



HAL
open science

Robustesse aux erreurs de transmission: configuration optimale d'un réseau TTP/C

Nicolas Navet, Bruno Gaujal

► **To cite this version:**

Nicolas Navet, Bruno Gaujal. Robustesse aux erreurs de transmission: configuration optimale d'un réseau TTP/C. Journée Qualité et Sûreté du Logiciel sur les systèmes embarqués, Pôle Intelligence Logicielle, LORIA, 2003, Nancy/France. <inria-00107716>

HAL Id: inria-00107716

<https://inria.hal.science/inria-00107716v1>

Submitted on 19 Oct 2006

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Robustesse aux erreurs de transmission : configuration optimale d'un réseau TTP/C

Nicolas NAVET - Bruno GAUJAL
projet TRIO

<http://www.loria.fr/~nnavet>

Certaines images de cet exposé proviennent de :

- [1] Cours de P. Koopman (<http://www.ece.cmu.edu/~ece540/lecture/>)
- [2] Slides TTPtech (<http://www.tttech.com/>)
- [3] Normes TTP v1.0
- [4] Simulation of a Time Triggered Protocol – D. Bradbury

TTP – Time Triggered Protocol

- Développé à la T.U. Vienne + TTTech
- 2 variantes : TTP/C et TTP/A
- Objectifs techniques:
 - Déterminisme
 - Tolérance aux fautes
 - Favoriser la « composabilité »
 - Support des changements de mode de marche

⇒ un bon candidat pour le X-By-Wire ..

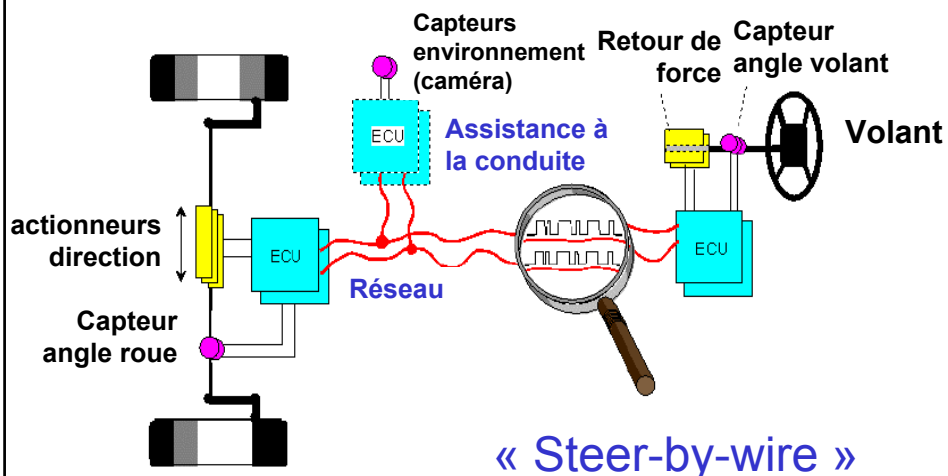
X-by-Wire

- Connexion mécanique remplacée par connexion digitale / informatique - utilisée en aéronautique depuis longtemps
- Pourquoi ?
 - Réduction encombrement - poids - vibration - maintenance
 - Assistance à la conduite - évitement des chocs
 - Moins de pollution (liquide de freins/transmission)
 - Ajout/remplacement d'équipements
 - ...

N. NAVET - QSL - 22/05/2003

3

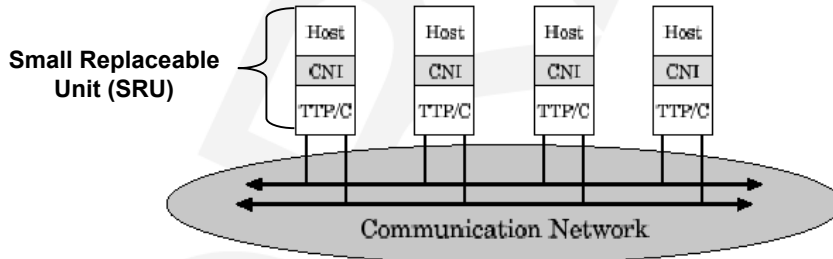
X-by-wire : un exemple



N. NAVET - QSL - 22/05/2003

4

Structure d'un réseau TTP



- Medium Access Control : **TDMA synchrone**
- **Support physique redondant**
- Débits: 500kbit/s, 1Mbit/s, 2Mbit/s, 5Mbit/s, 25Mbit/s
- Topologie: **bus** ou **étoile**

N. NAVET - QSL - 22/05/2003

5

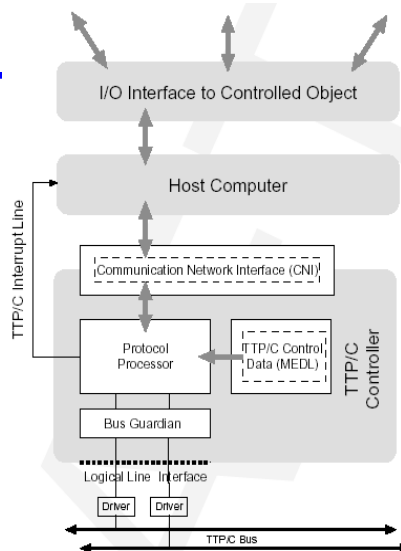
Un nœud TTP/C

Nœud ou SRU (Smallest Replaceable Unit) :

- Un micro-contrôleur
- Un contrôleur de communication TTP/C
- Une interface E/S

Contrôleur TTP/C:

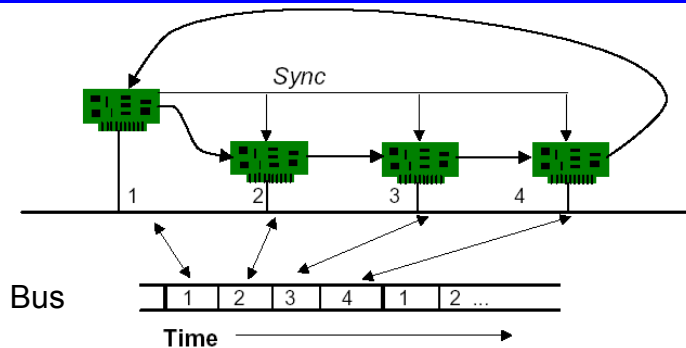
- Communication Network Interface
- Le « processeur du protocole »
- Message Descriptor List
- Le « gardien » du bus



N. NAVET - QSL - 22/05/2003

6

TDMA – Time Division Multiplexed Access (1/2)

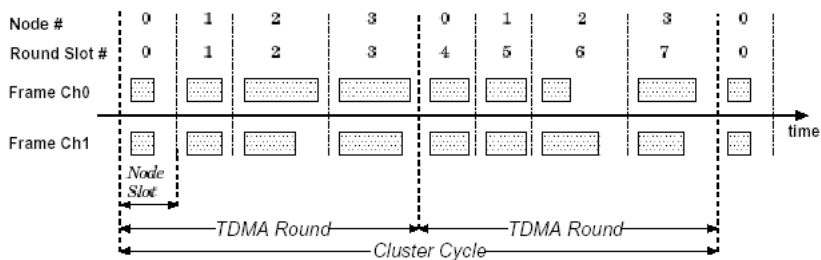


- Un **slot** est un intervalle de temps durant lequel une station émet un message
- Un **round TDMA** est une séquence de slots t.q. chaque station parle exactement 1 fois

N. NAVET - QSL - 22/05/2003

7

TDMA – Time division Multiplexed Access (2/2)



[Frame]

- Plusieurs rounds TDMA différents par les messages transmis peuvent être définis (**l'ordre de transmission et la taille des slots sont nécessairement identiques**)
- Un **cluster** est la suite de tous les rounds TDMA. Le cluster est exécuté en boucle.

N. NAVET - QSL - 22/05/2003

8

TTP/C: Implications du protocole MAC

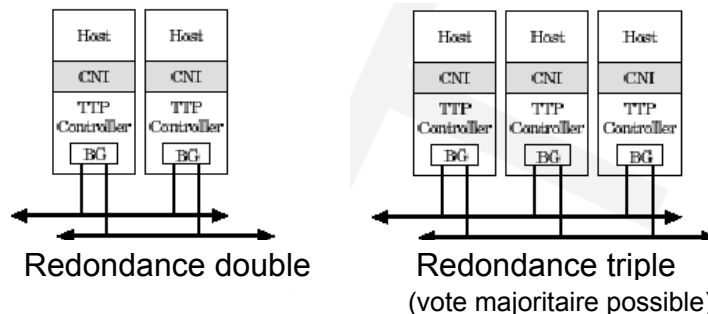
Temps de réponse borné et « heart-beat » mais:

- Perte de bande passante !
- Nécessité de micro-contrôleurs puissants
- Contrainte de temps maximum:
 - Si une station émet une seule donnée, le rafraîchissement ne peut être plus fréquent que le temps d'un round
 - Si une station émet plusieurs données, le rafraîchissement ne peut être plus fréquent que 2x le temps d'un round

Ex: contrainte de 5ms - réseau à 500kbit/s avec 200 bits par trames - au plus 12 trames (6 FTUs redondantes) ou 6 trames si la station émet 2 données.

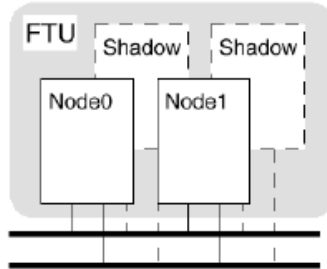
FTU: Unité tolérante aux fautes

- FTU (Fault Tolerant Unit) = ensemble de SRU's qui effectuent exactement les mêmes calculs



FTU: 2 types de redondance

- Node « fantôme » (shadow SRU) : émet dans les slots d'une station active lorsque celle-ci devient défaillante - ne possède pas de slots propres



- Node « réplique » : possède un slot propre

FTU: qu'en attendre ?

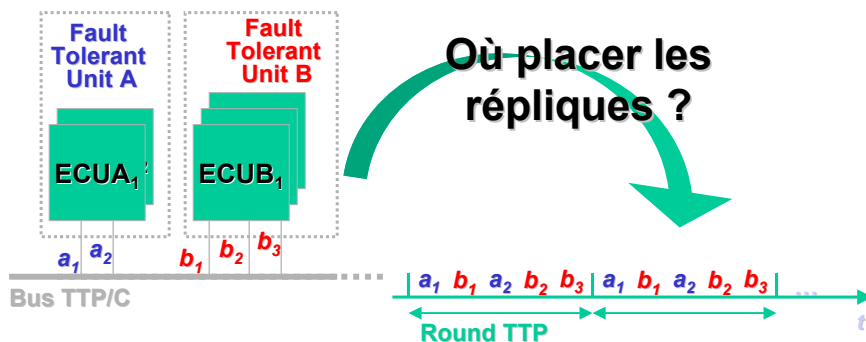
- Protection contre:
 - disparition d'une station (crash, déconnexion..)
 - des transmissions corrompues par des EMI
 - des erreurs de mesure (capteurs) ou de calcul
 - ...
- Sous l'hypothèse d'une défaillance unique (hypothèse de conception de TTP/C) :
 - une redondance double assure protection dans « le domaine temporel »
 - redondance triple assure en plus une protection dans « le domaine des valeurs »
- Problèmes: history-state

Station « Fail-silent »

- Une station est « fail-silent » si :
 1. elle émet au bon instant une donnée correcte ou
 2. elle n'émet rien
- Des stations « fail-silents » simplifient grandement la conception d'une application ..
- En pratique, il n'est pas toujours possible de garantir cette propriété

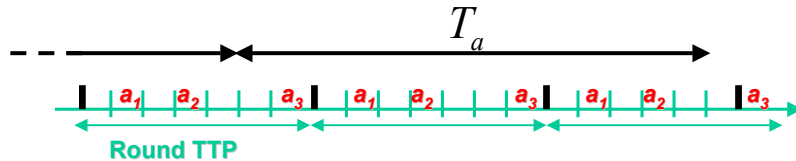
Objectif: rendre le système robuste aux perturbations

- En pratique, les erreurs de transmission sont souvent fortement corrélées



Modèle de l'application

- T_a : période de production de l'information sur chacune des stations de la FTU a



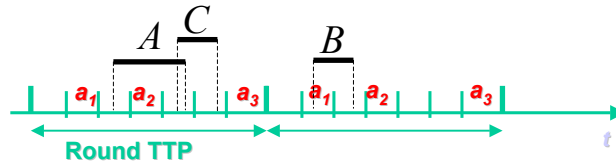
- Hypothèses:
 - pas de synchronisation entre émission (round) et production
 - période de production est multiple de la taille d'un round

Objectifs / fail-silence

- **Les stations sont fail-silents:** « minimiser P_{all} : la probabilité que toutes les trames d'une FTU soient corrompues pdt un cycle de production »
- **Les stations ne sont pas fail-silents:** « minimiser P_{one} : la probabilité que une trame de la FTU ou plus soit touchée par une perturbation»

Hypothèses sur le modèle d'erreurs

- Chaque bit transmis pendant la perturbation est corrompu avec une probabilité π
- Si une perturbation recouvre la totalité d'une trame alors corruption avec proba. 1
- Les instants de début des perturbations sont uniformément répartis dans le temps
- La distribution de la taille des rafales est arbitraire



Objectif 1 : Minimiser *Pone*

Majorisation - Schur-Convexit 

- Le vecteur $u = (u_1, \dots, u_n)$ **major**e $v = (v_1, \dots, v_n)$ si:

$$\sum_{i=1}^n u_i = \sum_{i=1}^n v_i \quad \text{et} \quad \sum_{i=1}^k u_{[i]} \leq \sum_{i=1}^k v_{[i]} \quad k \leq n$$

avec $(u_{[1]}, \dots, u_{[n]})$ permutation de u t.q. $u_{[i]} \leq \dots \leq u_{[n]}$

Exemple: $(1, 3, 5, 10) \succ (2, 4, 4, 9)$

- Une fonction $f : \mathfrak{R}^n \rightarrow \mathfrak{R}$ est

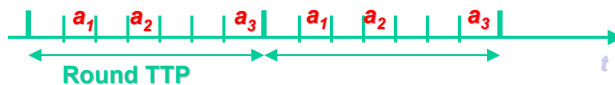
Schur-convexe si $u \succ v \rightarrow f(u) \geq f(v)$

Schur-concave si $u \succ v \rightarrow f(u) \leq f(v)$

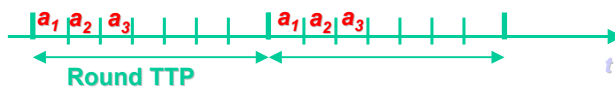
Minimiser P_{one}

- $I_i(x)$ est l'intervalle de temps entre la fin du r plica r_{i-1} et le d but de r_i sous l'allocation x
- $\mathbf{I}(x)$ est le vecteur des intervalles de temps (tri  par ordre croissant) pendant la dur e d'un round

Exemple: $\mathbf{I}(x) = (1, 1, 2)$



Exemple: $\mathbf{I}(x) = (0, 0, 4)$



Minimiser P_{one}

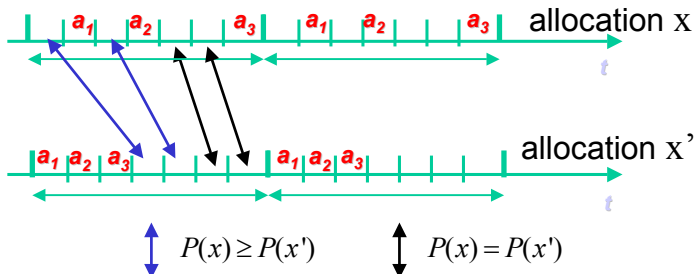
Théorème: la meilleure allocation vis-à-vis de P_{one} est de grouper les replicas (allocation g)

Arguments:

- P_{one} est shur concave: $\mathbf{I}(x') \succ \mathbf{I}(x) \rightarrow P_{one}(x') \leq P_{one}(x)$
- $\mathbf{I}(g)$ est maximum pour la majoration (toujours de la forme $(0, 0, S - k)$ avec k le nbre de réplicas de la FTU et S le le nbre de slots par round)

Minimiser P_{one}

- **Idee de la preuve:** plus une rafale d'erreurs commence loin d'un replica, moins elle a de chances de le corrompre. Les allocations « non-groupées » ont plus de zones proches des réplicas

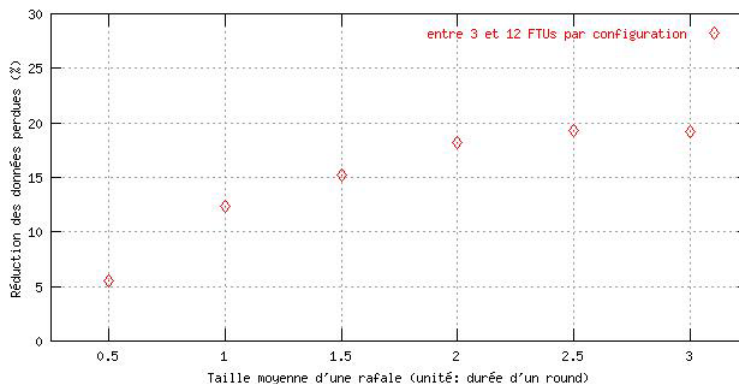


Minimiser P_{one}

- Validité du résultat :
 - π quelconque / distribution taille arbitraire
 - pour une période de production multiple de la taille d'un round
 - pour tout réseau TDMA
- Il est possible de minimiser simultanément P_{one} pour chacune des FTU's du système

Gain en robustesse : P_{one}

- Réduction du nombre de messages perdus par rapport à une allocation aléatoire:



- Gain moyen > 15%

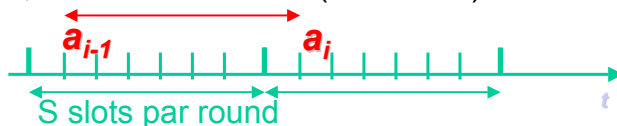
Objectif 2 : Minimiser P_{all}

2.1 Le cas TTP/C

2.2 Le cas général TDMA

TTP/C : la règle de la majorité

- **Cliques:** ensembles de stations ayant une vision \neq du système (ex: vision des stations qui fonctionnent correctement)
- **Principe:** pour éviter la formation de cliques, **déconnexion des stations « minoritaires »**
- **Mécanisme:** avant d'émettre, une station vérifie que dans le dernier round (S slots), le nbre de messages correctement émis est supérieur au nbre de messages incorrects, sinon déconnexion (« freeze »)

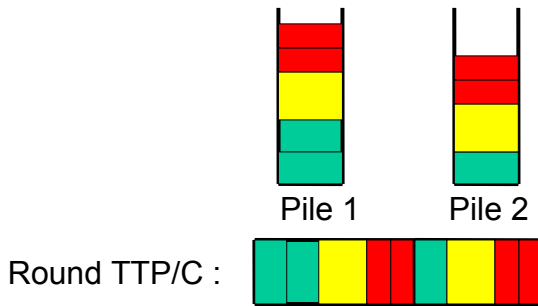


- En cas d'erreurs de transmission multiples: si une station « freeze » alors les stations s'arrêtent une à une ..

TTP/C : minimiser P_{all}

Algorithme: 1) pour chaque FTU i avec C_i slots mettre $\lceil C_i/2 \rceil$ slots dans la pile 1 et $\lfloor C_i/2 \rfloor$ dans la pile 2
2) concatener les deux piles

Ex: FTU A: 3 replicas – FTU B: 2 replicas – FTU C: 4 replicas



N. NAVET - QSL - 22/05/2003

27

TTP/C : minimiser P_{all}

Théorème: L'algorithme « des deux piles » est optimal sous TTP/C

Arguments:

Cas 1) une rafale par réplica : identique \square allocation

Cas 2) une rafale touche plusieurs réplicas avec une probabilité décroissante avec distance entre réplicas.

Une rafale de plus de $\lfloor S/2 \rfloor$ slots arrête le système or l'algo garantit un écart de $\lfloor S/2 \rfloor$ slots

Corollaire: Il est inutile d'avoir plus de 2 replicas par FTU si la probabilité d'avoir plus d'une rafale par round est suffisamment faible

N. NAVET - QSL - 22/05/2003

28

Objectif 2 : Minimiser $Pall$

2.1 Le cas TTP/C

2.2 Le cas général TDMA

Mots équilibrés

- Un mot « équilibré » (ou mot de Sturm) est une suite binaire $\{u_n\}_{n \in \mathbb{N}}$ t.q. :

$$\forall k, n, m \in \mathbb{N} \left| \sum_{i=n}^{n+k} u_i - \sum_{j=m}^{m+k} u_j \right| \leq 1$$

- Calcul des mots équilibrés à l'aide des suites crochets :

$$u_n = \left\lfloor n \frac{a}{b} \right\rfloor - \left\lfloor (n-1) \frac{a}{b} \right\rfloor$$

où a/b est la pente du mot (nbre 1/ nbre 0)

- Exemple: mot équilibré de pente $3/8$
(0, 0, 1, 0, 0, 1, 0, 1)

Fonction multimodulaire

- **Multimodularité [Hajek]** : équivalent de la convexité pour les fonctions $f : \mathbb{Z}^m \rightarrow \mathbb{R}$

Définition [Hajek85] : une fonction $f : \mathbb{Z}^m \rightarrow \mathbb{R}$ est multimodulaire si

$$f(x+v) + f(x+w) \geq f(x) + f(x+v+w)$$

$$x \in \mathbb{Z}^m \text{ et } v, w \in F \text{ (une base), } v \neq w$$

- **Exemple**: $x = (0, 1, 0, 1, 1, 0)$ est une **séquence de contrôle**, f une fonction de coût et v, w des opérations élémentaires comme le déplacement d'un client vers la gauche $v = (1, -1, 0, 0, 0, 0)$

Optimisation et fonction multimodulaire

- **Opérateur de décalage global à gauche de i positions**: $s_i(x)$
ex: $s_2((0, 1, 0, 1, 1, 0)) = (0, 1, 1, 0, 0, 1)$

Théorème [Altman, Gaujal, Hordijk 97]: Si f est multimodulaire alors $G(x) = 1/m \sum_{i=1}^m f(s_i(x))$ (version shift-invariante de f) est minimum si x est une séquence balancée.

Théorème : Si la taille des rafale est exponentiellement distribuée alors $Pall$ est multimodulaire. Or $Pall$ est égale à sa version shift invariante donc $Pall$ est minimale pour une séquence balancée.

Algorithme optimal : une seule FTU

- FTU avec C réplicas de taille h bits dans un round de taille totale R bits
 - Calcul de v_i mot balancé de densité $C/(R - C(h - 1))$
 - x est le round initialement vide
 - Si $v_i = 1$ alors $x := x + 1 \dots 1$ (h '1' concaténés)
 - Si $v_i = 0$ alors $x := x + 0$

Ex: FTU: 3 replicas de taille 3 sur un round de taille 14

$v_i = (0, 0, 1, 0, 0, 1, 0, 1)$ de densité $3/8$

$x = (0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1)$ (\neq mot balancé de densité $9/14$)



Algorithme optimal : plusieurs FTUs

- **Problème** : conflits entre les allocations

Ex: FTU A: 3 replicas – FTU B: 2 replicas – FTU C: 1 replica

$x_A = (0, 1, 0, 1, 0, 1)$ densité $3/6$

$x_B = (0, 0, 1, 0, 0, 1)$ densité $2/6$

$x_C = (0, 0, 0, 0, 0, 1)$ densité $1/6$

- Une allocation optimale est néanmoins possible si
 - le nbre de cardinalités des FTU est une puissance de 2
 - tous les réplicas ont la même taille
- **Remarque**: une séquence équilibrée est minimale pour la majoration, c'est donc la moins bonne solution pour *Pone* ! Les objectifs sont antagonistes...

Heuristique : plusieurs FTUs

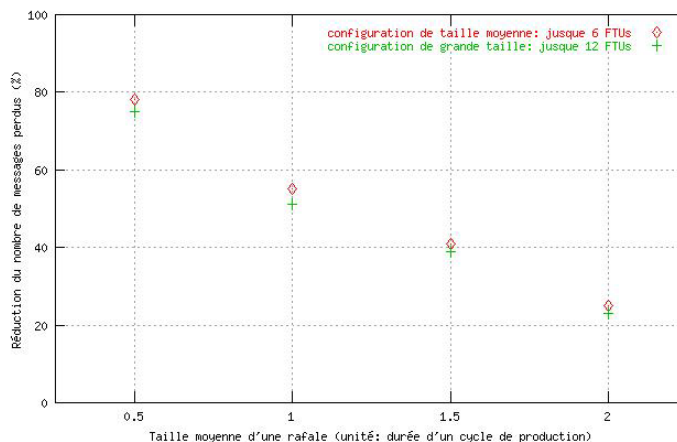
- La « densité » d'émission: quantité de bits d'une FTU A qui doit être émis par bit d'un round

$$d_A = C_A h_A / R$$

- A l'étape i, on décide l'émission d'une trame de la FTU pour laquelle le nombre de bits dus – nombre de bits déjà alloués est maximum

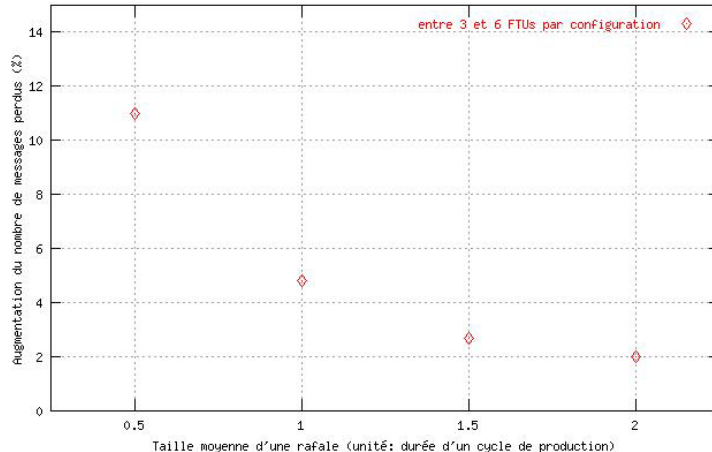
Pall : Heuristique vs aléatoire

- Réduction du nombre de messages perdus par rapport à une allocation aléatoire:



Pall : Heuristique vs optimal

- Augmentation du nombre de messages perdus avec l'heuristique par rapport à l'optimal:



N. NAVET - QSL - 22/05/2003

37

Conclusions

- Choix d'une allocation influe fortement sur la robustesse du système sur TDMA –TTP/C
- Allocations optimales ou proches :
 - Pour minimiser Pall, la probabilité que toutes les répliques soient corrompues
 - Pour minimiser Pone, la probabilité qu'une réplique ou plus soit corrompue

Perspectives :

- Configuration mixte fail-silent / non fail-silent (minimiser Pone et Pall pour des FTUs différentes)
- Etude du protocole Flexray

N. NAVET - QSL - 22/05/2003

38

Références

- B. Gaujal, N. Navet, *Optimal Replica Allocation for TTP/C based Systems*, à paraître dans IFAC FeT, Juillet 2003.
- B. Gaujal, N. Navet, *Maximizing the Robustness of TDMA Networks with applications to TTP/C*, INRIA RR-4614, 2002.

Convexité - Compléments

Inégalité de convexité :

$$f(\alpha x + (1 - \alpha)y) \leq \alpha f(x) + (1 - \alpha)f(y) \quad (1)$$

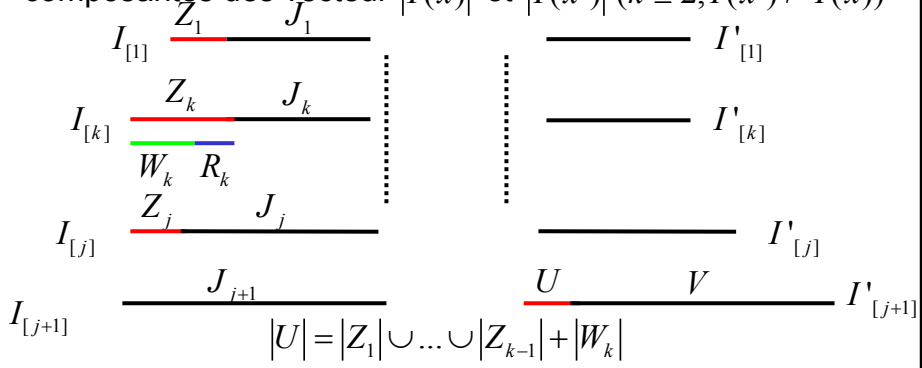
Fonctions convexes entières: satisfont (1) pour α, x et $\alpha x + (1 - \alpha)y$ dans Z^n

Problème: pas de garantie qu'un minimum local est un minimum global

➤ Une meilleure notion de convexité est la multimodularité [Hajek 85]

Schur-Concavité de P_{one}

- Preuve par couplage avec récurrence sur les composantes des vecteur $|I(x)|$ et $|I(x')|$ ($k \geq 2, I(x') \succ I(x)$)



$$P_x(U) \leq P_{x'}(Z_1 \cup \dots \cup Z_{k-1} \cup W_k) \text{ car } |V| \geq |J_i| \text{ pour } i \leq k$$

Fonction multimodulaire

- $x \in \mathbb{N}^m$ modélise une **séquence de contrôle**
exemple: $x = (0, 1, 0, 1, 1, 0)$
- $F \in \mathbb{Z}^m$ est la **base** : l'ensemble des opérations possibles
 - Ajout d'un client à l'instant m : $e_m = (0, 0, 0, 0, 0, 1)$
 - Retrait d'un client 1 : $-e_1 = (-1, 0, 0, 0, 0, 0)$
 - Décalage vers la gauche d'un client : $s_3 = (0, 1, -1, 0, 0, 0)$

Définition [Hajek85] : une fonction $f : \mathbb{Z}^m \rightarrow \mathbb{R}$ est multimodulaire si

$$f(x+v) + f(x+w) \geq f(x) + f(x+v+w)$$

$$x \in \mathbb{Z}^m \text{ et } v, w \in F, v \neq w$$