Fountain Code Design for Broadcasting Systems With Intermediate-State Users

Youngkil Suh, *Student Member, IEEE*, Jonghyun Baik, *Student Member, IEEE*, Nazanin Rahnavard, *Member, IEEE*, and Jun Heo, *Member, IEEE*

***Abstract*—Several studies on fountain codes have proposed degree distribution optimization schemes to maximize symbol recovery rate. However, if the number of transmitted coded symbols is limited or the channel erasure probability is high, it may be impossible that a user recovers all of the data symbols regardless of degree distribution employed by the source. In this study, we focus on a new system model where one source transmits fountain-coded symbols to multiple users who already possess some data symbols and coded symbols. Assuming that each user can transmit a feedback packet containing its own state information before the source transmits coded symbols, we propose two types of degree distribution design schemes that are suitable for the system model. Simulation results demonstrate the efficiency of our proposed schemes by comparing with conventional methods in terms of symbol recovery rate and full recovery rate.**

***Index Terms*—Degree distribution design, erasure codes, fountain codes, rateless codes.**

I. Introduction

FOUNTAIN codes [1]–[4] are representative forward error-correcting codes for the erasure channel [9]. A well-designed degree distribution enables the decoder to recover all k data symbols with $n_{\mathrm{R}} = (1 + \Delta)k$ received coded symbols, where Δ is a small positive number. Various studies [4]–[8] on design of degree distribution have introduced optimization schemes that maximize *symbol recovery rate* (SRR). Sanghavi [5] introduced a degree distribution optimization scheme that maximizes the asymptotic SRR when a fixed coding overhead $r := n_{\mathrm{R}}/k$ is given. Talari and Rahnavard [7] studied a degree distribution optimization with multiple objectives when multiple r's are given. Zeng *et al.* [6] regarded the overhead r of the received symbols as a random variable and proposed a best-effort optimization scheme that maximizes the average SRR.

In general, the previous studies assumed that users do not possess any data symbols and coded symbols before transmissions. In this work, we refer to such users as *empty-state users* (ESU). On the other hand, we consider the case where some users have received insufficient coded symbols at the *previous transmission*. Then they have already recovered several data symbols and possess some unreleased[1] coded symbols. We refer to such users as *intermediate-state users* (ISUs). In this paper, we describe how to design an efficient degree distribution for broadcasting systems with multiple ISUs in terms of SRR.

ISUs appear in several scenarios. For example, we can consider a case where a source transmits a finite number n_{T} of coded symbols to multiple ESUs. If n_{T} is large enough, most of the users can recover all of the data symbols. However, if some users are in a shadow area, they received many erased symbols and may fail to recover some data symbols. At this time, if additional resources are available for transmitting coded symbols, the users received the coded symbols as ISUs. In this case, a performance improvement can be achieved if the degree distribution employed by the source is designed by considering the states of the ISUs. In addition, we can consider a wireless sensor network as an example. In wireless sensor networks, some global and important information is broadcast to distributed sensor nodes by a control unit such as a satellite. Moreover, the circumstances are considered to be hostile in general. Due to the fragile channel conditions, the transmission can be terminated before the sensor nodes recover all of the data symbols.

In this paper, we assume the availability of feedback to inform the source of each user's state. There are some previous studies [11]–[15] on fountain coding schemes using feedback. The previous works mainly dealt with one-to-one transmission scenario. Hagedorn *et al.* [11] proposed a shifted LT (SLT) coding scheme that employs multiple degree distributions modified from the RSD. Kim and Lee [12] proposed a similar manner with growth codes [18] using multiple feedback packets to improve intermediate performance. Talari and Rahnavard in [15] proposed LT coding scheme using two types of feedback and enhance the decoding performance for small k.

The authors in [13] proposed LT feedback codes and Raptor feedback codes, which showed significant improvements in terms of coding overhead and encoding/decoding complexity by employing a few feedback packets. In [13], the feedback was used to exclude the recovered data symbols from the encoding process. However, the method is not scalable for multi-user

[1] *Unreleased* indicates the state where an coded symbol's degree is greater than or equal to *two* after removing the edges that correspond to recovered data symbols on the bipartite graph.

Manuscript received September 26, 2014; revised January 29, 2015 and April 4, 2015; accepted April 19, 2015. Date of publication April 30, 2015; date of current version September 3, 2015. This work (Grant No. C0192210) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded by Korea Small and Medium Business Administration in 2014 and the U.S. National Science Foundation under Grant No. ECCS-1056065. The associate editor coordinating the review of this paper and approving it for publication was A. Graell i Amat.

Y. Suh, J. Baik, and J. Heo are with the School of Electrical Engineering, Korea University, Seoul 136-701, Korea (e-mail: dongzizuk@korea.ac.kr; bell211@korea.ac.kr; junheo@korea.ac.kr).

N. Rahnavard is with the Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816 USA (e-mail: nazanin@eecs.ucf.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2015.2428244

systems because the sets of the recovered symbols for each user are different in general due to random erasures. To make our scheme scalable for a multi-user system, in this paper no data symbol is excluded. In addition, each user transmits a feedback packet only once before the transmission of coded symbols, while in [13] the user transmits a few feedback packets during the transmission.

Sejdinović *et al.* [16] studied a fountain code design for a data multicast system when the users have some data symbols. In [16], no data symbol is excluded during encoding process because the authors assumed a multi-user system. Similarly, we also assume a multi-user system, so no data symbol is excluded as well in this paper. Moreover, Our proposed scheme is efficiently applicable for the case where the users have not only some data symbols but also some coded symbols and the erasure rates of the users may be different.

In our work, we propose two types of degree distribution design schemes for the system model. These two schemes are based on the results of [6]; they are a fairly generalized optimization scheme and a suboptimal code generating scheme.

The remainder of this paper is organized as follows. In Section II we review some previous works and in Section III our system model is specified. In Section IV, we describe our proposed optimization scheme for the system model, and an alternative design scheme is explained in Section V. In Section VI, we evaluate the performance of the degree distributions designed by the proposed optimization schemes and we provide our conclusions in Section VII.

II. Conventional Optimization Problem

In this paper, we establish an optimization problem by modifying the optimization scheme proposed in [6]. Zeng *et al.* [6] regarded the coding overhead r as a random variable and the optimization scheme was provided to maximize the average SRR over r given the probability distribution $h(r)$, which is referred to as *overhead distribution*. Note that it is commonly assumed that the source is informed of $h(r)$ in our work and [6]. The objective function defined in [6] is $\int_0^\infty h(r)y(r,\Omega(\cdot))dr$, where $y(r,\Omega(\cdot))$ is the asymptotic SRR obtained by AND-OR tree analysis [17] and can be represented by

$$y\left(r,\Omega(\cdot)\right)=\inf\left\{t\in[0,1):r\Omega'(t)+\ln(1-t)<0\right\}. \quad (1)$$

Using Riemann sum, the objective can be rewritten as

$$\max_{\Omega(\cdot)}\sum_{i=1}^{N^{\mathrm{R}}}p[i]y\left(\hat{r}_i,\Omega(\cdot)\right), \quad (2)$$

where $p[i]$ is a discretized overhead distribution of $h(r)$, $\hat{r}_i$ is an arbitrary value in i-th subinterval and N^{R} denotes the number of subintervals. The discretized overhead distribution is given by $p[i]=(r_i-r_{i-1})h(\hat{r}_i)/\sum_{i=1}^{N^{\mathrm{R}}}(r_i-r_{i-1})h(\hat{r}_i)$. In this paper, we use both of $h(r)$ and $p[i]$ for the sake of convenience.

Zeng *et al.* [6] also proposed a heuristic approach which does not require solving any optimization problem. The degree distribution $\Omega^+(x)$ obtained by the approach was referred to as *linearly mixed degree distribution* and it can be obtained by

$$\Omega^+(x)=x\Pr[0<r\le\ln 2]+x^2\Pr[\ln 2<r\le 1]+\Omega_{\mathrm{R}}(x)\Pr[r>1], \quad (3)$$

where $\Omega_{\mathrm{R}}(x)$ denotes an RSD with suitable parameters (c,δ). In Section V of this paper, we propose a generalized version of this scheme.

TABLE I
Important Acronyms

Acronym	Full term	Notation
ESU	Empty-state user	-
FRP	Full recovery probability	-
GASRR	Global average symbol recovery rate	$y_{\mathrm{g}}(\Omega(\cdot))$
ISU	Intermediate-state user	-
LCSRR	Local conditional symbol recovery rate	$y_m(r,\Omega(\cdot))$
LASRR	Local average symbol recovery rate	$y_m(\Omega(\cdot))$
PUI	Previously unrecovered input	-
PRI	Previously recovered input	-
RO	Remaining output	-
SDD	Single degree distribution	-
SRR	Symbol recovery rate	-
SRSD	Shifted robust soliton distribution	-
USI	User state information	-

III. System Model

Note that Table I shows important acronyms used in this paper. We first specify the flow of our proposed coding scheme as follows.

After the end of the *previous transmission*, some users fail to decode some input symbols due to the lack of received symbols. The users are regarded as ISUs in the *current transmission*. The recovered input symbols and the unrecovered input symbols are referred to as *previously recovered input* (PRI) symbols and *previously unrecovered input* (PUI) symbols, respectively. In addition, the unreleased output symbols, which can contribute to decoding later, are referred to as *remaining output* (RO) symbols.

In this work, we focus on the *current transmission*, which can be divided into the following phases. (A) The source collects each ISU's state information via a feedback packet. (B) The source designs an efficient degree distribution from one of our proposed schemes, which are described in Sections IV and V. (C) The source generates output symbols and broadcasts them continuously.

Let $\mathcal{B}=\{b_1,b_2,\cdots,b_k\}$ be a set (a sequence) of input symbols of the same length (bits), n_{T} be the number of output symbols transmitted at a source and n_{R} be the number of output symbols received by a user. In addition, we assume that $b_i\neq b_j$ for $i\neq j$ such that $|\mathcal{B}|=k$ without loss of generality, where $|\mathcal{B}|$ denotes the cardinality of a set $\mathcal{B}$.

Consider a case where a single ISU U_1 exists, and let $\mathcal{B}_1(\subset\mathcal{B})$ denote the set of PUI symbols of U_1. The user U_1 has already recovered the input symbols in $\mathcal{B}\setminus\mathcal{B}_1$ so the user regards the

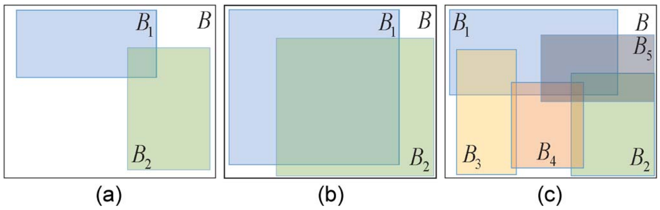

Fig. 1. (a) Small M and small $|\mathcal{B}_m|$, (b) Small M and large $|\mathcal{B}_m|$, (c) Large M and small $|\mathcal{B}_m|$. The union $\bigcup_{m=1}^{M} \mathcal{B}_m$ approaches to $\mathcal{B}$ as M and $|\mathcal{B}_m|$ increase.

elements only in $\mathcal{B}_1$ as the input symbols that need to be recovered. In this case, if we assume that the source is informed of the elements of $\mathcal{B}_1$ by a k-bit feedback, then we can consider two options for encoding of the input symbols in $\mathcal{B}_1$. The first option is to encode only the input symbols in $\mathcal{B}_1$ and the second option is to encode all of the input symbols in $\mathcal{B}$ regardless of $\mathcal{B}_1$. J. H. Sørensen *et al.* [14] showed that the first option weakens the code performance when the source employs an RSD. The authors also showed that the first option with a few adjustments of degree distribution provides a small gain.

However, the first option is not appropriate for multi-user systems because in most cases the sets of PUI symbols for the users are different. Consider a broadcasting system with multiple users $U_1, \cdots, U_M$ and let the corresponding set of PUI symbols of the users be denoted by $\mathcal{B}_1, \cdots, \mathcal{B}_M$, respectively. Every $\mathcal{B}_m$ is a subset of $\mathcal{B}$ and its elements are selected randomly, because the input symbols are recovered in an arbitrary order due to the nature of fountain codes. Fig. 1 shows graphically that $\bigcup_{m=1}^{M} \mathcal{B}_m \to \mathcal{B}$ as M and $|\mathcal{B}_m|$ increase. This means that none of the input symbols in $\mathcal{B}$ should be excluded when M and $\mathcal{B}_m$'s are sufficiently large.

Our system model is specified as shown in Fig. 2, which comprises a single source S, and M multiple users $U_1, \cdots, U_M$. In Fig. 2, the state of each user can be represented by three parameters that are defined as follows.

Definition 1: The state of a user U_m is represented by $(z_m, v_m, \Gamma_m(\cdot))$, which is referred to as *user state information* (USI). The three factors are defined as

$$z_m \triangleq \frac{|\mathcal{B}_m|}{k},$$
$$v_m \triangleq \frac{\text{No. of RO symbols for } U_m}{k},$$
$$\Gamma_m(x) \triangleq \sum_{d\geq 2} \Gamma_{m,[d]} x^d, \tag{4}$$

where the coefficients of $\Gamma_m(x)$ are defined as

$$\Gamma_{m,[d]} \triangleq \frac{\text{No. of degree-}d\text{ RO symbols for } U_m}{\text{No. of RO symbols for } U_m}. \tag{5}$$

In (5), the *degree* means the number of neighbors in $\mathcal{B}_m$.

In Definition 1, z_m and v_m are the ratios of the amounts of PUI symbols and RO symbols to k, respectively. The degree distribution $\Gamma_m(x)$ is the *statistical* degree distribution of the RO symbols for U_m. As mentioned previously, the RO symbols are unreleased output symbols so their degrees are greater than or equal to two, i.e., $\Gamma_{m,[1]} = 0$ for $m = 1, \cdots, M$.

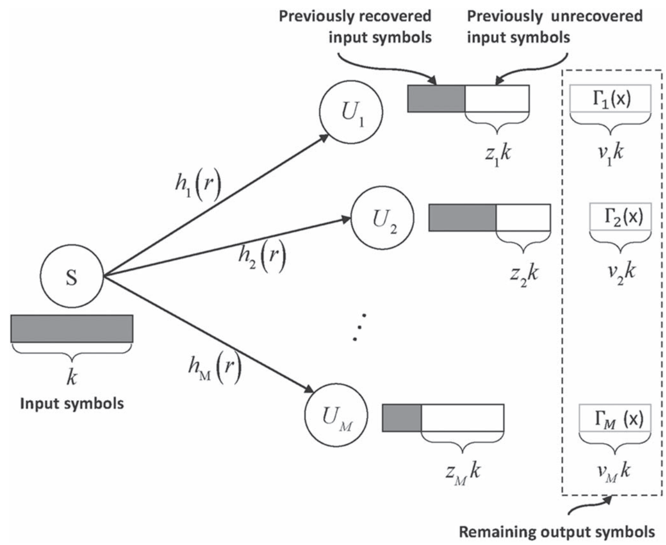

Fig. 2. Fountain-coded symbol broadcasting system with M ISUs. Each user U_m has $z_m k$ PUI symbols and $v_m k$ RO symbols with a degree distribution $\Gamma_m(x)$. The number of output symbols received by U_m from S depends on the overhead distribution $h_m(r)$.

Now we consider the size of a feedback packet. By transmitting a feedback packet, each user informs S of its own USI, which is composed of two decimals, z_m and v_m, and a degree distribution $\Gamma_m(x)$. The USI can be represented as integer values; as shown in Definition 1,$z_m k$ is a non-negative integer and $v_m k \Gamma_m(x)$ is a polynomial with non-negative integer coefficients. The integer $z_m k$ is always less than k, so $\lceil \log_2 k \rceil$ bits are required for a feedback of $z_m k$. Similarly, an arbitrary number $v_m k \Gamma_{m,[d]}$ is always less than $\max_d v_m k \Gamma_{m,[d]}$, so $\lceil \log_2(\max_d v_m k \Gamma_{m,[d]}) \rceil$ bits are required to represent a coefficient of $\Gamma_m(x)$. Note that the coefficient of x of $\Gamma_m(x)$ is always *zero*. Then all of the coefficients of $x^2, \cdots, x^{D_m}$ of $\Gamma_m(x)$ can be represented by $(D_m - 1) \cdot \lceil \log_2(\max_d v_m k \Gamma_{m,[d]}) \rceil$, where D_m is a sufficiently large integer to represent $\Gamma_m(x)$ with high enough accuracy. In practical cases, the coefficients of x^d for small d's are much greater than those for high d's, which can be represented with smaller bits. Thus we expect that the size of a feedback packet can be reduced significantly by adopting a more efficient method but in this paper we do not consider other methods to reduce the amount of feedback.

IV. Scheme-1: Optimal Degree Distribution Based on And-Or Tree Analysis

AND-OR tree analysis allows us to estimate the asymptotic SRR, which is considered to be an upper bound of the SRR of the finite-length fountain codes. In general, the SRR predicted by AND-OR tree analysis (asymptotic performance) is almost the same as that of the finite-length fountain codes if the codes are sparse enough. Otherwise, code performance do not matches the asymptotic performance.

In this section, we describe our first degree distribution design scheme, which we refer to as SCHEME-1. SCHEME-1 is divided into two steps. First, we explain how to design an asymptotically optimal degree distribution using the AND-OR tree analysis. When the obtained distribution is employed for finite-length fountain codes, its SRR performance may be significantly different from the asymptotic performance. Thus, we employ an optimization scheme with finite-length analysis, which is a revised version of AND-OR tree analysis. By using the finite-length analysis, we can reduce the difference between the code performance and the asymptotic performance.

A. Optimization With Asymptotic Analysis

In this paper, our goal is to maximize the expected sum of the number of *additionally recovered input symbols* out of PUI symbols. Let $\mathcal{C}_m(r, \Omega(\cdot))$ denote the set of the additionally recovered input symbols in the current transmission. Note that $\mathcal{C}_m(r, \Omega(\cdot)) \in \mathcal{B}_m$ and $\mathcal{C}_m(r, \Omega(\cdot))$ depends on r and $\Omega(\cdot)$ which denotes the degree distribution employed by S at the current transmission. Then our objective function can be represented as $\mathbb{E}_r[\sum_{m=1}^{M} |\mathcal{C}_m(r, \Omega(\cdot))|]$.

Now, we define three quantities to clarify the objective function.

Definition 2: Given r and $\Omega(\cdot)$, the *local conditional symbol recovery rate* (LCSRR), denoted by $y_m(r, \Omega(\cdot))$, is defined as

$$y_m(r, \Omega(\cdot)) \triangleq \frac{|\mathcal{C}_m(r, \Omega(\cdot))|}{|\mathcal{B}_m|}, \tag{6}$$

which represents the ratio of the additionally recovered input symbols relative to the PUI symbols for U_m with rk received output symbols.

Definition 3: Given $\Omega(\cdot)$ and $p_m[i]$, the *local average symbol recovery rate* (LASRR), denoted by $y_m(\Omega(\cdot))$, is defined as

$$y_m(\Omega(\cdot)) \triangleq \frac{\mathbb{E}_r[|\mathcal{C}_m(r, \Omega(\cdot))|]}{|\mathcal{B}_m|} = \frac{\sum_{i=1}^{N_m^{\mathrm{R}}} \left|\mathcal{C}_m(\hat{r}_i, \Omega(\cdot))\right| p_m[i]}{|\mathcal{B}_m|}, \tag{7}$$

where N_m^{R} denotes the number of subintervals of $h_m(r)$ for the Riemann sum. LASRR $y_m(\Omega(\cdot))$ is the expected value of LCSRR for U_m.

Definition 4: Given $\Omega(\cdot)$ and $p_m[i]$ for $m = 1, \cdots, M$, the *global average symbol recovery rate* (GASRR), denoted by $y_{\mathrm{g}}(\Omega(\cdot))$, is defined as

$$y_{\mathrm{g}}(\Omega(\cdot)) \triangleq \frac{\mathbb{E}_r\left[\sum_{m=1}^{M} |\mathcal{C}_m(r, \Omega(\cdot))|\right]}{\sum_{m=1}^{M} |\mathcal{B}_m|}. \tag{8}$$

The GASRR is defined as the ratio of the sum of the number of the additionally recovered input symbols relative to the sum of the number of PUI symbols for all users. The numerator of (8) is the objective mentioned above. The denominator is independent of $\Omega(\cdot)$ so it can be regarded as a constant. Thus the objective function is equivalent to $y_{\mathrm{g}}(\Omega(\cdot))$.

The objective function $y_{\mathrm{g}}(\Omega(\cdot))$ can be expressed as follows:

$$\begin{aligned} y_{\mathrm{g}}(\Omega(\cdot)) &= \frac{\mathbb{E}_r\left[\sum_{m=1}^{M} \frac{|\mathcal{C}_m(r,\Omega(\cdot))|}{k}\right]}{\sum_{m=1}^{M} \frac{|\mathcal{B}_m|}{k}} \qquad (9) \\ &= \frac{\mathbb{E}_r\left[\sum_{m=1}^{M} \frac{|\mathcal{B}_m|}{k} \frac{|\mathcal{C}_m(r,\Omega(\cdot))|}{|\mathcal{B}_m|}\right]}{\sum_{m=1}^{M} z_m} \\ &= \frac{\sum_{m=1}^{M} \left\{z_m \mathbb{E}_r\left[\frac{|\mathcal{C}_m(r,\Omega(\cdot))|}{|\mathcal{B}_m|}\right]\right\}}{\sum_{m=1}^{M} z_m} \\ &= \rho \sum_{m=1}^{M} z_m y_m(\Omega(\cdot)) \qquad (10) \end{aligned}$$

where $\rho = \left(\sum_{m=1}^{M} z_m\right)^{-1}$. From (6) and (7), we can rewrite (10) as

$$y_{\mathrm{g}}(\Omega(\cdot)) = \rho \sum_{m=1}^{M} \sum_{i=1}^{N_m^{\mathrm{R}}} z_m p_m[i] y_m\left(\hat{r}_i, \Omega(\cdot)\right). \tag{11}$$

Now we employ AND-OR tree analysis to obtain the asymptotic LCSRR $y_m(r, \Omega(\cdot))$. The conventional AND-OR tree analysis (1) needs to be modified to reflect new parameters of USI.

First, we investigate the *reduced degree distribution* for U_m, which we can observe in the bipartite graph after removing the edges connected to $\mathcal{B} \setminus \mathcal{B}_m$. The following lemma shows the relationship between the degree distribution employed by S and the reduced degree distribution for U_m.

Lemma 1: Let the degree distribution employed by S and the reduced degree distribution for U_m be denoted by $\Omega(x)$ and $\Omega_m(x)$, respectively. Then $\Omega_m(x)$ can be represented as

$$\Omega_m(x) \approx \Omega(1 - z_m + z_m x). \tag{12}$$

Proof of this lemma was briefly described in [16] as well, and here we provide the proof in detail in Appendix A.

In the proposed system model, each user U_m has two types of the output symbols. The first is the additionally received output symbols from S with an reduced degree distribution of $\Omega(1 - z_m + z_m x)$. The second is the RO symbols with a statistical degree distribution of $\Gamma_m(x)$. If U_m has rk additionally received output symbols, U_m has $(r + v_m)k$ output symbols including the RO symbols. Hence the degree distribution $\Phi_m(x)$ of all of the output symbols can be represented by the weighted summation of $\Omega(1 - z_m + z_m x)$ and $\Gamma_m(x)$ as follows:

$$\Phi_m(x) = \frac{r\Omega(1 - z_m + z_m x) + v_m \Gamma_m(x)}{r + v_m}. \tag{13}$$

Note that the input node degree distribution of PUI symbols is preserved although the edges connected to PRI symbols are removed. Then we can apply the conventional AND-OR tree analysis (1), to obtain the asymptotic LCSRR $y_m(r, \Omega(\cdot))$.

From (13) and (1), we have the asymptotic LCSRR

$$y_m\left(r,\Omega(\cdot)\right)=\inf\left\{t\in[0,1):\frac{(r+v_m)}{z_m}\frac{\partial}{\partial t}\Phi_m(t)+\ln(1-t)<0\right\}. \quad (14)$$

where $(r+v_m)/z_m$ is the relative overhead for U_m, which denotes the ratio of the number $(rk+v_mk)$ of the given output symbols relative to z_mk PUI symbols. Now we can obtain the asymptotic LASRR $y_m(r,\Omega(\cdot))$ from (13) and (14). Finally, our optimization problem is completed as (15), shown at the bottom of the page.

B. Optimization With Finite Length Analysis

In general, the SRR measured from simulations may not match well the asymptotic performance due to a shortage of ripple symbols,[2] which is caused by variance in the number of ripple symbols. For example, when $r=1$, the soliton distribution $\Omega(x)=\sum_{d=2}^{\infty}\frac{x^d}{d(d-1)}$ [4] is asymptotically optimal for an ESU because it generates one ripple on average at each iteration of decoding. However, since the number of ripple symbols is random, there might be no ripple symbols during the decoding process in finite-length cases.

Shokrollahi [4] provided a modified version of AND-OR tree analysis to maintain a sufficient number of the ripples, which is called *finite-length analysis*. Shokrollahi regarded the transitions in the number of the ripples as a random walk and increased the number of the ripples by considering the standard deviation of the random walk. The key idea of this analysis is to make the expected number of the ripples greater than or equal to $\alpha\sqrt{(1-t)k}$, where α is a suitable positive constant. As a result, [4] provides an optimization problem that obtains a degree distribution, which satisfies the following inequality constraint;

$$r\Omega'(t)+\ln\left(1-t-\alpha\sqrt{\frac{1-t}{k}}\right)\geq 0, \quad (17)$$

for $t\in[0,1-\delta]$, where δ is a suitably small positive constant.

[2]Ripple symbols mean output symbols of degree 1 in a bipartite graph after removing all of the edges connected with recovered input symbols.

Applying the similar approach, we can formulate the degree distribution optimization problem as (16), shown at the bottom of the page, by adding a term $\alpha\Re\{\sqrt{(\eta y_m(r,\Omega_{\mathrm{a}}^*(\cdot))-t)/z_mk}\}$ to (15). Here, η is a constant slightly less than one.

Note that there are three modifications in the square root terms of (16) and (17). The followings are the rationales behind these modifications.

- The number of the input symbols that we desire to recover is z_mk, not k.
- Note that $\alpha\sqrt{(1-t)/k}$ in (16) contributes to the expected number of ripple symbols for $0\leq t<1$. When r is small, full recovery may not be possible, i.e., achievable symbol recovery rate is less than 1. We regard $y_m(r,\Omega_{\mathrm{a}}^*(\cdot))$ as a target performance, which is the LCSRR of the asymptotically optimal solution $\Omega_{\mathrm{a}}^*(\cdot)$. Thus $(1-t)$ is replaced with $(\eta y_m(r,\Omega_{\mathrm{a}}^*(\cdot))-t)$ to maintain the number of the ripples only in $0\leq t\leq \eta y_m(r,\Omega_{\mathrm{a}}^*(\cdot))$.
- $\Re\{\cdot\}$ is added to prevent the optimization problem from generating an imaginary number.

V. SCHEME-2: LINEARLY MIXED DEGREE DISTRIBUTION

The optimization problems (15) and (16) in the previous section require a significant amount of computations for AND-OR tree analysis. Hence, we now propose a simple heuristic design scheme, called SCHEME-2, which requires much fewer computations for AND-OR tree analysis. We refer to the degree distribution designed obtained by SCHEME-2 as the *linearly mixed degree distribution* $\Omega^+(\cdot)$. In the following subsections we explain the key ideas of designing the linearly mixed degree distribution for a single-user system and then extend it to a multi-user system.

A. Single-User Case

In this subsection, we consider a single user with USI $(z,v,\Gamma(\cdot))$ and overhead distribution $h(r)$. First, we define *single degree distribution* (SDD) as follows.

Definition 5: Let $\Theta_d(x)$ be composed of a single degree component as follows:

$$\Theta_d(x)\triangleq x^d,\ \text{for } d=1,2,\cdots. \quad (18)$$

$$\Omega_{\mathrm{a}}^*(\cdot)\triangleq\arg\max_{\Omega(\cdot)}\rho\sum_{m=1}^{M}\sum_{i=1}^{N_m^r}z_mp_m[i]y_m\left(\hat{r}_i,\Omega(\cdot)\right)$$
$$\text{where } y_m(\hat{r}_i)=\inf\left\{t\in[0,1):\hat{r}_i\Omega'(1-z_m+z_mt)+\frac{v_m}{z_m}\Gamma_m'(t)+\ln(1-t)<0\right\} \quad (15)$$

$$\Omega^*(\cdot)\triangleq\arg\max_{\Omega(\cdot)}\rho\sum_{m=1}^{M}\sum_{i=1}^{N_m^r}z_mp_m[i]y_m\left(\hat{r}_i,\Omega(x)\right)$$
$$\text{where } y_m(\hat{r}_i)=\inf\left\{t\in[0,1):\hat{r}_i\Omega'(1-z_m+z_mt)+\frac{v_m}{z_m}\Gamma_m'(t)+\ln\left(1-t-\alpha\Re\left\{\sqrt{\frac{\eta y_m\left(\hat{r}_i,\Omega_{\mathrm{a}}^*(\cdot)\right)-t}{z_mk}}\right\}\right)<0\right\} \quad (16)$$

The linearly mixed degree distribution proposed in [6] is a weighted sum of the two SDD and one RSD as (3). In this paper, we define a generalized version of linearly mixed degree distribution as shown in the following definition.

Definition 6: A linearly mixed degree distribution $\Omega^{+}(\cdot)$ is defined as a weighted sum of several SDDs $\Theta_d(x)$ and a modified RSD $\Omega_{\mathrm{MR}}(x)$, i.e.,

$$\Omega^{+}(x) = \sum_{d=1}^{k} w_d \Theta_d(x) + \left(1 - \sum_{d=1}^{k} w_d\right) \Omega_{\mathrm{MR}}(x), \tag{19}$$

where $w_d \geq 0$ for $i = 1, \cdots, k$ and $\sum_{d=1}^{k} w_d \leq 1$. We describe $\Omega_{\mathrm{MR}}(x)$ later in this subsection.

First we describe how to set w_d for $d = 1, \cdots, k$ in a similar manner to that introduced in [6]. To set w_d, we find the interval of r where $\Theta_d(\cdot)$ is optimal. Thus we now describe the necessary conditions such that $\Theta_d(\cdot)$ is optimal.

Lemma 2: For a SDD $\Theta_d(x) = x^d$,

$$\Theta_d'(x) \geq \Theta_i'(x), \text{ for } x \in \left[\frac{d-1}{d}, \frac{d}{d+1}\right], \tag{20}$$

where i is an arbitrary positive integer and $\Theta'(x) = \frac{d}{dx}\Theta(x)$.

The proof of this lemma can be found in Appendix B.

Corollary 1: For SDD $\Theta_d(x) = x^d$,

$$\Theta_d'(x) \geq \Omega'(x), \text{ for } x \in \left[\frac{d-1}{d}, \frac{d}{d+1}\right], \tag{21}$$

where $\Omega(x)$ is an arbitrary degree distribution.

Proof: The proof of this corollary can be found in Appendix C. ■

Lemma 2 and Corollary 1 show that $\Theta_d'(x)$ is greater than or equal to the derivative of an arbitrary degree distribution in the interval $x \in \left[\frac{d-1}{d}, \frac{d}{d+1}\right]$. Now we recall AND-OR tree analysis;

$$y(r, \Theta_d(\cdot)) = \inf\left\{t \in [0,1) : r\Theta_d'(1-z+zt) + \frac{v}{z}\Gamma'(t) + \ln(1-t) < 0\right\}, \tag{22}$$

where $y(r, \Theta_d(\cdot))$ is the asymptotic SRR. If the infimum value exists in $t \in (\frac{\frac{d-1}{d}+z-1}{z}, \frac{\frac{d}{d+1}+z-1}{z}]$, $\Theta_d(\cdot)$ is optimal because $\Theta_d(1-z+zt)$ is greater than an arbitrary distribution $\Omega(1-z+zt)$ in the interval. Thus we can summarize necessary conditions such that $\Theta_d(\cdot)$ is optimal as the follows;

Condition 1: The infimum value of (22) is greater than $\frac{\frac{d-1}{d}+z-1}{z}$;

$$r\Theta_d'(1-z+zt) + \frac{v}{z}\Gamma'(t) + \ln(1-t) \geq 0, \quad \forall\, t \in \left(0, \frac{\frac{d-1}{d}+z-1}{z}\right]. \tag{23}$$

Condition 2: The infimum value of (22) is less than or equal to $\frac{\frac{d}{d+1}+z-1}{z}$;

$$\exists t \in \left(\frac{\frac{d-1}{d}+z-1}{z}, \frac{\frac{d}{d+1}+z-1}{z}\right]: \quad r\Theta_d'(1-z+zt) + \frac{v}{z}\Gamma'(t) + \ln(1-t) < 0. \tag{24}$$

By substituting $\frac{t+z-1}{z}$ with t in (23) and (24), we have simpler conditions (25) and (26), respectively:

$$r\Theta_d'(t) \geq g(t), \ \forall\, t \in \left(1-z, \frac{d-1}{d}\right], \tag{25}$$

$$\exists t \in \left(\frac{d-1}{d}, \frac{d}{d+1}\right] : r\Theta_d'(t) < g(t), \tag{26}$$

where $g(t) := -\frac{v}{z}\Gamma'\left(\frac{t+z-1}{z}\right) - \ln\frac{1-t}{z}$. Using (25) and (26), we can obtain the interval satisfying the necessary conditions (27) and (28), respectively;

$$r \geq \max_{t \in \left(1-z, \frac{d-1}{d}\right]} \frac{g(t)}{\Theta_d'(t)}. \tag{27}$$

$$r \leq g\left(\frac{d}{d+1}\right) \Big/ \Theta_d'\left(\frac{d}{d+1}\right). \tag{28}$$

Let $(r_d^{\mathrm{L}}, r_d^{\mathrm{R}}]$ denote the interval satisfying (27) and (28). Then the interval can be represented as the following recursions:

$$\begin{aligned} r_0^{\mathrm{R}} &= 0, \\ r_d^{\mathrm{L}} &= \min\left(z - v, \max\left(r_{d-1}^{\mathrm{R}}, \max_{t \in \left(1-z, \frac{d-1}{d}\right]} \frac{g(t)}{\Theta_d'(t)}\right)\right), \\ r_d^{\mathrm{R}} &= \min\left(z - v, \max\left(r_d^{\mathrm{L}}, g\left(\frac{d}{d+1}\right) \Big/ \Theta_d'\left(\frac{d}{d+1}\right)\right)\right). \end{aligned} \tag{29}$$

The first line of (29) is redundant but it is added to restrict the following r_d^{L} and r_d^{R} to a non-negative number. In the second and third lines, maximal values of r_d^{L} and r_d^{R} are limited to $z - v$ which is the asymptotic overhead required to recover zk PUI symbols when vk RO symbols are already possessed. The operation $\max(\cdot,\cdot)$ of second and third lines in (29) is added to establish the relation; $0 \leq r_1^{\mathrm{L}} \leq r_1^{\mathrm{R}} \leq r_2^{\mathrm{L}} \leq \cdots \leq r_d^{\mathrm{L}} \leq r_d^{\mathrm{R}} \leq \cdots \leq z - v$. The following definition turns out to be useful.

Definition 7: Denote D^{+} as the maximum value of d, where $(r_d^{\mathrm{L}}, r_d^{\mathrm{R}}]$ is not a null set.

Table II shows four examples of the intervals $(r_d^{\mathrm{L}}, r_d^{\mathrm{R}}]$ for $d = 1, \cdots, 9$ and D^{+}, which were obtained from (29). The first example $z = 1.0$, $v = 0$ (the second column) shows $(r_d^{\mathrm{L}}, r_d^{\mathrm{R}}]$ for an ESU. The results show that $\Theta_1(x)$ and $\Theta_2(x)$ are optimal in $r \in (0, \ln 2]$, $r \in (\ln 2, 0.75 \ln 3]$, respectively, which are consistent with the results derived in [5]. In the example, no interval exists such that $\Theta_d(\cdot)$ is optimal for $d \geq 3$. On the other hand, we can see that $\Theta_d(x)$ can be optimal for $d \geq 3$ in other

TABLE II

INTERVALS $\left(r_d^{\mathrm{L}}, r_d^{\mathrm{R}}\right]$ AND D^+ FOR THE GIVEN EXAMPLES. THE SYMBOL $\emptyset$ MEANS THE NULL SET

(z, v)	(1.0, 0.0)	(0.7, 0.15)	(0.5, 0.15)	(0.3, 0.15)
$\Gamma(x)$	-	$0.5x^2 + 0.3x^3 + 0.2x^4$		
$(r_1^{\mathrm{L}}, r_1^{\mathrm{R}}]$	(0.0000,0.6931]	(0.0000,0.2555]	$\emptyset$	$\emptyset$
$(r_2^{\mathrm{L}}, r_2^{\mathrm{R}}]$	(0.6931,0.8240]	(0.2555,0.4141]	(0.0000,0.1999]	$\emptyset$
$(r_3^{\mathrm{L}}, r_3^{\mathrm{R}}]$	$\emptyset$	(0.4141,0.4543]	(0.1999,0.2641]	(0.0000, 0.0502]
$(r_4^{\mathrm{L}}, r_4^{\mathrm{R}}]$	$\emptyset$	$\emptyset$	(0.2641,0.2867]	(0.0502, 0.0850]
$(r_5^{\mathrm{L}}, r_5^{\mathrm{R}}]$	$\emptyset$	$\emptyset$	(0.2867,0.2934]	(0.0850, 0.1002]
$(r_6^{\mathrm{L}}, r_6^{\mathrm{R}}]$	$\emptyset$	$\emptyset$	$\emptyset$	(0.1002, 0.1077]
$(r_7^{\mathrm{L}}, r_7^{\mathrm{R}}]$	$\emptyset$	$\emptyset$	$\emptyset$	(0.1077, 0.1118]
$(r_8^{\mathrm{L}}, r_8^{\mathrm{R}}]$	$\emptyset$	$\emptyset$	$\emptyset$	(0.1118, 0.1141]
$(r_9^{\mathrm{L}}, r_9^{\mathrm{R}}]$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
D^+	2	3	5	8

examples. For example, in the fifth column, intervals $(r_d^{\mathrm{L}}, r_d^{\mathrm{R}}]$ for $3 \leq d \leq 8$ exist while $(r_1^{\mathrm{L}}, r_1^{\mathrm{R}}]$ and $(r_2^{\mathrm{L}}, r_2^{\mathrm{R}}]$ are null sets.

According to (29), there is a slight possibility that $r_d^{\mathrm{L}} \neq r_{d-1}^{\mathrm{R}}$ although Table II shows $r_d^{\mathrm{L}} = r_{d-1}^{\mathrm{R}}$ for all of the examples. Consider the case where $r_{d-1}^{\mathrm{R}} \neq r_d^{\mathrm{L}}$. Both $\Theta_{d-1}(\cdot)$ and $\Theta_d(\cdot)$ are not optimal in the interval $(r_{d-1}^{\mathrm{R}}, r_d^{\mathrm{L}}]$. Nevertheless, we regard $\Theta_{d-1}(\cdot)$ as a nearly optimal solution in $r \in (r_{d-1}^{\mathrm{R}}, r_d^{\mathrm{L}}]$. Similarly, we regard $\Theta_{D^+}(\cdot)$ as a nearly optimal solution in $r \in (r_{D^+}^{\mathrm{R}}, z - v]$ although it is not optimal in the region. Then, we have the weights w_d as follows:

$$w_d = \begin{cases} \int_{r_d^{\mathrm{L}}}^{r_{d+1}^{\mathrm{L}}} h(r)dr, & \text{for } d = 1, 2, \cdots, D^+ - 1, \\ \int_{r_d^{\mathrm{L}}}^{z-v} h(r)dr, & \text{for } d = D^+, \\ 0, & \text{otherwise.} \end{cases} \tag{30}$$

To complete $\Omega^+(\cdot)$, we need to set $\Omega_{\mathrm{MR}}(\cdot)$. In theory, zk output symbols at least including the RO symbols are required to recover zk input symbols. Thus, $r > z - v$ is the region where full recovery is possible in theory. Thus, we employ the *shifted robust soliton distribution* (SRSD) introduced in [11]. The SRSD is designed by utilizing only z of USI and it does not requires solving an optimization problem. Nevertheless, it obtains a significantly good performance. The SRSD can be represented by the following definition.

Definition 8: Given z and an RSD $\Omega_{\mathrm{R}}(x) = \sum_{d=1}^{zk} \Omega_{\mathrm{R},[d]} x^d$, which is an appropriate distribution when the number of input symbols is zk, the SRSD $\Omega_{\mathrm{SR}}(x)$ is defined as

$$\Omega_{\mathrm{SR}}(x) \triangleq \sum_{d \geq 1} \Omega_{\mathrm{R},[d]} x^{\lceil d/z \rfloor}, \tag{31}$$

where $\lceil \cdot \rfloor$ rounds to the nearest integer.

Finally, the linearly mixed degree distribution is established as follows.

Definition 9: Given an RSD $\Omega_{\mathrm{R}}(\cdot)$, USI $(z, v, \Gamma(\cdot))$ and $r_1^{\mathrm{L}}, r_2^{\mathrm{L}}, \cdots, r_{D^+}^{\mathrm{L}}$, the *linearly mixed degree distribution* $\Omega^+(x)$ is defined as

$$\Omega^+(x) \triangleq \sum_{d=1}^{D^+-1} \left[\Theta_d(x) \int_{r_d^{\mathrm{L}}}^{r_{d+1}^{\mathrm{L}}} h(r)dr \right] + \Theta_{D^+}(x) \int_{r_{D^+}^{\mathrm{L}}}^{z-v} h(r)dr + \Omega_{\mathrm{SR}}(x) \int_{z-v}^{\infty} h(r)dr. \tag{32}$$

B. Multiple-User Case

In the previous subsection, only the single-user case was considered. In this subsection, we explain how to design $\Omega^+(\cdot)$ for a multi-user case. Let $\Omega_m^+(\cdot)$ denote the linearly mixed degree distribution designed with the USI of U_m. There are many possible options to design $\Omega^+(\cdot)$ from $\Omega_m^+(\cdot)$ but we describe only two simple ones. The first option is to set $\Omega^+(\cdot) = \Omega_{\hat{m}}^+(\cdot)$, where $\hat{m}$ is selected such that GASRR $y_{\mathrm{g}}(\Omega_m^+(\cdot))$ is maximized, i.e. $\hat{m} = \arg\min_m y_{\mathrm{g}}(\Omega_m^+(\cdot))$. The second option is to combine $\Omega_1^+(x), \cdots, \Omega_M^+(x)$ with certain weights $q_1, \cdots, q_M$ i.e., $\Omega^+(x) = \sum_{m=1}^{M} q_m \Omega_m^+(x)$. The second option seems more reasonable than the first one but it requires solving an additional problem about how to determine $q_1, \cdots, q_M$. In this work, we do not address this problem. Note that the first option is employed in evaluation of the performance of SCHEME-2 in Section VI.

VI. EXPERIMENTAL RESULTS

In this section, we evaluate the performance of SCHEME-1 and SCHEME-2 in terms of the GASRR by comparing them with the conventional scheme (denoted by SCHEME-3) introduced in [6]. In addition, we compare the degree distribution obtained by our scheme with RSD in terms of the FRP [3].

We consider three USIs, denoted by USI_1, USI_2 and USI_3, whose (z_m, v_m) for $m = 1, 2, 3$ are (0.7, 0.1), (0.6, 0.1) and (0.5, 0.1), respectively. In addition, we assume that the users received some output symbols with RSD at the previous transmission, so we set $\Gamma_m(x) = \frac{\hat{\Omega}_{\mathrm{R}}(x)}{1 - \hat{\Omega}_{\mathrm{R},[0]} - \hat{\Omega}_{\mathrm{R},[1]}}$, where $\hat{\Omega}_{\mathrm{R}}(x) = \sum_{d \geq 0} \hat{\Omega}_{\mathrm{R},[d]} x^d = \Omega_{\mathrm{R}}(1 - z_m + z_m x)$. In most of the simulations, we set $k = 2000$, $(c, \delta) = (0.05, 0.5)$ for RSD

TABLE III
DEGREE DISTRIBUTIONS DESIGNED BY SCHEME-1 AND SCHEME-2: $\alpha = 0.5$ EXCEPT $\Omega_8^*(x)$, $\eta = 0.95$

i	Parameters	SCHEME-1 $\Omega_i^*(x)$ $\langle$average degree$\rangle$	SCHEME-2 $\Omega_i^+(x)$ $\langle$average degree$\rangle$
1	$n = 600, \varepsilon = 0.0 - 0.3$	x^2 $\langle 2.00 \rangle$	x^2 $\langle 2.00 \rangle$
2	$n = 1100, \varepsilon = 0.0$	$0.2272x^3 + 0.7728x^4$ $\langle 3.77 \rangle$	x^3 $\langle 3.00 \rangle$
3	$n = 1100, \varepsilon = 0.1$	$0.9349x^3 + 0.0651x^4$ $\langle 3.07 \rangle$	$0.0054x^2 + 0.9946x^3$ $\langle 2.99 \rangle$
4	$n = 1100, \varepsilon = 0.2$	x^3 $\langle 3.00 \rangle$	x^2 $\langle 2.00 \rangle$
5	$n = 1100, \varepsilon = 0.3$	x^2 $\langle 2.00 \rangle$	x^2 $\langle 2.00 \rangle$
6	$n = 1100, \varepsilon = 0.0, \alpha = 1.0$	$0.3312x^3 + 0.6688x^4$ $\langle 3.67 \rangle$	-
7	$n = 1050, \varepsilon = 0.0$	$0.4201x^3 + 0.5799x^4$ $\langle 3.58 \rangle$	-
8	$n = 1300, \varepsilon = 0.0$	$0.2580x^3 + 0.5558x^4 + 0.0389x^5$ $\cdots + 0.0102x^{21} + 0.0127x^{22} + \cdots$ $\langle 18.70 \rangle$	$0.0104x^1 + 0.4640x^3 + 0.1561x^4$ $+ \cdots + 0.0331x^{136} + \cdots$ $\langle 15.31 \rangle$

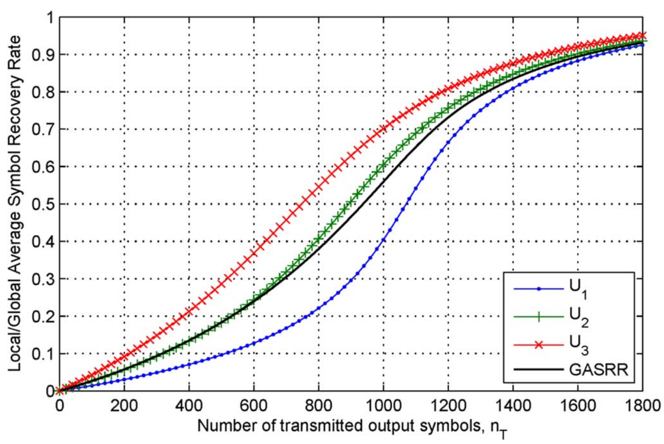

Fig. 3. LASRR/GASRR versus the number of transmitted output symbols. The degree distribution $\Omega_3^*(\cdot)$ is employed and $\varepsilon = 0.1$.

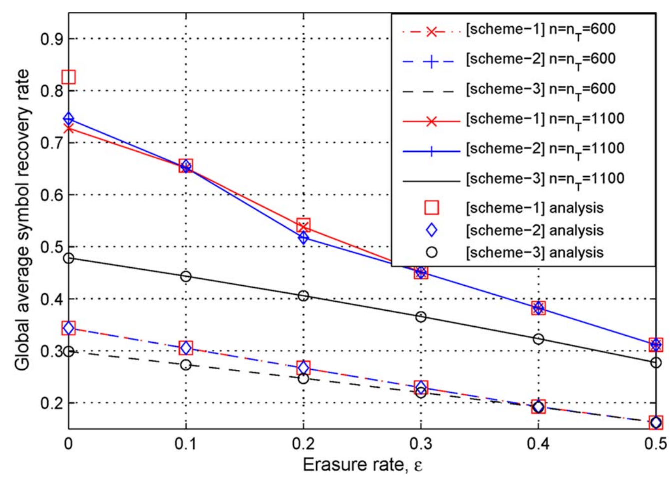

Fig. 4. GASRR versus erasure rate: $k = 2000$, $\alpha = 0.5$, $\eta = 0.95$.

and SRSD, and $\alpha = 0.5$, $\eta = 0.95$ for SCHEME-1. Here, let us calculate the amount of feedback informing of USI_1 roughly as described at the last paragraph in Section III. First, 11 bits are required to represent z_1. In case of $\Gamma_1(x)$, most of the RO symbols have a degree smaller than or equal to 80 with a probability greater than 0.99, so the coefficients of $v_1 k \Gamma_1(x)$ can be represented by 79 integers with satisfactory accuracy, where each integer is 7 bits. Thus 564 bits are required to represent USI_1. Similarly, we can see that 501 bits and 438 bits are required for feedback of USI_2, USI_3, respectively.

We assume that overhead distributions are identical and $r \sim \frac{\text{Bin}(n,(1-\varepsilon))}{k}$, where $\text{Bin}(n, 1-\varepsilon)$ denotes a binomial distribution with mean $n(1-\varepsilon)$ and variance $n\varepsilon(1-\varepsilon)$ with an erasure rate ϵ. Note that n_{T} and n are different. The notation n_{T} is the number of transmitted output symbols while n is a parameter used to determine the overhead distributions in the optimization schemes. Some degree distributions used in this section are provided in Table III.

A. GASRR With Varying n and ϵ

In this subsection, we consider three users, U_1, U_2 and U_3, whose USIs are USI_1, USI_2 and USI_3, respectively. Fig. 3 shows the performance of $\Omega_3^*(x)$ in Table III in terms of GASRR and LASRRs. We can see that U_1's LASRR is the worst whereas U_3's LASRR is the best. This is because a smaller z_m makes the relative overhead r/z_m larger. For example, when 1100 output symbols are given, the relative overheads for U_1 and U_3 are $\frac{1100}{1400} \approx 0.79$ and $\frac{1100}{1000} = 1.10$, respectively. The GASRR $y_g(\Omega(\cdot))$ is a weighted sum of the LASRRs $y_1(\Omega(\cdot))$, $y_2(\Omega(\cdot))$ and $y_3(\Omega(\cdot))$; thus, the GASRR curve is plotted between the curves for U_1 and U_3.

Note that the most meaningful part in Fig. 3 is the GASRR curve around $n_{\text{T}} = 1100$, because $\Omega_3^*(\cdot)$ is designed for $n = 1100$. Fig. 4 shows the GASRR curves plotted by connecting only the meaningful segments. The x-axis and y-axis represent the *erasure rate* $\varepsilon \in \{0, 0.1, \cdots, 0.5\}$ and *GASRR*, respectively. Note that we employ six degree distributions for each curve and the distributions are optimized for each ε. Some degree distributions employed in Fig. 4 are shown in Table III.

Fig. 4 shows that the code performance observed by the simulation matches the asymptotic performance. SCHEME-1 and SCHEME-2 outperform SCHEME-3 for all ε and n. In addition, SCHEME-1 seems to be slightly better than or similar as SCHEME-2. However, when $n = 1100$ and $\varepsilon = 0.0$, the simulation result of SCHEME-1 is significantly worse than the asymptotic performance. Moreover, SCHEME-1 shows worse performance than SCHEME-2 at the point.

We suggest two methods to improve the GASRR performance at $\varepsilon = 0.0$. The first method is to control α in (16). By increasing α, we can increase the expected number of the ripple symbols and reduce the possibility of decoding failure

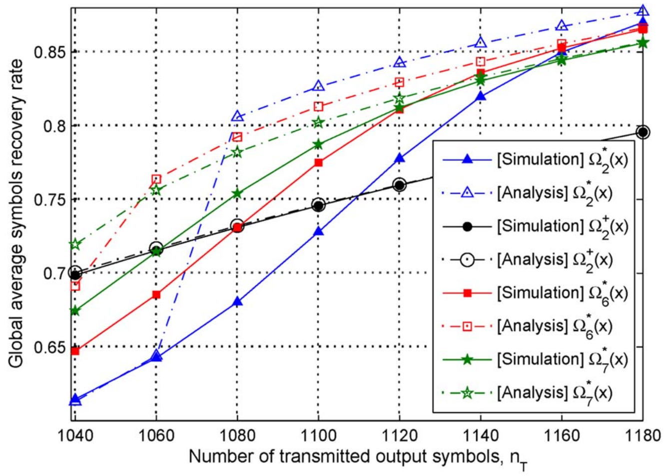

Fig. 5. GASRR versus the number of transmitted output symbols: $k = 2000$, $\varepsilon = 0.0$.

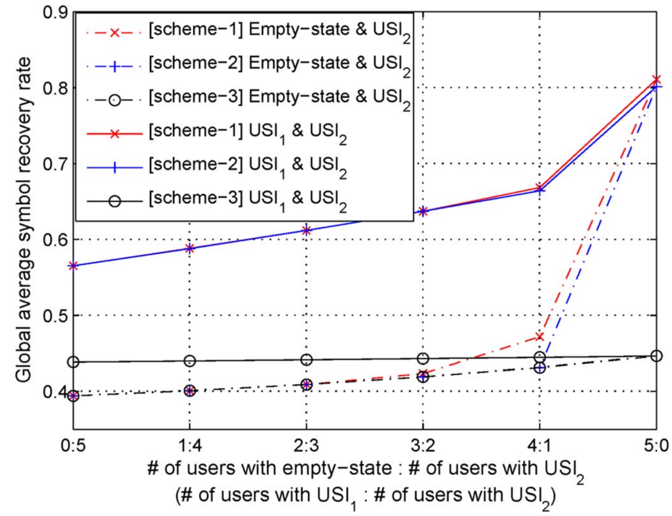

Fig. 6. GASRR versus the ratio of U_2 to all of the users: $k = 2000$, $n = n_T = 1000$, $\varepsilon = 0$, $\alpha = 0.5$, $\eta = 0.95$.

during the early decoding iterations. The second is to choose n slightly smaller than 1100. The reason is that in general finite-length fountain codes require additional output symbols to achieve the asymptotic performance. We have $\Omega_6^*(\cdot)$ and $\Omega_7^*(\cdot)$ in Table III, which are obtained by the two methods, respectively. In Fig. 5, it is shown that the performances are improved by the two approaches at $n_T = 1100$. While the GASRRs with $\Omega_2^*(\cdot)$ obtained by the simulation and analysis show a significantly large gap, those with $\Omega_7^*(\cdot)$ and $\Omega_8^*(\cdot)$ show the smaller gap. In addition, Fig. 7 shows that $\Omega_7^*(\cdot)$ and $\Omega_8^*(\cdot)$ outperform $\Omega_2^+(\cdot)$.

B. GASRR With Various Sets of USIs

In this subsection we evaluate the performance of our proposed schemes with varying combinations of users. We first consider the cases where some users are of empty-state and the others are of USI_2. As shown by the dashed lines in Fig. 6, our proposed schemes provide no gain when the ratio of ESUs are high because ESUs are dominant factors in designing degree distribution. Meanwhile, our proposed schemes provide a significant gain when the ratio of ISUs is large.

Fig. 6 shows also that our proposed schemes provide gains significantly over the conventional scheme when all of the users are intermediate-state; their USIs are either USI_1 or USI_2. In addition, we can see that GASRRs of the proposed schemes increase as the ratio of the users with USI_2 grows. Note that the users with USI_2 have a smaller z than that of USI_1. Because n_T is fixed in the simulation, an increase of the ratio of users with USI_2 causes a decrease of the sum of the number of PUI symbols, which is the denominator of (8). In general, when n_T is fixed and the number of input symbol decreases, SRR increases. From the characteristic, we can expect that GASRR increases when the number of the users with smaller z grows, and the tendency can be seen in Fig. 6.

C. GASRR With Small Input Length

In this subsection, we investigate the efficiency of our proposed schemes in terms of GASRR when k is small. For the simulation, we assume that there are three users U_m whose parameters (z_m, v_m), $m = 1, 2, 3$ are (0.7, 0), (0.6, 0) and (0.5, 0), respectively. Note that using a fixed set of RSD parameters (c, δ) for every k does not guarantee good performance and adjusting RSD parameters for each k is not proper to show an influence of k. Thus we set $v_m = 0$ for $m = 1, 2, 3$ to exclude the effect of RO symbols.

In Fig. 7, we can see that the proposed schemes show much better performances than SCHEME-3 in terms of GASRR. In addition, it can be seen that the asymptotic GASRR performance for each scheme seems almost independent of k. Meanwhile, the simulation results show that the performances of SCHEME-1 and SCHEME-2 are different from the asymptotic performances when k is small. In addition, we can see that the simulation results approach the corresponding asymptotic performance as k increases. In particular, SCHEME-1 shows the tendency clearly; at $k = 2^5$ the difference between simulation and analysis is significantly large, but at $k = 2^{10}$ the result of simulation is almost consistent with the result of analysis. Note that when $k = 2^5$, the degree distributions optimized by SCHEME-1 and SCHEME-2 are $\Omega^*(x) = x^3$ and $\Omega^+(x) = 0.4315x^2 + 0.5666x^3 + \cdots$, respectively. In general, the asymptotic SRR matches well the SRR of finite-length codes when k is large enough or the codes are sparse enough. Due to the characteristic, as shown in Fig. 7, SCHEME-1 shows a larger gap than in terms of GASRR between the analysis and simulation and has even worse performance at $k = 2^5$ than SCHEME-2.

D. Full Recovery Performance

This subsection compares the FRP of our schemes and LT codes with an RSD. We assume that there are three users U_1, U_2 and U_3 whose USIs are USI_1, USI_2 and USI_3, respectively.

In general, when evaluating FRP performance, it is assumed that n_T is sufficiently large for all of the users to achieve full recovery, so we set $\varepsilon = 0$. Moreover we set $n = \max_m(z_m - v_m + 0.05)k = 1300$, because at least $\max_m(z_m - v_m)k$ output symbols are required to guarantee full recovery of all users. The

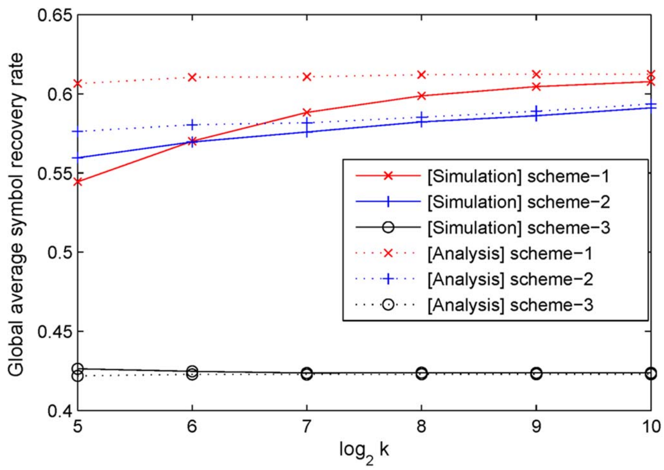

Fig. 7. GASRR versus the number of input symbols k: $n = n_{\mathrm{T}} = \frac{22}{32}k$, $\varepsilon = 0.2$, $\alpha = 0.5$, $\eta = 0.95$.

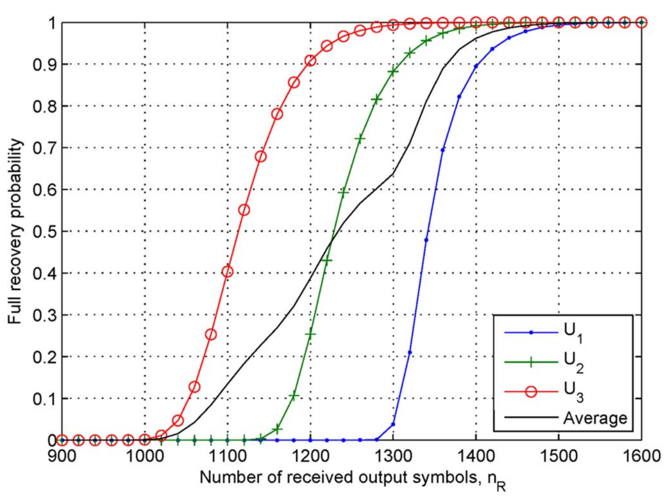

Fig. 8. FRP for each user and their average FRP versus the number of received output symbols n_{R} with $\Omega_8^*(\cdot)$: $k = 2000$.

degree distributions $\Omega_8^*(\cdot)$ and $\Omega_8^+(\cdot)$ in Table III are designed by SCHEME-1 and SCHEME-2, respectively.

Fig. 8 shows that U_3 and U_1 require the smallest and the largest overhead, respectively, to achieve high FRP. In Fig. 8, the so-called "water fall" regions, where the FRP of each user increases rapidly, are distinguishable because the values of z_m for $m = 1, 2, 3$ are different. This produces the fluctuations in the curve of the average FRP, which is the probability that a randomly selected user achieves full recovery.

Fig. 9 shows the full recovery performance of our proposed schemes and LT codes with RSD. Note that the degree distribution obtained by SCHEME-2 is an SRSD [11] with RSD parameters $(c, \delta) = (0.05, 0.5)$, which is designed without considering RO symbols. Thus it is reasonable that SCHEME-1 outperforms the others at the high FRP region in terms of average FRP. In addition, Fig. 9 shows the FRP performance for U_1 which is the user requiring the most output symbols for full recovery. Likewise, SCHEME-1 shows better performance than the others in terms of the FRP performance for U_1. Table IV shows the expected number of output symbols for full recovery.

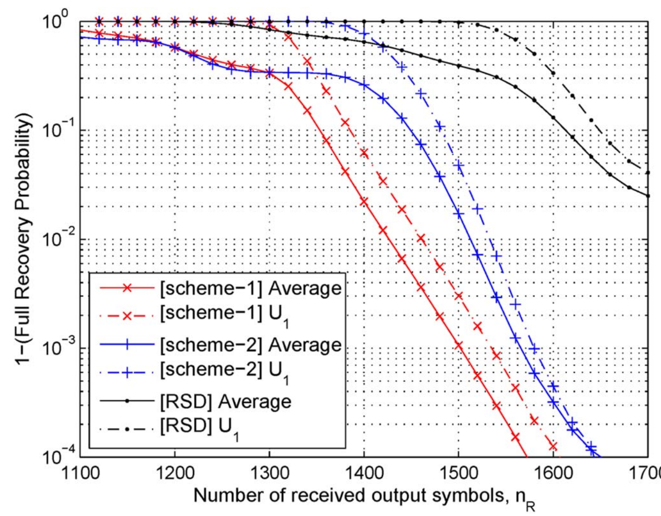

Fig. 9. Average FRP and U_1's FRP versus the number of received output symbols n_{R}: $k = 2000$, $c = 0.05$, $\delta = 0.5$, Ω_8^* and Ω_8^+ are employed.

TABLE IV
EXPECTED NUMBER OF REQUIRED OUTPUT SYMBOLS FOR FULL RECOVERY

	SCHEME-1	SCHEME-2	RSD
Avg.	1224.5	1239.8	1428.7
U_1	1341.4	1430.5	1546.9

E. Computational Complexity

We investigate encoding/decoding complexities of designed degree distributions in terms of average degrees. Table III shows $\Omega_i^*(\cdot)$ and $\Omega_i^+(\cdot)$, $i = 1, \cdots, 7$, which are the degree distributions used in Section VI-A, and $\Omega_8^*(\cdot)$ and $\Omega_8^+(\cdot)$ which are used in Section VI-B. We can see that their average degree tends to increase as ε decreases and n increases. In general, degree distributions designed for small overhead tend to have low average degrees; the average degrees of $\Omega_i^*(\cdot)$ and $\Omega_i^+(\cdot)$ for $i = 1, \cdots, 7$ are less than 4. Meanwhile, degree distributions designed for large overhead, such as RSD and raptor distribution, have high average degrees; the average degrees of RSD with $(k, c, \delta) = (2000, 0.05, 0.5)$ and raptor distribution [4] are approximately 11.0 and 5.9, respectively. From Table III, we can see that the average degrees (18.7 and 15.3, respectively) of $\Omega_8^*(\cdot)$ and $\Omega_8^+(\cdot)$ are higher than those of RSD and raptor distribution. Here, we should note that our proposed schemes cause higher encoding/decoding complexities.

For example, in case of Fig. 9, if $\Omega_8^*(\cdot)$ is employed, $25084(\approx 1341.4 \times 18.7)$ edges should be processed for full recovery of U_1 on average. If RSD is employed, $17016(\approx 1546.9 \times 11.0)$ edges should be processed for full recovery of U_1 on average. As a result, about 47% more computations are required for encoding/decoding of $\Omega_8^*(\cdot)$, if we exclude decoding computations of RO symbols.

VII. CONCLUSION

In this study, we considered a broadcasting system that is composed of a source and multiple intermediate-state users, which hold some previously recovered input symbols and some output symbols that are insufficient to recover all of the input symbols. We showed that conventional degree distribution optimization schemes are inefficient for our proposed system model because they cannot utilize the states of the users as design parameters or they are not scalable for multi-user systems. Thus, we proposed a generalized degree distribution optimization scheme, called SCHEME-1, which maximizes the global average symbol recovery rate. Additionally, we proposed another degree distribution design scheme, called SCHEME-2, where the degree distribution design procedure has a low computational complexity. Based on Monte Carlo simulations, we showed that our optimization schemes outperform the conventional schemes in terms of global average symbols recovery rate and full recovery probability. Meanwhile, the degree distributions obtained by our schemes shows higher encoding/decoding complexity than the conventional degree distributions such as RSD and raptor distribution.

APPENDIX A
PROOF OF LEMMA 1

Proof: Consider an output symbol that neighbors d input symbols in $\mathcal{B}$. The probability ($P_{d\to d'}$) that a degree-d output symbol neighbors $d'(\le d)$ PUI symbols ($\in \mathcal{B}_m$) is

$$P_{d\to d'} = \frac{\binom{kz_m}{d'}\binom{k(1-z_m)}{d-d'}}{\binom{k}{d}}. \tag{33}$$

When $k \gg d$, (33) can be approximated as

$$P_{d\to d'} \approx \binom{d}{d'} z_m^{d'}(1-z_m)^{d-d'}. \tag{34}$$

Then the reduced degree distribution $\Omega_m(x)$ is

$$\begin{aligned}\Omega_m(x) &\approx \sum_{d'\ge 0}\left[x^{d'}\sum_{d\ge 0}\Omega_{[d]}P_{d\to d'}\right]\\ &= \sum_{d'\ge 0}\left[x^{d'}\sum_{d\ge 0}\Omega_{[d]}z_m^{d'}\binom{d}{d'}(1-z_m)^{d-d'}\right]. \end{aligned}\tag{35}$$

If we change the order of the summations, (35) can be represented as

$$\begin{aligned}\Omega_m(x) &\approx \sum_{d\ge 0}\left[\Omega_{[d]}\sum_{d'\ge 0}\binom{d}{d'}(xz_m)^{d'}(1-z_m)^{d-d'}\right]\\ &= \Omega(1-z_m+z_m x). \end{aligned}\tag{36}$$

■

APPENDIX B
PROOF OF LEMMA 2

Proof: Let $f_{d,i}(x)$ be a ratio of $\Theta'_d(x)$ to $\Theta'_i(x)$, i.e.,

$$f_{d,i}(x) \triangleq \frac{\Theta'_d(x)}{\Theta'_i(x)}. \tag{37}$$

Then $f_{d,i}(x) = \frac{d}{i}x^{d-i}$ and the problem changes into showing that $f_{d,i}(x) \ge 1$ in $x \in \left[\frac{d-1}{d}, \frac{d}{d+1}\right]$.

Now we consider two cases where $d > i$ and $d < i$. Let a is an arbitrary positive integer. When $i = d - a$ (i.e., $d > i$) $f_{d,i}(x)$ is a monotonically increasing function in $x \ge 0$ since $\frac{d}{dx}f_{d,i}(x) = \frac{da}{d-a}x^{a-1} \ge 0$. Furthermore, $f_{d,i}\left(\frac{d-1}{d}\right) = \left(\frac{d-1}{d-a}\right)\left(\frac{d-1}{d}\right)^{a-1} \ge 1$ for an arbitrary positive integer a. Therefore $f_{d,i}(x) \ge 1$ is true for $x \ge \frac{d-1}{d}$. Similarly, when $i = d + a$ (i.e., $d < i$), $f_{d,i}(x)$ is a monotonically decreasing function in $x \ge 0$ since $\frac{d}{dx}f_{d,i}(x) = -\frac{da}{d-a}x^{-a-1} < 0$ in $x \ge 0$ and $f_{d,i}\left(\frac{d}{d+1}\right) \ge 1$, so $f_{d,i}(x) \ge 1$ in $x \in \left[0, \frac{d}{d+1}\right]$. Consequently, $\Theta'_d(x)$ is greater than or equal to $\Theta'_i(x)$ for an arbitrary positive integer i for the interval $x \in \left[\frac{d-1}{d}, \frac{d}{d+1}\right]$. ■

APPENDIX C
PROOF OF COROLLARY 1

Proof: Let $\Omega(x) = \sum_i \Omega_{[i]}x^i$ be an arbitrary degree distribution, then it can be rewritten as $\Omega(x) = \sum_i \Omega_{[i]}\Theta_i(x)$. An SDD $\Theta_d(\cdot)$ can be represented by $\Theta_d(x) = \Theta_d(x)\sum_i \Omega_{[i]}$ because $\sum_i \Omega_{[i]} = 1$. Then the first derivative of $\Theta_d(x)$ can be represented by $\Theta'_d(x) = \sum_{[i\ge 1]}\Omega_{[i]}\Theta'_d(x)$. Using Lemma 2, the Corollary 1 is proven as follows;

$$\Theta'_d(x) = \sum_{[i\ge 1]}\Omega_{[i]}\Theta'_d(x) \tag{38}$$

$$\ge \sum_{[i\ge 1]}\Omega_{[i]}\Theta'_i(x) = \Omega'(x), \tag{39}$$

for $x \in \left[\frac{d-1}{d}, \frac{d}{d+1}\right]$. ■

REFERENCES

[1] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, “A digital fountain approach to reliable distribution of bulk data,” in *Proc. ACM SIGCOMM*, Vancouver, BC, Canada, Sep. 1998, pp. 56–67.
[2] J. W. Byers, M. Luby, and M. Mitzenmacher, “A digital fountain approach to asynchronous reliable multicast,” *IEEE J. Sel. Areas Commun.*, vol. 20, no. 8, pp. 1528–1540, Aug. 2002.
[3] M. Luby, “LT codes,” in *Proc. 43rd Annu. IEEE Symp. Found. Comput. Sci.*, Vancouver, BC, Canada, Nov. 2002. pp. 271–280.
[4] A. Shokrollahi, “Raptor codes,” *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, Jun. 2006.
[5] S. Sanghavi, “Intermediate performance of rateless codes,” in *Proc. IEEE Inf. Theory Workshop*, 2007, pp. 478–482.
[6] M. Zeng, R. Calderbank, and S. Cui “On design of rateless codes over dying binary erasure channel,” *IEEE Trans. Commun.*, vol. 60, no. 4, pp. 889–894, Apr. 2012.
[7] A. Talari, and N. Rahnavard, “Rateless codes with optimum intermediate performance,” in *Proc. IEEE Global Telecommun. Conf.*, 2009, pp. 1–6.

[8] N. Rahnavard, B. N. Vellambi, and F. Fekri "Rateless codes with unequal error protection property," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1521–1532, Apr. 2007.

[9] P. Elias, "Coding for two noisy channels," in *Proc. 3rd London Symp. Inf. Theory*, 1956, pp. 61–76.

[10] S. Puducheri, J. Kliewer, and T. E. Fuja "The design and performance of distributed LT Codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3740–3755, Oct. 2007.

[11] A. Hagedorn, S. Agarwal, D. Starobinski, and A. Trachtenberg "Rateless coding with feedback," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 1791–1799.

[12] S. Kim and S. Lee, "Improved intermediate performance of rateless codes," in *Proc. ICACT*, Feb. 2009, pp. 1682–1686.

[13] J. H. Sørensen, T. Koike-Akino, and P. Orilik "Rateless feedback codes," in *Proc. ISIT*, Jul. 2012, pp. 1767–1771.

[14] J. H. Sørensen, P. Popovski, and J. Østergaard "Feedback in LT codes for prioritized and non-prioritized data," in *Proc. IEEE VTC*, Sep. 2012, pp. 1–5.

[15] A. Talari, and N. Rahnavard, "LT-AF codes: LT codes with alternating feedback," in *Proc. ISIT*, Jul. 2013, pp. 2646–2650.

[16] D. Sejdinović, R. J. Piechocki, A. Doufexi, and M. Ismail "Fountain code design for data multicast with side information," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5155–5165, Oct. 2009.

[17] M. Luby, M. Mitzenmacher, A. Shokrollahi, D. A. Spielman, and V. Stemann "Practical loss-resilient codes," in *Proc. 29th Annu. ACM Symp. Theory Comput.*, 1997, pp. 150–159.

[18] A. Kamra, V. Misra, J. Feldman, and D. Rubenstein, "Growth codes: Maximizing sensor network data persistence," in *Proc. Conf. Appl., Technol., Archit. Protocols Comput. Commun.*, 2006, pp. 255–266.

Youngkil Suh received the B.S. and M.S. degrees in electrical and electronic engineering from Korea University, Seoul, Korea in 2009 and 2011, respectively. He is currently working toward the Ph.D. degree with the School of Electrical Engineering, Korea University. His current research interests include channel coding theory and optimization.

Jonghyun Baik received the B.S. and M.S. degrees in electrical engineering from Korea University, Seoul, Korea, in 2010 and 2012, respectively. He joined the School of Electrical Engineering at Korea University as a Ph.D. student in March 2012. His research interests include novel error control coding techniques for unequal error protection and distributed networks.

Nazanin Rahnavard received her B.S. and M.S. degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 1999 and 2001, respectively. She then received the Ph.D. degree from the School of Electrical and Computer Engineering at the Georgia Institute of Technology, Atlanta, in 2007. She is currently an Associate Professor in the Department of Electrical Engineering and Computer Science at the University of Central Florida, Orlando, FL. She is the recipient of NSF CAREER award in 2011. She also received the 2007 Outstanding Research Award from the Center of Signal and Image Processing at Georgia Tech. She has interest and expertise in a variety of research topics in the communications, networking, and signal processing areas. She serves on the editorial board of the *Journal on Computer Networks* (COMNET) (Elsevier) and on the Technical Program Committee of several prestigious international conferences.

Jun Heo received the B.S. and M.S. degrees in electronics engineering from Seoul National University, Seoul, Korea in 1989 and 1991, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, USA, in 2002. During 1991–1997, he was a Senior Research Engineer at LG Electronics Co., Inc. He is presently a Professor in the School of Electrical Engineering at Korea University, Seoul, Korea. His research interests include channel coding theory and quantum communication.