MI11

Systèmes temps réel critique

Jérôme De Miras

Poste : 59 02
e-Mail : demiras@hds.utc.fr

Temps global

Temps et ordre

Notion de temps

- Permet de se référer à des événements passés ou à des événements qui pourraient se produire dans le futur
- Base pour la construction d'une partie des unités de la physique
- En physique Newtonienne, variable indépendante qui conduit l'évolution des variables d'état

Temps réel et ordre

- Dans un système TR toutes les actions sont réparties dans le temps
- Pour assurer un comportement cohérent, il est essentiel que chaque nœud partage le même ordre des événements
- Cet ordre est si possible l'ordre temporel ; une base de temps peut aider à satisfaire ce besoin

Ordre temporel

- Le continuum du temps peut se représenter par une ligne orientée :
  ensemble infini **{T}** d'instants
  i. **{T}** est ordonné :
     soit **p** = **q**
     soit **p** < **q**,
     soit **p** > **q**
  ii. {T} est dense : entre **p** et **q** on peut placer **r** si p≠q
- Une section de la ligne est une durée
- Un événement n'a pas de durée
- Les instants sont totalement ordonnés, pas les événements (simultanéité)

Ordre causal

- La dépendance causale des événements est importante
- Permet de retrouver l'événement primaire qui précède une succession d'autres (alarmes)
  - ⇒ Utile pour identifier une cause de faute
- L'ordre temporel est nécessaire mais pas suffisant à l'ordre causal
- Si l'ordre ne peut être que partiel, on peut essayer d'exclure les événements arrivés trop tard pour être l'événement premier

Ordre de livraison

- Existe si le système de communication garantie que tous les calculateurs hôte auront accès à une séquence d'événements de la même manière
- Ne correspond pas forcément à l'ordre temporel ou causal

Horloges

- Horloges physiques :
  - Un appareil muni d'un compteur et d'un oscillateur (ticks)
  - La durée entre deux ticks est la granularité de l'horloge (discrétisation du temps)
- Horloge de référence :
  - Observateur possédant une horloge unique Z servant à dater les événements
  - On suppose que f^z est suffisamment grande pour que sa granularité soit sans influence sur son utilisation

    $Z(e)$: date absolue de e

    n^k : granularité de l'horloge k en microticks de Z

Dérive d'horloges

- La dérive se mesure par rapport à Z entre 2 microticks

$$drift_i^k = \frac{Z\left(microtick_{i+1}^k\right) - Z\left(microtick_i^k\right)}{n^k}$$

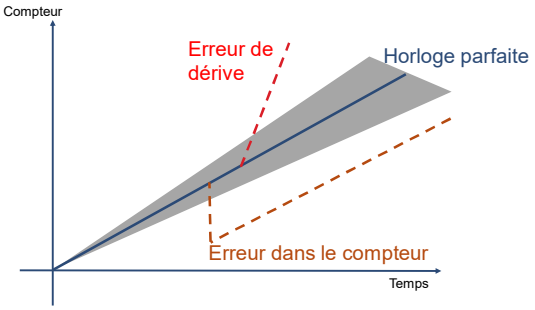
  - Très proche de 1

- Taux de dérive

$$\rho_i^k = \left| drift_i^k - 1 \right|$$

  - Ce taux n'est jamais nulle ; une horloge réelle non synchronisée finit toujours par dériver

Modes de défauts d'horloges



Précision d'horloges

- Offset entre deux horloges de même granulosité

$$offset_i^{j,k} = \left| Z\left(microtick_i^j\right) - Z\left(microtick_i^k\right) \right|$$

- Précision de n horloges $\{1,2,3, \ldots,n\}$

$$\Pi_i = \max_{\forall i \le j,k \le n} \left\{ offset_i^{j,k} \right\}$$

  - Π est la précision de l'ensemble sur un intervalle d'intérêt

$$\Pi = \max\left(\Pi_i\right)$$

  - Dérive entre les horloges : nécessité de resynchroniser le groupe en interne

Fidélité d'horloges

- Offset et précision pris entre une horloge k et Z
- Pour garder une horloge dans un intervalle borné par rapport à Z, on doit procéder à une synchronisation externe
- Ensemble d'horloges synchronisé avec Z avec une fidélité A
  ⇒synchronisation interne avec une précision $2A$
  - L'inverse est faux

Temps standard

- Temps Atomique International (IAT)
  - 1 second = 9 192 631 770 périodes de radiation d'une transition sur un atome de césium 133
- Temps Universel Coordonné (UTC)
  - Dérivé de l'observation astronomique entre la terre et le soleil
  - Introduit en 1972 à la place du GMT
  - La seconde correspond au TAI et on ajoute une seconde de temps en temps

Mesure du temps

Problème

- Si dans un système on pouvait mesurer la date d'un événement par rapport à Z, tout serait facile
- L'ordre temporel pourrait être donné quelque soit la variation des délais de communication
- Réalité : n nœuds ⇒ n horloges

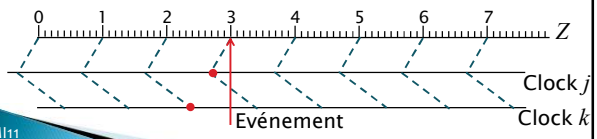
⇒Notion de temps global moins forte que la référence universelle

Temps global

- Soient n nœuds, n horloges c^k (g^k), synchronisées en interne avec une précision Π

$$Z\left(microtick_i^j\right) - Z\left(microtick_i^k\right) < \Pi$$

- Sur chaque horloge on choisit un sous-ensemble de microticks (tous les p microticks) pour former les ticks t_i d'un temps global



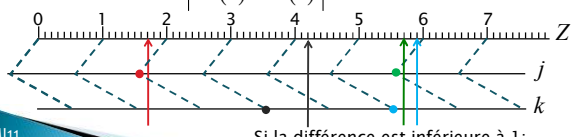
Temps global : condition d'existence

- Le temps global est raisonnable si toutes les réalisations locales satisfont

$g < \Pi$ $\quad$ g : granulosité

- Assure que la que la borne de l'erreur de synchronisation est inférieure à 1 micro-granule

$$\left| t^j(e) - t^k(e) \right| \leq 1$$



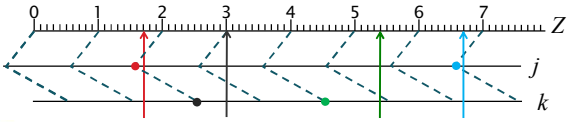
Si la différence est inférieure à 1: pas de reconstruction de l'ordre

Mesure d'un intervalle

- Un intervalle est un segment de temps dont la durée vraie est

$$d_{obs} - 2g < d_{vraie} < d_{obs} + 2g$$

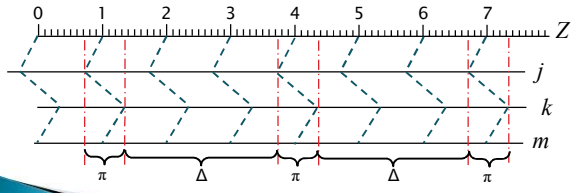
  - 2 est par définition du temps global la valeur max d'erreur



Précédence Π/Δ

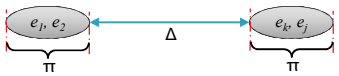
- Un ensemble d'événement est Π/Δ précédent si pour tout couple e_i, e_j avec $\pi << \Delta$

$$\left(\left|Z(e_i) - Z(e_j)\right| \le \pi\right) \vee \left(\left|Z(e_i) - Z(e_j)\right| > \Delta\right)$$



Précédence Π/Δ

- Regroupe les événements sous forme de « boule »



Event set	L'intervalle observé est sup ou égal	Ordre temporel possible
0/1 g préc	$\lvert t^j(e_1) - t^k(e_2)\rvert \ge 0$	Non
0/2 g préc	$\lvert t^j(e_1) - t^k(e_2)\rvert \ge 1$	Non
0/3 g préc	$\lvert t^j(e_1) - t^k(e_2)\rvert \ge 2$	Oui
0/4 g préc	$\lvert t^j(e_1) - t^k(e_2)\rvert \ge 3$	Oui

2 événements vus par 2 nœuds

Limite dans la mesure du temps

- Dans un système distribué avec un temps global raisonnable (granularité g)
  - 1 événement observé, 2 nœuds : la date peut différer de 1
  - Un intervalle observé est tel que

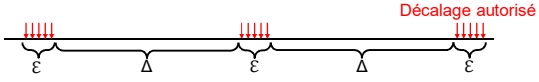
$$d_{obs} - 2g < d_{vraie} < d_{obs} + 2g$$

  - L'ordre de deux événements peut être retrouvé si les dates diffèrent d'au moins 2
  - L'ordre temporel d'un ensemble 0/3g peut toujours être retrouvé

Temps dense
Temps clairsemé

Temps dense ou clairsemé

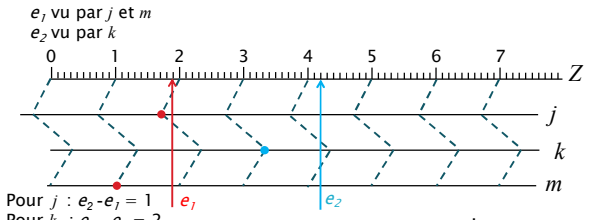
- Soit un ensemble d'événements **{E}**
  - Si ces événements peuvent se produire à n'importe quel instant de la ligne de temps, la base de temps est dense
  - Si l'arrivée des événements est restreint à des intervalles séparés par des silences, la base de temps est ε/Δ clairsemée



- On ne peut restreindre l'occurrence d'un événement que s'il est dans la sphère de contrôle du calculateur qui veut la restreindre

Base de temps dense

- Si deux événements sont écartés de moins de 3g, il n'est pas toujours possible de les ordonner si l'acquisition est répartie sur plusieurs nœuds

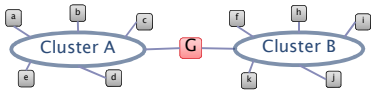


j ne peut pas ordonner
m peut ordonner
⇒ vue inconsistante

Protocole d'entente

- Les nœuds doivent exécuter un ***protocole d'entente*** pour arriver à une vue consistante (pas forcément l'ordre temporel)
  - Echange d'information entre nœuds pour comparer leur différents points de vue sur l'état du monde
  - Algorithme déterministe exécuté sur chaque nœud
  - ⇒ Cher en communication et puissance de calcul

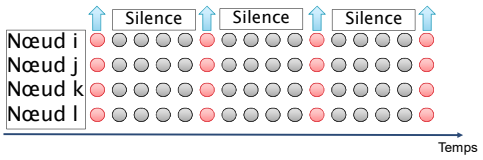
Base de temps clairsemée



Pas de base de temps commune

- Si deux événements de A sont générés par j et k dans un même intervalle de temps inférieur à π alors B ne pourra jamais établir d'ordre
- Un 1g/3g événement précédent n'est pas suffisant
  - 2 événements peuvent être vus séparé de 2 par B s'il sont :
    - dans le même « tick boule »
    - dans 2« ticks boule » différents
  - ⇒Indécidable donc utiliser un 1g/4g pour établir l'ordre en B

Base de temps clairsemée : construction



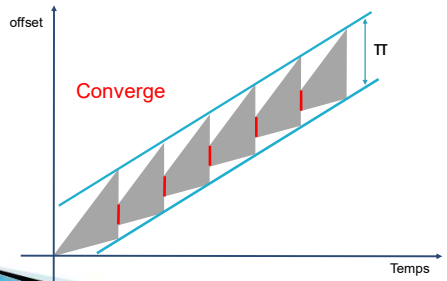
- Au interface avec le matériel, les événement sont dans un temps dense
  ⇒protocole d'entente nécessaire sur les interfaces d'instrumentation

Synchronisation d'horloges

Interne
Externe

Synchronisation interne

- Garder toutes les horloges dans une précision π
- Opération tolérante au faute



Synchronisation interne : condition

- Resynchronisation périodique sur chaque nœud
- Intervalle de resynchronisation : R_{int}
  - Φ : offset de temps juste après la synchro
  - Γ : offset de dérive, divergence maximum entre 2 horloges

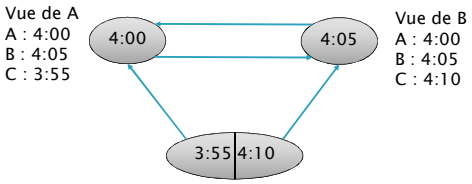
$$\Gamma = 2\,\rho\,R_{\text{int}}$$

  - Condition de synchronisation

$$\Phi + \Gamma \leq \Pi$$

Erreur byzantine

- Peut se produire lors des échanges de données



C : horloge malicieuse

Erreur byzantine : résolution

- 2 possibilités de résolution :
  - Algorithmes de consistance itératifs
    - Introduction d'échange supplémentaire d'information
  - Algorithme fonctionnant avec l'information inconsistante
    - Fault tolerance average algorithme
    - Il faut que

$$N \geq (3k+1)$$

avec k le nombre d'horloges byzantines
N le nombre total d'horloges

Synchronisation par un maitre central

- Un maitre envoie périodiquement sa valeur d'horloge
- Les nœuds regarde la différence avec la leur
  - Correction avec prise en compte du temps de transport)
  - La précision dépend de la gigue sur le temps de transport

$$\Pi = \varepsilon + \Gamma$$

- Tolérance aux fautes :
  multiplication des masters

Algorithmes de synchronisation distribués

- Echange de donnée compteur de temps de chaque nœud
- Exécution d'une fonction de convergence
- Si le résultat dépasse la précision, désactivation du nœud
- Mise à jour du compteur local de temps

ASD : lecture des temps

- Le temps minimum d'envoi peut être compensé
- Problème : la gigue qui dépend du lieu de traitement de l'information
  - Niveau application : 500 µs à 5 ms
  - Dans le noyau de l'OS : 10 µs à 100 µs
  - Dans le contrôleur de comm : moins de 10 µs
- Précision atteignable

$$\Pi = \varepsilon\left(1 - \frac{1}{N}\right)$$

N : nombre de nœuds
ε : gigue
$\rho = 0$ (drift rate)

ASD : fonction de convergence

- Fault tolerance Average Algorithm
  - Fonctionne en 1 passe
  - N nœuds, k byzantines au maximum
- Calcul des différences entre c^k et les autres
- Trie et élimination des k plus basses et hautes
- Moyenne des N-$2k$ restantes

ASD : précision du FTA

- Erreur max dans la moyenne pour une byzantine

$$E_{byz} = \Pi/(N-2k)$$

- Pire cas pour k byzantines

$$E_{byz} = k\,\Pi/(N-2k)$$

- Précision atteignable (avec gigue)

$$\Pi(N,k,\varepsilon,\Gamma) = (\varepsilon+\Gamma)\frac{N-2k}{N-3k} = (\varepsilon+\Gamma)\,\mu(N,k)$$

μ : terme d'erreur byzantine

	Nombre de nœuds							
Fautes	4	5	6	7	10	15	20	30
1	2	1.5	1.33	1.25	1.14	1.08	1.06	1.03
2				3	1.5	1.22	1.14	1.08
3					4	1.5	1.27	1.22

ASD : étape de correction

- Soit par modification directe de la valeur d'horloge
  - Problème : provoque des sauts temporel
- Soit en appliquant une correction de taux de variation de l'horloge

Synchronisation externe

- Un serveur extérieur impose sa vision du temps
- Les nœuds peuvent en tenir compte ou pas (trop grande différence par rapport à leur point de vue)