Base Station Cooperation for Mission Critical Communications

Marceau Coupechoux\textsuperscript{1}

Joint work with Alaa Daher\textsuperscript{2}, Deepa Jagyasi\textsuperscript{1}, Philippe Godlewski\textsuperscript{1} with the help of the company ETELM (project EXTRANGE4G)

\textsuperscript{1}Telecom Paris, Institut Polytechnique de Paris
\textsuperscript{2}ETELM, France

IEEE Int. Conf. on Advanced Communication Technologies and Signal Processing (ACTS)

4 Dec. 2020
Future Wireless Networks Challenges

- **5G Mobile Broadband Access**
  - Critical Communications
  - Massive IoT Access
  - Virtualized Network Management
  - Intelligent Transportations Systems

- **Connected vehicles**
  - Autonomous vehicles
  - Platooning

- **5G**
  - High throughput apps
  - Very HD video
  - Broadcast services
  - Downloading

- **High priority com.**
  - Remote control
  - Interactive games
  - Tactile internet
  - Industrial automatisation
  - Industrial control

- **Flexibility and scalability**
  - Network slicing
  - Security
  - Multi-technology connectivity
  - QoS, priorities management
  - Mobility
  - Content management, caching

- **Bio-connectivity**
  - Home networking
  - Smart meters
  - Sensors
  - Logistics
  - Agriculture
Mission Critical Communications

Source: ETELM
MCC = All communications related to the safety and the security of the civil society. Public safety services, like police forces, firemen, rescue and ambulance services, or employees critical infrastructures, like energy and transportation suppliers.

MCC are conveyed by Professional Mobile Radio (PMR) networks.

One of the most important and indispensable services offered by mission-critical networks is the group communication.

MCC unique requirements: coverage, reliability and secure communications.

Group communication is based on Multimedia Broadcast/Multicast Service (MBMS) in 3GPP.
Mission Critical Communications

Mission-Critical Communications requirements

- Special services
- Secure Communications
- Priority access
- Wide coverage
- Reliability
Outlines

1. **A Dynamic Clustering Algorithm**
   - Motivation
   - Model
   - Problem Formulation
   - Algorithms
   - Numerical Results

2. **Secure Multi-User MIMO Transceiver**
   - Motivation
   - Model
   - Transceiver Design
   - Numerical Results

3. **Conclusions and Future Works**
Outline

1. A Dynamic Clustering Algorithm
   - Motivation
   - Model
   - Problem Formulation
   - Algorithms
   - Numerical Results

2. Secure Multi-User MIMO Transceiver
   - Motivation
   - Model
   - Transceiver Design
   - Numerical Results

3. Conclusions and Future Works
Motivation

Multicast/Broadcast Single Frequency Network

User SINRs are maximized

Radio resources can be wasted
A Dynamic Clustering Algorithm

Motivation

Single-Cell Point-To-Multipoint

Degraded user SINRs

Maximized network capacity
Motivation

**SC-PTM**
- Degraded users SINRs
- Maximized network capacity

**MBSFN**
- Users SINRs are maximized
- Radio resources can be wasted

Our objective: design a dynamic clustering algorithm to solve the reliability-capacity tradeoff in MCC
Motivation

Clustering for cooperative transmissions

- State-of-the-art is mostly on unicast best effort traffic with the goal of maximizing user data rates under static traffic models
- Greedy algorithms based approaches have been widely used in network-centric clustering algorithms [PGH08, YKL16, DdV14, BBB14, Sch17]
  ⇒ Not optimal and requires adaptations for group communications
- Dynamic user centric clustering [LHYZ16, GZS14, LZG\textsuperscript{+}18, BJIX16, ZWZ\textsuperscript{+}17]
  ⇒ Focus on PHY data rate, dynamic traffic constraints ignored, only unicast, no reliability constraint
- MBMS literature [REH11, CCE\textsuperscript{+}15]
  ⇒ Do not address the reliability-capacity tradeoff
System Model

- Downlink of a cellular network
- A set $V = \{1, \ldots, n\}$ of $n$ cells forming an MBSFN synchronization area
- A cluster is a subset $S \subseteq V$ serving a group $U$ of users using multi-point transmissions
- Signal to interference plus noise ratio (SINR) at user $u \in U$:

$$\gamma_u(S) = \frac{\sum_{b \in S} \xi_{ub} g_{ub} P_T}{\sum_{b \in S} (1 - \xi_{ub}) g_{ub} P_T + \sum_{b \notin S} P_T g_{ub} + N_{th}},$$

where $\xi_{ub}$ denotes the useful portion of the signal received by $u$ from $b$ (see [RHE08] for the detailed calculation)
- For a multicast group $U$ of $N$ users served by cells in $S$, the average SINR is:

$$\bar{\gamma}_U(S) = \frac{1}{N} \sum_{u \in U} \gamma_u(S).$$
Dynamic Traffic Model

- Call blocking model: group of users arrive in the synchronization area, use a resource for a group communication for a certain duration and leave the system.
- Poisson arrival ($\lambda$), exponential service duration ($\mu$), $R$ resources in every BS.
- When a group arrives in the system, it is served by a subset $S$ of BSs with probability $p_S$ and one resource is consumed in every BS in $S$.
- We can approximate the blocking probability in BS $b$ by using Erlang-B:

$$\tilde{\Pi}(b) \approx E_B(b, R) = \frac{\rho_b^R}{R!} \sum_{r=0}^{R} \frac{\rho_b^r}{r!},$$

where $\rho_b$ is the load in station $b$ (depends on $\lambda$, $\mu$ and the probability mass function $p_S$).
Cell clustering (inner) problem: find a minimizer set $S$ that solves the following set function minimization problem, for a given group $\mathcal{U}$:

$$\min_{S \in \mathcal{P}_V} \psi_{\mathcal{U}}(S) \triangleq W(S) - \bar{\gamma}_{\mathcal{U}}(S)$$

- $S$: set of serving BSs
- $\mathcal{P}_V$: set of all subsets of $V$
- $W(S) = \sum_{b \in S} w_b$: sum of the weights of BSs $b \in S$
- $\bar{\gamma}_{\mathcal{U}}(S)$: average SINR of group $\mathcal{U}$ served by cells in $S$

⇒ For a fixed $w = (w_1, \cdots, w_n) \in \mathbb{R}^n$, the traffic demand and the clustering policy $p_S$ induces a blocking probability $\tilde{\Pi}(b; w)$ in every $b$
Problem Formulation : Weights Optimization

Weights optimization (outer) problem : find a minimizer of the quadratic error of the blocking probability wrt target blocking probabilities :

$$\min_{w \in \mathbb{R}^n} G(w) \triangleq \sum_{b=1}^{n} \| \tilde{\Pi}(b; w) - \bar{\Pi}(b) \|^2$$  \hspace{1cm} (5)

- $\tilde{\Pi}(b; w)$ : blocking probability in a BS $b$ that depend on the weights vector ($w$)
- $\bar{\Pi}(b)$ : target blocking probability that BS $b$ should attain
Dynamic Clustering Algorithm (DCA)

- At every group arrival
- Statistics on groups and clusters
- Cluster $S$ Call duration $D$
- Group Call Clustering Algorithm (GCCA)
- Cluster $S$
- Group is served using cluster $S$
- Cell Weights Optimization Algorithm (CWOA)
- Use existing weights
- Update weights
- End of period of duration $T$?
- Yes
- No
- Weights
- At every group arrival
A Dynamic Clustering Algorithm

Group Call Cell Clustering Algorithm (GCCA)

\[
\min_{S \in \mathcal{P}_V} \Psi_U(S) \triangleq w(S) - \bar{\gamma}_U(S)
\]

\(\Psi_U\) is a submodular function.

Submodular functions: A set function \(F : 2^V \mapsto \mathbb{R}\) is submodular if and only if, for all subsets \(A, B \subseteq V\) and \(b \in V\) such that \(A \subseteq B\) and \(b \notin B\), we have:

\[
F(A \cup b) - F(A) \geq F(B \cup b) - F(B).
\]

Adding \(b\) to set \(A = \{s_1, s_2\}\)

Adding \(b\) to set \(B = \{s_1, ..., s_4\}\)
Group Call Cell Clustering Algorithm (GCCA)

\[
\min_{S \in \mathcal{P}_v} \psi_\mathcal{U}(S) \triangleq w(S) - \bar{\gamma}_\mathcal{U}(S)
\]

\(\psi_\mathcal{U}\) is a submodular function.

- Minimizing \(\psi_\mathcal{U}\) is a submodular minimization problem.
- This problem is solved using the Minimum-Norm Algorithm [Fuj84, Wol76].
- The performance of this solution is compared to a Greedy based approach.
Cell Weights Optimization Algorithm (CWOA)

\[
\min_{w \in \mathbb{R}^n} G(w) \triangleq \sum_{b=1}^{n} \| \bar{\Pi}(b; w) - \bar{\Pi}(b) \|^2
\]

- We rely on direct search methods to minimize \( G \).
- These methods provide simpler calculations and relatively low storage requirements over derivative based methods.
- The most popular is the Nelder-Mead simplex method.
Cell Weights Optimization Algorithm (CWOA)

\[
\min_{w \in \mathbb{R}^n} G(w) \triangleq \sum_{b=1}^{n} \|\tilde{\Pi}(b; w) - \bar{\Pi}(b)\|^2
\]

- Nelder-Mead algorithm can stagnate, fail to converge or converge to a non-optimal vertex.
- A possible improvement of the original algorithm is to impose restarts of the algorithm during the optimization run.
- An oriented restart of the Nelder-Mead algorithm adapted to our model:
  - If \(\tilde{\Pi}(b; w)\) is too small, weight \(w_b\) is decreased randomly;
  - If \(\tilde{\Pi}(b; w) > \bar{\Pi}(b)\), weight \(w_b\) is increased randomly.
Numerical Results: Group Call Clustering

Figure – Evolution of $\Psi_u$ along the iterations of the minimum-norm algorithm

SC-PTM and full MBSFN cooperation schemes are outperformed by the proposed algorithm in very few iterations.
Evolution of $G$ and cell blocking probabilities along the iterations of the Nelder-Mead algorithm

The reliability-capacity tradeoff is well handled by the proposed scheme.
The proposed scheme lies in-between MBSFN and SC-PTM in terms of SINR.
Conclusion

⇒ Our algorithm is able to adapt to traffic variations by maximizing the coverage under the constraint of a blocking probability.

Related publications:


Outline

1. A Dynamic Clustering Algorithm
   - Motivation
   - Model
   - Problem Formulation
   - Algorithms
   - Numerical Results

2. Secure Multi-User MIMO Transceiver
   - Motivation
   - Model
   - Transceiver Design
   - Numerical Results

3. Conclusions and Future Works
Motivation

- The previous study is ignoring security aspects and relies on simple physical layer models.

⇒ Our goal now: design a multi-BS multi-antenna transceiver for MCC that is robust to CSI errors (*reliability requirement of MCC*) and that is secured with respect to the presence of multiple eavesdroppers (*security*).

- Specifically, we incorporate security in two ways:
  - MIMO beamforming is used to achieve the desired performance gain at legitimate users while degrading eavesdroppers channel;
  - Artificial Noise (AN) is added at the transmitter to guarantee additional security over the designed transceivers.

- Robustness is considered wrt:
  - Stochastic errors
  - Norm-bounded errors
Network Model

Figure – Blue cells are serving a group of legitimate users (green diamonds); multiple eavesdroppers may overhear the communication (red stars).
A greedy clustering is adopted for simplicity:

**Algorithm 1 Greedy Clustering**

1: **Input**: Locations of BSs and group users, $K_T' \leq |B|$: minimum cluster size
2: **Init**: $S \leftarrow \emptyset$
3: **for** every user **do**
4: Find the BS $t$ providing the highest receive power
5: $S \leftarrow S \cup \{t\}$
6: **end for**
7: **if** $|S| < K_T'$ **then**
8: Find the set $S'$ of $K_T' - |S|$ BSs maximizing the sum SINR for group users
9: $S \leftarrow S \cup S'$
10: **end if**
11: **return** $S$
Transceiver Model

Coordinated BSs

Eavesdroppers

Legitimate UEs

$V_1$, $V_2$, $\cdots$, $V_{KT}$

$E_1$, $E_2$, $\cdots$, $E_{KE}$

$R_1$, $R_2$, $\cdots$, $R_{KR}$
Transceiver Model

- The signal transmitted from $t$-th BS is given by:
  \[ x_t = V_t d + W_t z_t, \]  
  where $V_t$ is a precoder, $z_t$ is an zero-mean additional AN vector with variance $E[z_t z_t^H] = \sigma_{zt}^2 I_{NT}$ and $W_t$ is an AN-shaping matrix.

- The estimated data at user $l$ is:
  \[ \hat{d}_l = R_l C_{tl} V_t d + R_l C_{tl} W_t z_t + R_l n_l. \]  
  where $R_l$ is a receive filter.

- The MSE at the $l$-th legitimate UE is:
  \[ \epsilon_l \triangleq E[\|d - \hat{d}_l\|^2], \]  

- In the same way, the MSE at eavesdropper $e$ is:
  \[ \epsilon_e \triangleq E[\|d - \overline{d}_e\|^2]. \]
Transceiver Model

CSI errors:
- At legitimate users: \( \mathbf{G}_{te} = \hat{\mathbf{G}}_{te} + \Delta_{te} \)
- At eavesdroppers: \( \mathbf{C}_{tl} = \hat{\mathbf{C}}_{tl} + \Delta_{tl} \)

**Assumption (Stochastic error model)**

CSI errors \( \Delta_{te} \) and \( \Delta_{tl} \) are modeled as Gaussian random variables such that
\[
\mathbb{E}[\Delta_{te}\Delta_{te}^H] = \sigma_{te}^2 \mathbf{I} \quad \text{and} \quad \mathbb{E}[\Delta_{tl}\Delta_{tl}^H] = \sigma_{tl}^2 \mathbf{I}.
\]

**Assumption (Norm-bounded error model)**

CSI errors \( \Delta_{te} \) and \( \Delta_{tl} \) are respectively taken in continuous sets, called uncertainty regions:
\[
\mathcal{G}_{te} = \{ \Delta_{te} : \|\Delta_{te}\|^2 \leq \tau_{te} \}, \tag{10}
\]
\[
\mathcal{C}_{tl} = \{ \Delta_{tl} : \|\Delta_{tl}\|^2 \leq \tau_{tl} \}, \tag{11}
\]

where \( \tau_{te} \) and \( \tau_{tl} \) denote the radii of the uncertainty regions.
In presence of stochastic errors:

\[
\begin{align*}
\text{minimize} & \quad \sum_{l=1}^{K_R} \epsilon_l, \\
\text{subject to} & \quad C1: \quad \epsilon_e \geq \Gamma, \quad \forall e \in \{1, \ldots, K_E\}, \\
& \quad C2: \quad P_t \leq P_T, \quad \forall t \in \{1, \ldots, K_T\},
\end{align*}
\]

(P1)

where \( \Gamma \) is a design parameter that represents a lower bound on the achievable MSE expected at each eavesdropper.


Stochastic Errors : Stationary Point

**Proposition**

\[ V_t = (A_t)^{-1} \left( \sum_{l=1}^{K_R} \hat{C}_t^H R_l^H - \sum_{e=1}^{K_E} \lambda_e \hat{G}_e^H \lambda_e \right) \]  

\[ W_t = B_t / \sqrt{\text{tr}(B_t B_t^H)} \]  

\[ R_l = \left( \sum_{t=1}^{K_T} V_t^H \hat{C}_t^H \right) \left( \sum_{t=1}^{K_T} \hat{C}_t V_t V_t^H \hat{C}_t^H + \sum_{t=1}^{K_T} \sigma_{zt}^2 \hat{C}_t W_t W_t^H \hat{C}_t^H + \sigma_{nl}^2 I + \sum_{t=1}^{K_T} \sigma_{zl}^2 \text{tr}(V_t V_t^H) I + \sum_{t=1}^{K_T} \sigma_{zl}^2 \sigma_{zt}^2 \text{tr}(W_t W_t^H) I \right)^{-1} \]  

\[ B_t = I - A_t^H (A_t A_t^H)^{-1} A_t, \]

\[ A_t = \sum_{l=1}^{K_R} \hat{C}_t^H R_l^H \hat{C}_t^H + \sum_{l=1}^{K_R} \sigma_{zl}^2 \text{tr}(R_l R_l^H) - \sum_{e=1}^{K_E} \lambda_e \hat{G}_e^H \hat{G}_e \lambda_e \]  

\[ + \sum_{e=1}^{K_E} \lambda_e \sigma_{te}^2 \text{tr}(E_e E_e^H) + \lambda_t I. \]
Stochastic Errors : Block Descent Algorithm

Algorithm 2 Block Descent Algorithm

1: Input : $\beta$, $K_T$, $K_R$, $K_E$, $\hat{C}_{tl}$, $\hat{G}_{te}$, $\sigma_{nl}$, $\sigma_{ne}$, $P_t \ \forall \ t \in \{1, \cdots , K_T\}$, $l \in \{1, \cdots , K_R\}$, and $e \in \{1, \cdots , K_E\}$
2: Init : Randomly generate $V_t$, $W_t \ \forall \ t \in \{1, \cdots , K_T\}$, $\epsilon'_l \leftarrow 0$, $\epsilon_l \leftarrow 0$, $\forall \ l \in \{1, \cdots , K_R\}$
3: repeat
4: $\epsilon'_l \leftarrow \epsilon_l$, $\forall \ l \in \{1, \cdots , K_R\}$
5: Update $E_e \ \forall e \in \{1, \cdots , K_E\}$ (MMSE filter)
6: Update $R_l$ using $V_t$, $W_t$ in (14) $\forall l \in \{1, \cdots , K_R\}$
7: Solve for $\lambda_e$ and $\lambda'_t$ using $C1$, $C2 \ \forall t \in \{1, \cdots , K_T\}$, and $\forall e \in \{1, \cdots , K_E\}$
8: Update $V_t$ using $\lambda_e$, $\lambda'_t$, $R_l$, $E_e$ in (12) $\forall t = \{1, \cdots , K_T\}$
9: Update $W_t$ using $V_t$ in (13) $\forall t = \{1, \cdots , K_T\}$
10: Compute $\epsilon_l$ using $V_t$, $\lambda_e$, $\lambda'_t$, $W_t$, and $R_l$
11: until $|\epsilon_l - \epsilon'_l| \leq \beta$, $\forall l \in \{1, \cdots , K_R\}$
12: return $V_t$, $W_t$, $\forall t \in \{1, \cdots , K_T\}$, $R_l$, $\epsilon_l$ $\forall l \in \{1, \cdots , K_R\}$
Norm-Bounded Errors: Problem Formulation

In presence of norm-bounded errors:

\[
\begin{align*}
\text{minimize} & \quad \sum_{t=1}^{K_T} \sum_{l=1}^{K_R} \epsilon_l, \\
\text{subject to} & \quad C_1, C_2 \\
& \quad C_4: \quad \Delta_{te} \in G_{te}, \quad \forall t \in \{1, \ldots, K_T\}, \forall e \in \{1, \ldots, K_E\} \\
& \quad C_5: \quad \Delta_{tl} \in C_{tl}, \quad \forall t \in \{1, \ldots, K_T\}, \forall l \in \{1, \ldots, K_R\}
\end{align*}
\]

An equivalent (robust) formulation:

\[
\begin{align*}
\text{minimize} & \quad \max_{\Delta_{tl} \in C_{tl}} \sum_{t=1}^{K_T} \sum_{l=1}^{K_R} \epsilon_l, \\
\text{subject to} & \quad C_2, \\
& \quad C_6: \quad \min_{\Delta_{te} \in G_{te}} \epsilon_e \geq \Gamma, \quad \forall e \in \{1, \ldots, K_E\}
\end{align*}
\]
Norm-Bounded Errors : Problem Decomposition

**Sub-problem $\bar{P}'_2$** : Assume that the worst-case channel errors $\Delta_{te}$ and $\Delta_{tl}$ are known and solve for the transceiver matrices :

$$
\min_{V_t,W_t,R_l} \sum_{l=1}^{K_R} \epsilon_l,
\text{subject to } C1, C2
$$

($\bar{P}'_2$)

**Sub-problem $\bar{P}''_2$** : Assume that transceiver matrices and the worst-case error $\Delta_{te}$ are known and solve for the worst-case error $\Delta_{tl}$.

$$
\min_{\Delta_{tl}} \sum_{l=1}^{K_R} \epsilon_l,
\text{subject to } C5 : ||\Delta_{tl}||^2 \leq \tau_{tl} \quad \forall t \in \{1, \cdots, K_T\}, \forall l \in \{1, \cdots, K_R\}
$$

($\bar{P}''_2$)
Sub-problem $\tilde{P}_{2}'''$: Assume that transceiver matrices and the worst-case error $\Delta_{tl}$ are known and solve for the worst-case error $\Delta_{te}$.

$$\begin{align*}
\text{minimize} & \quad \epsilon_e \geq \Gamma, \\
\text{subject to} & \quad C4 : \|\Delta_{te}\|^2 \leq \tau_{te} \quad \forall t \in \{1, \cdots, K_T\}
\end{align*}$$

($\tilde{P}_{2}'''$)
Algorithm 3 Iterative Algorithms for NBE

1: **Input**: $\beta$, $K_T$, $K_R$, $K_E$, $E_e$, $\hat{C}_{tl}$, $\hat{G}_{te}$, $\tau_{tl}$, $\tau_{te}$, $P_t$, $\forall$ $t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$, and $e \in \{1, \cdots, K_E\}$

2: **Init**: Randomly generate $V_t$, $W_t$, $\forall$ $t \in \{1, \cdots, K_T\}$, $\Delta_{tl} \in C_{tl}$, $\Delta_{te} \in G_{te}$, $\epsilon_l \leftarrow 0$, $\forall t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$, $e \in \{1, \cdots, K_E\}$

3: **repeat**

4: $\epsilon'_l \leftarrow \epsilon_l$, $\forall l \in \{1, \cdots, K_R\}$

5: Solve $\tilde{P}_2'$ and update $V_t$, $W_t$, $R_l$ using $\Delta_{tl}$, $\Delta_{te}$, $E_e$ and Algorithm 2 $\forall t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$, $e \in \{1, \cdots, K_E\}$

6: Solve $\tilde{P}_2''$ and update $\Delta_{tl}$ using $V_t$, $W_t$, $R_l$ $\forall t \in \{1, \cdots, K_T\}$, $l \in \{1, \cdots, K_R\}$

7: Solve $\tilde{P}_2'''$ and update $\Delta_{te}$ using $V_t$, $W_t$, $E_e$ $\forall t \in \{1, \cdots, K_T\}$, $e \in \{1, \cdots, K_E\}$

8: Compute $\epsilon_l$ using $V_t$, $W_t$, and $R_l$, $\Delta_{tl}$, $\Delta_{te}$

9: **until** $|\epsilon_l - \epsilon'_l| \leq \beta$, $\forall l \in \{1, \cdots, K_R\}$
Robust design improves the reliability of MCC.

Due to increased uncertainty, norm-bounded errors leads to poorer performances compared to stochastic errors.
System performance decreases with increasing CSI error variance.

The higher the variance, the higher the gap bw robust and non-robust.
Numerical Results : Physical Layer

- Security gap: \( S_g = SNR^{L}_{\min} - SNR^{E}_{\max} \)
- Below \( SNR^{E}_{\max} \) at eavesdroppers, the communication is secure, above \( SNR^{L}_{\min} \) at legitimate UEs, the communication is reliable.
- NR: 4dB, R-NBE: 2dB, R-SE: -2dB at BER \( 10^{-4} \) for leg. UEs and 0.3 for eaves
- Robust designs achieve reduced security gap (enhanced secrecy performance).
Presence of AN degrades the performance at eavesdropper whereas it has a very low impact on BER of legitimate UE.
All the systems, MBSFN, SC-PTM and dynamic clustering demonstrate enhanced performance for legitimate UEs as compared to eavesdroppers.

At legitimate UEs, MBSFN performs the best, SC-PTM performs worst, whereas dynamic clustering shows a good trade off.
Conclusion

⇒ We designed an efficient multi-BS multi-antenna secure MIMO transceiver that meets the unique requirements of MCC.

Related publications:


Conclusions and Future Works

- Mission critical communications for public safety, critical infrastructure, etc is a relatively unexplored topic.
- They deserve specific designs because of a unique set of joint constraints like security, reliability, coverage, multicast services.
- Traditional designs focusing on capacity and user data rate maximization no longer apply.
- Future works includes mm waves studies and new approaches to reduce energy consumption.
Thank you for your attention!


References II


