

# Reliability of Multicast Under Random Linear Network Coding

Evgeny Tsimbalo<sup>✉</sup>, *Member, IEEE*, Andrea Tassi<sup>✉</sup>, *Member, IEEE*, and Robert J. Piechocki

**Abstract**—We consider a lossy multicast network in which the reliability is provided by means of random linear network coding. Our goal is to characterize the performance of such network in terms of the probability that a source message is delivered to all destination nodes. Previous studies considered coding over large finite fields, small numbers of destination nodes or specific, often impractical, channel conditions. In contrast, we focus on a general problem, considering arbitrary field size and number of destination nodes, and a realistic channel. We propose a lower bound on the probability of successful delivery, which is more accurate than the approximation commonly used in the literature. In addition, we present a novel performance analysis of the systematic version of RLNC. The accuracy of the proposed performance framework is verified via extensive Monte Carlo simulations, where the impact of the network and code parameters are investigated. Specifically, we show that the mean square error of the bound for a ten-user network can be as low as  $9 \cdot 10^{-5}$  for non-systematic RLNC.

**Index Terms**—Multicast networks, broadcast networks, reliability, fountain coding, non-systematic RLNC, systematic RLNC.

## I. INTRODUCTION

**R**ELIABILITY is a key performance metric in modern wireless multicast networks, in which a single transmitter, or a *source* node, broadcasts to multiple receivers, or *destination* nodes, also referred to as *users*. Traditionally, the reliability in multicast networks is provided by Application Level Forward Error Correction (AL-FEC) [1], where coding is performed over packets rather than bits. AL-FEC is typically based on a digital fountain approach [2] implemented, for instance, in Raptor codes [3]. These codes, however, operate efficiently only when the number of packets per block is large, which makes them prohibitive in applications where the block size is limited - for instance, due to delay constraints [4].

As an alternative to traditional fountain codes, the idea of combining packets using *random* linear coefficients [5],

also known as *Random Linear Network Coding* (RLNC) [6], has attracted significant research interest. RLNC is based on the original concept of network coding proposed by R. Ahlswede *et al.* [7] and is proved to be capacity-achieving for lossy multicast networks [8], [9]. In contrast with traditional fountain codes, schemes based on RLNC do not require a large block size [4].

In a multicast network operated under RLNC, the source node encodes an information message of  $K$  packets by combining the packets using random coefficients belonging to a finite field [10]. An encoded packet is therefore associated with a vector of coding coefficients. Each user needs to collect  $K$  linearly independent vectors of coding coefficients to be able to decode the source message, typically by means of Gaussian elimination. A key performance indicator of such network can be the probability that all users collect  $K$  linearly independent vectors of coding coefficients, which will be referred to as *probability of successful delivery*. As an alternative to traditional, non-systematic encoding, a systematic version of RLNC, in which the information message is transmitted first, was also proposed [11]–[13]. As shown in [14], systematic RLNC can reduce decoding delay and complexity.

The traditional approach to the performance analysis of RLNC and multicast networks is to assume an infinite, or sufficiently large, field size [6], [15], [16], so that any  $K$  vectors of coding coefficients are linearly independent with a high probability. Under this assumption, the multicast network can be viewed as a set of independent unicast connections. While the assumption significantly simplifies the analysis, the field size is limited in practice [17], [18]. As a consequence of that, the probability that the vectors of coding coefficients collected by a user are linearly *dependent* can be non-negligible, even if their number is larger than  $K$ . In addition, some vectors of coding coefficients can be received simultaneously by multiple users, giving rise to statistical correlation. As a result, with a finite field size, the multicast network cannot be approximated as a set of independent unicast connections, and the probability of successful delivery needs to be calculated jointly.

The analysis of multicast networks and codes with coefficients generated from a small field size has been also studied in the literature. The initial studies [19], [20] were based on Markov chain models, but due to complexity the number of users was limited to two. Another study [12] applied a Markov chain model to a network with an arbitrary number of users, assuming that the users receive disjoint sets of packets. In [21], an *exact* probability of successful delivery, valid for any field

Manuscript received September 7, 2017; revised December 11, 2017; accepted January 31, 2018. Date of publication February 5, 2018; date of current version June 14, 2018. This work is partially supported by the VENTURER Project, which is supported by Innovate UK under Grant Number 102202. The associate editor coordinating the review of this paper and approving it for publication was V. Stankovic. (*Corresponding author: Andrea Tassi.*)

E. Tsimbalo is with the Telecommunications Research Laboratory, Toshiba Research Europe Ltd., Bristol BS1 4ND, U.K. (e-mail: evgeny.tsimbalo@toshiba-trel.com).

A. Tassi and R. J. Piechocki are with the Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, U.K. (e-mail: a.tassi@bristol.ac.uk; r.j.piechocki@bristol.ac.uk).

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.2018.2801791

0090-6778 © 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

See [http://www.ieee.org/publications\\_standards/publications/rights/index.html](http://www.ieee.org/publications_standards/publications/rights/index.html) for more information.

size, was derived for the simple case of a unicast, point-to-point connection. The result was extended to the systematic version of RLNC in [22]. Following that, in [23] and [24], a two-user multicast network was considered in the context of security and relay communication, respectively. Assuming a sufficiently high packet erasure rate (PER), so that the users are likely to receive disjoint sets of packets, the probability of successful delivery was approximated as a product of those corresponding to each individual user. In contrast, an *exact* expression for the probability of successful delivery for the same network, valid for any field size and PER, was obtained in [25] for non-systematic RLNC, based on the rank analysis of structured random matrices [26].

To summarise, the previous studies on the performance of RLNC and multicast networks considered large finite fields, a limited number of users or specific (often impractical) channel conditions. In the cases when the exact formulation was obtained, the analysis was limited to two users. Moreover, the existing studies focus mainly on traditional, non-systematic RLNC. To the best of our knowledge, there is no study in the literature that considers a general case of arbitrary field size, number of users and channel conditions for both non-systematic and systematic RLNC.

In this work, we address the limitations of the previous studies and provide the following contributions:

- In contrast with [6], [15], [16], [23], [24], we calculate the probability that all users recovered the source message *jointly*, taking into account a finite field size and commonly received packets.
- We generalise the analysis limited to a two-user network [20], [25] to an *arbitrary* number of users, and derive a tight lower bound for the probability of successful delivery in the case of traditional, non-systematic RLNC. In contrast with [23], [24], the bound takes into account the correlation effect due to commonly received packets.
- We also present a novel analysis for the systematic version of RLNC. We argue that the correlation effect is less profound than in the non-systematic case, and each user can be considered independently, even if the field size is small. We formulate the result explicitly and prove that it is a tight lower bound.
- We perform thorough benchmarking of the proposed bounds via extensive Monte Carlo simulation, where the effects of the number of users, the PER, the source message size and the field size are investigated. We demonstrate that the considered bounds are especially accurate under realistic channel conditions. In the non-systematic case, the derived bound provides a much closer approximation than the traditional bound used in the literature. In particular, this holds true in those scenarios where users are spread across the coverage area of the transmitter and experience heterogeneous PERs.
- We provide an extensive study into the performance of multicast networks under RLNC and offer an insight into the selection of code parameters for various network configurations.

The remainder of the paper is organised as follows. Section II describes the system model and provides the necessary background on multicast networks. The proposed theoretical framework is presented in Section III, where the bounds for the probability of successful delivery are derived for both non-systematic and systematic versions of RLNC. In Section IV, the proposed bounds are compared with simulated results and existing bounds. Section V draws conclusions and highlights future research avenues.

## II. SYSTEM MODEL AND BACKGROUND

Consider a multicast network, in which a source node transmits to  $L$  destination nodes, or users. Each of the  $L$  links is assumed to be lossy and characterised by a PER  $\epsilon_j$  for  $j = 1, \dots, L$ . Here, we assume that packet erasures occur as statistically independent events. The goal is to deliver a message of  $K$  source packets to each user. It will be assumed that the  $i$ -th source packet  $\mathbf{s}_i$ ,  $i = 1, \dots, K$ , is a column vector of elements from a finite field  $\mathbb{F}_q$  of size  $q$ . The number of elements in vector  $\mathbf{s}_i$  is equal to  $\lceil t/\log_2 q \rceil$  [27], where  $t$  denotes the packet length in bits, which is assumed to be the same for all packets.

Given  $K$  source packets, the encoder generates  $N \geq K$  coded packets  $\{\mathbf{c}_k\}_{k=1}^N$ , each being a vector consisting of  $\lceil t/\log_2 q \rceil$  elements from  $\mathbb{F}_q$ . Using the matrix notation, the encoding operation can be expressed as follows:

$$[\mathbf{c}_1, \dots, \mathbf{c}_N] = [\mathbf{s}_1, \dots, \mathbf{s}_K] \cdot \mathbf{G}, \quad (1)$$

where  $\mathbf{G} \in \mathbb{F}_q^{K \times N}$  is a  $K \times N$  matrix of *coding coefficients* generated uniformly at random from  $\mathbb{F}_q$ . In the case of systematic RLNC, the first  $K$  columns of  $\mathbf{G}$  form an  $K \times K$  identity matrix. In this way, the first  $K$  transmissions are the source packets, also referred to as *systematic* packets, followed by  $N - K$  coded, non-systematic packets. It is beyond the scope of the paper to address sparse implementations of RLNC [28].

Due to packet erasures, each user will receive a subset of transmitted packets. Let  $U_j \subseteq \{1, \dots, N\}$  denote a set of indices of transmitted packets received by the  $j$ -th user,  $j = 1, \dots, L$ . Let also  $m_j = |U_j|$  denote the number of packets received by the  $j$ -th user. It is assumed that all users have a knowledge of the coding coefficients associated with each received packet. This can be achieved by transmitting the coefficients or the seed used to generate them in the packet header [6]. The  $j$ -th user can therefore construct an  $m_j \times K$  matrix of coding coefficients, which is obtained from  $\mathbf{G}$  by deleting the rows corresponding to lost packets. This matrix will be denoted as  $\mathbf{C}_j$  and will be referred to as the *coding matrix* of the  $j$ -th user. A user can recover the source message if its coding matrix is full rank. We now define the *probability of successful delivery*  $P_L(\epsilon)$  of an  $L$ -user multicast network with PERs  $\epsilon = (\epsilon_1, \dots, \epsilon_L)$  as the probability that all users have successfully recovered the source message.

The simplest case of a multicast network is a point-to-point link with a single user characterised by a PER  $\epsilon$ . For a non-systematic code characterised by  $(N, K, q)$ , the probability of

successful delivery for such link is given by [24]:

$$P(\epsilon) = \sum_{m=K}^N \binom{N}{m} (1-\epsilon)^m \epsilon^{N-m} \mathbb{P}(m, K). \quad (2)$$

Here,  $\mathbb{P}(m, K)$  is the probability that an  $m \times K$  matrix of elements generated uniformly at random from  $\mathbb{F}_q$  is full rank, which is given by [21]:

$$\mathbb{P}(m, K) = \prod_{i=0}^{K-1} (1 - q^{i-m}). \quad (3)$$

It can be observed that (2) can be thought of as a marginalisation of the rank of the user's coding matrix over the distribution of the number of rows  $m$  in this matrix.

For a systematic  $(N, K, q)$  code and a point-to-point link, the probability of successful delivery can be expressed as follows [22]:

$$P^*(\epsilon) = \sum_{m=K}^N (1-\epsilon)^m \epsilon^{N-m} \sum_{h=h_{\min}}^K \binom{K}{h} \binom{N-K}{m-h} \cdot \mathbb{P}(m-h, K-h), \quad (4)$$

where  $h$  denotes a possible number of received systematic packets and  $h_{\min}$  is defined as  $\max(0, m - N + K)$ . Compared with (2) for the non-systematic case, we observe that an additional marginalisation over the distribution of  $h$  is required for the systematic code. In addition, the number of ways to select  $m$  received packets out of  $N$  is replaced with the number of ways to select  $h$  systematic packets out of  $K$  and  $m-h$  non-systematic packets out of  $N-K$ . Given that the user receives  $h$  systematic packets out of  $m$ ,  $h$  columns of its coding matrix will be linearly independent. Therefore, for the matrix to be full rank, the remaining  $K-h$  columns formed by the non-systematic coding vectors should be linearly independent. The minimum value of  $h$ ,  $h_{\min}$ , is chosen as the difference between the total number of received packets  $m$  and a maximum possible number of non-systematic packets,  $\min(m, (N-K))$ .

Consider now the general case of an  $L$ -user multicast network. As mentioned in Section I, if the field size  $q$  is sufficiently large, each user is able to recover the message with a high probability once it receives at least  $K$  packets. Indeed, (3) is close to 1 for large  $q$ . In this case, the users will recover the message independently from each other and the probability of successful delivery can be approximated as follows (in the case of a non-systematic  $(N, K, q)$  code):

$$P_L(\epsilon) \cong \prod_{j=1}^L P(\epsilon_j), \quad (5)$$

where  $P(\epsilon_j)$  is the probability of successful delivery of a source message over a point-to-point link with a PER  $\epsilon_j$  corresponding to the  $j$ -th user, as calculated by (2). It should be noted, however, that with a limited field size  $q$ , the accuracy of (5) is expected to decrease as the number of users grows.

For a specific case of  $L = 2$ , it was shown in [24] that (5) is a good approximation even if  $q$  is small, provided that the number of transmissions and PER are high enough for the users to receive independent subsets of packets. By contrast,

TABLE I  
NOTATION USED THROUGHOUT THE PAPER

Notation	Description
$L$	Number of user forming a multicast network
$K$	Number of packets forming an information message
$N$	Number of coded packet transmissions
$q$	Size of the finite field under consideration
$U_j$	Set of indices of transmitted packets received by the $j$ -th user
$m_j$	Total number of packets received by the $j$ -th user
$\mu$	Random variable denoting the number of packets received simultaneously by all the users
$\theta_J$	Random variable denoting the number of packets received simultaneously by a subset $J$ of $L$ users, $1 <  J  < L$
$\theta$	Tuple of variables $\theta_J$ for all possible subsets $J$ , $1 <  J  < L$
$\mathbb{P}(m, K)$	Probability that an $m \times K$ matrix of elements generated uniformly at random from $\mathbb{F}_q$ is full rank
$\mathbb{P}^{(i)}(m, K)$	Probability that an $m \times K$ matrix of elements generated uniformly at random from $\mathbb{F}_q$ has rank $i$
$P(\epsilon)$	Probability of successful delivery over a point-to-point link with PER $\epsilon$ for non-systematic RLNC
$P^*(\epsilon)$	Probability of successful delivery over a point-to-point link with PER $\epsilon$ for systematic RLNC
$P_L(\epsilon)$	Probability of successful delivery over a multicast network with $L \geq 2$ users and PERs $\epsilon = (\epsilon_1, \dots, \epsilon_L)$ for non-systematic RLNC
$P_L^*(\epsilon)$	Probability of successful delivery over a multicast network with $L \geq 2$ users and PERs $\epsilon = (\epsilon_1, \dots, \epsilon_L)$ for systematic RLNC

an exact formulation for the probability of successful delivery, valid for any field size, number of transmissions and channel conditions, was obtained for a two-user multicast network in [25] for non-systematic RLNC. The exact formulation is given as follows:

$$P_2(\epsilon) = \sum_{m_1=K}^N \sum_{m_2=K}^N \left( \prod_{j=1}^2 (1-\epsilon_j)^{m_j} \epsilon_j^{N-m_j} \right) \cdot \sum_{\mu} \binom{N}{\mu} \binom{N-\mu}{m_1-\mu} \binom{N-\mu}{m_2-\mu} \mathbb{P}_2(\mathbf{m}, \mu; K), \quad (6)$$

where  $\mathbf{m} = (m_1, m_2)$  and the innermost summation is performed over  $\mu = \max(0, m_1 + m_2 - N), \dots, \min(m_1, m_2)$ . Here,  $\mu$  denotes the number of common packets received by the two users and  $\mathbb{P}_2(\mathbf{m}, \mu; K)$  denotes the probability of two correlated random matrices with dimensions  $m_1 \times K$  and  $m_2 \times K$  and  $\mu$  common rows being simultaneously full rank, for  $m_1, m_2 \geq K$ . This probability is given by

$$\mathbb{P}_2(\mathbf{m}, \mu; K) = \sum_i \mathbb{P}^{(i)}(\mu, K) \prod_{j=1}^2 \mathbb{P}(m_j - \mu, K - i), \quad (7)$$

where the summation is performed over the values of  $i$  from  $\max(0, K - m_1 + \mu, K - m_2 + \mu)$  to  $\min(\mu, K)$ . Term  $\mathbb{P}^{(i)}(\mu, K)$  denotes the probability that a random  $\mu \times K$  matrix has rank  $i$  [25]:

$$\mathbb{P}^{(i)}(\mu, K) = \frac{1}{q^{(\mu-i)(K-i)}} \prod_{l=0}^{i-1} \frac{(1-q^{l-\mu})(1-q^{l-K})}{1-q^{l-i}}. \quad (8)$$

The notation introduced in this section is summarised in Table I.



### III. PROPOSED THEORETICAL FRAMEWORK

We now turn our attention toward the general case of an  $L$ -user multicast network described at the beginning of the previous section. Our goal is to derive the probability of successful decoding in such a network for two cases - non-systematic and systematic RLNC. We start by formulating a general framework, and then consider each case individually.

The transmission of  $N$  coded packets over  $L$  lossy links can be modelled as  $N$  independent trials. In each trial, the packet can be received by a single user, by a selection of at least two users or by none of the users. The total number of outcomes is equal to  $\sum_{i=0}^L \binom{L}{i} = 2^L$ .

Consider first the packets received by a group of at least two users. Let  $\mu$  be a random variable denoting a number of packets received simultaneously by all the users, i.e.,  $\mu = |U_1 \cap \dots \cap U_L|$ . Furthermore, let  $\theta_J = \left| \left( \bigcap_{j \in J} U_j \right) \cap \left( \bigcap_{j \notin J} \bar{U}_j \right) \right|$ , where  $J \subset \{1, \dots, L\}$ ,  $1 < |J| < L$ , be a random variable denoting the number of transmitted packets received simultaneously by at least two, but less than  $L$  users and *not* received by the remaining users. For convenience, let  $\theta_J$  obtained for all possible subsets  $J$  be assembled in a tuple of  $2^L - L - 2$  random variables  $\theta$ .

Consider now the packets received by a single user only. However, instead of introducing another set of  $L$  random variables, we observe that if the total number of packets received by the  $j$ -th user,  $m_j$ , is known, the number of packets received only by this user can be calculated as  $m_j - \mu - \sum_{J: j \in J} \theta_J$ , where the summation is performed over all possible subsets  $J \subset \{1, \dots, L\}$ ,  $1 < |J| < L$ , that include  $j$ . In other words, the number of packets unique to the  $j$ -th user is fully determined by  $m_j$ ,  $\mu$  and  $\theta$ .

Finally, the number of packets received by *none* of the users,  $\left| \bigcap_{j=1}^L \bar{U}_j \right|$ , can be calculated as follows. If the numbers of packets  $m_j$ , for  $j = 1, \dots, L$ , received by each user are added up, the number of packets  $\mu$  common to all users will be counted  $L$  times. Similarly, the number of packets  $\theta_J$  received by a subset of users  $J \subset \{1, \dots, L\}$ ,  $1 < |J| < L$ , will be counted  $|J|$  times. Since each transmitted packet should be counted only once, the number of packets not received by any user can be computed as follows:

$$\left| \bigcap_{j=1}^L \bar{U}_j \right| = N - \sum_{j=1}^L m_j + (L-1)\mu + \sum_{l=2}^{L-1} (l-1) \sum_{J: |J|=l} \theta_J. \quad (9)$$

*Example 1:* For a multicast network of  $L = 3$  users,

- $\mu = |U_1 \cap U_2 \cap U_3|$ ,
- $\theta_{\{1,2\}} = |U_1 \cap U_2 \cap \bar{U}_3|$ ,
- $\theta_{\{1,3\}} = |U_1 \cap \bar{U}_2 \cap U_3|$ ,
- $\theta_{\{2,3\}} = |\bar{U}_1 \cap U_2 \cap U_3|$ .

The number of packets received uniquely, for instance, by the first user is  $m_1 - \mu - \theta_{\{1,2\}} - \theta_{\{1,3\}}$ , and the number of packets received by none of the users is  $N - \sum_j m_j + 2\mu + \theta_{\{1,2\}} + \theta_{\{1,3\}} + \theta_{\{2,3\}}$ .

To summarise, the combination of  $m_1, \dots, m_L$ ,  $\mu$  and  $\theta$  describes all possible outcomes of the transmission of  $N$  coded packets. Let  $f(\mathbf{m}, \mu, \theta; N; \epsilon)$  be the joint probability mass

function (PMF) of these variables, where  $\mathbf{m} = (m_1, \dots, m_L)$ . The PMF can be expressed as follows:

$$f(\mathbf{m}, \mu, \theta; N; \epsilon) = \gamma(\mathbf{m}, \mu, \theta; N) \varphi_L(\mathbf{m}, N, \epsilon). \quad (10)$$

The first term,  $\gamma(\mathbf{m}, \mu, \theta; N)$ , denotes the number of ways to select  $\mathbf{m}$ ,  $\mu$  and  $\theta$  out of  $N$ . It can be calculated as a product of binomial coefficients, the number of which is equal to  $2^L - 1$ , the total number of elements in  $\mathbf{m}$ ,  $\mu$  and  $\theta$ . The second term in (10) denotes the probability of a particular combination of values contained in  $\mathbf{m}$ ,  $\mu$ ,  $\theta$  and can be calculated as follows. Consider probability  $1 - \epsilon_j$ , which is associated with coded packets received by the  $j$ -th user,  $j = 1, \dots, L$ . The total number of such packets is  $m_j$ . On the other hand, probability  $\epsilon_j$  is associated with packets not received by the  $j$ -th user, the total number of which is  $N - m_j$ . Therefore,  $\varphi_L(\mathbf{m}, N, \epsilon)$  can be calculated as follows:

$$\varphi_L(\mathbf{m}, N, \epsilon) = \prod_{j=1}^L (1 - \epsilon_j)^{m_j} \epsilon_j^{N - m_j}. \quad (11)$$

We observe that the probability of particular combination of  $\mathbf{m}$ ,  $\mu$  and  $\theta$  does not depend on  $\mu$  or  $\theta$ .

In general, the probability of successful decoding for a multicast network of  $L$  users can be calculated by marginalising the probability of all  $L$  coding matrices being full rank over the joint distribution of  $\mathbf{m}$ ,  $\mu$  and  $\theta$ :

$$P_L(\epsilon) = \sum_{\mathbf{m}, \mu, \theta} f(\mathbf{m}, \mu, \theta; N; \epsilon) \mathbb{P}_L(\mathbf{m}, \mu, \theta; K), \quad (12)$$

where

$$\mathbb{P}_L(\mathbf{m}, \mu, \theta; K) = \Pr \left[ \bigcap_{j=1}^L \text{rank}(\mathbf{C}_j) = K \right] \quad (13)$$

is the probability that coding matrices  $\mathbf{C}_1, \dots, \mathbf{C}_L$  are simultaneously full rank. We note that (12) applies to both non-systematic and systematic codes. One can observe two challenges associated with the direct calculation of (12). The first challenge is to express the summation over  $\mathbf{m}$ ,  $\mu$  and  $\theta$  and to calculate the PMF  $f(\mathbf{m}, \mu, \theta; N; \epsilon)$ . Based on the discussion above, the number of nested sums in (12) and the number of binomial coefficients in  $f(\mathbf{m}, \mu, \theta; N; \epsilon)$  will grow exponentially with the number of users  $L$ , thus making the direct approach impractical.

The second challenge associated with computing (12) is to calculate the probability (13) of  $L$  correlated matrices being full rank, for a given combination of  $\mathbf{m}$ ,  $\mu$  and  $\theta$ . In Section II, (7) shows how this probability can be exactly calculated for  $L = 2$  by marginalising it over the distribution of the rank of the submatrix formed by the common rows. Applying this approach to a larger number of matrices, however, is impractical, since the number of distinct sets of common rows, hence the number of submatrices whose ranks need to be considered, grows exponentially with  $L$ .

Next, we address the problem of calculating (12) for non-systematic and systematic RLNC.

### A. Non-Systematic RLNC

We start with the second challenge, the calculation of the probability (13) of  $L$  correlated coding matrices being full rank. First, we establish the following result:

**Lemma 1:** The probability (13) that  $L$  correlated random matrices generated over  $\mathbb{F}_q$  with dimensions  $m_j \times K$  are full rank,  $j = 1, \dots, L$ , is lower-bounded as follows:

$$\Pr \left[ \bigcap_{j=1}^L \text{rank}(\mathbf{C}_j) = K \right] \geq \prod_{j=1}^L \Pr [\text{rank}(\mathbf{C}_j) = K] \\ = \prod_{j=1}^L \mathbb{P}(m_j, K), \quad (14)$$

where  $\mathbb{P}(m_j, K)$  is given by (3).

*Proof:* See Appendix A. ■

The lower bound (14) is often implicitly used in the literature. For instance, by substituting (14) to (12), the approximation (5) can be obtained. In contrast with the literature, however, Lemma 1 establishes that this approximation is indeed a lower bound. At the same time, we note that the bound (14) becomes loose if significant correlation between the matrices is present. For instance, consider two matrices with dimensions  $m_1 \times K$  and  $m_2 \times K$ , such that  $m_1 \geq m_2 \geq K$  and  $\mu = m_2$ . Clearly, in this case the probability of both matrices having full rank is equal to  $\mathbb{P}(m_2, K)$ . However, the same probability as predicted by bound (14) is equal to  $\mathbb{P}(m_1, K)\mathbb{P}(m_2, K)$ , which is smaller than the exact value by  $\mathbb{P}(m_1, K)$  times.

Based on Lemma 1, we now establish a tighter bound for (13):

**Lemma 2 (Improved Bound):** The probability (13) that  $L$  correlated random matrices generated over  $\mathbb{F}_q$  are full rank is lower-bounded by  $\tilde{\mathbb{P}}_L(\mathbf{m}, \mu; K)$ , which is given by

$$\tilde{\mathbb{P}}_L(\mathbf{m}, \mu; K) = \sum_i \mathbb{P}^{(i)}(\mu, K) \prod_{j=1}^L \mathbb{P}(m_j - \mu, K - i), \quad (15)$$

where the summation is performed over the values of  $i$  from  $\max_j(0, K - m_j + \mu)$  to  $\min(\mu, K)$  and  $\mathbb{P}^{(i)}(\mu, K)$  is the probability that an  $\mu \times K$  matrix has rank  $i$ , as given by (8).

*Proof:* Using the notation introduced earlier, each of the coding matrices  $\mathbf{C}_1, \dots, \mathbf{C}_L$  has  $\mu$  rows common to all of them. By averaging over the distribution of the rank of the matrix formed by these  $\mu$  common rows, probability (13) for non-systematic RLNC can be expressed as follows:

$$\mathbb{P}_L(\mathbf{m}, \mu, \theta; K) = \sum_{i=\max_j(0, K-m_j+\mu)}^{\min(\mu, K)} \mathbb{P}^{(i)}(\mu, K) \\ \cdot \Pr \left[ \bigcap_{j=1}^L \text{rank}(\mathbf{C}'_j) = K - i \right], \quad (16)$$

where  $\mathbf{C}'_j$  denotes a matrix formed by the intersection of the  $m_j - \mu$  rows of  $\mathbf{C}_j$  not common to all matrices and  $K - i$  columns. The starting value of  $i$  in the summation in (16) is chosen such that for any matrix  $\mathbf{C}'_j$ , there are at least as many rows as columns, i.e.,  $m_j - \mu \geq K - i$ . Such starting

value excludes unnecessary summation terms. As regards the maximum value of the summation index  $i$ , it is chosen as the minimum dimension of the matrix formed by  $\mu$  common rows. The application of Lemma 1 to the second term in the product under the summation in (16) results in the lower bound (15). ■

**Remark 1:** For a two-user multicast network, the bound (15) is exact and reduces to (7).

We note that by marginalizing over the distribution of the rank of the matrix formed by the rows common to all matrices, the bound (15) is expected to be tighter than that of Lemma 1, especially if the number of common rows  $\mu$  is large. We illustrate this statement using the following example.

**Example 2:** Consider three  $6 \times 5$  matrices generated uniformly at random over the binary field  $\mathbb{F}_2$ , such that all three matrices have  $\mu = 4$  common rows. Furthermore, assume that each of the three possible pairs of matrices has an additional common row between them. In this case, none of the matrices has rows generated independently from the other matrices. The probability of all three matrices being full rank estimated by Monte Carlo simulations and obtained by averaging over  $10^4$  random realisations is equal to 0.33. The same probability obtained using the bounds (14) and (15) is equal to 0.20 and 0.27, respectively. Clearly, in this example the new bound of Lemma 2 provides closer approximation.

At this point, we have established a more accurate lower bound for the probability (13) that all  $L$  coding matrices are simultaneously full rank for a given distribution of received packets among the users. We now proceed to the derivation of the probability of successful delivery (12) for the non-systematic case.

**Theorem 1:** The probability of successful delivery in an  $L$ -user multicast network characterised by PERs  $\epsilon$  and employing an  $(N, K, q)$  non-systematic code is lower-bounded as follows:

$$P_L(\epsilon) \geq \sum_{\mathbf{m}} \varphi_L(\mathbf{m}, N, \epsilon) \sum_{\mu} \alpha_L(\mathbf{m}, \mu; N) \tilde{\mathbb{P}}_L(\mathbf{m}, \mu; K), \quad (17)$$

where

$$\alpha_L(\mathbf{m}, \mu; N) = \binom{N}{\mu} \sum_{l=0}^{\min_j(m_j-\mu)} (-1)^l \binom{N-\mu}{l} \\ \cdot \prod_{j=1}^L \binom{N-\mu-l}{m_j-\mu-l} \quad (18)$$

and the summation is performed over  $m_j = K, \dots, N$  and

$$\mu = \max \left( 0, \sum_{j=1}^L m_j - (L-1)N \right), \dots, \min_j m_j. \quad (19)$$

*Proof:* Substituting (10) into (12) and using the fact that  $\varphi_L$  (11) does not depend on  $\mu$  and  $\theta$ , the probability in question can be expressed as follows:

$$P_L(\epsilon) = \sum_{\mathbf{m}} \varphi_L(\mathbf{m}, N, \epsilon) \\ \cdot \sum_{\mu, \theta} \gamma(\mathbf{m}, \mu, \theta; N) \mathbb{P}_L(\mathbf{m}, \mu, \theta; K). \quad (20)$$

We now employ Lemma 2 and bound (20) from below:

$$P_L(\epsilon) \geq \sum_{\mathbf{m}} \varphi_L(\mathbf{m}, N, \epsilon) \sum_{\mu} \tilde{\mathbb{P}}_L(\mathbf{m}, \mu; K) \cdot \sum_{\theta} \gamma(\mathbf{m}, \mu, \theta; N). \quad (21)$$

To prove (17), we now show that the innermost sum in (21) is equal to  $\alpha_L(\mathbf{m}, \mu; N)$  given by (18). To this end, we rewrite this sum as follows:

$$\sum_{\theta} \gamma(\mathbf{m}, \mu, \theta; N) = \binom{N}{\mu} \beta, \quad (22)$$

where

$$\beta = \sum_{\theta} \gamma(\mathbf{m} - \mu, 0, \theta; N - \mu). \quad (23)$$

In other words, by selecting  $\mu$  out of  $N$  packets common to all users,  $\beta$  is the total number of possible selections of  $\sum_{j=1}^L (m_j - \mu)$  packets out of  $N - \mu$  such that none of the packets is received by all users at the same time. The value of  $\beta$  can be calculated by the inclusion-exclusion principle in its complementary form [29]. To this end, let  $S$  denote a set of all possible selections of  $\sum_{j=1}^L (m_j - \mu)$  packets out of  $N - \mu$ . The number of elements in this set is

$$|S| = \prod_{j=1}^L \binom{N - \mu}{m_j - \mu}. \quad (24)$$

Consider now subsets  $S_k$  of  $S$ ,  $k = 1, \dots, N - \mu$ , containing selections corresponding to the  $k$ -th transmitted packet received by all the  $L$  users. Let  $\bar{S}_k$  denote the complement of  $S_k$  in  $S$ . It can be observed that  $\beta$  can be thought of as the cardinality of a set constructed as the intersection of all  $\bar{S}_k$ ,  $k = 1, \dots, N - \mu$ . Using the inclusion-exclusion principle,

$$\begin{aligned} \beta &= \left| \bigcap_{k=1}^{N-\mu} \bar{S}_k \right| \\ &= |S| - \sum_{k=1}^{N-\mu} |S_k| + \sum_{1 \leq k_1 < k_2 \leq N-\mu} |S_{k_1} \cap S_{k_2}| - \dots \\ &\quad - (-1)^z \sum_{1 \leq k_1 < \dots < k_z \leq N-\mu} |S_{k_1} \cap \dots \cap S_{k_z}|, \end{aligned} \quad (25)$$

where  $z = \min_j (m_j - \mu)$  is the minimum possible number of packets received by all the  $L$  users. The first summation in (25) corresponds to  $N - \mu$  possible selections of a single packet received by all the users, with  $\prod_{j=1}^L \binom{N-\mu-1}{m_j-\mu-1}$  selections for other  $N - \mu - 1$  available packets. Similarly, the second summation in (25) corresponds to  $\binom{N-\mu}{2}$  selections of two commonly received packets and  $\prod_{j=1}^L \binom{N-\mu-2}{m_j-\mu-2}$  selections of other packets. Expression (25) can therefore be written in a compact form as follows:

$$\beta = \sum_{l=0}^z (-1)^l \binom{N-\mu}{l} \prod_{j=1}^L \binom{N-\mu-l}{m_j-\mu-l}, \quad (26)$$

thus making the inner sum in (21) equal to  $\alpha_L(\mathbf{m}, \mu; N)$  (18).

The values of  $(m_1, \dots, m_L)$  over which the outer-most summation in (17) is performed are chosen so that each user

should receive at least  $K$  packets. As regards the number of packets  $\mu$  received by all users, its maximum value cannot exceed the smallest  $m_j$ , for  $j = 1, \dots, L$ . The starting value of  $\mu$  can be found assuming that all other  $N - \mu$  transmitted packets have been simultaneously received by  $L - 1$  users. As a result,  $\mu \geq \sum_j m_j - (L - 1)N$ . If  $(L - 1)N > \sum_j m_j$ , the starting value of  $\mu$  should be 0. ■

*Remark 2:* We note that bound (17) is obtained by applying Lemma 2, meaning that only packets received simultaneously by all users are considered to take into account the correlation effect. As a result, the bound is expected to be especially tight if the number of such packets  $\mu$  is likely to be large, which is typical in scenarios where a non-negligible fraction of users experiences PERs that are relatively small. We observe that this is the case of multicast networks where users are spread across the coverage area of the source node (namely, a base station serving a cell). As argued in [30], 3GPP's LTE-A systems [31] are likely to ensure reduced user PERs across the majority of the cell area. Finally, for large values of PER,  $\mu$  is likely to be small and the bound converges to the traditional approximation (5).

*Remark 3:* The derived bound is exact for  $L = 2$  users and matches (6). Indeed, the product of binomial coefficients in (6) can be shown to be equal to  $\alpha_2(\mathbf{m}, \mu; N)$  defined by (18) as follows. Without loss of generality, let  $m_1 \leq m_2$ . The last binomial coefficient in (6) is equivalent to the number of  $N - m_2$  selections out of  $N - \mu$  packets, such that each selection includes  $m_1 - \mu$  packets. We can again employ the inclusion-exclusion principle and denote  $S$  as a set of all possible selections, with the number of elements in this set equal to  $\binom{N-\mu}{N-m_2}$ . Let  $S_k$  denote a subset of  $S$  containing selections in which the  $k$ -th packet belonging to the group of  $m_1 - \mu$  packets is not included,  $k = 1, \dots, m_1 - \mu$ . The last binomial coefficient in (6) can be expressed as follows:

$$\begin{aligned} \binom{N-m_1}{m_2-\mu} &= \left| \bigcap_{k=1}^{m_1-\mu} \bar{S}_k \right| \\ &= \sum_{l=0}^{m_1-\mu} (-1)^l \binom{m_1-\mu}{l} \binom{N-\mu-l}{N-m_2}. \end{aligned} \quad (27)$$

Multiplying the right-hand side of (27) with the first two binomial coefficients of (6) yields:

$$\begin{aligned} &\binom{N}{\mu} \binom{N-\mu}{m_1-\mu} \sum_{l=0}^{m_1-\mu} (-1)^l \binom{m_1-\mu}{l} \binom{N-\mu-l}{N-m_2} \\ &= \binom{N}{\mu} \sum_{k=0}^{m_1-\mu} (-1)^k \binom{N-\mu-k}{m_1-\mu-k} \binom{N-\mu-k}{m_1-\mu-k} \\ &= \alpha_2(\mathbf{m}, \mu; N). \end{aligned}$$

## B. Systematic RLNC

As pointed out in Remark 2, the bound (17) derived for non-systematic RLNC was obtained by considering packets received simultaneously by all users, thus partially taking into account the correlation between their coding matrices. In the case of systematic RLNC, the correlation arises only

from commonly received *non-systematic* packets, since the systematic packets correspond to deterministic vectors of coding coefficients. For small values of PER, each user is likely to receive all  $K$  systematic packets regardless of the number of received non-systematic packets. Even for large values of PER, the correlation effect is smaller than in the case of non-systematic RLNC, since the number of transmitted non-systematic packets for systematic RLNC is smaller than the total number of transmissions. Therefore, it is expected that for systematic RLNC, considering a multicast network as a set of independent unicast connections will result in an approximation close enough for any field size and PER. We now state this result formally and prove that such approximation is a lower bound, as in the case of non-systematic RLNC.

**Theorem 2:** The probability of successful delivery  $P_L^*(\epsilon)$  of the  $L$ -user multicast network characterised by PERs  $\epsilon$  and employing an  $(N, K, q)$  systematic code is lower-bounded as follows:

$$P_L^*(\epsilon) \geq \prod_{j=1}^L P^*(\epsilon_j), \quad (28)$$

where  $P^*(\epsilon_j)$  is the probability of successful delivery of a point-to-point link with a PER  $\epsilon_j$  given by (4).

*Proof:* Consider the general formulation for the probability of successful delivery of the multicast network (12), but with marginalisation over the distribution of  $\mathbf{m}$  only:

$$P_L^*(\epsilon) = \sum_{\mathbf{m}} \varphi_L(\mathbf{m}, N, \epsilon) \mathbb{P}_L^*(\mathbf{m}, K) \prod_{j=1}^L \binom{N}{m_j}, \quad (29)$$

where  $\mathbb{P}_L^*(\mathbf{m}, K)$  denotes the probability that all  $L$  coding matrices are simultaneously full rank. This probability can be marginalised over the probability distribution of the number of systematic packets  $h_j$  received by the  $j$ -th user as follows:

$$\mathbb{P}_L^*(\mathbf{m}, K) = \sum_{h_1} \dots \sum_{h_L} \left[ \prod_{j=1}^L \frac{\binom{K}{h_j} \binom{N-K}{m_j-h_j}}{\binom{N}{m_j}} \right] \cdot \Pr \left[ \bigcap_{j=1}^L \text{rank}(\mathbf{C}'_j) = K - h_j \right], \quad (30)$$

where matrix  $\mathbf{C}'_j$  is composed of the intersection of  $m_j - h_j$  non-systematic rows and  $K - h_j$  columns of the  $j$ -th coding matrix  $\mathbf{C}_j$ . Equation (30) can be lower-bounded by applying Lemma 1 to its probability term and employing the distributive law as follows:

$$\mathbb{P}_L^*(\mathbf{m}, K) \geq \prod_{j=1}^L \sum_{h_j} \frac{\binom{K}{h_j} \binom{N-K}{m_j-h_j}}{\binom{N}{m_j}} \mathbb{P}(m_j - h_j, K - h_j). \quad (31)$$

The bound (28) can now be obtained by substituting (31) into (29). ■

Bound (28) will be investigated in Section IV-B, where we will show that it is sufficiently tight even for binary codes and small values of PER.

### C. Computational Complexity Consideration

Comparing bounds (17) and (28) for non-systematic and systematic codes, it can be observed that the former is significantly more complex than the latter, especially if the number of users  $L$  is large. In this section, we show how the calculation of bound (17) in the non-systematic case can be optimised.

Consider the outermost summation in (17), which is performed over  $L$  variables contained in tuple  $\mathbf{m}$ , with each variable taking values from  $K$  to  $N$ . As a result, the number of terms in the summation is equal to  $(N - K + 1)^L$ , which makes (17) computationally prohibitive if the number of users  $L$  is large. At the same time, it can be observed that  $\alpha_L(\cdot)$  and  $\mathbb{P}_L(\cdot)$  in (17), the most computationally intensive terms, do not depend on the order of elements within  $\mathbf{m}$ . Thus, the number of times these terms are calculated can be significantly reduced as follows.

Let us rewrite relation (17) as follows:

$$P_L(\epsilon) \geq \sum_{\mathbf{m}'} \left( \sum_{\pi(\mathbf{m}')} \varphi_L(\mathbf{m}, N, \epsilon) \right) \cdot \sum_{\mu} \alpha_L(\mathbf{m}', \mu; N) \tilde{\mathbb{P}}_L(\mathbf{m}', \mu; K), \quad (32)$$

where the outer summation is now performed over all possible combinations  $\mathbf{m}'$  of  $L$  values from  $K$  to  $N$  with no reference to order, and  $\pi(\mathbf{m}')$  denotes a permutation of  $\mathbf{m}'$ . The problem of calculating the number of possible combinations of  $L$  values from  $K$  to  $N$  can be recast as that of finding the number of ways to place  $L$  balls into  $N - K + 1$  urns. Indeed, a particular combination  $\mathbf{m}'$  is equivalent to one way of assigning each of the  $N - K + 1$  values (urns) a non-negative number of occurrences (balls)  $L_i$ ,  $i = 1, \dots, N - K + 1$ , so that

$$\sum_{i=1}^{N-K+1} L_i = L. \quad (33)$$

The number of solutions to (33), and hence the number of terms in the outer summation in (32), can be found using the stars and bars principle [32] and is equal to

$$\binom{N - K + 1 + L - 1}{L} = \binom{N - K + L}{L}. \quad (34)$$

This number is much smaller than  $(N - K + 1)^L$ , the number of terms in the outer summation in the original expression (17), as illustrated in the following example.

**Example 3:** Let  $L = 4$  and  $N - K = 10$ . Based on (34), the number of terms in the outer summation in (32) is equal to  $\binom{14}{4} = 1001$ , which is 14.6 times smaller than  $11^4 = 14641$ , the number of terms in the outer summation in the original expression (17). As a result, the number of times  $\alpha_L(\cdot)$  and  $\mathbb{P}_L(\cdot)$  are calculated is significantly reduced compared with the original expression. Clearly, the reduction factor will increase with  $L$ .

Further complexity reduction can be achieved in the case of a homogeneous network, in which each user has the same



TABLE II  
NETWORK AND CODE PARAMETERS USED TO EVALUATE  
THE ACCURACY OF THE PROPOSED BOUNDS

Parameter	Values
Number of users $L$	$\{2, 6, 10\}$
PER $\epsilon$	$\{0.01, 0.1\}$
Number of source packets $K$	$\{5, 10, 15, 20\}$
Number of transmissions $N$	$\{K, K+1, \dots, K+10\}$
Finite field size $q$	$\{2, 2^8\}$

PER  $\epsilon = \epsilon_j$  for  $j = 1, \dots, L$ . In this case, (32) simplifies to

$$P_L(\epsilon) \geq \sum_{\mathbf{m}'} \phi'_L(\mathbf{m}', N, \epsilon) \sigma(\mathbf{m}') \cdot \sum_{\mu} \alpha_L(\mathbf{m}', \mu; N) \tilde{\mathbb{P}}_L(\mathbf{m}', \mu; K), \quad (35)$$

where

$$\phi'_L(\mathbf{m}', N, \epsilon) = (1 - \epsilon)^{\sum \mathbf{m}' \epsilon^{LN - \sum \mathbf{m}'}} \quad (36)$$

and  $\sigma(\mathbf{m}') = \sum_{\pi(\mathbf{m}')} \pi(\mathbf{m}')$  is the number of permutations of a particular combination  $\mathbf{m}'$  of  $L$  values from  $K$  to  $N$ . This number depends on a particular solution to (33) and can be calculated as follows:

$$\sigma(\mathbf{m}') = \frac{L!}{\prod_{i=1}^{N-K+1} L_i!}. \quad (37)$$

To further speed up calculation, probabilities  $\mathbb{P}(\cdot)$  and  $\mathbb{P}^{(i)}(\cdot)$ , which are used repetitively in the calculation of  $\tilde{\mathbb{P}}_L(\cdot)$ , can be pre-computed offline for a given  $(N, K, q)$  code and stored in a look-up table.

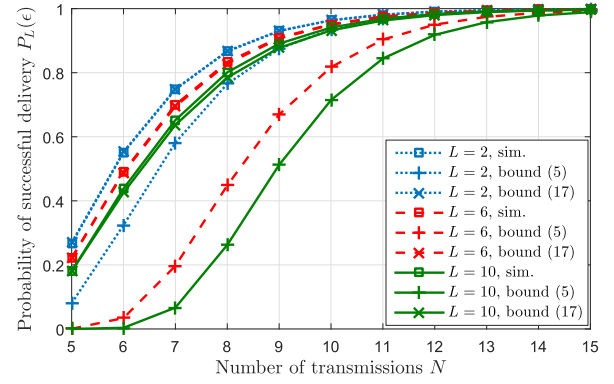
#### IV. NUMERICAL RESULTS

In this section, we investigate the performance of a multicast network under non-systematic and systematic RLNC via simulation and compare the results with the derived theoretical bounds. Simulation results in terms of probability of successful delivery were obtained using the Kodo C++ network coding library [33] and the Monte Carlo method, with each point being the result of an average over  $10^5$  iterations. The results are compared for various combinations of network and code parameters, as summarised in Table II. The accuracy of the bounds is evaluated in terms of Mean Square Error (MSE) for a given combination of  $L$ ,  $\epsilon$ ,  $K$  and  $q$  over the range of numbers of transmissions  $N$ . Unless otherwise stated, a homogeneous scenario is assumed, in which each user experiences the same PER  $\epsilon$ .

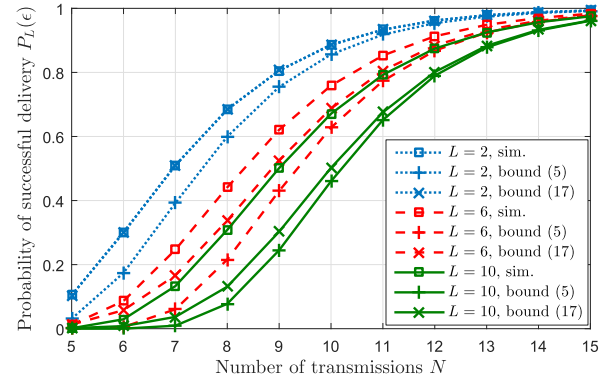
##### A. Non-Systematic RLNC

We start with a multicast network operating under a binary, non-systematic code corresponding to  $q = 2$ . Specifically, we compare the proposed bound (17) against bound (5) used in the literature for large field sizes. In addition, we benchmark both bounds against simulated results.

Fig. 1 shows the probability of successful delivery  $P_L(\epsilon)$  to  $L \in \{2, 6, 10\}$  users as a function of the number of coded transmissions  $N$ . The number of source packets is fixed to



(a)  $\epsilon = 0.01$



(b)  $\epsilon = 0.1$

Fig. 1. Probability of successful delivery for a binary non-systematic code as a function of  $N$  for  $K = 5$  and  $L \in \{2, 6, 10\}$ .

$K = 5$  and two PER values common to all users are considered:  $\epsilon = 0.01$  and  $0.1$ . The latter value of  $\epsilon$  is commonly used in practice as the maximum acceptable PER. For instance, in 3GPP's LTE-A systems, the link adaptation mechanism typically switches the modulation and coding scheme once the transport block error rate reaches 0.1 [31], [34]. Therefore, this value of PER can be thought of as a worst-case scenario. It can be observed that the proposed bound as per (17) provides better approximation than bound (5). Specifically, bound (17) is particularly accurate for  $\epsilon = 0.01$ , where it matches the simulated results for  $L = 2$  ( $\text{MSE} = 2 \cdot 10^{-6}$ ) and closely follows them when  $L \in \{6, 10\}$  ( $\text{MSE} = 8 \cdot 10^{-6}$  and  $9 \cdot 10^{-5}$ , respectively). The tightness of the proposed bound in this scenario is explained by a large number of packets likely to be received simultaneously by all users. Indeed, when  $\epsilon$  is small, the probability that a single transmitted packet is received by all users, which is equal to  $(1 - \epsilon)^L$ , is large. This leads to a high correlation between the users coding matrices. This is in contrast with the traditional bound (5), which does not take into account commonly received packets. As a result, bound (5) is particularly loose when  $\epsilon$  is small, with the absolute gap from the simulated results being up to 0.58 when  $L = 10$  and  $N = 7$ , in contrast with 0.016 for the new bound. At the same time, as  $\epsilon$  or  $L$  increase, the probability that a packet will be received by all users decreases, so the accuracy of the proposed bound decreases too, as can be observed for



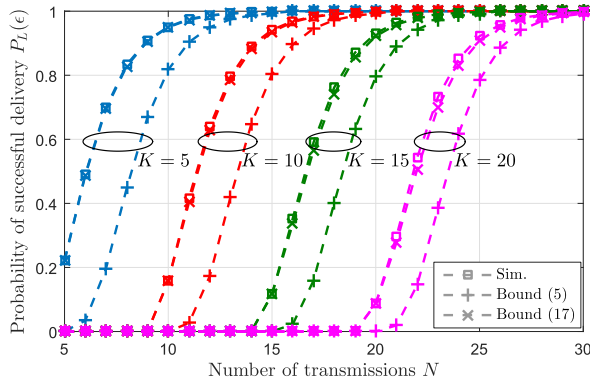
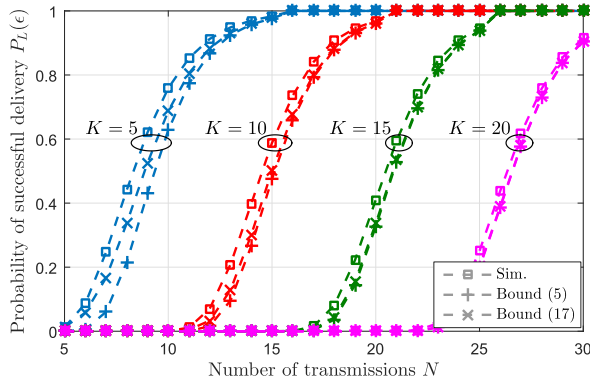
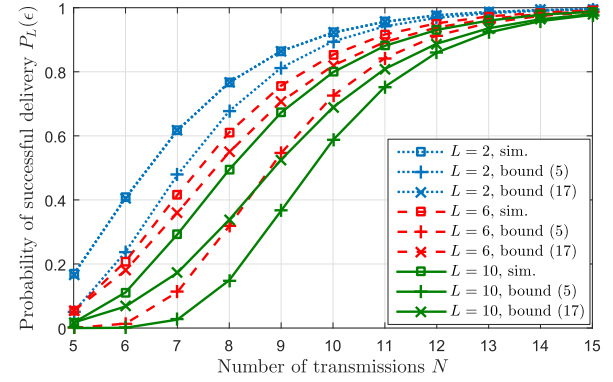

 (a)  $\epsilon = 0.01$ 

 (b)  $\epsilon = 0.1$ 

 Fig. 2. Probability of successful delivery for a binary non-systematic code as a function of  $N$  for  $L = 6$  and  $K \in \{5, 10, 15, 20\}$ .

$\epsilon = 0.1$  and  $L = 10$  ( $\text{MSE} = 0.01$ ). We reiterate, however, that bound (17) is exact for  $L = 2$  and any  $\epsilon$ , as per Remark 3.

Fig. 2 illustrates the results for the same scenario as in Fig. 1, but this time for different numbers of source packets  $K \in \{5, 10, 15, 20\}$  and a fixed number of users  $L = 6$ . In line with the previous results, the proposed bound (17) closely follows the simulated performance at  $\epsilon = 0.01$ , exhibiting the MSE of  $8 \cdot 10^{-6}$ ,  $6 \cdot 10^{-5}$ ,  $1 \cdot 10^{-4}$  and  $3 \cdot 10^{-4}$  for  $K \in \{5, 10, 15, 20\}$ , respectively. The new bound is significantly more accurate than bound (5) at  $\epsilon = 0.01$ , with the latter having the MSE of up to  $7 \cdot 10^{-2}$ . It can be observed that for this PER, the accuracy of the proposed bound somewhat decreases as  $K$  grows. The reason is that longer source messages require more coded transmissions, which leads to a higher number of packet erasures for a given PER. As a result, the correlation between the users coding matrices reduces for larger  $K$ , which means a smaller number of packets received simultaneously by all users. For the same reason, it can be observed from Fig. 2 that the gap between the simulated results and bound (5) becomes smaller as  $K$  grows. For example, for  $\epsilon = 0.01$ , the maximum gap between bound (5) and the simulated results reduces from 0.5 for  $K = 5$  ( $N = 7$ ) to 0.4 for  $K = 20$  ( $N = 22$ ). Fig. 2b demonstrates that both bounds are close to the simulated results for the worst-case scenario in terms of PER, especially when  $K = 20$  –  $\text{MSE} = 9 \cdot 10^{-4}$  and  $8 \cdot 10^{-4}$  for bounds (5) and (17), respectively. It should be


 Fig. 3. Probability of successful delivery for a binary non-systematic code as a function of the number of transmissions  $N$  for the case when each user has a unique PER from 0.01 to 0.1, for  $L \in \{2, 6, 10\}$  and  $K = 5$ .

noted, however, that due to the high decoding complexity of non-systematic RLNC [13],  $K$  is likely to be small in practice, and in this regime the proposed bound (17) is noticeably more accurate ( $\text{MSE} = 3 \cdot 10^{-3}$  when  $K = 5$ ) than (5) ( $\text{MSE} = 1.4 \cdot 10^{-2}$  for the same value of  $K$ ) even if  $\epsilon$  is high.

The results so far were collected for a homogeneous network, in which each user has the same PER  $\epsilon$ . It is also relevant to verify the performance of the bounds for a more general case of a heterogeneous network, in which users have distinct PERs. To this end, we allocate  $L$  unique PER values from 0.01 to 0.1 with a constant step equal to  $0.99/(L - 1)$ , which is equivalent to a set of users placed on the symmetry axis of a cellular cell sector [35]. Fig. 3 compares the bounds and simulated results for such network, for the same values of  $L$  and  $K$  as in Fig. 1. It is clear that the proposed bound (17) is significantly more accurate than (5) even for  $L = 10$ , with the maximum absolute gap between the two bounds being 0.17, 0.24 and 0.19 for  $L = 2$  ( $N = 6$ ),  $L = 6$  ( $N = 7$ ) and  $L = 10$  ( $N = 8$ ), respectively.

*Remark 4:* Comparing with Fig. 1, it can be observed that the gap between the proposed bound and simulation results is larger than when each user has  $\epsilon = 0.01$ , but smaller than when each user has  $\epsilon = 0.1$ . This is an expected result, since the users have varying PERs between those two values. Still, we observe that the correlation effect given by the number  $\mu$  of packets received simultaneously by all the users is relevant and accounting for this makes our bound (17) tighter than (5).

Finally, Fig. 4 compares the bounds and simulated results for a non-binary, non-systematic code. A relatively large field size,  $q = 2^8$ , is selected, in which the traditional bound (5) is expected to be accurate. It can be observed that while bound (5) closely follows the simulated performance when  $L = 2$  ( $\text{MSE} = 10^{-6}$ ), it somewhat diverges from the simulated results at small  $N$  for a larger number of users and  $\epsilon = 0.01$ : for  $N = 5$ , the absolute gap is 0.01 and 0.02 for  $L = 6$  and 10, respectively. It is expected that the deviation of bound (5) will grow further when  $L$  is increased beyond 10. In other words, bound (5), traditionally used in the literature, has a noticeable approximation error, that grows with  $L$ , even for a large field size. By contrast, the proposed

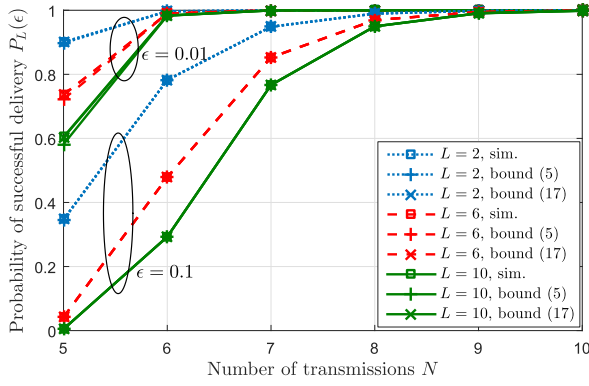


Fig. 4. Probability of successful delivery for a non-binary ( $q = 2^8$ ), non-systematic code as a function of the number of transmissions  $N$  for  $L \in \{2, 6, 10\}$ ,  $\epsilon \in \{0.01, 0.1\}$  and  $K = 5$ .

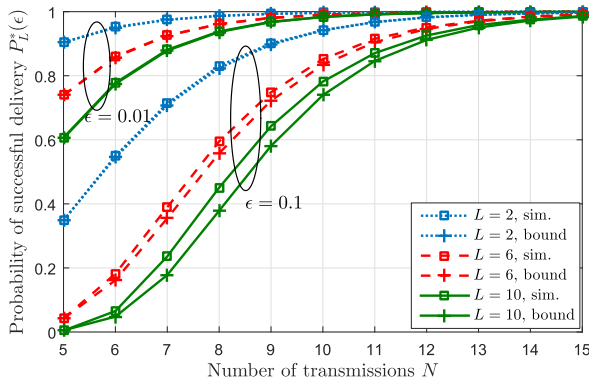


Fig. 5. Probability of successful delivery for a binary systematic code as a function of the number of transmissions  $N$  for  $L \in \{2, 6, 10\}$ ,  $\epsilon \in \{0.01, 0.1\}$  and  $K = 5$ .

bound (17) is clearly more accurate when  $\epsilon = 0.01$ , with the largest deviation from the simulated results (corresponding to  $L = 10$  and  $N = 5$ ) being  $2 \cdot 10^{-3}$ , 10 times lower than that of bound (5). As regards  $\epsilon = 0.1$ , both bounds accurately describe the performance, with the worst-case MSE (corresponding to  $L = 10$ ) equal to  $8 \cdot 10^{-4}$  and  $7 \cdot 10^{-4}$  for bound (5) and (17), respectively.

To summarise, the proposed bound (17) for non-systematic RLNC is tighter than the existing bound (5) traditionally used in the literature. The difference between the bounds is especially profound in realistic channel conditions, when users have small values of PER.

### B. Systematic RLNC

We now turn our attention to a multicast network operating under systematic RLNC, the performance bound for which was proposed in Theorem 2. In this scenario, the first  $K$  transmissions are the original source packets, followed by coded, non-systematic packets. Fig. 5 compares bound (28) with simulated performance for various numbers of users  $L$  and PER  $\epsilon$ . The number of source packets  $K$  is fixed to 5. It can be observed that the bound is accurate when  $\epsilon = 0.01$ , with the MSE of  $4 \cdot 10^{-7}$ ,  $7 \cdot 10^{-7}$  and  $2 \cdot 10^{-6}$  for  $L = 2, 6$  and  $10$ , respectively. This is in contrast with

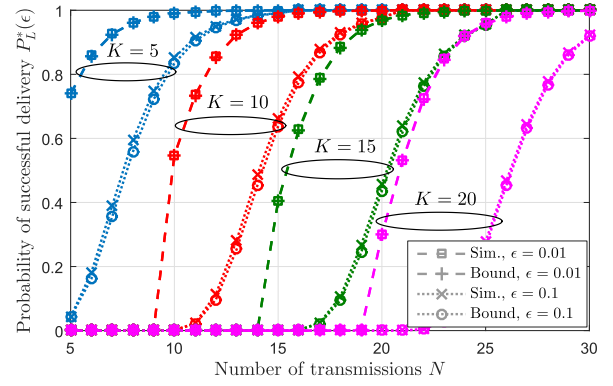


Fig. 6. Probability of successful delivery for a binary systematic code as a function of the number of transmissions  $N$  for  $L = 6$ ,  $\epsilon \in \{0.01, 0.1\}$  and  $K \in \{5, 10, 15, 20\}$ .

the same bound applied to non-systematic RLNC (5), which exhibited significant inaccuracy at small PER. Such behaviour of bound (28) at small  $\epsilon$  was predicted in Section III-B and explained by the high probability that each user receives all  $K$  source packets. Even when  $\epsilon = 0.1$  and  $L = 10$ , the vertical gap between the bound and simulated results is relatively small: up to  $7 \cdot 10^{-2}$  for  $N = 8$ , compared to 0.58 in the non-systematic case. This phenomenon was again predicted in Section III-B and is due to the fact that the correlation between the users coding matrices arises from the non-systematic packets only, the number of which is smaller than the total number of transmissions. Due to the tightness of bound (28) for both considered PER values, the results for a heterogeneous scenario, in which every user has a distinct PER, are omitted.

By analogy to Fig. 2 for non-systematic RLNC, Fig. 6 illustrates the performance results for the systematic case, for fixed  $L = 6$  and variable  $K$ , for two values of PER  $\epsilon$ . The bound provides close approximation for all  $K$  at  $\epsilon = 0.01$ : the MSE ranges from  $7 \cdot 10^{-7}$  (for  $K = 5$ ) to  $5 \cdot 10^{-6}$  (for  $K = 20$ ). At the same time, a small deviation can be observed when  $\epsilon = 0.1$ , which decreases as  $K$  becomes larger – the MSE drops from  $4 \cdot 10^{-4}$  (for  $K = 5$ ) to  $9 \cdot 10^{-5}$  for ( $K = 20$ ). The deviation can be explained by a larger influence of the correlation between the users coding matrices when  $\epsilon$  is high, which is not taken into account by the proposed bound. The deviation reduction as  $K$  increases is due to a decreasing amount of correlation, as in the case of non-systematic RLNC.

Finally, Fig. 7 demonstrates the performance results for a systematic non-binary code, corresponding to  $q = 2^8$ . The accuracy of the bound can be observed for all considered values of  $L$  and  $\epsilon$ , with the worst-case MSE (corresponding to  $L = 10$ ) equal to  $4 \cdot 10^{-7}$  and  $2 \cdot 10^{-7}$ , for  $\epsilon = 0.01$  and  $0.1$ , respectively. We note that the results in Fig. 7 are similar to those shown in Fig. 4 for a non-systematic code. Indeed, when the field size is large, the probability of successful delivery in both cases can be closely approximated by the probability of each user collecting at least  $K$  packets, which does not depend on the nature of the code.

All in all, it can be concluded that for systematic RLNC, bound (28) is sufficiently tight for most considered combina-

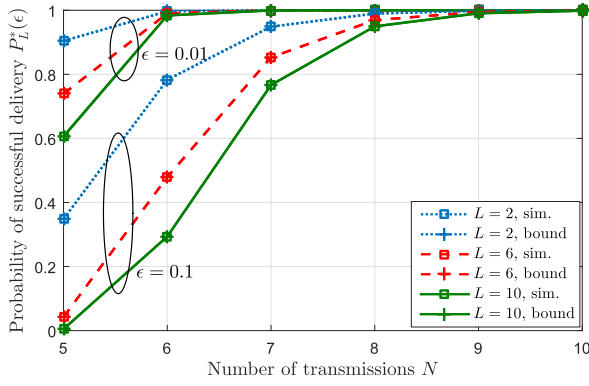


Fig. 7. Probability of successful delivery for a non-binary  $q = 2^8$ , systematic code as a function of the number of transmissions  $N$  for  $L \in \{2, 6, 10\}$ ,  $\epsilon \in \{0.01, 0.1\}$  and  $K = 5$ .

tions of  $K$ ,  $L$ ,  $\epsilon$  and  $q$ , with a small deviation occurring when  $K = 5$ ,  $L \geq 6$  and  $\epsilon = 0.1$ .

## V. CONCLUSIONS AND FUTURE WORK

In this paper, we have addressed the issue of calculating the probability of successful delivery in a multicast network operating under RLNC. In contrast with the previous studies focused on specific network or code parameters, we considered the most general scenario of arbitrary number of users and finite field size, as well as realistic channel conditions. In addition to the traditional, non-systematic form of RLNC, we have also considered the systematic version.

For non-systematic RLNC, we proposed a novel lower bound for the probability of successful delivery, which takes into account a limited finite field size and potential correlation between the users. This is in contrast with the bound traditionally used in the literature, which assumes an infinite or sufficiently large field size and independence between subsets of packets received by each user. For systematic RLNC, however, we argued that the correlation effect between the users is negligible, and the traditionally used bound is sufficiently tight.

The accuracy of the considered bounds was thoroughly investigated via Monte Carlo simulations for various combinations of network and code parameters. In the non-systematic scenario, it was demonstrated that the proposed bound is significantly more accurate than the traditional bound used in the literature. The accuracy of the new bound was shown to be especially high at low PER, exhibiting an MSE of  $9 \cdot 10^{-5}$  for a ten-user network. In contrast, the absolute deviation of the state-of-the-art bound is as large as 0.58 for the same network. Even for a large finite field, it was shown that the traditional bound deviates from the simulated results, while the proposed bound is up to 10 times more accurate. In particular, this holds true in scenarios where the multicast users experience heterogeneous PERs. In the systematic case, the considered bound was shown to be sufficiently tight for most configurations, with a small deviation occurring at high PER and small message size. By examining the accuracy of the bounds, we provided a unique insight into the selection of code parameters for various network configurations.

The considered bounds for the probability of successful delivery could be used to obtain other performance metrics, such as the average decoding delay or energy efficiency. In addition, the derived results can be utilised in the analysis of other network topologies, such as relay networks. To improve the utility of the bounds, a further reduction in their complexity, especially in the non-systematic case, can be investigated.

## APPENDIX A PROOF OF LEMMA 1

Let  $A_j$ ,  $j = 1, \dots, L$ , denote an event corresponding to matrix  $\mathbf{C}_j$  being full rank. Using this notation, (14) can be rewritten as

$$\Pr \left[ \bigcap_{j=1}^L A_j \right] \geq \prod_{j=1}^L \Pr[A_j]. \quad (38)$$

We first show that (38) is valid for  $L = 2$ . Consider the two matrices in question,  $\mathbf{C}_1$  and  $\mathbf{C}_2$ . Using the notation of Section III, let  $\mu$  denote the number of common rows in these matrices. Let also  $\mathbf{X}$  denote a matrix formed by those rows. The joint probability of both matrices being full rank can be expressed as follows:

$$\Pr[A_1 \cap A_2] = \sum_i \Pr[\text{rank}(\mathbf{X}) = i, A_1 \cap A_2], \quad (39)$$

where the maximum value of the summation index  $i$  is limited by  $\min(\mu, K)$ . Let  $Z$  be a random variable representing the rank of  $\mathbf{X}$ , so that both matrices are full rank. Therefore, (39) can be thought of as the Cumulative Distribution Function (CDF) of  $\mu$ ,  $F(\mu)$ :

$$\Pr[A_1 \cap A_2] = \sum_i \Pr[Z = i] = \Pr[Z \leq \mu]. \quad (40)$$

Since the CDF is a non-decreasing function, it follows that its minimum value corresponds to  $\mu = 0$ , for which the matrices are independent from each other. Hence,

$$\Pr[A_1 \cap A_2] \geq F(0) = \Pr[A_1] \Pr[A_2], \quad (41)$$

which proves (38) for  $L = 2$ .

For  $L > 2$ , the left-hand side of (38) can be expressed based on the chain rule as follows:

$$\begin{aligned} \Pr \left[ \bigcap_{j=1}^L A_j \right] &= \Pr \left[ A_L \middle| \bigcap_{j=1}^{L-1} A_j \right] \cdot \Pr \left[ A_{L-1} \middle| \bigcap_{j=1}^{L-2} A_j \right] \cdots \\ &\quad \cdot \Pr[A_2 | A_1] \cdot \Pr[A_1] \\ &= \prod_{l=1}^L \Pr \left[ A_l \middle| \bigcap_{j=1}^{l-1} A_j \right]. \end{aligned} \quad (42)$$

From (41), it follows that

$$\Pr[A_2 | A_1] = \frac{\Pr[A_1 \cap A_2]}{\Pr[A_1]} \geq \Pr[A_2]. \quad (43)$$

Consider now the term in the product (42) corresponding to  $l = 3$ ,  $\Pr[A_3 | A_1 \cap A_2]$ . It can be expressed as follows:

$$\Pr[A_3 | A_1 \cap A_2] = \frac{\Pr[A_3 \cap A_2 | A_1]}{\Pr[A_2 | A_1]}. \quad (44)$$



From (41), it follows that

$$\Pr[A_3 \cap A_2 | A_1] \geq \Pr[A_3 | A_1] \Pr[A_2 | A_1]. \quad (45)$$

Substituting this into (44) leads to

$$\Pr[A_3 | A_1 \cap A_2] \geq \Pr[A_3 | A_1] \geq \Pr[A_3]. \quad (46)$$

Using the same logic, it is straightforward to show that if  $\Pr[A_{l-1} | \bigcap_{j=1}^{l-2} A_j] \geq \Pr[A_{l-1}]$  holds, so does  $\Pr[A_l | \bigcap_{j=1}^{l-1} A_j] \geq \Pr[A_{l-1}]$ . Indeed,

$$\begin{aligned} \Pr \left[ A_l | \bigcap_{j=1}^{l-1} A_j \right] &= \frac{\Pr \left[ A_l \cap A_{l-1} | \bigcap_{j=1}^{l-2} A_j \right]}{\Pr \left[ A_{l-1} | \bigcap_{j=1}^{l-2} A_j \right]} \\ &\geq \Pr \left[ A_l | \bigcap_{j=1}^{l-2} A_j \right] \geq \Pr[A_l]. \end{aligned} \quad (47)$$

As a result, every term in the product (42) is lower-bounded by the corresponding marginal probability, which leads to (38) and proves the lemma. ■

## REFERENCES

- [1] D. Gomez-Barquero, D. Gozalvez, and N. Cardona, "Application layer FEC for mobile TV delivery in IP datacast over DVB-H systems," *IEEE Trans. Broadcast.*, vol. 55, no. 2, pp. 396–406, Jun. 2009.
- [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, Oct. 2002.
- [3] P. Wang *et al.*, "Performance analysis of raptor codes under maximum likelihood decoding," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 906–917, Mar. 2016.
- [4] E. Magli, M. Wang, P. Frossard, and A. Markopoulou, "Network coding meets multimedia: A review," *IEEE Trans. Multimedia*, vol. 15, no. 5, pp. 1195–1212, Aug. 2013.
- [5] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE ISIT*, Jun./Jul. 2003, p. 442.
- [6] T. Ho *et al.*, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
- [7] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.
- [8] D. S. Lun, M. Médard, R. Koetter, and M. Effros, "On coding for reliable communication over packet networks," in *Proc. 42nd Annu. Allerton Conf. Commun., Control, Comput.*, Jan. 2004, pp. 1–33.
- [9] D. S. Lun, M. Médard, R. Koetter, and M. Effros, "Further results on coding for reliable communication over packet networks," in *Proc. ISIT*, Sep. 2005, pp. 1848–1852.
- [10] I. Chatzigeorgiou and A. Tassi, "Decoding delay performance of random linear network coding for broadcast," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7050–7060, Aug. 2017.
- [11] B. Shrader and N. M. Jones, "Systematic wireless network coding," in *Proc. IEEE MILCOM*, Oct. 2009, pp. 1–7.
- [12] J. Heide, M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, "Network coding for mobile devices—Systematic binary random rateless codes," in *Proc. ICC*, Jun. 2009, pp. 1–6.
- [13] D. E. Lucani, M. Médard, and M. Stojanovic, "Systematic network coding for time-division duplexing," in *Proc. IEEE ISIT*, Jun. 2010, pp. 2403–2407.
- [14] J. Barros, R. A. Costa, D. Munaretto, and J. Widmer, "Effective delay control in online network coding," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 208–216.
- [15] A. Eryilmaz, A. Ozdaglar, and M. Médard, "On delay performance gains from network coding," in *Proc. 40th Annu. Conf. Inf. Sci. Syst.*, Mar. 2006, pp. 864–870.
- [16] D. E. Lucani, M. Médard, and M. Stojanovic, "Broadcasting in time-division duplexing: A random linear network coding approach," in *Proc. Workshop Netw. Coding, Theory, Appl.*, Jun. 2009, pp. 62–67.
- [17] M. V. Pedersen, D. E. Lucani, F. H. P. Fitzek, C. W. Sørensen, and A. S. Badr, "Network coding designs suited for the real world: What works, what doesn't, what's promising," in *Proc. IEEE ITW*, Sep. 2013, pp. 1–5.
- [18] D. Ferreira, R. A. Costa, and J. Barros, "Real-time network coding for live streaming in hyper-dense WiFi spaces," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 4, pp. 773–781, Apr. 2014.
- [19] D. E. Lucani, M. Médard, and M. Stojanovic, "Random linear network coding for time-division duplexing: Field size considerations," in *Proc. IEEE GLOBECOM*, Nov./Dec. 2009, pp. 1–6.
- [20] M. Nistor, D. E. Lucani, T. T. V. Vinhoza, R. A. Costa, and J. Barros, "On the delay distribution of random linear network coding," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 5, pp. 1084–1093, May 2011.
- [21] O. Trullols-Cruces, J. M. Barcelo-Ordinas, and M. Fiore, "Exact decoding probability under random linear network coding," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 67–69, Jan. 2011.
- [22] A. L. Jones, I. Chatzigeorgiou, and A. Tassi, "Binary systematic network coding for progressive packet decoding," in *Proc. IEEE ICC*, Jun. 2015, pp. 6115–6120.
- [23] A. S. Khan, A. Tassi, and I. Chatzigeorgiou, "Rethinking the intercept probability of random linear network coding," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1762–1765, Oct. 2015.
- [24] A. S. Khan and I. Chatzigeorgiou, "Performance analysis of random linear network coding in two-source single-relay networks," in *Proc. IEEE ICCW*, Jun. 2015, pp. 991–996.
- [25] E. Tsimbaló, A. Tassi, and R. J. Piechocki, "Novel performance analysis of network coded communications in single-relay networks," in *Proc. IEEE GLOBECOM*, Dec. 2016, pp. 1–6.
- [26] P. J. S. G. Ferreira, B. Jesus, J. Vieira, and A. J. Pinho, "The rank of random binary matrices and distributed storage applications," *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 151–154, Jan. 2013.
- [27] T. Ho and D. Lun, *Network Coding: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, Apr. 2008.
- [28] S. Brown, O. Johnson, and A. Tassi, "Reliability of broadcast communications under sparse random linear network coding," *IEEE Trans. Veh. Technol.*, to be published.
- [29] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.
- [30] A. Tassi, I. Chatzigeorgiou, D. Vukobratović, and A. L. Jones, "Optimized network-coded scalable video multicasting over eMBMS networks," in *Proc. IEEE ICC*, Jun. 2015, pp. 3069–3075.
- [31] S. Sesia, I. Toufik, and M. Baker, *LTE—The UMTS Long Term Evolution*. Hoboken, NJ, USA: Wiley, 2011.
- [32] W. Feller, *An Introduction to Probability Theory and Its Applications*, vol. 1, 3rd ed. Hoboken, NJ, USA: Wiley, 1968.
- [33] M. V. Pedersen, J. Heide, and F. H. P. Fitzek, *Kodo: An Open and Research Oriented Network Coding Library* (Lecture Notes in Computer Science), vol. 6827. Cham, Switzerland: Springer, 2011, pp. 145–152.
- [34] L. Carlà, F. Chiti, R. Fantacci, C. Khirallah, and A. Tassi, "Power efficient resource allocation strategies for layered video delivery over eMBMS networks," in *Proc. ICC*, Jun. 2014, pp. 3505–3510.
- [35] A. Tassi, I. Chatzigeorgiou, and D. Vukobratović, "Resource-allocation frameworks for network-coded layered multimedia multicast services," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 2, pp. 141–155, Feb. 2015.



**Evgeny Tsimbaló** (S'14–M'17) received the Ph.D. degree from the University of Bristol, U.K., in 2017. From 2013 to 2017, he was a Research Associate with the Department of Electrical and Electronic Engineering, University of Bristol, where he focused on energy-efficient wireless communications. Since 2017, he has been a Research Engineer with the Toshiba Telecommunications Research Laboratory, Bristol. His research interests include communication theory, reliable communications, and wireless networks.





**Andrea Tassi** (S'11–M'14) received the M.Sc. degree (*cum laude*) in computer engineering in 2010, and the Ph.D. degree in telecommunication systems and telematics from the University of Florence, Italy, in 2014. He is currently a Senior Research Associate in wireless connectivity for autonomous vehicles with the Department of Electrical and Electronic Engineering, University of Bristol, U.K. Before joining the University of Bristol, he was a Research Associate in joint coding designs for error correction with the School of Computing and Communications, Lancaster University, U.K. His research interests involve ultra-reliable and delay-constrained communications, resource allocation strategies, coding theory, and information theoretical aspects of next-generation networks for intelligent transportation systems.



**Robert J. Piechocki** received the M.Sc. degree from the Technical University of Wroclaw and the Ph.D. degree from the University of Bristol. He is currently an Associate Professor (U.K. Reader) in wireless connectivity and a member of Communications Systems and Networks group. His research interests span all areas of wireless and wired connectivity, with emphasis on applications to eHealth and transportation. In his research, he uses tools from statistical signal processing, information and communication theory, IoT, wireless networking, body and ad-hoc networks, ultra-low power communications, and vehicular communications. He has published over 150 papers in international journals and conferences and holds 13 patents in these areas. He is leading the development of IoT, wireless connectivity and sensing for the Sphere project—UK's flagship EPSRC funded eHealth IoT project and the winner of 2016 World Technology Award. He is leading several U.K. funded projects developing connected technology for Autonomous Vehicles.