The Marriage between Random Access and Codes on Graphs: Coded ALOHA for Massive Random Access

Marco Chiani
CNIT, University of Bologna, Italy

Based on joint works with Gianluigi Liva, Enrico Paolini

PhD Summer School on Signal Processing for ICT
Bressanone, 7-11 Luglio 2014

Research supported in part by the EC under the FP7 grant agreement n. 288502
The problem of multiple access for a potentially very large population of users who wish to transmit over a shared communication medium is receiving an increasing attention.
The problem of multiple access for a potentially very large population of users who wish to transmit over a shared communication medium is receiving an increasing attention.

- WSNs with a high density of sensors;
- RF-ID systems with a high density of tags;
- IoT applications;
- M2M communications;
- 5G mobile communications systems;
- ...

M. Chiani, Univ. of Bologna
Prologue

Erasure Correcting Codes

\[ c_1 + c_2 + c_3 + c_4 = 0 \]
Prologue

Erasure Correcting Codes

\[ c_1 + c_2 + c_4 = 0 \]
\[ c_2 + c_3 + c_5 = 0 \]
\[ c_1 = c_2 + c_4 \]
\[ c_2 + c_3 + c_5 = 0 \]
Correcting Packets

\[ c_1 + c_2 + c_3 + c_4 = 0 \]

M. Chiani, Univ. of Bologna
Prologue

Generalization (generalized/doubly generalized LDPC codes)
Prologue

Multiple Access: Slotted ALOHA

Pr(success in one slot) = M \frac{1}{N_{SA}} \left(1 - \frac{1}{N_{SA}}\right)^{M-1} \rightarrow \frac{M}{N_{SA}} e^{-\frac{M}{N_{SA}}} = Ge^{-G}

M. Chiani, Univ. of Bologna
Summary of this talk

- Review of some modern coded random access schemes (e.g., CRDSA, IRSA, CSA) for feedback-free uncoordinated access by a large user population.
- Analytical framework to analyze the performance of coded multiple access with finite frame sizes, based on enumeration techniques.
Background

The problem of multiple access for a potentially very large population of users who wish to transmit over a shared communication medium is receiving an increasing attention.
The problem of multiple access for a potentially very large population of users who wish to transmit over a shared communication medium is receiving an increasing attention.

- WSNs with a high density of sensors;
- RF-ID systems with a high density of tags;
- IoT applications;
- M2M communications;
- 5G mobile communications systems;
- ...
The problem of multiple access for a potentially very large population of users who wish to transmit over a shared communication medium is receiving an increasing attention.

- WSNs with a high density of sensors;
- RF-ID systems with a high density of tags;
- IoT applications;
- M2M communications;
- 5G mobile communications systems;
- ...

With large number of active users, demand assignment multiple access (DAMA) protocols may become impractical.
Uncoordinated access protocols may represent an appealing solution. However ...

- They necessarily lead to collisions among packets being transmitted by the users.
- A collision notification mechanism may not be feasible for a large population of users and for delay-constrained applications.
- Severe stability issues are expected with traditional random access schemes, for a large number of users wishing to access the channel.

Recent “modern” random access protocols have performance close to DAMA, but supporting large number of uncoordinated users, even without retransmissions ...
Some “Classical” Random Access Schemes

- **Slotted ALOHA (SA)** [Abramson1970]: Still adopted as the initial access scheme in both cellular terrestrial and satellite communication networks.

- **Diversity slotted ALOHA (DSA)** [Choudhury1983]: Introduces a packet repetition (twin replicas) to achieve a slight throughput enhancement respect to SA at low loads.

---


Some “Modern” Random Access Schemes

- **Contention resolution diversity slotted ALOHA (CRDSA)** [Casini2007]: Packet repetition is combined with iterative interference cancelation.

- **Irregular repetition slotted ALOHA (IRSA)** [Liva2011]: A generalization of CRDSA that allows an irregular repetition rate.

- **Coded Slotted ALOHA (CSA)** [Paolini2011]: A generalization of IRSA in which generic linear block codes are employed by the users.

- **Constant Rate Assignment (CRA)** [Kissling2011]: An extension of CRDSA to the asynchronous (unslotted) case.

- **Frameless CSA** [Stefanovic2013]: A variant of CSA/IRSA/CRDSA in which the duration of the contention period is adaptively tuned.

**References**


There are $M$ users, each attempting a packet transmission within a MAC frame of time duration $T_F$.

Number of slots $N_{SA} = N_{IRSA}$, each of duration $T_{SA} = T_{IRSA} = T_F/N_{SA}$.

Each user performs a single transmission attempt within the frame
- either a new packet or a previously collided one if retransmissions are allowed
- a new packet if retransmissions are not allowed - the scheme is reliable also without retransmissions.

The normalized offered traffic (or channel traffic) is given by

$$G = \frac{M}{N_{SA}}$$

and represents the average number of packet transmissions per slot.

We define the normalized throughput $T$ as the probability of successful packet transmission per time slot.
Contention Resolution Diversity Slotted ALOHA (CRDSA)

- **Idea:** adopt successive **interference cancellation (SIC)** to resolve collisions.
  - Each of the transmitted twin replicas has a pointer to the slot position where the respective copy was sent.
  - If a burst (i.e., packet) is detected and successfully decoded, the pointer is extracted and the interference contribution caused by the burst replica on the corresponding slot is removed.
  - Procedure iterated, hopefully yielding the recovery of the whole set of bursts transmitted within the same MAC frame.

- **Peak normalized throughput** (defined as the probability of successful packet transmission per slot):
  \[ T \approx 0.55 \]
  versus \( T = \frac{1}{e} \approx 0.37 \) achieved by SA.

- Larger (by a factor of 2) **average transmitted power** than SA for the same peak power.

M. Chiani, Univ. of Bologna
SA and CRDSA

a) Slotted ALOHA

Frame, $T_s$ seconds, $N_{SA}$ slots

Slot, $T_{SA}$ seconds

User 1
User 2
User 3

Collision

Frame, $T_s$ seconds, $N_{RSA}$ slots

Slot, $T_{RSA}$ seconds

User 1
User 2
User 3

__M. Chiani, Univ. of Bologna__
CRDSA/IRSA and iterative decoding over graphs

M. Chiani, Univ. of Bologna
With respect to CRDSA, a **variable repetition rate** for each burst is allowed.

Letting $\delta_h$ be the fraction of time a user repeats his packet $h$ times, the rate of the scheme is

$$ R = \frac{1}{\sum_h \delta_h h} \leq 1/2. $$

The increment in the average transmitted power w.r.t. pure SA is $\Delta P = 10 \log_{10}(1/R) \geq 3$ dB.

We introduce coded slotted ALOHA as a solution to obtain rates $R \geq 1/2$. 
CSA: Preliminary Definitions

- We consider a **framed** and **slotted** scheme where slots are grouped in medium access control (MAC) frames, all with the same length $m$ (in slots).

- Each slot has a time duration $T_{\text{slot}}$, whereas the MAC frame is of time duration $T_{\text{frame}}$, so $m = T_{\text{frame}} / T_{\text{slot}}$.

- We consider a large population of users, whose number is $N$.

- Each user is frame- and slot-synchronous.

- Neglecting guard times, the time duration of a burst is $T_{\text{slot}}$.

- At the beginning of a MAC frame each user generates a burst with probability $\pi \ll 1$ (activation probability).

- Users attempting the transmission within a MAC frame are referred to as active users, and users that are idle as inactive users.
The number of active users is modeled by the random variable $N_a$, which is binomially-distributed with mean value $\mathbb{E}[N_a] = \pi N$.

**Instantaneous channel load:**

$$G_a = \frac{N_a}{m}.$$ 

**Average channel load** (expected number of burst transmissions per slot):

$$G = \frac{\mathbb{E}[N_a]}{m} = \frac{\pi N}{m} = \pi \alpha$$

where $\alpha$ is the population size normalized to the number of slots.
CSA: Encoding Procedure

- Each of the \( N_a \) active users divides his burst sent (duration \( T_{\text{slot}} \)) into \( k \) information (or data) segments.

- The \( k \) data segments are encoded via an \((n_h, k)\) linear block code \( C_h \) generating \( n_h \) encoded segments all of the same length as the data segments.

- The \((n_h, k)\) code is picked by the user from a set \( C = \{C_1, C_2, \ldots, C_{n_c}\} \) of \( n_c \) candidate codes, all having the same dimension \( k \). The set \( C \) is known to the receiver.

- Each active user draws his local code from the set \( C \) independently of all his previous choices and without any coordination with the other users.

- The code is picked according to a probability mass function (p.m.f.) \( \delta = \left\{ \delta_h \right\}_{h=1}^{n_c} \) which is the same for all users.
CSA: Encoding Procedure

- The time duration of each transmitted segment is $T_{\text{segment}} = T_{\text{slot}}/k$. The MAC frame is composed of $M = km$ slices, each of time duration $T_{\text{segment}}$.
- The $n_h$ encoded segments are transmitted by the active user over $n_h$ slices picked uniformly at random.
- **Rate** of the CSA scheme:
  \[
  R = \frac{k}{\bar{n}}
  \]
  where
  \[
  \bar{n} = \sum_{h=1}^{n_c} \delta_h n_h.
  \]
- Increment in the average transmitted power w.r.t. pure SA is
  \[
  \Delta P = 10 \log_{10}(1/R).
  \]
- If $\mathcal{C}$ contains only repetition codes ($k = 1$) then we obtain the IRSA scheme. Note that with CSA we can achieve $R > 1/2$. 

M. Chiani, Univ. of Bologna
CSA: Transmission Example

Frame, $T_F$ seconds, $N_{CSA} = kN_{SA}$ slots

Slot, $T_{CSA}$ seconds

User 1, $C_1(n_1,k)$

User 2, $C_2(n_2,k)$

User 3, $C_3(n_3,k)$

\[ \vdots \]

User M, $C_M(n_M,k)$

Parity sub-packet

c) Coded SA

M. Chiani, Univ. of Bologna
CSA: Bipartite Graph Representation

- For an instantaneous population of $N_a$ users and a frame with $M$ slices, the frame status can be described by a **bipartite graph** $G = (B, S, E)$.
- It consists of a set $B$ of $N_a$ **burst nodes** (one for each active user), a set $S$ of $M$ **slice nodes** (one for each slice in the frame), and a set $E$ of edges.
- An edge connects a burst node $b_i \in B$ to a slice node $s_j \in S$ if and only if the $i$-th active user has transmitted an encoded segment in the $j$-th slice.
- Degree of a node: Number of edges connected to it.
- Example ($N_a = 5$, $M = 8$, $k = 2$):

![Bipartite Graph Diagram](image-url)
CSA: Distributions

- The component code distribution is
  \[ \delta(x) = \sum_{h=1}^{n_c} \delta_h x^h. \]

- The slice node degree distribution “from an edge perspective” is
  \[ \rho(x) = \sum_{i=1}^{M} \rho_i x^{i-1} \]

  where \( \rho_i \) is the probability that an edge is connected to a slice node of degree \( i \).
CSA: Decoding Example

- $N_a = 3$, $M = 7$, $k = 2$. Each user employs a $(3, 2)$ single parity-check code.
CSA: Decoding Example

- \( N_a = 3, \ M = 7, \ k = 2 \). Each user employs a (3, 2) single parity-check code.

\[ \begin{array}{cccccccc}
S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_7 \\
\hline
\end{array} \]

\[ \begin{array}{cccccccc}
B_1 & B_2 & B_3 \\
\hline
\end{array} \]

b) IC iteration 1
CSA: Decoding Example

- \( N_a = 3, \ M = 7, \ k = 2 \). Each user employs a (3, 2) single parity-check code.

\[ \begin{align*}
S_1 & \quad S_2 & \quad S_3 & \quad S_4 & \quad S_5 & \quad S_6 & \quad S_7 \\
\square & \quad \square & \quad \square & \quad \square & \quad \square & \quad \square & \quad \square \\
\end{align*} \]

c) IC iteration 2
In each slice of the MAC frame the decoder is able to discriminate between:

- a “silence”;
- a signal corresponding to a unique slice;
- a “mess” being the result of a collision. (This signal provides no information to the decoder about the number and the values of colliding segments.)

When a segment experiences no collisions, it is correctly received.

Interference cancelation is ideal, as so is the estimation of the channel parameters necessary to perform it.

Cancelation of the interference contribution of a slice in a slice consists of subtracting the corresponding signal from the “mess” currently present in the slice.
CSA: The XOR Multiple Access Channel

M. Chiani, Univ. of Bologna
Under the previous assumptions, we can establish a connection with modern codes on graphs.

- **SIC process** represented as a *message-passing decoding* algorithm along the edges of a bipartite graph.

- Equivalent to iterative erasure decoding of a doubly-generalized LDPC code [Paolini2010].

CSA: Density Evolution Equations

- Let \( m \rightarrow \infty \) for a constant population size \( \alpha \).
- Assume MAP decoding is used at the burst nodes.
- Let \( \ell \) be the SIC iteration index. Moreover, let:
  - \( p_\ell = \Pr\{\text{an edge is connected to a SN where a collision still persists}\} \);
  - \( q_\ell = \Pr\left\{\begin{array}{l}
\text{an edge is connected to a BN whose contribution of interference on the corresponding segment cannot yet be canceled}
\end{array}\right\} \)
- Then we can formulate density evolution equations as follows:

\[
q_\ell = \frac{1}{n} \sum_{h=1}^{n_c} \sum_{t=0}^{n_h-1} n_h^{-1-t} [(n_h - t)\tilde{e}^{(h)}_{n_h-t} - (t + 1)\tilde{e}^{(h)}_{n_h-1-t}]
\]

\[
p_\ell = 1 - \rho(1 - q_\ell) = 1 - \exp\left\{-\frac{\pi \alpha}{R} q_\ell\right\}
\]
CSA: Density Evolution Equations

- In the previous equations, $\tilde{e}_g^{(h)}$ is the $g$-th un-normalized information function of code $C_h$.
- This is equal to the sum of the ranks of all $k \times g$ submatrices of a generator matrix of $C_h$ [Helleseth1997] [Ashikhmin2004].


CSA: Asymptotic Threshold

- Outcome of density evolution analysis: Existence of a threshold:

\[ \pi^*(C, \Lambda, \alpha) = \sup\{\pi \text{ s.t. } p_\ell \to 0 \text{ as } \ell \to \infty\}. \]

Equivalently (in terms of channel load):

\[ G^* = \sup\{G \text{ s.t. } p_\ell \to 0 \text{ as } \ell \to \infty\} = \alpha \times \pi^*(C, \Lambda, \alpha). \]

- For a given \( C = \{C_1, \ldots, C_{nc}\} \) and a given \( \Lambda = \{\Lambda_h\}_{h=1,\ldots,n_c} \) there exists \( G^*(C, \Lambda) \) s.t.
  - for all \( 0 < G < G^*(C, \Lambda) \), the residual packet erasure probability tends to zero as the number of IC iterations tends to infinity;
  - for all \( G > G^*(C, \Lambda) \), decoding fails with a probability that is essentially 1.

- The access scheme is reliable even without retransmissions.
CSA: Threshold Optimization

- For a given set $C$ of component codes and for a given rate $R$, we optimize the threshold $G^*(C, \Lambda)$ with respect to the p.m.f. $\Lambda$.

- The optimization problem may be formulated as

\[
\text{maximize } G^*(C, \Lambda) \\
\text{subject to } C = \{C_1, \ldots, C_{n_c}\} \\
R = \frac{k}{\sum_{h=1}^{n_c} \Lambda_h n_h}
\]

- Optimization was performed via Differential Evolution algorithm [Price1997].

Threshold $G^*$ Optimization

- In the table some distribution profiles $\Lambda$ and thresholds $G^*$ are reported for optimized IRSA and optimized CSA (with $k = 2$) schemes under the random code hypothesis.
- IRSA schemes with rates $1/3$, $2/5$ and $1/2$ and CSA schemes with rates $1/3$, $2/5$, $1/2$ and $3/5$.
- Rates higher than $R = 1/2$ are possible only in the CSA framework.
- IRSA closely approached or outperformed by CSA in all examined cases.

<table>
<thead>
<tr>
<th></th>
<th>$IRSA$</th>
<th>$G^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$(2, 1)$</td>
<td>$(3, 1)$</td>
</tr>
<tr>
<td>$R = 1/3$</td>
<td>0.554016</td>
<td>0.261312</td>
</tr>
<tr>
<td>$R = 2/5$</td>
<td>0.622412</td>
<td>0.255176</td>
</tr>
<tr>
<td>$R = 1/2$</td>
<td>1.000000</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$CSA \ k = 2$</th>
<th>$G^*$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$(3, 2)$</td>
<td>$(4, 2)$</td>
</tr>
<tr>
<td>$R = 1/3$</td>
<td>0.088459</td>
<td>0.544180</td>
</tr>
<tr>
<td>$R = 2/5$</td>
<td>0.153057</td>
<td>0.485086</td>
</tr>
<tr>
<td>$R = 1/2$</td>
<td></td>
<td>1.000000</td>
</tr>
<tr>
<td>$R = 3/5$</td>
<td>0.666667</td>
<td>0.333333</td>
</tr>
</tbody>
</table>
Throughput Comparison

Simulation results for a finite number $M$ of users adopting the optimized degree profiles in the previous table.

- $m = 500,$
  $M = k m = 1000,$
  $N_a = G \times m$ for each $G.$

- Linear block codes all with $k = 2,$ and $n \in \{2, 4, 5, 8, 9, 12\}.$

- Remarkable performance of CSA over IRSA even for $R = 1/2$ (peak throughput about 0.6)

- All peak throughput close to the asymptotic thresholds

M. Chiani, Univ. of Bologna
Information-Theoretic Upper Bound on $G^*(C, \Lambda)$

**Theorem**

For rational $R$ and $0 < R \leq 1$, let $G(R)$ be the unique positive solution to the equation

$$G = 1 - e^{-G/R}$$

in $[0, 1)$. Then, the threshold $G^*(C, \Lambda)$ fulfills

$$G^*(C, \Lambda) < G(R)$$

for any choice of $C = \{C_1, C_2, \ldots, C_{n_c}\}$ and $\Lambda$ associated with a rate $R$.

- Two proofs developed: One based on algebraic considerations, one via the Area Theorem [Ashikhmin2004].

$G^*(C, \Lambda)$ for Optimized CSA Schemes with MDS Codes

- **Remark:** Pure SA: $R = 1$ and $G^* = 0$ (unreliable without retransmissions)

M. Chiani, Univ. of Bologna
\( \tilde{G}^*(C, \Lambda) \) for Optimized CSA Schemes with MDS Codes

- In the previous chart:
  - \( \star \) denotes a CSA scheme employing repetition codes \((k = 1)\);
  - \( \square \) denotes a CSA scheme employing MDS codes with \(k = 2\);
  - \( \triangle \) denotes a CSA scheme employing MDS codes with \(k = 3\);
  - \( + \) denotes a CSA scheme employing MDS codes with \(k = 4\).

- Example \((x^h)\) is associated with a \((k + h, k)\) MDS code:

\[
\begin{align*}
\Lambda_7(x) &= 0.322200x^1 + 0.230500x^2 + 0.049100x^4 + 0.398300x^5 \\
R &= 0.502 \\
G^*(C, \Lambda_7) &= 0.7462 \\
G(R) &= 0.7946.
\end{align*}
\]

- In general, for a given \(R\) we observed an improvement in terms of threshold when increasing \(k\).
Coded Slotted Aloha without Feedback Channel

- Packet Loss Rate for Coded SA based on optimized profiles.
- $N = 5000, 1000, 500$, maximum iteration count set to 100.
- Throughput close to 1 packet/frame without feedback channel - no retransmissions!!!
Throughput Analysis for Optimized Regular Codes

Asymptotic throughput vs. $G$ for the CSA scheme based on: No code, i.e. Slotted Aloha ($R = 1$); repetition 2 codes ($R = 1/2$) (CRDSA); a $(3, 2)$ single parity-check code; a $(5, 3)$ code; a $(4, 2)$ code; a $(7, 2)$ code.

M. Chiani, Univ. of Bologna
Packet Loss Rate Analysis for Optimized Regular Codes

Asymptotic PLR vs. $G$ for the CSA scheme based on: No code, i.e. Slotted Aloha ($R = 1$); repetition 2 codes ($R = 1/2$) (CRDSA); a $(3, 2)$ single parity-check code; a $(5, 3)$ code; a $(4, 2)$ code; a $(7, 2)$ code.

M. Chiani, Univ. of Bologna
Packet Loss Rate Analysis for Optimized Regular Codes

PLR for the RA scheme based on the repetition-2 code (CRDSA).

Line: asymptotic analysis. Points: simulation for $\rho = 200$, maximum iteration count set to 200.

PLR for the RA scheme based on a $(6, 3)$ code.
Some results on Coded Slotted Aloha

- Assuming infinitely long frames, we studied:
  - the codes design in CSA, based on density evolution techniques
  - the information-theoretic limits on the throughput for a given rate
  - the residual packet loss rate with a maximum number of iterations.

- Current research includes the theoretical analysis for the case of finite-size frames.
Conclusions

**Analogy:**

**Errors:** Forward Error Correction ⇔ ARQ

**Collisions:** Coded Slotted Aloha ⇔ Slotted Aloha

- The CSA graph-based random access scheme can approach an efficiency of 1 packet/slot without retransmissions.
- Theoretical limits and design tools are available.
References

References

Thanks to:

- Enrico Paolini
- Gianluigi Liva
- Michael Lentmaier

Research supported in part by the EC under the FP7 project CONCERTO, grant agreement n. 288502