

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/225025038>

# Graph-Based Random Access for the Collision Channel without Feedback: Capacity Bound

Conference Paper · January 2012

DOI: 10.1109/GLOCOM.2011.6134205 · Source: DLR

CITATIONS

30

READS

102

3 authors:



[Enrico Paolini](#)

University of Bologna

137 PUBLICATIONS 1,803 CITATIONS

[SEE PROFILE](#)



[Gianluigi Liva](#)

German Aerospace Center (DLR)

219 PUBLICATIONS 2,838 CITATIONS

[SEE PROFILE](#)



[Marco Chiani](#)

University of Bologna

366 PUBLICATIONS 8,888 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



CONCERTO [View project](#)



GNSS Signal Design [View project](#)

# Graph-Based Random Access for the Collision Channel without Feedback: Capacity Bound

Enrico Paolini, Gianluigi Liva and Marco Chiani

**Abstract**—A random access scheme for the collision channel without feedback is proposed. The scheme is based on erasure correcting codes for the recovery of packet segments that are lost in collisions, and on successive interference cancellation for resolving collisions. The proposed protocol achieves reliable communication in the asymptotic setting and attains capacities close to 1 [packets/slot]. A capacity bound as a function of the overall rate of the scheme is derived, and code distributions tightly approaching the bound developed.

## I. INTRODUCTION

Since the introduction of the ALOHA protocol [1], several random access (RA) schemes have been introduced. Among them, some feedback-free RA protocols originally proposed in [2], [3] re-gained attention in the recent past [4]–[6]. In [2], the capacity of the so-called collision channel without feedback (CCw/oFB) was analyzed, assuming slot-aligned but completely asynchronous users' transmissions. Moreover, a simple approach to achieve error-free transmission over the CCw/oFB was proposed. The approach of [2] consists of assigning different periodic protocol (access) sequences to the users. Each sequence defines in which slots each user is allowed to access the shared channel. Furthermore, the users encode their packets by means of erasure correcting codes. The user's packet can be recovered whenever a sufficient number of codeword segments are received collision free. Hence, by selecting proper protocol sequences, it is possible to ensure that a sufficient number of segments per user are recovered, even if the beginning of the different protocol sequences is unsynchronized. In this way, a capacity equal to  $1/e$  [packets/slot] is achieved as  $M \rightarrow \infty$ , where  $M$  is the number of users accessing the RA channel. The same capacity is achieved also in the unslotted case. Although simple, the approach of [2] poses some challenges, especially if a large (and varying) number of users has to be served [3], [4].

Recently, RA schemes profiting from SIC have been introduced and analyzed [7]–[10]. These schemes share the feature of canceling the interference caused by collided packets on the slots where they have been transmitted whenever a clean (uncollided) copy of them is detected. In [9], [10] it was shown that the successive interference cancellation (SIC) process can be well modeled by means of a bipartite graph. The analysis

proposed in [9], [10] resembles density evolution analysis of low-density parity-check (LDPC) and doubly-generalized LDPC (D-GLDPC) codes over erasure channels [11]–[13]. By exploiting design techniques from the LDPC context, a remarkably-high throughput (e.g. up to 0.8 [packets/slot]) can be achieved in practical implementations. The schemes considered in [7]–[10] assume a feedback from the receiver to achieve a zero packet loss rate. Furthermore, the approaches proposed in [7], [9] has been recently considered for inclusion in the next generation Digital Video Broadcasting Return Channel via Satellite (DVB-RCS) standard [14].

In this paper, we investigate the application of SIC to collision channels without feedback. With respect to [2], the proposed RA scheme does *not* require the assignment of protocol sequences to users, who select time slots for their transmissions in a randomized and uncoordinated fashion. The proposed scheme stems from the coded slotted ALOHA (CSA) protocol proposed in [10].

Each user splits his generic packet into segments, that are encoded through a binary linear (erasure) block code chosen on a packet-by-packet basis, according to some probability distribution. The resulting encoded segments are then transmitted in time slots selected with uniform probability out of the slots composing the medium access control (MAC) frame. If for a packet a sufficient number of encoded segments are correctly received, its entire set of encoded segments can be recovered by the erasure code. Moreover, the contribution of interference of cleaned segments can be canceled from the slots in which they caused collisions. It is shown how, iterating this process, for a channel traffic below a threshold value, arbitrarily low error probabilities can be achieved. We refer to this threshold as the *capacity* of the scheme. By suitably selecting the distribution of erasure codes, capacities close to 1 [packets/slot] can be obtained. It is also shown that there is a fundamental trade-off between the rate of the scheme and its capacity. An upper bound on the capacity is proved, and code distributions tightly approaching it derived.

## II. SYSTEM MODEL

We consider a slotted RA scheme where slots are grouped in MAC frames, all with the same length (in slots). Each user is frame- and slot-synchronous, and attempts one *burst* (i.e., packet) transmission per MAC frame. Consider  $M$  users, each attempting the transmission of a burst of time duration  $T_{\text{slot}}$  over a MAC frame of time duration  $T_{\text{frame}}$ . Neglecting guard times, the MAC frame is composed of  $N = T_{\text{frame}}/T_{\text{slot}}$  slots. We say that the offered (channel) traffic is  $G = M/N$ .

Enrico Paolini and Marco Chiani are with DEIS/WiLAB, University of Bologna, via Venezia 52, 47521 Cesena (FC), Italy. Email: {e.paolini, marco.chiani}@unibo.it.

Gianluigi Liva is with the Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, 82234 Wessling, Germany. Email: Gianluigi.Liva@dlr.de.

Supported in part by the EC under Project FP7 OPTIMIX (ICT-214625).

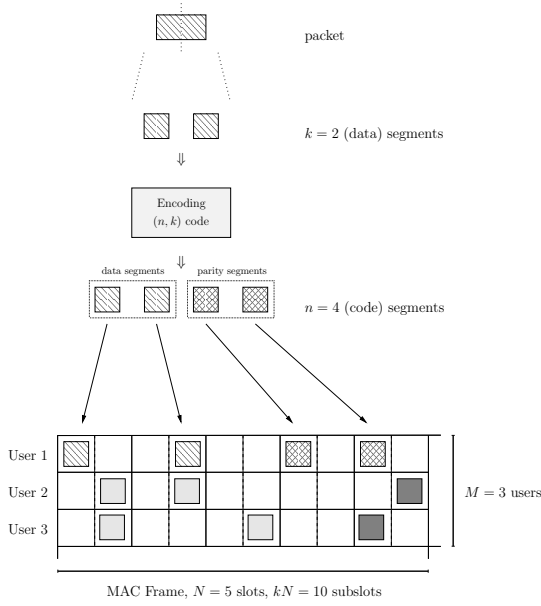


Fig. 1. Model of the access scheme. Each user splits his bursts into  $k = 2$  segments. User 1 encodes them by a  $(4, 2)$  linear block code, users 2 and 3 by a  $(3, 2)$  single parity-check (SPC) code. The darkened squares denote parity segments.

The proposed access scheme works as follows. Prior to transmission of a user's burst of time duration  $T_{\text{slot}}$ , the burst is divided into  $k$  information *segments*, each of time duration  $T_{\text{seg}} = T_{\text{slot}}/k$ . The  $k$  information segments are then encoded by the user via a packet-oriented linear block code generating  $n_h$  encoded segments, each of time duration  $T_{\text{seg}}$ . For each transmission, the  $(n_h, k)$  code is chosen randomly by the user from a set  $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{n_c}\}$  of  $n_c$  candidate codes. For  $h \in \{1, 2, \dots, n_c\}$  the code  $\mathcal{C}_h$  has length  $n_h$ , dimension  $k$ , rate  $R_h = k/n_h$ , and minimum distance at least 2. Each code  $\mathcal{C}_h$  has no idle symbols. At any transmission, each user draws his local code from the set  $\mathcal{C}$  independently of his previous choices and without any coordination with the other users. The code is drawn according to a probability mass function (p.m.f.)  $\Lambda = \{\Lambda_h\}_{h=1}^{n_c}$  which is the same for all users. The MAC frame is composed of  $kN$  (sub-)slots.<sup>1</sup> The  $n_h$  coded segments are then transmitted by the user over  $n_h$  slots picked uniformly at random. An example for  $k = 2$  is provided in Fig. 1. For the special case of  $k = 1$ ,  $T_{\text{seg}} = T_{\text{slot}}$  and each  $\mathcal{C}_h$  is a repetition code of length  $n_h$ . The overall *rate* of the scheme is defined as  $R = k/\bar{n}$ , where  $\bar{n} := \sum_{h=1}^{n_c} \Lambda_h n_h$  is the expected length of the code.<sup>2</sup> We also define the polynomial  $\Lambda(x) = \sum_{h=1}^{n_c} \Lambda_h x^h$  and the polynomial  $\lambda(x) = \sum_{h=1}^{n_c} \lambda_h x^{h-1}$ , where  $\lambda_h = \Lambda_h n_h / (\sum_{i=1}^{n_c} \Lambda_i n_i)$ . We refer to  $\Lambda(x)$  as the component code distribution.

We adopt a graph representation of the RA scheme, depicted in Fig. 2 (related to the same example as Fig. 1). Consider

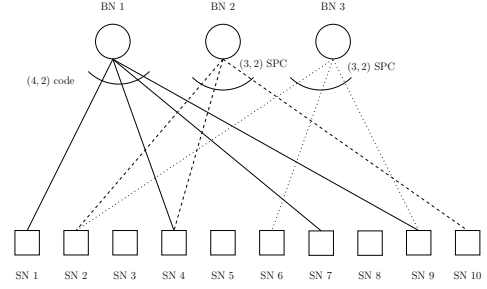


Fig. 2. Bipartite graph representation of the access scheme of Fig. 1. Subslots are represented by SNs, bursts by BNs. Each segment corresponds to an edge.

$M$  users transmitting over a frame composed of  $kN$  slots. The situation can be represented by a bipartite graph,  $\mathcal{G} = (\mathcal{B}, \mathcal{S}, \mathcal{E})$ , consisting of a set  $\mathcal{B}$  of  $M$  *burst nodes* (one for each user), a set  $\mathcal{S}$  of  $kN$  *sum nodes* (one for each slot), and a set  $\mathcal{E}$  of edges. An edge connects the  $i$ -th burst node (BN) to the  $j$ -th sum node (SN) if and only if an encoded segment associated with the burst of the  $i$ -th user is transmitted in the  $j$ -th slot. The number of edges connected to a BN or SN is the node degree. Therefore, a burst encoded via the code  $\mathcal{C}_h$  is represented as a degree- $n_h$  BN, and a slot where  $d$  segments collide as a degree- $d$  SN. Moreover, a BN where  $\mathcal{C}_h$  is used during the current transmission is named a BN of type  $h$ .

Each coded segment associated with a type- $h$  BN is equipped with information about its relevant user and with pointers to the other  $n_h - 1$  segments of the user.<sup>3</sup> We assume that collisions are always detected at the receiver and that they determine a complete loss of information about the colliding segments. We also assume that, when a burst is received in a clean slot, it is always successfully decoded. Therefore, after transmission, we can think of each BN as connected to “known” edges and to “unknown” ones, so that some of its information segments are known, and the others unknown. At a BN of type  $h$ , erasure decoding of the code  $\mathcal{C}_h$  may recover some of the unknown encoded and information segments. It is now possible to subtract the interference contribution of the newly recovered encoded segments from the signal received in the corresponding slots. If  $d - 1$  segments that collided in a SN of degree  $d$  have been recovered by the corresponding BNs, the remaining segment becomes known. The SIC process combined with local decoding at the BNs proceeds iteratively, i.e., cleaned segments may allow to resolve other collisions. In this paper, ideal SIC is assumed.<sup>4</sup> This procedure is equivalent to iterative decoding of a D-GLDPC code over the erasure channel, where variable nodes are generic linear block codes and check nodes are single-parity-check (SPC) codes.

<sup>3</sup>In practical implementations, the overhead due to the inclusion of pointers in the segment header may be reduced by adopting more efficient techniques. For fixed  $k$ , one may include in the segment header the code index  $h$  together with a random seed, out of which it is possible to reconstruct (by a pre-defined pseudo-random number generator) the positions of the  $n_h$  segments.

<sup>4</sup>To summarize, our analysis relies on three assumptions: i) *Destructive (and detectable) collisions*; ii) *Sufficiently high signal-to-noise ratio (SNR)* (segments received in clean slots are always successfully decoded); iii) *Ideal channel estimation* (an hypothesis under which, together with the previous one, we can assume an ideal SIC). These assumptions simplify the analysis without substantially affecting the performance, as shown in [7], [9].

<sup>1</sup>The definition of MAC frame as sequence of  $N$  slots is instrumental to the definition of load  $G$  only. The actual minimum unit that can be allocated to a segment transmission are the sub-slots.

<sup>2</sup>Note that  $R$  does not represent the average code rate  $\bar{R}$  adopted by each user. It is easy to prove (Jensen's inequality) that the average rate  $\bar{R} = \sum_h \Lambda_h R_h$  is lower bounded by  $R$ .

### III. ASYMPTOTIC ANALYSIS

In this section, the evolution of the SIC process for given  $k$  and  $G$ , in the asymptotic case where  $M \rightarrow \infty$  (and  $N \rightarrow \infty$ ) is overviewed. Most of the results presented in this section were developed in [10]. This serves to define the extrinsic information transfer (EXIT) functions for the BN and SN sets, used in the proof of our main result presented in Section IV, and to formalize the concept of capacity under iterative SIC.

We start by briefly recalling the definition of information function of a linear block code [15]. Consider an  $(n, k)$  linear block code  $\mathcal{C}$ , where  $n$  is the codeword length and  $k$  the code dimension, and let  $\mathbf{G}$  be any generator matrix of  $\mathcal{C}$ . Then, the  $g$ -th un-normalized information function of  $\mathcal{C}$ , denoted by  $\tilde{e}_g$ , is defined as the summation of the ranks of all possible submatrices obtained selecting  $g$  columns (with  $0 \leq g \leq n$ ) out of  $\mathbf{G}$ , regardless their order.

Next, assume that maximum a-posteriori (MAP) decoding is used locally at each BN. At the  $i$ -th iteration of the SIC process, let  $p_{i-1}$  be the average probability that an edge is connected to a SN associated with a slot where a collision still persists, before MAP decoding is performed at each BN. Moreover, let  $q_i$  be the average probability that an edge is connected to a BN whose contribution of interference on the corresponding SN cannot be yet canceled, after MAP decoding has been performed at each BN. Then:

$$q_i = \frac{1}{\bar{n}} \sum_{h=1}^{n_c} \Lambda_h \sum_{t=0}^{n_h-1} p_{i-1}^t (1-p_{i-1})^{n_h-1-t} [(n_h-t)\tilde{e}_{n_h-t}^{(h)} - (t+1)\tilde{e}_{n_h-1-t}^{(h)}] =: f_b(p_{i-1}). \quad (1)$$

Adopting a consolidated terminology in the theory of modern error correcting codes, the function  $f_b(p)$  is referred to as the average EXIT function of the BN set. It is easy to verify that  $f_b(p) = \sum_{h=1}^{n_c} \lambda_h f_b^{(h)}(p)$ , where

$$f_b^{(h)}(p) := \frac{1}{n_h} \sum_{t=0}^{n_h-1} p^t (1-p)^{n_h-1-t} [(n_h-t)\tilde{e}_{n_h-t}^{(h)} - (t+1)\tilde{e}_{n_h-1-t}^{(h)}] \quad (2)$$

is called the average EXIT function of a type- $h$  BN, under MAP decoding.

Equation 1 allows to update  $q_i$  given  $p_{i-1}$ . The dependence of  $p_i$  on  $q_i$  is instead obtained by observing that the number of segments received in a slot follows the distribution

$$\Psi_l = \binom{M}{l} \left( \frac{\bar{n}G}{kM} \right)^l \left( 1 - \frac{\bar{n}G}{kM} \right)^{M-l},$$

where  $\Psi_l$  is the probability to receive  $l$  segments in the generic slot. Defining  $\Psi(x) = \sum_l \Psi_l x^l$  and letting  $M \rightarrow \infty$ , yields

$$\Psi(x) = \exp \left( -\frac{G}{R}(1-x) \right).$$

It follows that  $p_i$  can be obtained from  $q_i$  by the relationship

$$p_i = 1 - \rho(1 - q_i) = 1 - e^{-\frac{G}{R}q_i} =: f_s(q_i), \quad (3)$$

where  $\rho(x) = \Psi'(x)/\Psi'(1)$  and  $\Psi'(x) = d\Psi(x)/dx$ . The function  $f_s(q)$  is called the average EXIT function of the SN

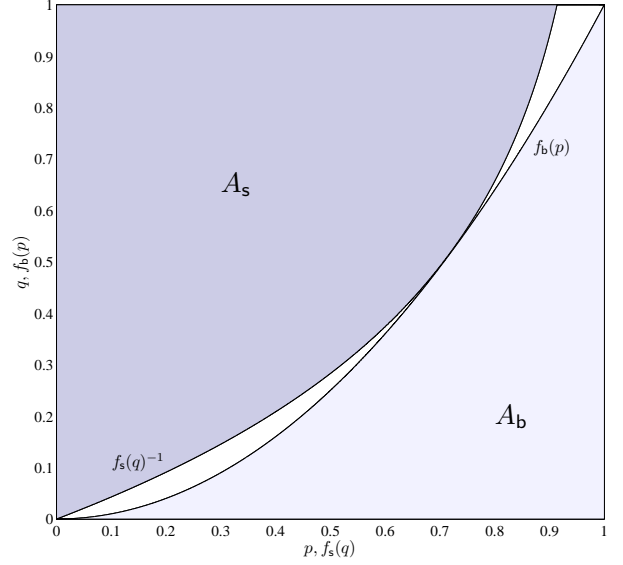


Fig. 3. EXIT chart for a regular coded random access scheme employing a rate-1/3 repetition code at each BN, characterized by  $G^* = 0.816$ .

set. The equations (1) and (3) define a discrete-time dynamical system  $q_i = q_i(q_{i-1})$  with starting point  $q_1 = f_b(0)$ , whose stability was analyzed in [10]. Note that the normalized offered traffic  $G$  is involved in the recursion through (3). The asymptotic threshold of the SIC process, denoted by  $G^* = G^*(\mathcal{C}, \Lambda)$ , is defined as the sup of the ensemble of all  $G \geq 0$  such that  $q_i \rightarrow 0$  as  $i \rightarrow \infty$ . In the asymptotic setting  $M \rightarrow \infty$ , for all  $G < G^*(\mathcal{C}, \Lambda)$  the throughput is  $S = G$ , i.e., all collisions are resolved. In this sense,  $G^*(\mathcal{C}, \Lambda)$  represents the *capacity* of the RA scheme conditional to the specific choice of  $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{n_c}\}$  and  $\Lambda$ .<sup>5</sup>

The recursion defined by (1) and (3) can be visualized in a so-called *EXIT chart*, which displays  $f_b(p)$  vs.  $f_s^{-1}(p)$ . An example of EXIT chart for a scheme employing a (3, 1) repetition code at each BN is provided in Fig. 3. As the iteration index  $i$  increases, the evolution of the pair of probabilities  $(p_i, q_i)$  traces a zig-zag pattern inside the tunnel between the two curves. Whenever we operate the scheme below its capacity,  $G < G^*(\mathcal{C}, \Lambda)$ , the two curves do not intersect, leaving the tunnel open. This lets the probabilities  $(p, q)$  achieve the  $(0, 0)$  point. On the contrary, if the scheme is operated above its capacity,  $G > G^*(\mathcal{C}, \Lambda)$ , the two curves intersect (closing the tunnel) in a point  $(\hat{p}, \hat{q})$  with  $\hat{p} > 0, \hat{q} > 0$ , and the iterative SIC process converges to a fixed point corresponding to a non-zero residual erasure probability.

### IV. CAPACITY BOUND

In this section, we present our main result along with its proof. The proposed proof is based on the EXIT functions reviewed in Section III and on the Area Theorem, a well-known result in the theory of EXIT functions [16]. An alternative proof (not proposed here for space reasons) can be given exploiting algebraic arguments.

<sup>5</sup>Readers with a background in modern coding theory may prefer the nomenclature “asymptotic threshold” to “capacity”.



*Theorem 4.1:* For rational  $R$  and  $0 < R \leq 1$ , let  $\bar{G}(R)$  be the unique positive solution of the equation

$$G = 1 - e^{-G/R} \quad (4)$$

in  $[0, 1)$ . Then, the capacity  $G^*(\mathcal{C}, \Lambda)$  of the RA scheme fulfills

$$G^*(\mathcal{C}, \Lambda) < \bar{G}(R) \quad (5)$$

for any choice of  $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{n_c}\}$  and  $\Lambda$  corresponding to a rate  $R$ .

*Proof:* For given  $\mathcal{C}$  and  $\Lambda$ , the evolution of the probabilities  $(p_i, q_i)$  is governed by the recursion  $p_i = f_s(q_i)$  and  $q_i = f_b(p_{i-1})$  in (3) and (1), for all  $i \geq 1$  and with  $q_1 = f_b(0)$ . Let's furthermore denote the areas below the BN and the SN EXIT functions (over the interval  $[0, 1]$ ) by

$$A_b = \int_0^1 f_b(p) dp \quad \text{and} \quad A_s = \int_0^1 f_s(q) dq$$

respectively. A necessary condition for successful decoding is to have an open tunnel between the two curves in the EXIT chart (see Fig. 3). For all  $G \leq G^*(\mathcal{C}, \Lambda)$ , we must have an open tunnel in the EXIT chart, which implies

$$A_b + A_s < 1. \quad (6)$$

In particular, (6) must be satisfied for  $G = G^*(\mathcal{C}, \Lambda)$ . The area below the SN EXIT function (3) is given by

$$A_s = 1 + \frac{R}{G} e^{-\frac{G}{R}} - \frac{R}{G}. \quad (7)$$

Moreover, the area below the BN EXIT function (1) is given by

$$A_b = \sum_{h=1}^{n_c} \lambda_h \int_0^1 f_b^{(h)}(p) dp = \sum_{h=1}^{n_c} \lambda_h \frac{k}{n_h}, \quad (8)$$

where the second equality holds under the assumption of MAP erasure decoding at the burst node, and is due to the Area Theorem in [16], which states that the area below the MAP EXIT function of a binary linear block code without idle symbols equals its code rate. By incorporating (7) and (8) in (6) we obtain

$$\sum_{h=1}^{n_c} \lambda_h \frac{k}{n_h} + 1 + \frac{R}{G} e^{-\frac{G}{R}} - \frac{R}{G} < 1. \quad (9)$$

Observing that  $\lambda_h = n_h \Lambda_h / \sum_l (n_l \Lambda_l) = n_h \Lambda_h / \bar{n}$ , we have  $\sum_h k \lambda_h / n_h = k \sum_h \Lambda_h / \bar{n} = k / \bar{n} = R$ . Thus, (9) reduces to  $R + (R/G) e^{-G/R} < R/G$  which, for  $G = G^*(\mathcal{C}, \Lambda)$  yields

$$G^*(\mathcal{C}, \Lambda) < 1 - e^{-\frac{G^*(\mathcal{C}, \Lambda)}{R}}. \quad (10)$$

Defining  $\bar{G}(R)$  as the unique solution in  $(0, 1]$  of (4), we have  $R(\bar{G}) = -\bar{G} / \log(1 - \bar{G})$ . Moreover, from (10) we have  $R(G^*) > -G^* / \log(1 - G^*)$ . Since the function  $y = -x / \log(1 - x)$ ,  $x \in [0, 1)$ , is monotonically decreasing, we obtain (5).  $\square$

Note that, while  $G^*(\mathcal{C}, \Lambda)$  depends on  $R$  through  $\mathcal{C}$  and  $\Lambda$ , its upper bound  $\bar{G}(R)$  depends *solely* on  $R$ .

## V. CAPACITY-APPROACHING SCHEMES

Theorem 4.1 establishes an upper bound on the capacity of the proposed RA scheme. In this section, we show that this bound can be indeed approached. To do so, for a given  $k$ , a given set  $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{n_c}\}$  of component codes, and a given target rate  $R$ , we generated by differential evolution (DE) [17] optimization the distribution  $\Lambda$  which maximizes  $G^*(\mathcal{C}, \Lambda)$ . In order to limit the search space, we focused on schemes based on codes of moderate-low length.

For example, for the case of  $k = 1$  and  $R = 0.2$ , we limited  $n_h$  to 30 (i.e., repetition codes with rate down to  $1/30$  have been considered). In this case, we obtained the distribution

$$\begin{aligned} \Lambda_1(x) = & 0.494155x^2 + 0.159085x^3 + 0.107372x^4 \\ & + 0.070336x^5 + 0.045493x^6 + 0.019898x^7 + 0.024098x^{11} \\ & + 0.008636x^{12} + 0.005940x^{13} + 0.008749x^{15} + 0.002225x^{18} \\ & + 0.001261x^{20} + 0.002607x^{22} + 0.008092x^{23} + 0.002287x^{24} \\ & + 0.012274x^{25} + 0.002530x^{26} + 0.003094x^{27} + 0.002558x^{28} \\ & + 0.005891x^{29} + 0.013419x^{30}, \end{aligned}$$

where  $\Lambda_1(x) = \sum_h \Lambda_h x^h$  and  $\mathcal{C}_h$  is the  $(h, 1)$  repetition code. The associated threshold is  $G^* = 0.977$ . The corresponding point on the  $G \times R$  plane is reported in Fig. 4 and compared with the bound given by Theorem 1. On the same plot, other distributions, denoted by  $\Lambda_i(x)$  for  $i \in \{2, \dots, 5\}$ , are reported for  $k = 1$ . Whereas for low rates  $R$  repetition-based scheme approach tightly the bound, for rates close to  $1/2$  they show visible losses. The distribution  $\Lambda_5(x) = 0.8x^2 + 0.2x^3$  (obtained by allowing a maximum  $n_h$  of 5) presents a rate  $R = 5/11 \simeq 0.45$  and attains a threshold  $G^* = 0.625$ , whereas  $\bar{G}(5/11) \simeq 0.843$ . This effect is somehow expected, since in the limiting case of  $R = 1/2$  each user employs a  $(2, 1)$  repetition code, and the corresponding threshold is  $G^* = 0.5$ .<sup>6</sup>

As the rate  $R$  grows, it is convenient to adopt codes with  $k > 1$ . To this purpose, we designed further schemes where each  $\mathcal{C}_h \in \mathcal{C}$  is maximum distance separable (MDS).<sup>7</sup> It is assumed that each burst node adopts a sub-optimum (in the symbol-wise MAP sense) decoding approach, which consists of decoding its lost segments only if the number of its collision-free received segments is at least  $k$ . Under this assumption, the EXIT function of a BN using an  $(n_h, k)$  MDS codes is given by

$$f_b^{(h)}(p) = \sum_{l=0}^{k-1} \binom{n_h-1}{l} (1-p)^l p^{n_h-l-1}. \quad (11)$$

We define in this case the distribution  $\Lambda(x) = \sum_h \Lambda_h x^h$ , where  $\mathcal{C}_h$  is an  $(h + k, k)$  MDS code.

For  $k = 2$  we designed a distribution  $\Lambda_6(x) = 0.276023x + 0.366641x^2 + 0.127979x^3 + 0.229357x^7$  characterized by  $R = 0.4$  and  $G^* = 0.83$ . For the same rate, the best found repetition-based ( $k = 1$ ) distribution for a maximum  $n_h$  set to 10, denoted by  $\Lambda_4(x)$ , achieves  $G^* = 0.79$ . Moving to the

<sup>6</sup>For  $k = 1$ ,  $R = 1/2$  represents a limiting case because, for rates  $R > 1/2$ , the rate-1 repetition code (i.e., no coding) must be included in the set  $\mathcal{C}$ . In this case, it is easy to prove that the threshold  $G^*$  would drop to 0.

<sup>7</sup>Imposing limits on  $n_h$ , this assumption is realistic. For instance, (generalized) Reed-Solomon codes on finite fields of moderate order may be used.

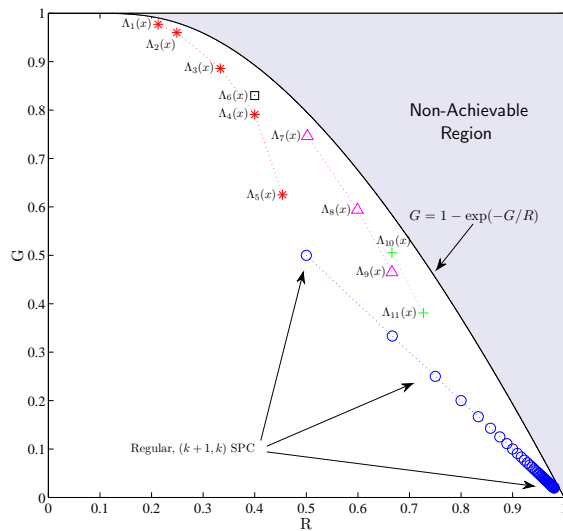


Fig. 4. Upper bound to the capacity vs. rate  $R$ . Thresholds  $G^*$  are reported for selected distributions. Distributions  $\Lambda_i(x)$ ,  $i = 1, \dots, 5$  (\*) are based on repetition codes ( $k = 1$ ). Distribution  $\Lambda_6(x)$  ( $\square$ ) is based on MDS codes ( $k = 2$ ). Distributions  $\Lambda_i(x)$ ,  $i = 7, 8, 9$  ( $\triangle$ ) are based on MDS codes ( $k = 3$ ). Distributions  $\Lambda_i(x)$ ,  $i = 10, 11$  ( $+$ ) are based on MDS codes ( $k = 4$ ). Distributions based on  $(k + 1, k)$  SPC codes are also displayed ( $\circ$ ).

moderate-rate regime, we heuristically found that the bound can be better approached by adopting distributions based on higher code dimensions (see Fig. 4). We conjecture that the bound can be approached even more tightly for larger code dimensions ( $k$ ). In Fig. 4 the thresholds achieved by regular schemes based on SPC codes of increasing rates are provided. It has been proved in [10] that for these schemes the threshold admits the close form  $G^* = (k + 1)^{-1}$ . As  $k$  grows, the rate of these scheme,  $R = k/(k + 1)$  approaches 1 and the corresponding threshold tends to 0. For large  $k$ , the scheme tends to operate close to the capacity bound for high rates.

Fig. 5 shows the packet loss rate (PLR) achieved by the scheme employing the distribution  $\Lambda_1(x)$ . The results have been derived via Monte Carlo simulations for MAC frames of size  $N = 5000, 1000$  and  $500$  slots, and are compared with the capacity of the scheme,  $G^* = 0.977$ . For the  $N = 5000$  case, a PLR close to  $2 \cdot 10^{-3}$  is achieved at a channel traffic  $G = 0.94$  [packets/slot], only  $0.05$  [packets/slot] away from the bound established by Theorem 4.1 ( $\approx 0.99$  [packets/slot]).

## VI. CONCLUSIONS

We introduced a RA protocol for the CCw/oFB which achieves large efficiencies with mild coordination demands. The scheme is based on the use of erasure correcting codes to recover packet segments that are lost in collisions, and on SIC to resolve collisions. The proposed protocol achieves reliable communication in the asymptotic setting and attains capacities close to 1 [packet/slot]. A simple capacity bound as a function of the code rates employed to encode the segments has been proved. The derived bound can be approached by means of judiciously designed component code distributions.

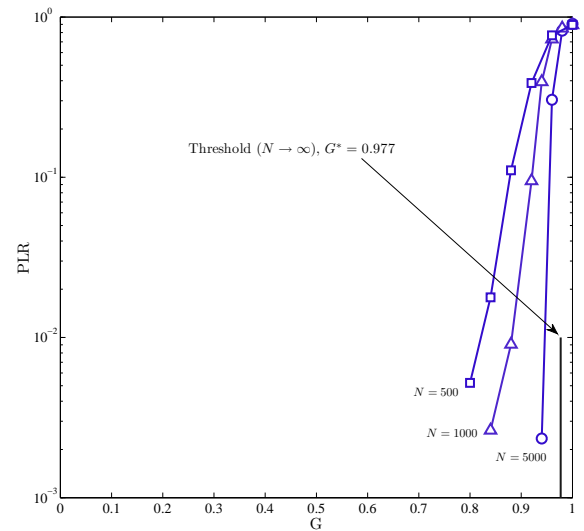


Fig. 5. PLR for the RA scheme based on the distribution  $\Lambda_1(x)$ .  $N = 5000, 1000, 500$ , maximum iteration count set to 100.

## REFERENCES

- [1] N. Abramson, "The ALOHA system - another alternative for computer communications," in *Proc. 1970 Fall Joint Computer Conf.*, vol. 37. AFIPS Press, 1970, pp. 281–285.
- [2] J. L. Massey and P. Mathys, "The collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 2, pp. 192–204, Mar. 1985.
- [3] J. Y. N. Hui, "Multiple accessing for the collision channel without feedback," *IEEE Trans. Veh. Technol.*, vol. VT-33, no. 3, pp. 191–198, Aug. 1984.
- [4] G. Thomas, "Capacity of the wireless packet collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1141–1144, May 2000.
- [5] S. Tinguely, M. Rezaeian, and A. J. Grant, "The collision channel with recovery," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3631–3638, Oct. 2005.
- [6] K. W. Shum, C. S. Chen, C. W. Sung, and W. S. Wong, "Shift-invariant protocol sequences for the collision channel without feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3312–3322, Jul. 2009.
- [7] E. Casini, R. D. Gaudenzi, and O. del Rio Herrero, "Contention resolution diversity slotted ALOHA (CRDSA): An enhanced random access scheme for satellite access packet networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 4, pp. 1408–1419, Apr. 2007.
- [8] Y. Yu and G. B. Giannakis, "High-throughput random access using successive interference cancellation in a tree algorithm," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4628–4639, Dec. 2007.
- [9] G. Liva, "Graph-based analysis and optimization of contention resolution diversity slotted ALOHA," *IEEE Trans. Commun.*, vol. 59, no. 2, pp. 477–487, Feb. 2011.
- [10] E. Paolini, G. Liva, and M. Chiani, "High throughput random access via codes on graphs: Coded slotted ALOHA," in *Proc. of 2011 IEEE Int. Conf. Commun.*, Kyoto, Japan, Jun. 2011.
- [11] R. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: M.I.T. Press, 1963.
- [12] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.
- [13] —, "Generalized and doubly-generalized LDPC codes with random component codes for the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1651–1672, Apr. 2010.
- [14] Next Generation DVB-RCS Standardization Group. [Online]. Available: <http://www.dvb.org/technology/dvbrcs/>.
- [15] T. Helleseth, T. Kløve, and V. I. Levenshtein, "On the information function of an error-correcting code," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 549–557, Mar. 1997.
- [16] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: Model and erasure channel properties," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2657–2673, Nov. 2004.
- [17] R. Storn and K. Price, "Differential evolution – a simple and efficient heuristic for global optimization over continuous spaces," *Journal of Global Optimization*, vol. 11, no. 4, pp. 341–359, Dec. 1997.