Optimal Replica Allocation for TTP/C Based Systems

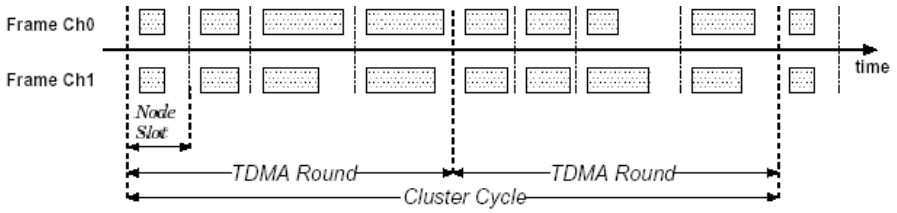
Bruno GAUJAL - Nicolas NAVET
LORIA Lab. (Nancy, France)
TRIO Team
http://www.loria.fr/~nnavet

TTP/C – Time Triggered Protocol

- Designed at T.U. Vienna + TTTech
- TTP/C main technical characteristics:
  - Determinism
  - Fault-Tolerance
  - Composability
  - Support of mode changes

⇨ A good candidate for X-By-Wire ..

TDMA – Time division Multiplexed Access



- Slot: time window given to a station for a transmission
- TDMA Round: sequence of slots s.t. each station transmits exactly once
- Cluster Cycle: sequence of the ≠ TDMA rounds

TTP/C: Implications of the MAC protocol

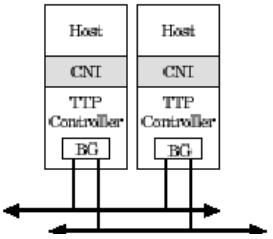
Bounded response times and « heartbeats » but:

- loss of Bandwidth
- need of powerful CPU's
- maximum timing contraint:
  - If a station sends a single information, the refresh cannot be more frequent than the length of a round
  - If a station sends several informations, the refresh cannot be more frequent than 2x the length of a round

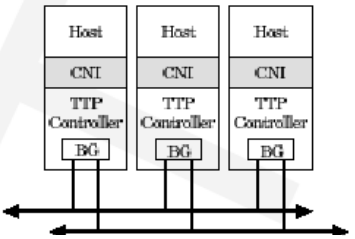
Ex: 5ms time constraint - 500kbit/s network with 200 bits per frames - at most 12 frames (6 FTUs of two nodes) or 6 frames if the station sends 2 distinct informations

FTU: Fault Tolerant Unit

- FTU = set of stations that act identically



FTU of cardinality 2



FTU of cardinality 3
(majority vote is possible)

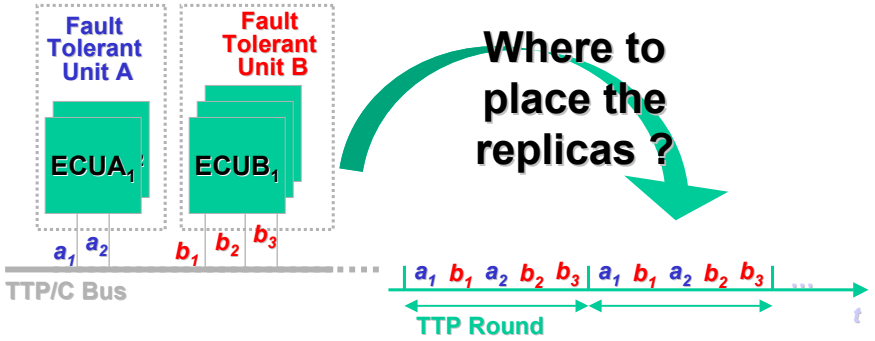
- Replica = a frame sent by a node of the FTU

FTU: which protection ?

- Protection against:
  - disappearance of a station (crash, disconnection..)
  - corrupted frames (EMI)
  - sensors or computation errors
  - …
- Under the assumption of a single failure (TTP/C fault-hypothesis) :
  - A dual redundancy ensures a protection in « the temporal domain »
  - A triple redundancy ensures in addition a protection in « the value domain »
- Problem: history-state

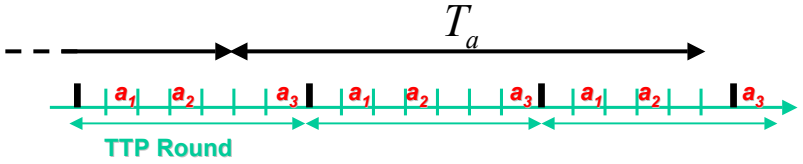
Goal of the study: maximize the robustness against transmission errors

- Transmission errors are usually highly correlated



Application model

- T_a: production cycle of the data sent by the stations of the FTU a



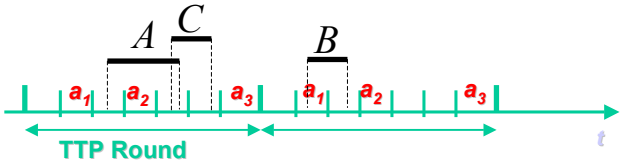
- Assumptions:
  - no synchronization between production and transmission (round)
  - production cycle is a multiple of the length of a round

Objective w.r.t. fail-silence

- A node is « fail-silent » if one can safely consume its data when the frame carrying the data is syntaxically correct
- Stations are fail-silent: « minimize P*all* : the probability that all frames of the FTU sent during a production cycle will be corrupted »
- Stations are not fail-silent: « minimize P*one* : the probability that at least one frame of the FTU will be corrupted»

Assumptions on the error model

- Each bit transmitted during an EMI will be corrupted with probability π
- If a perturbation overlaps a whole slot, the corresponding frame is corrupted with probability 1
- Starting times of the EMI bursts are independent and uniformly distributed over time
- The distribution of the size of the bursts is arbitrary



Objective 1 : Minimize P*one*

Majorization - Schur-Convexity

- vector $u = (u_1, ..., u_n)$ majorizes $v = (v_1, ..., v_n)$ if:

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

with $(u_{[i]}, ..., u_{[n]})$ permutation of u s.t. $u_{[i]} \leq ... \leq u_{[n]}$

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

- A fonction $f : \Re^n \rightarrow \Re$ is

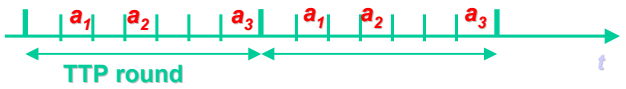
Schur-convex if $u \succ v \rightarrow f(u) \geq f(v)$

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

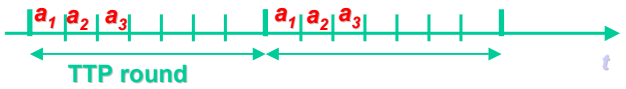
Minimize P*one*

- $I_i(x)$ is the interval between the end of replica r_{i-1} and the beginning of r_i under allocation x
- $\mathbf{I}(x)$ is the vector of the time intervals (in ascending order) during the length of a round

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



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



Minimize P*one*

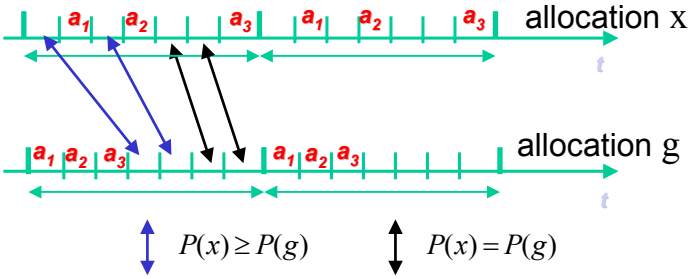
Theorem: the best allocation for P*one* is to group together all replicas (denoted allocation g)

Arguments:

- P*one* is shur-concave: $\mathbf{I}(x') \succ \mathbf{I}(x) \rightarrow P_{one}(x') \leq P_{one}(x)$
- $\mathbf{I}(g)$ is maximum for the majorization (equal to $(0,0,...,S-k)$ with k the number of replicas of the FTU and S the number of slots per round)

Minimize P*one*

- Idea of the proof (step 1): the farther the beginning of an error burst from a replica, the less likely the replica becomes corrupted. « Non-grouped » allocations have more areas close to replicas



Minimize P*one*

- Validity of the result :
  - Arbitrary π value and burst size distribution
  - Production period multiple of the round length
  - for all TDMA networks

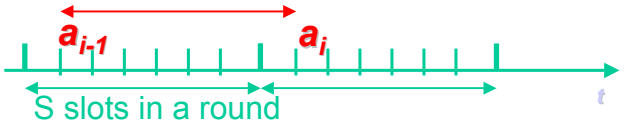
➢ Combined minimization of P*one* for all FTU's is possible

➢ Robustness improvement: against a random allocation, the number of lost data is reduced from 15 to 20% on average

Objective 2 : Minimize P*all*

TTP/C : the majority rule

- Cliques: sets of stations that disagree on the state of the network
- Principle: to avoid cliques, stations in the minority disconnect (« freeze »)
- Mechanism: before sending, a station checks that in the last round (S slots), the number of correct messages is greater than the number of incorrect messages, otherwise it disconnects



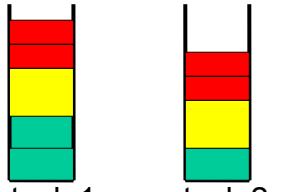
➢ If a station « freezes » due to transmission errors, the others follow one by one...

TTP/C : minimize P*all*

Algorithm: 1) for each FTU i with C_i slots, push $\lceil C_i/2 \rceil$ slots in the smallest stack and $\lfloor C_i/2 \rfloor$ in the largest stack

2) concatenate the two stacks

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



TTP/C round :

TTP/C : minimize P*all*

Theorem: the « 2-stacks » algorithm is optimal under TTP/C

Arguments:

Case 1) a perturbation for each replica : identical allocation

Case 2) a perturbation can corrupt several replicas with a probability decreasing in the distance between the replicas. A burst of more than $\lfloor S/2 \rfloor$ slots freezes the system, now the algorithm ensures a distance of $\lfloor S/2 \rfloor$ slots

Corollary: it is useless to have more than 2 replicas per FTU if the probability to have more than one perturbation in the same round is sufficiently low

Conclusion

- Choice of the locations of the slots have a strong influence on the robustness of the network
- Optimal Allocation on TTP/C for
  - the minimizing of P*all*, the probability that all replicas are corrupted
  - The minimizing of P*one*, the probability that at least one replica becomes corrupted
- Minimizing of P*one* for TDMA (in submission – available as research report)

Future work :

- Configurations made of fail-silent and non fail-silent nodes (minimizing P*one* and P*all* for different FTU's)
- Flexray protocol