless code based broadcast scheme for a network with one BS as the transmitter and a known number of receivers. The scheme does not need feedback information from the receivers.
2) The performance of the proposed scheme is analyzed. The probability that under the proposed rateless code based broadcast scheme, all receivers successfully receive all broadcast packets from the BS is obtained analytically.
3) Based on the above analysis, the number of transmissions required by the BS to ensure that the probability that all receivers successfully receive all broadcast packets is above a pre-designated objective is obtained.

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

4) Simulations are conducted which validate both the accuracy of the analysis and the performance improvement of the proposed scheme.

The rest of the paper is organized as follows. Section II reviews the related work. Section III describes the system model and problem formulation. In Section IV, we carry out performance analysis of rateless codes and present a technique to estimate the number of transmissions required by rateless code based broadcast to meet the above-mentioned reliability constraint. In Section V, we validate our analytical results using simulations. Section VI concludes the paper.

II. Related work

In this section, we review related work on the study of rateless codes and on the analysis of the corresponding decoding success probability.

The first practical digital fountain code is LT codes [6], which was invented by Luby. The packet length can be arbitrary. To transmit a traffic session containing M source packets, each coded packet can be independently generated by the BS, and the entire session can be recovered from any $M + O(\sqrt{M}\log^2(M/\delta))$ coded packets with a probability of $1-\delta$. Based on [6], Shokrollahi [5] developed "Raptor codes" which have less encoding and decoding complexities than LT codes.

It was shown in [5] that LT codes can deliver excellent performance when the value of M is large. In reality, a traffic session may contain a small numbers of packets only. Under this scenario, a high packet overhead is however reported [7]. Hyytia et al. [7] optimized the configuration of the degree distribution for LT codes when the number of packets is small. However, as presented in [7], the proposed methods are not scalable and can only handle the situation when the number of packets $M \sim 10$. The authors in [8] proposed a new algorithm for decoding. Using this algorithm, the packet overhead is reduced.

The above work on rateless codes focuses on the study of the transmission between a single transmitter-receiver pair. In this paper, we shall use rateless codes for packet broadcast between a single transmitter and multiple receivers without the use of feedback information from the receivers.

A major challenge in analyzing the performance of rateless codes is that the decoding success probability of rateless codes is difficult to analyze. In [9], the authors proposed a method to recursively compute the decoding success probability of rateless codes. The detailed proof of their method was presented in [10] . The recursion involved in the computation makes it very difficult to derive a closed-form analytical result for the decoding success probability. In [8], the authors proposed a decoding algorithm called full-rank decoding that improves the decodability of LT codes. Particularly, mathematical analysis on the rank of the random coefficient matrix was presented and then used to evaluate the decoding success probability of the proposed algorithm. However the proof of their method was not shown and the analysis was also incomplete.

In this paper, we present theoretical analysis on the rank of the random coefficient matrix. This analysis is subsequently used to calculate the overall transmission success probability, i.e. the probability that all receivers successfully receive all broadcast packets. Finally, the minimum number of transmissions required by the BS to meet a pre-designated target on the overall transmission success probability is determined.

III. System model and Problem Formulation

We consider a network with one BS and a known number of receivers. Denote the number of receivers by N. The channels between the BS and the receivers are assumed to be independent[1] with known packet transmission success probabilities, denoted by $P_1, P_2, \ldots, P_N$ respectively. Further, we assume that for the same 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 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 for estimating the (long-term average) channel conditions [2].

The BS needs to broadcast M source packets of equal length to all N receivers. The BS may choose to transmit either the source packets directly or coded copies of the source packets. Denote by η_j the event that all receivers have received, i.e. successfully decoded, the j^{th} source packet from the BS. Let $\eta = \bigcap_{j\in\Gamma} \eta_j$, where Γ denotes the set of indices of all source packets. Denote by ϵ a pre-determined small positive constant. The objective is to determine the number of (coded) packets that the BS needs to transmit with or without the use of network coding 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 network coding respectively, we shall establish the performance benefit of using network coding in packet broadcast. Fig. 1 illustrates the system model.

IV. Broadcast Using Rateless Codes

In this section, we first analyze the decoding success probabilities using rateless codes (RCs) in transmission. On that basis, we then estimate the number of transmissions required for meeting the objective $\Pr(\eta) \geq 1-\epsilon$.

When the BS broadcasts M source packets by using RCs, the BS applies this coding scheme to generate a limitless stream of coded packets. RCs utilize the following encoding rules for producing coded packets: for each coded packets, first draw an integer d (the "degree" of coded packets) from

[1] We acknowledge that in some environments the assumption of independence of channels may not be valid while in some other environments (e.g. open space) it is a reasonable assumption. For example, in [11] it was shown that the coherence distance in an omnidirectional Rayleigh channel is: $\frac{9\lambda}{16\pi}$ [11, Eq. (5.116)] where λ is the wavelength and the value for a non-omnidirectional channel is only slightly different [11, Eq. (5.117)]. In a more recent work it was shown [12] that if a pair of receivers are separated by more than λ, their received signals from a common transmitter can be considered independent [11, p. 243] (with a correlation coefficient less than 0.15). At 800 MHz $\lambda = 0.375$ m, thus the requirement on the separation of receivers (in order for the channels to be considered independent) can be easily met.

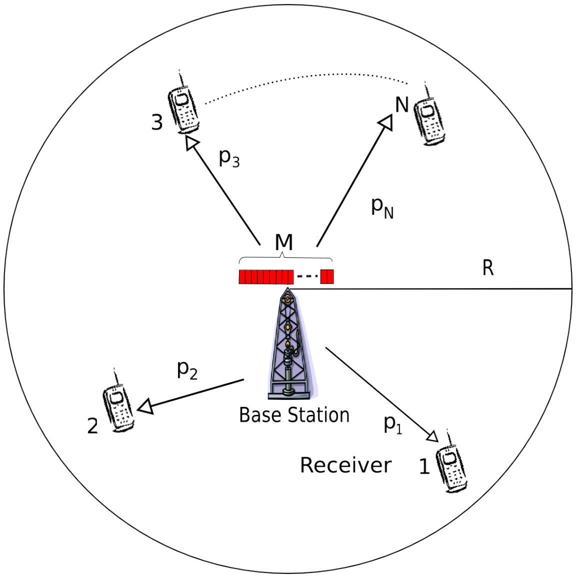

Figure 1. An illustration of the basic architecture of system model

the set $\{1,...,M\}$ according to a probability distribution $\mathbf{\Omega} = (\Omega_1,...,\Omega_M)$ where Ω_d is the probability that d is drawn and $\sum_{i=1}^{M}\Omega_i = 1$. Then, pick d distinct source packets randomly and independently, where each source packet is picked with equal probability, and XOR them to generate the corresponding coded packet [5], [6]. Then, these coded packets will be sequentially broadcasted to all receivers.

A typically used decoding process for RCs is the so-called "LT process" [6]. The LT process is efficient to implement, 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 criteria to determine whether source packets can be decoded. More specifically, let L ($L \geq M$) be the number of coded packets that have already been successfully received by a receiver. The information in each coded packet can be represented by a $1 \times M$ row vector 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. In this way, the information contained in the L coded packets can be represented by a $L \times M$ matrix, i.e. $B_{L\times M}$, which is termed as the encoding coefficient matrix in the paper. We say that the receiver can recover all M source packets from the L coded packets if and only if $B_{L\times M}$ is a full rank matrix, i.e. its rank equals to M.

From now on, we use a row vector to represent the information contained in a coded packet. Thus, a random row vector in this paper means the row vector of a randomly chosen coded packet where the coded packet is generated using the encoding process introduced earlier in this section.

A. Analysis of the rank of a random matrix

In this subsection, we give procedure on computing the probability that a receiver which has already successfully received L coded packets is able to decode all M source packets successfully, where $L \geq M$. The analysis can be divided into two major steps. First, we give results on how to compute the probability of the event that the encoding coefficient matrix $\mathbf{B}_{L\times M}$ is of full rank in Theorem 1. Only when $B_{L\times M}$ is a full rank matrix, the receiver can recover all M source packets from the L coded packets. The computation of the probability that $B_{L\times M}$ is of full rank however requires the knowledge that a randomly chosen row vector is independent of other z, $1 \leq z \leq M$, linearly independent row vectors. Therefore in the second step, we give the procedure to compute the above probability and the results are summarized in Lemmas 2 and 3.

As explained, the probability that a receiver, which has already successfully received L coded packets, is able to recover all M source packets can be computed using Theorem 1 below:

Theorem 1. *Let $p(L,r)$ denote the probability that the rank of the encoding coefficient matrix $\mathbf{B}_{L\times M}$, which contains L row vectors of size $1 \times M$, is r. Define the rank profile of $\mathbf{B}_{L\times M}$ to be a vector $\mathbf{p}(L) = (p(L,1), p(L,2), \ldots, p(L,M))^T$. When $L = 1$, it can be readily shown that $\mathbf{p}(1) = (p(1,1), p(1,2), \ldots, p(1,M))^T = (1,0,\ldots,0)^T$. Let O_z be the probability that a random row vector is linearly independent of other z linearly independent random row vectors (O_z can be calculated by using Lemmas 2 and 3 introduced later). Then the rank profile $\mathbf{p}(L)$ can be approximately calculated using O_z by the following equation:*

$$\mathbf{p}(L) \approx (\mathbf{R}_M)^{(L-1)}\mathbf{p}(1), \tag{1}$$

where

$$\mathbf{R}_M = \begin{pmatrix} 1-O_1 & 0 & \cdots & 0 & 0 \\ O_1 & 1-O_2 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1-O_{M-1} & 0 \\ 0 & 0 & \cdots & O_{M-1} & 1-O_M \end{pmatrix}.$$

Proof: We compute the rank profile of $\mathbf{B}_{L\times M}$ recursively.

For $L = 1$, the rank profile is obviously $(1,0,\ldots,0)^T$.

For $L > 1$, the rank profile of $\mathbf{B}_{L\times M}$ can be obtained from the rank profile of $\mathbf{B}_{(L-1)\times M}$. $\mathbf{B}_{L\times M}$ can be considered as $\mathbf{B}_{(L-1)\times M}$ with an additional row $\mathbf{x}$ added into $\mathbf{B}_{(L-1)\times M}$. 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 $\mathbf{\Omega} = (\Omega_1,...,\Omega_M)$ and each non-zero element is then placed randomly and uniformly into $\mathbf{x}$. Let $rk(\mathbf{B}_{L\times M})$ be the rank of the matrix $\mathbf{B}_{L\times M}$ and $Im(\mathbf{B}_{L\times M})$ be the row vector space generated by the rows of $\mathbf{B}_{L\times M}$. If a row vector $\mathbf{x}$ can be expressed as a linear combination of the row vectors of $\mathbf{B}_{L\times M}$, we express it as $\mathbf{x} \in Im(\mathbf{B}_{L\times M})$; otherwise $\mathbf{x} \notin Im(\mathbf{B}_{L\times M})$. For $r \geq 2$, it can be shown:

$$\begin{aligned} &\Pr\left[rk(\mathbf{B}_{L\times M}) = r\right] \\ =&\Pr\left[rk(\mathbf{B}_{(L-1)\times M}) = r\right] \times \\ &\Pr\left[\mathbf{x} \in Im(\mathbf{B}_{(L-1)\times M}) \mid rk(\mathbf{B}_{(L-1)\times M}) = r\right] \\ &+ \Pr\left[rk(\mathbf{B}_{(L-1)\times M}) = r-1\right] \times \\ &\Pr\left[\mathbf{x} \notin Im(\mathbf{B}_{(L-1)\times M}) \mid rk(\mathbf{B}_{(L-1)\times M}) = r-1\right]. \end{aligned} \tag{2}$$

Note that the conditional probability that a (random) $1\times M$ row vector is independent of all row vectors of a $(L-1)\times M$ (random coding coefficient) matrix, whose rank is $r-1$, *is not equal to* the conditional probability that a (random) $1\times M$ row vector is independent of all row vectors of a $(r-1)\times M$ (random coding coefficient) matrix, whose rank is $r-1$ (i.e. a full rank matrix). Following the same technique used in [8], we ignore the difference and consider that the two values are *approximately* equal. As will be shown later via simulations, the approximation is reasonably accurate. Using the approximation, it follows that:

$$\begin{aligned}
& \Pr\left[\mathbf{x}\notin Im(\mathbf{B}_{(L-1)\times M}) \mid rk(\mathbf{B}_{(L-1)\times M})=r-1\right] \\
\approx\; & \Pr\left[\mathbf{x}\notin Im(\mathbf{B}_{(r-1)\times M}) \mid rk(\mathbf{B}_{(r-1)\times M})=r-1\right] \quad (3)\\
=\; & \frac{F(r)}{F(r-1)}=O_{r-1}, \quad (4)
\end{aligned}$$

where $F(r)$ represents the probability that a random (encoding coefficient) matrix $\mathbf{B}_{r\times M}$, $r\le M$, is of full rank and O_r denotes the probability that a random row vector is linearly independent of other r linearly independent random row vectors. The method to calculate $F(r)$ will be provided later in Lemma 2.

From equations (2) and (4), the following recursive relationship can be obtained:

$$p(L,r)\approx\;\; p(L-1,r)(1-O_r)+p(L-1,r-1)O_{r-1}. \quad (5)$$

Gathering all the above equations, the following equation can be obtained:

$$\begin{aligned}
&\mathbf{p}(L)\\
\approx&\begin{pmatrix}1-O_1 & 0 & \cdots & 0 & 0\\ O_1 & 1-O_2 & \cdots & 0 & 0\\ \vdots & \ddots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 1-O_{M-1} & 0\\ 0 & 0 & \cdots & O_{M-1} & 1-O_M\end{pmatrix}\mathbf{p}(L-1)\\
\approx&\mathbf{R}_M^{L-1}\mathbf{p}(1). \quad (6)
\end{aligned}$$

Using Theorem 1, the probability that $\mathbf{B}_{L\times M}$ is of full rank can be calculated by:

$$\begin{aligned}
p(L,M) &= \begin{pmatrix}0\\0\\ \vdots\\0\\1\end{pmatrix}^T\begin{pmatrix}p(L,1)\\p(L,2)\\ \vdots\\ p(L,M-1)\\ p(L,M)\end{pmatrix}\\
&= \mathbf{u}(M)^T(\mathbf{R}_M)^{(L-1)}\mathbf{u}(1), \quad (7)
\end{aligned}$$

where $\mathbf{u}(s)$, $1\le s\le M$, is the unit row vector with the s^{th} element equal to 1 and all other elements equal to 0. ■

Theorem 1 relies on the knowledge of $O_z, 1\le z\le M$. In the following paragraphs, we present analysis leading to the computation of $O_z, 1\le z\le M$. We will first compute $F(r)$ in (4):

Lemma 2. *Let $F(r)$ be the probability that $\mathbf{B}_{r\times M}$, $r\le M$, is of full rank and $\mathbf{v}_i$ be the i^{th} row vector of $\mathbf{B}_{r\times M}$. Denote I_q (whose value will be determined later in Lemma 3) by 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 $\mathbf{B}_{r\times M}$ is not equal to $\mathbf{0}$, where $\mathbf{0}$ is a $1\times M$ row vector with all elements equal to 0, $w\in\mathbb{Z}^+,\ 1<w<q$. $F(r)$ can be determined by:*

$$F(r)\;\;=\;\;\prod_{q=2}^{r}\left[(1-I_q)^{\binom{r}{q}}\right].$$

Proof: We observe that $\mathbf{B}_{r\times M}$ 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 $\mathbf{B}_{r\times M}$ being full rank is a sufficient and necessary condition for that for every integer $2\le q\le r$, the summation of any q row vectors of $\mathbf{B}_{r\times M}$ is not equal to $\mathbf{0}$, where $\mathbf{0}$ is a $1\times M$ row vector with all elements equal to 0. This observation forms the basis of the proof.

Let $NZ(q)$ denote the event that the summation of any q row vectors in $\mathbf{B}_{r\times M}$ are not equal to $\mathbf{0}$. Since all row vectors are generated randomly independently, the events that summation of two distinct row vectors is not equal to $\mathbf{0}$ are independent; the probability that the summation of two distinct row vectors is not equal to $\mathbf{0}$ is $(1-I_2)$; and there are $\binom{r}{2}$ of choice of any 2 row vectors. Therefore the probability that $NZ(2)$ happens can be expressed as $\Pr(NZ(2))=(1-I_2)^{\binom{r}{2}}$.

Further, for every integer $3\le q\le r$,

$$\Pr(\cap_{i=2}^{q}NZ(i))=\Pr(NZ(q)\mid\cap_{i=2}^{q-1}NZ(i))\Pr(\cap_{i=2}^{q-1}NZ(i)), \quad (8)$$

where $\Pr(NZ(q)\mid\cap_{i=2}^{q-1}NZ(i))$ is the probability that the summation of any q row vectors is not equal to $\mathbf{0}$, conditioned on that the summation of any w row vectors is not equal to $\mathbf{0}$, $1<w<q$. A recursive application of equation (8), together with a similar analysis leading to $\Pr(NZ(2))$, allows us to conclude that the probability that $\mathbf{B}_{r\times M}$, $r\le M$, is of full rank can be obtained as

$$F(r)\;\;=\;\;\Pr(\cap_{i=2}^{r}NZ(i))=\prod_{q=2}^{r}\left[(1-I_q)^{\binom{r}{q}}\right].$$

■

Now we shall derive I_q, which is required in Lemma 2. To obtain I_q, 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. Assume that summing the first $q-1$ row vectors generates a row vector $\mathbf{S}_{q-1}$ with degree i, i.e. a row vector that carries i number of 1s. We can summarize the conditions where its degree changes to j when one additional row vector being added as follow. Firstly, the additional row vector is assumed to contain a, $0\le a\le i$, number of 1s in the same positions where the i number of 1s in $\mathbf{S}_{q-1}$ occur. Moreover, it also need $b=j-i+a$, $0\le b\le M-i$, number of 1s in positions where the corresponding positions in $\mathbf{S}_{q-1}$ contain 0 only. Therefore the degree of the q^{th} (additional) row vector $\mathbf{v}_q$ should be $\deg(\mathbf{v}_q)=a+b$; $b=j-i+a$ and $0\le a\le i$, $0\le b\le M-i$. It follows that the probability that the additional row vector

$\mathbf{v}_q$ causes a transition from degree i (in $\mathbf{S}_{q-1}$) to a degree j (in $\mathbf{S}_q$), conditioned on that $\mathbf{v}_q$ has a degree $(a+b)$, can be expressed as $\frac{\binom{i}{a}\binom{M-i}{b}}{\binom{M}{a+b}}$.

Based on the above analysis, we can derive the Q_{ij} [8] as:

$$Q_{ij} = \begin{cases} \sum\limits_{\substack{0\le a\le \min(M-j,i)\\ b=j-i+a}} \Omega_{a+b}\dfrac{\binom{i}{a}\binom{M-i}{b}}{\binom{M}{a+b}}, & i<j \\ \sum\limits_{\substack{1\le a\le \min(M-j,i)\\ b=j-i+a}} \Omega_{a+b}\dfrac{\binom{i}{a}\binom{M-i}{b}}{\binom{M}{a+b}}, & i=j \\ \sum\limits_{\substack{i-j\le a\le \min(M-j,i)\\ b=j-i+a}} \Omega_{a+b}\dfrac{\binom{i}{a}\binom{M-i}{b}}{\binom{M}{a+b}}, & i>j \end{cases}$$

where Ω_d, $1 \le d \le M$ is the degree distribution of rateless codes, which is defined in Section IV.

Now we are ready to analyze I_q.

Lemma 3. *Let I_q denote the probability that $\sum_{i=1}^{q}\mathbf{v}_i = 0$, conditioned on that the summation of any w row vectors is not equal to $\mathbf{0}$, where $\mathbf{0}$ is a $1\times M$ row vector with all elements equal to 0, $w \in \mathbb{Z}^+$, $1 < w < q$. Let $\mathbf{Tr}$ be a $M\times M$ transition matrix with dimension $M\times M$ whose $(j,i)^{th}$ element equal to Q_{ij}. The matrix $\mathbf{Tr}$ can be expressed as:*

$$\mathbf{Tr} = \begin{pmatrix} Q_{11} & \cdots & Q_{(M-1)1} & Q_{M1} \\ Q_{12} & \cdots & Q_{(M-1)2} & Q_{M2} \\ \vdots & \ddots & \vdots & \vdots \\ Q_{1(M-1)} & \cdots & Q_{(M-1)(M-1)} & Q_{M(M-1)} \\ Q_{1M} & \cdots & Q_{(M-1)M} & Q_{MM} \end{pmatrix},$$

the probability I_q can be derived as:

$$I_{q,\ q\geq 2.} = (Q_{10}, Q_{20}, \ldots, Q_{M0})\mathbf{Tr}^{q-2}\cdot(\Omega_1, \Omega_2, \ldots, \Omega_M)^T.$$

Proof: To obtain I_q, we analyze the degree distribution of row vector $\mathbf{S}_w$, which is the sum of w row vectors and the degree of $\mathbf{S}_w$ should not equal to 0. Let $\mathbf{D}^w = (D_1^w, \ldots, D_M^w)^T$ 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, $1 \le i \le M$. When $w=1$, the degree distribution $\mathbf{D}^1$ is obviously $(\Omega_1, \Omega_2, \ldots, \Omega_M)^T$. To evaluate the degree distribution of the sum of w random row vectors, we first consider the degree distribution of the sum of $w-1$ row vectors. The degree distribution of the sum of w random row vectors can be considered as the degree distribution of the sum of $w-1$ random row vectors with an extra row vector $\mathbf{x}$ added, which causes a transition from the degree distribution of the sum of $w-1$ random row vector to the degree distribution of the sum of w random row vectors. For $w \geq 2$, the relationship can be analytically described as:

$$D_m^w = (Q_{1m}, Q_{2m}, \ldots, Q_{Mm})(D_1^{w-1}, \ldots, D_M^{w-1})^T.$$

From the above equation, it follows that:

$$\begin{aligned}\mathbf{D}^w =& (D_1^w, \ldots, D_M^w)^T \\ =& \begin{pmatrix} Q_{11} & \cdots & Q_{(M-1)1} & Q_{M1} \\ Q_{12} & \cdots & Q_{(M-1)2} & Q_{M2} \\ \vdots & \ddots & \vdots & \vdots \\ Q_{1(M-1)} & \cdots & Q_{(M-1)(M-1)} & Q_{M(M-1)} \\ Q_{1M} & \cdots & Q_{(M-1)M} & Q_{MM} \end{pmatrix}\begin{pmatrix} D_1^{w-1} \\ D_2^{w-1} \\ \vdots \\ D_{M-1}^{w-1} \\ D_M^{w-1}\end{pmatrix} \\ =& \mathbf{Tr}^{w-1}\cdot(\Omega_1, \Omega_2, \ldots, \Omega_M)^T.\end{aligned}$$

As an easy consequence of the above equation, I_q can be obtained:

$$\begin{aligned} I_q &= D_0^q = \sum_{i=1}^{M} D_i^{q-1}Q_{i0} \\ &= (Q_{10}, Q_{20}, \ldots, Q_{M0})\mathbf{D}^{q-1} \\ &= (Q_{10}, Q_{20}, \ldots, Q_{M0})\mathbf{Tr}^{q-2}\cdot(\Omega_1, \Omega_2, \ldots, \Omega_M)^T. \end{aligned}$$

■

B. Analysis of the minimum number of transmissions

Let ρ_L be the decoding success probability of a receiver who have already successfully receive L, $L \geq M$, packet and $\rho_L = \mathbf{u}(M)^T(\mathbf{R}_M)^{(L-1)}\mathbf{u}(1)$ according to Theorem 1. Denote by $\overline{C}$ the total number of transmissions the BS needs in order to meet the objective $\Pr(\eta) \geq 1-\epsilon$. The probability that all the M source packets can be successfully received by all N receives after $\overline{C}$ transmissions by the BS can be expressed as:

$$\Pr(\eta_{M,\overline{C}}) = \prod_{i=1}^{N}\Pr(\overline{C}, M, P_i),$$

where

$$\Pr(\overline{C}, M, P_i) = \sum_{L=M}^{\overline{C}} \binom{\overline{C}}{L} P_i^L (1-P_i)^{\overline{C}-L}\rho_L.$$

Therefore

$$\Pr(\eta_{M,\overline{C}}) = \prod_{i=1}^{N}\left(\sum_{L=M}^{\overline{C}} \binom{\overline{C}}{L} P_i^L (1-P_i)^{\overline{C}-L}\rho_L\right). \quad (9)$$

Inserting the results of equation 7 into the above equation, equation 9 can be rewritten as:

$$\prod_{i=1}^{N}\left(\sum_{L=M}^{\overline{C}} \binom{\overline{C}}{L} P_i^L (1-P_i)^{\overline{C}-L}\rho_L\right) \geq 1-\epsilon. \quad (10)$$

Using equation (10), the minimum number of transmissions required by the BS to meet the objective $\Pr(\eta) \geq 1-\epsilon$ can be readily computed.

V. Simulation Results

In this section, we verify our analytical results using simulations.

We set the number of source packets to be 5 and the number of receivers to be 6. The degree distribution of the rateless code follows the widely used Luby's Ideal Soliton distribution [6]. 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

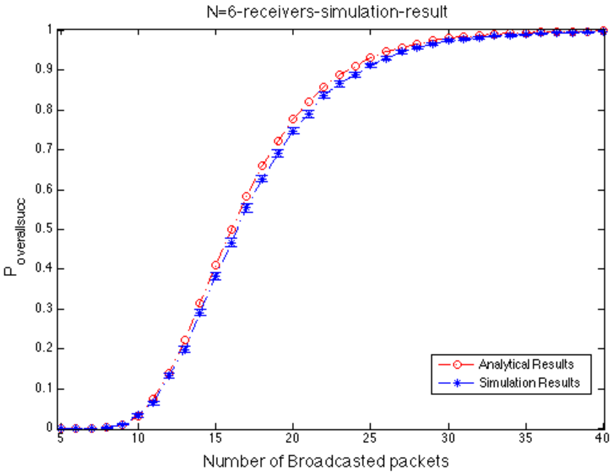

Figure 2. The Probability of successfully decoding 5 source packets by 6 receivers with packet transmission successful probabilities of the 6 receivers being 0.4, 0.5, 0.6, 0.7, 0.8 and 0.9 respectively. Simulations using other packet transmission successful probabilities showed the same match between analytical and simulation results.

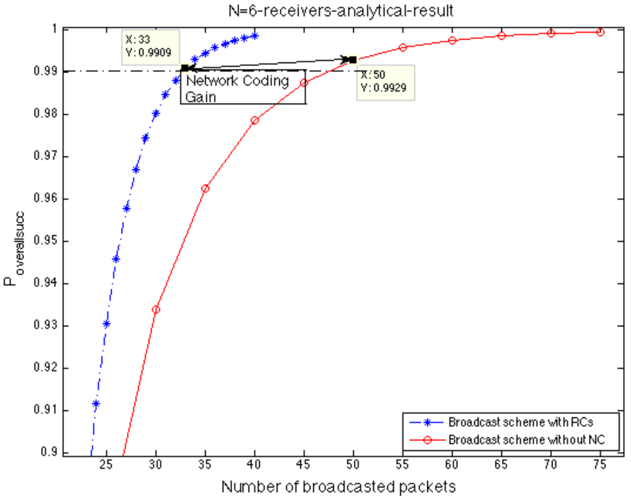

Figure 3. The probabilities of successfully decoding 5 source packets by 6 receivers with and without using network coding. The transmission success probabilities of the receivers are 0.4, 0.5, 0.6, 0.7, 0.8 and 0.9 respectively. Simulations using other packet transmission successful probabilities showed the same trend.

rateless code by the BS. Each simulation is repeated 10000 number of times and the average result is presented in the figs, 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, particularly the accuracy of the approximation in equation 3.

In Fig. 3, we further compare the successful probabilities with and without using network coding. As shown in Fig. 3, it can be seen that the the use of network coding, particularly rateless codes, yields much better performance in terms of the number of transmitted packets required to meet the same reliability constraint. In comparison, when network coding is not used, the BS need to transmit more packets to meet the reliability constraint. For example, when the reliability constraint is set to be 0.99, 33 transmissions are needed when rateless codes are used, while 50 broadcasts are required when network coding is not used, i.e. a saving of 50% transmissions is obtained when using network coding.

VI. Conclusion

In this paper we studied reliable broadcast in a wireless network with one common transmitter 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 constraint without using acknowledgement/feedback from the receivers. The reliability constraint is given by that the probability that all receivers successfully receive all broadcast packets is above a pre-defined threshold. Theoretical analysis has been conducted on the performance of the broadcast with network coding. On the basis of the analysis, the number of transmissions required by the transmitter to meet the reliability constraint is obtained. It was shown that the use of network coding can significantly reduce the number of transmissions required to meet the same reliability constraint, compared with that without using network coding. Simulations were conducted which indicated the good accuracy of the analytical results.

In the future, we plan to expand the analysis to incorporate the situation that the exact channel conditions of receivers are not known, instead one only has some 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] H. D. T. Nguyen, T. Le-Nam, and H. Een-Kee, "On transmission efficiency for wireless broadcast using network coding and fountain codes," *IEEE Commu Letters*, vol. 15, no. 5, pp. 569–571, 2011.

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

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

[7] E. Hyytia, T. Tirronen, and J. Virtamo, "Optimal degree distribution for LT codes with small message length," in *Proceedings of 26th IEEE INFOCOM*, 2007, pp. 2576–2580.

[8] 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.

[9] R. Karp, M. Luby, and A. Shokrollahi, "Finite length analysis of LT codes," in *Proceedings of IEEE ISIT*, 2004, p. 39.

[10] A. Shokrollahi, *Theory and applications of Raptor codes*. Springer-Verlag, 2009.

[11] T. Rappaport, *Wireless Communications: Principles and Practice*, ser. Prentice Hall Communication Engineering and Emerging Technologies. Prentice Hall PTR, 2002.

[12] 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.