

Combinatorial Code Designs for Ultra-Reliable IoT Random Access

Christopher Boyd, Roope Vehkalahti and Olav Tirkkonen
School of Electrical Engineering, Aalto University, Finland
{christopher.boyd, roope.vehkalahti, olav.tirkkonen}@aalto.fi

Abstract—We consider Combinatorial Code Designs (CCD) for ensuring ultra-reliability in the random access channel. By constructing user-specific repetition patterns to be utilised over a synchronised uplink frame consisting of a number of access slots, we guarantee successive reception up to a given number of simultaneously active users. Employing advanced receivers capable of Successive Interference Cancellation (SIC) further improves reliability. As an example, we consider a system with access frames of 24 bundled slots, repetition factor 3, and reliability target 99.999%. When compared to slotted repetition ALOHA, SIC provides a 30% gain in the tolerated user activity; CCD a 30% gain; whereas CCD combined with SIC provides a gain of more than 700%. These gains come at the cost of a strict limit on the supported user population. In the given example, the system can support a total of 2024 users.

I. INTRODUCTION

Massive Machine-Type Communication (mMTC) and Ultra-reliable Machine-Type Communication (uMTC) are two of the major application domains forecast for the fifth generation (5G) of mobile networks [1]. These are among the key facilitators of the Internet of Things (IoT). Emerging and future IoT applications in automotive, power distribution and industrial automation, as well as the tactile internet, will place ever stricter demands on the wireless networks that enable them [2]. Contemporary wireless systems are unable to accommodate the many billions of low-power, sporadically transmitting devices that will characterise the IoT, nor are they optimised for the stringent Quality of Service (QoS) requirement that constitutes ultra-reliability [3]. In order to support such a diverse set of use cases and offer sub-ms end-to-end latencies, and “five nines” of reliability, an entirely new and highly versatile radio access technology (RAT) is required. Central to this is the challenge of providing reliable multiple-access to large numbers of uncoordinated and infrequently active devices.

In this paper, we explore two approaches for achieving ultra-reliability on the random access channel (RACH): Combinatorial Code Designs (CCD) amounting to repetition patterns of access attempts, and Successive Interference Cancellation (SIC) at the receiving base station (BS). In the case where the receiver cannot

perform SIC, typical random approaches amount to different versions of ALOHA [4], [5]. The code design problem assuming that patterns can be preallocated to users has been discussed in [6], where the authors employed combinatorial designs. The zero error approach has been considered in classical coding theory and combinatorics literature [7] under the name of *superimposed codes*. The closest works that consider IC include [8], [9] and [10], wherein slotted ALOHA transmissions are considered at the MAC layer with SIC. During a frame, a random subset of users tries to send one packet each by transmitting a random number of copies inside of the frame. The authors in [9], [10] achieve very high throughput with limited packet loss. However, this approach seem to be most effective in the case when the number of slots is in the hundreds or thousands, instead of tens.

Here we consider a deterministic version of [9], [10], where instead of random patterns we use relatively short patterns that are designed to avoid or recover from collisions. To the best of our knowledge the question of almost zero error probability under the assumption of interference cancellation has not been considered before. In a combinatorial language, the required codes have appeared as building blocks for collision resolution protocols with feedback, and are called $(\leq M, 1, n)$ -locally thin codes [11].

The unavoidable cost of ultra-reliability is that the number of supported and active users will not be very large when compared to random methods. A further downside is the necessity that the predetermined patterns need to be distributed to every possible user. The upside is that our approach ultra-reliable random access works already for very small frame sizes, and we can guarantee 100% certainty when the number of active users stays below the predetermined threshold.

II. SYSTEM MODEL

A. Random Access Framework

This paper takes the following perspective on the of question ultra-reliable random access. We consider a multi-user communication system accommodating N users, where each randomly accessing user wishes to transmit one packet of information to a central receiver.

No feedback is allowed. We assume that the users are synchronised with the BS, so that a rough timing advance is known, making it possible to have slot and frame synchrony between the users. Communication happens during frames consisting of some n time slots, and transmitting one access packet takes exactly one of the time slots. Upon generating a packet, a user attempts to transmit it during the next synchronised frame interval, along with $k < n$ repetitions. The user will independently, i.e. without knowledge of the other users, decide on how many repetitions and onto which time slots the replicas will be placed. During the duration of a single frame we assume that a random subset of N users is transmitting, and that the size of this subset is upper bounded by M .

We consider two different scenarios. In the first, the receiver simply reads each time slot in the frame. If two packets collide in a slot, then all the data is considered lost. If there is no collision, we consider the transmission successful. Ideally, we would like to guarantee that the transmissions of at most M active users are successful. This condition immediately prohibits us from considering typical random access approaches, where the user chooses the positions (inside the frame) of the packet replicas in a random manner. Instead, each of the system's N users will require a unique, predetermined "pattern", according to which the k replicas will be distributed on the n time slots.

The main question of this paper can be summarised as follows. Given the number of slots in a frame n , and an upper bound on the number of active users M , what is the maximum number of possible users N we can support such that we guarantee reception with 100% certainty? The obvious lower bound is given by time division. However, we will show that when $M \ll n$, we can have considerably more possible users than n and have inference free reception.

The second scenario considers this same question as the first, but under the assumption that the receiver can perform perfect interference cancellation. Given that each transmitted packet contains pointers to the time slots occupied by its copies, and given M and n , how many patterns exist (how many users can be supported) such that a 100% success rate is maintained? Successive IC algorithms allow us to expand the set of patterns obtainable in the interference-free case.

Our take on the topic of ultra-reliable random access assumes a hard limit on the number of active users. However, as seen in Section V, using hard limits for small numbers of active users can lead to effective codes even in the scenario when the number of active users is random, as long as the user activity is sufficiently low.

B. Basic Notation

Throughout this paper we consider three different perspectives on code design for the RACH. Let us now

explain this trichotomy. If we have n available slots for communication, we may number these slots by index forming a set of elements $S = \{1, 2, 3, \dots, n\}$. When a single user is sending a packet x , they place replicas of this packet on some k slots. This is equivalent to selecting a subset of S . For example, when $k = 2$ and the user is sending replicas on the first and seventh slot, we would have the subset $\{1, 7\}$. We represent the pattern by which a user spreads the packets replicas over a frame as a binary vector, where zeroes represent slots that do not have replica. For example, the subset $\{1, 7\}$ corresponds to the vector $(1000010 \dots 0)$. We will freely move between these different representations when presenting activity patterns for different users.

Let us now consider the trivial example where we have a frame of $n = 7$ slots and N potential users (ordered). The second user is allocated pattern (1110000) , the third user pattern (1000011) , and the seventh user pattern (0010110) . When the second, third and seventh users transmit simultaneously, the receiver sees $(x_2 + x_3, x_2, x_2 + x_7, 0, x_7, x_3 + x_7, x_3)$, where x_i refers to packets from the i th user. In binary, we have a packet collision when the involved vectors have one or more 1's in the same slot, while in set theoretic language there is a collision in the k th slot if at least two of the involved sets include k .

III. INTERFERENCE-FREE RECEPTION

We begin with the scenario where the receiver cannot perform interference cancellation and thus the system cannot recover from packet collisions. This means that, given M active users, the receiver must obtain at least one copy of each packet from each of the users free of interference from other users. We will see that this leads us to consider classical concepts in superimposed codes [7]. In this section we will shortly present some known results from this theory, and discuss the limitations. For further results we refer the reader to [7] and all papers referring to it.

The condition for interference free reception immediately suggests to us the following code design criterion. Let us suppose that we have N users, each in possession of a unique pattern of length n , and let us denote by W the $n \times N$ matrix consisting of all the patterns of the N users.

Definition 1 [7]. *The set of patterns W is a M -superimposed code if any $n \times M$ matrix formed from columns of W has a submatrix consisting of a $M \times M$ permutation matrix.*

In some cases this definition is suitable for our needs. However, in others it is more beneficial to see the problem from a set theoretical point of view. For example, when there are 3 active users, the set theoretic condition for interference free communication is that

each of the sets include an element that is not included in the other sets.

Let us now suppose we have a set $S = \{1, 2, \dots, n\}$. We are interested in collections of \mathcal{B} distinct subsets of S with the following property.

Definition 2 [12]. *A collection of sets \mathcal{B} is M -covering free if it satisfies the following condition. Given any subset $X \in \mathcal{B}$, there does not exist sets $Y_1, \dots, Y_{M-1} \in \mathcal{B}/X$ such that $X \subseteq Y_1 \cup Y_2 \cup \dots \cup Y_{M-1}$.*

When $M = 2$, this definition is the classical definition of the *Sperner-system*. We have thus translated the interference free random access problem onto the language of combinatorics. Given now a target activity, we would like to find the largest possible collection of sets \mathcal{B} such that they are M covering free. While there exists a rich literature on superimposed codes, explicit constructions are lacking. In the following we describe some of the known results.

1) *Two Simultaneously Active Users*: In this case, the problem of optimal code design for interference free random access can be solved completely. This is based on a simple observation that if \mathcal{B} is a collection of k element subsets of an n element set S , then \mathcal{B} is already 2-covering free. The surprising results by Sperner is that simply taking all the subsets of size $\lfloor n/2 \rfloor$ gives us the optimal solution $\binom{n}{\lfloor n/2 \rfloor}$ of subsets. This result proves that if we are satisfied with the condition that a maximum of two users may be active at the same time, the number of supported users grows dramatically as n increases. For example, for $n = 8$ we may have 70 potential users and with $n = 20$ we can have as many as 184756.

2) *Examples for $M = 3$* : We provide a short overview of the properties of some of the best known codes. In the case where $M = 3$, with frame size $n = 13$, we may obtain a code supporting a total of 26 users. With framesize $n = 21$, 70 users. For $n = 26$, we can obtain 260 patterns.

IV. CODES FOR INTERFERENCE CANCELLATION

A major drawback of superimposed codes is that if we want to have guaranteed reception for more than two simultaneous users, the set of supported users starts to become severely limited. However, as we will see, the situation is much less dire if we assume that the receiver can perform successive interference cancellation. Previously, the receiver attempted to decode all slots in a frame, and could correctly receive an access packet if and only if the slot was occupied by a single user. However, given that a decodable packet includes pointers to all of its replica in a frame, the receiver can freely erase these copies and nullify their impact on any remaining users. The decoding process continues recursively until there are no users left, or there are no interference free packets in frame. This latter case would

constitute a unrecoverable collision and a failure on the RACH.

Let us now assume that we have n available access slots inside a frame, some activity factor M , and wish to guarantee SIC reception of all active users. In set theoretic language, we have the set $S = \{1, \dots, n\}$. The recursive nature of the interference cancellation algorithm suggest the following definition.

Definition 3. *We say that a collection \mathcal{B} of subsets of S are interference cancelling with activity factor M if they satisfy the following. Given any collection of subsets A_1, \dots, A_s , $s \leq M$ from \mathcal{B} then at least one A_i contains at least one element that is not contained in any other A_k .*

In the binary vector language, we have the following.

Lemma 1. *Let us suppose we have a random access code C with N length n binary patterns (vectors) and let us denote with A the $n \times N$ -binary matrix formed of these vectors. If then each sub matrix Y formed of M or less columns has the property that at least one of the rows have weight one then C guarantees correct decoding as long as there is at most M active users.*

This binary vector presentation now reveals that this set of vectors form a $(\leq M, 1, n)$ -locally thin code [11]. Compared to Definition 1, we see that the assumption of IC-decoding does significantly relax the code design. Instead of having M rows with 1 (and on different columns), it is enough to have one on at least one row.

A. Examples for Different Activity Factors

While the $(\leq M, 1, n)$ -locally thin codes are a known construction, they have not been under heavy study as there seems to be no known small (or large) explicit optimal constructions in the literature.

1) *Activity $M = 2$* : When the number of active users in limited to two, the condition for decodability is simply that the subsets must satisfy that each pair are different. We deduce from this that for $M = 2$, we can support up to $2^n - 1$ users.

2) *Activity $M = 3$ and Greater*: Again, the problem becomes increasingly difficult as M grows. Relying on exhaustive computer search, we have obtained an optimal code of 11 patterns that guarantee SIC decodability for $M = 3$ active users in uplink frames of size $n = 5$. A result based on a random proof shows that, asymptotically, it is enough to use $O(M \log N/M)$ time slots n to guarantee that at most M users are decodable [13].

V. FAILURE PROBABILITY ANALYSIS FOR FRAME SIZE 24

In this section we establish approximate expressions for the failure probability in the RACH by assessing the more rudimentary contention cases, and evaluate

them by simulation. To obtain a concrete example, we assume that we have frames of $n = 24$ access slots. The motivation for this is that in the narrowest LTE version there are 6 physical resource blocks in the frequency domain, and, dividing a LTE sub-frame into 4 parts, one can convey a small amount of data in a sub-frame. To make analysis possible, we consider a limited cardinality code set. Each user possesses a single repetition pattern of weight $k = 3$ from a random or deterministic code, according to which they spread their access packets over a frame, allowing the system to support a finite population of $N = \binom{24}{3}$ users with distinct patterns.

For this performance analysis we continue to consider a synchronous system. Users that have a packet to transmit in the same frame may have patterns that collide in some of the slots. We note that with CCD, there are no collisions between two users that would not be recoverable. We provide an analytical lower bound by considering situations where there are up to three colliding users, and show by simulation that, for very low activity, this is sufficient to approximate the expected failure performance and motivate deterministic codes with SIC decoding for ultra-reliability on the RACH.

A. Three-way User Collisions

We assume three of N users each transmit k times in a given frame according to their allotted or generated patterns. To find the failure probability for a given user, i.e. the probability that none of the user's k repeated access packets can be successfully decoded, it is sufficient to compute the probability that all k slots in their pattern are occupied by the other two contesting users. In the case where the receiver is capable of performing SIC, failures occur when (at any point in the algorithm) no users have an interference-free slot.

In order to analyse the failure probability, we take the following approach. We note that, without loss of generality and for arbitrary n , in order for two users to collide they must occupy a span S_2 of at most five access slots. In this isolated case, the repetition coding guarantees decodability of both users. In order for failure to occur, the third user must then occupy S_2 or expand the span to at most 6 slots. In the latter case, the packet residing outside of S_2 serves to guarantee decodability of User 3, while the remaining two packets cause failure with some probability. We have thus divided up the probability space into the various collision scenarios that result in failure. The probability of failure occurring for $S_2 = 5$ is given by

$$P_{3u,5s} = \frac{3 \cdot \binom{n-2}{2}}{\binom{n}{3} - \lambda/2} \cdot \sum_{i=2}^3 \frac{\binom{n-5}{3-i} \binom{5}{i} - \lambda \delta_{K,3}}{\binom{n}{3} - \lambda} \cdot P_i, \quad (1)$$

where λ depends on the user codes: $\lambda = 0$ for randomly generated patterns, and $\lambda = 2$ for uniquely assigned patterns, and where $P_2 = 1/15$ and $P_3 = 1/2$ for

$\lambda = 2$ and $P_3 = 8/15$ for $\lambda = 0$. We continue with the case that the first two users span only 4 access slots in a frame with a certain probability. Once again, when isolated, decodability of these two users is guaranteed. A third user must then occupy S_2 , or expand the total span to 5 or 6 slots for there to be the possibility of failure occurring. The probability of failure occurring when $S_2 = 4$ is given by

$$P_{3u,4s} = \frac{\binom{3}{2} \binom{n-3}{1}}{\binom{n}{3} - \lambda/2} \cdot \sum_{i=1}^3 \frac{\binom{n-4}{3-i} \binom{4}{i} - \lambda \delta_{K,3}}{\binom{n}{3} - \lambda} \cdot P_i, \quad (2)$$

where $P_1 = 1/6$, $P_2 = 1/3$, and $P_3 = 1$ for $\lambda = 2$ and $P_3 = 5/6$ for $\lambda = 0$.

It is clear that when $S_2 = 3$, failure may only occur when the patterns are randomly generated, as all users must collide on all slots in the span. Outage probability in this instance is simply

$$P_{2u,3s} = \binom{n}{3}^{-2}. \quad (3)$$

Finally, the total probability of failure in the case of three-way collisions with random patterns is

$$P_{3u,rand} = P_{3u,5s} + P_{3u,4s} + P_{2u,3s}, \quad (4)$$

and for unique patterns $P_{3u,ccd}$ is the sum of only first two terms in (4).

B. Three-way Failure with Interference Cancellation

A sufficient condition for the progression of the SIC algorithm is that at each stage there is a contesting user who occupies an access slot free of interference. This user may then be identified, their unmolested packet decoded, and their entire presence in the frame removed. As such, in the case of $k = 3$ and three-way collisions, the only scenario in which IC fails to recover all user data is when all users occupy a space of four access slots. User 3 expanding beyond $S_2 = 4$ guarantees that at least one packet is free of interference. Therefore, the total probability of failure with IC in the case of three-way collisions with random patterns reduces to the sum of the first term in (2) and (3), while with unique patterns it is simply the first term in (2).

C. Evaluation With Simulation

To complete our analysis, we further assume that each user generates access packets according to a Poisson process with intensity μ . The complete failure probability under Poisson arrivals with random patterns may therefore be lower bounded as

$$P_{rnd}(\mu) \geq \frac{e^{-\mu} \mu^2}{2} \cdot \binom{n}{3}^{-1} + \frac{e^{-\mu} \mu^3}{6} \cdot P_{3u,rand}, \quad (5)$$

for random patterns, and corresponding expressions for random patterns with IC, CCD and CCD with IC, can be similarly derived. Figure 1 illustrates the analytically

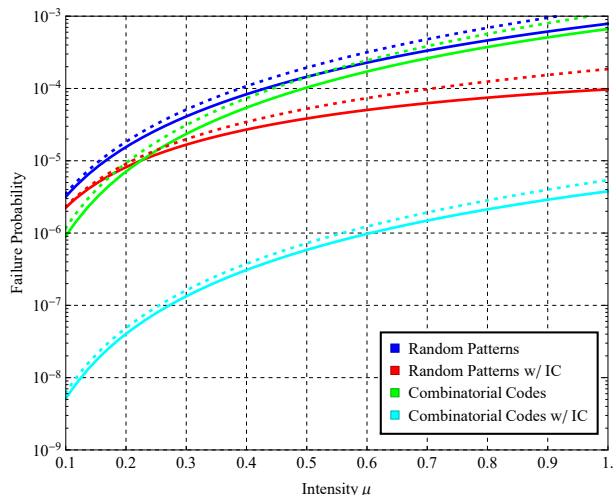


Fig. 1. Analytical lower bound (solid) and simulated (dotted) performance for random and combinatorial codes for random access in frames of 24 slots.

approximated and simulated failure probabilities for arrivals following a Poisson process as a function of the total access intensity of all users, for random and combinatorial user patterns with and without IC, for $k = 3$ repetitions, and frames of size $n = 24$. The simulated failure probabilities represent those for up to 10-way collisions inside a single frame. Evidently, consideration of only three-way collisions in the analysis leads to a deviation from the simulation that grows as the probability of higher order collisions increases. As expected, we observe that the use of deterministic codes reduces the failure probability significantly compared to random selection, with gains diminishing as the load on the RACH increases. This confirms that two-way user collisions dominate at lower access intensities, which cannot result in failures for uniquely allocated codes. By design, the deterministic codes may never have two fully overlapping user patterns, which reduces the probability of the IC algorithm becoming stuck during an iteration. With increasing access intensity, the less probable multi-way collisions start to dominate performance. This can be attributed to the birthday paradox: when the patterns are random, there is an quadratically growing number of user pairs that may happen to have the same pattern, thus preventing SIC from resolving the collisions.

Given that we pursue ultra-reliability on the RACH, and can therefore tolerate a maximum failure probability of 10^{-5} , combining IC with combinatorial codes clearly allows the system to support substantially higher loads. When compared to slotted repetition ALOHA, SIC alone provides a 30% gain in the tolerated user activity, whereas employing CCD provides a 30% gain without SIC decoding, and more than 700% gain with interference cancellation.

VI. CONCLUSION

In this work we suggested that, in order to support ultra-reliable communication in the random access channel with synchronised frames of small size, one should preassign user-specific repetition patterns for the intended users, such that no two patterns are the same. This guarantees that users active in a frame can always be received. The reliability may be further improved when these patterns are chosen such that decodability of access packets is guaranteed when a limited number of users $2 < M < N$ are active in a frame. We studied this approach in the case when the frame size is 24 slots, and found that it is particularly effective when combined with successive interference cancellation decoding.

ACKNOWLEDGEMENTS

This work was funded in part by the Academy of Finland (grant 299916), EIT ICT (HII:ACTIVE), and the Kaute Foundation. The authors would also like to thank P. Östergård, F. Szöllösi and K. Meagher for the help on finding combinatorial references.

REFERENCES

- [1] A. Osseiran, J. Monserrat, and P. Marsch, eds., 5G Mobile and Wireless Communications Technology. Cambridge University Press, 2016.
- [2] G. P. Fettweis, "The tactile internet: Applications and challenges," *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, pp. 6470, March 2014.
- [3] P. Popovski, "Ultra-reliable communication in 5G wireless systems," in 5G for Ubiquitous Connectivity (5GU), Nov. 2014, pp. 146151.
- [4] L. G. Roberts, "Aloha packet system with and without slots and capture", *SIGCOMM Comput. Commun. Rev.*, vol. 5, no. 2, pp. 28–42, Apr. 1975.
- [5] H. Okada, Y. Igarashi, and Y. Nakanishi, "Analysis and application of framed ALOHA channel in satellite packet switching networks- FADRA method, *Electronics and Communications in Japan*, vol. 60, pp. 60–72, Aug. 1977.
- [6] G. T. Peeters, R. Bocklandt and B. Van Houdt, "Multiple Access Algorithms Without Feedback Using Combinatorial Designs, *IEEE Trans. Commun.*, vol. 57, no. 9, Sept. 2009.
- [7] W. H. Kautz, and R. C. Singleton, "Nonrandom Binary Superimposed Codes, *IEEE Trans. Inf. Theory*, vol. 10, issue 4, October 1964.
- [8] E. Casini, R. De 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.
- [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, C. Stefanovic, G. Liva and P. Popovski, "Coded random access: applying codes on graphs to design random access protocols," in *IEEE Communications Magazine*, vol. 53, no. 6, pp. 144–150, June 2015.
- [11] M. Csurös and M. Ruzinkó, "Single-user tracing and disjointly superimposed codes, *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1606–1611, 2005.
- [12] P. Erdős, P. Frankl, Z. Füredi, "Families of Finite Sets in which No Set Is Covered by the Union of r Others, *Israel Journal of Math.* 51, no. 1-2, pp. 75–89, 1985.
- [13] A. E. F. Clementi, Angelo Monti, and Riccardo Silvestri. "Selective families, superimposed codes, and broadcasting on unknown radio networks", in *Proc. of the 12th Ann. Sym. on Disc. Algorithms*, pp. 709–718, 2001.