Résumé étendu en français

Chapitre 1 : Introduction

Cette thèse s'intéresse à la dimension temporelle de la qualité de service dans des réseaux industriels temps-réel critiques (centrales nucléaires, avionique, etc.). Plus précisément, l'environnement considéré est un réseau Ethernet commuté devant satisfaire un ensemble de propriétés, notamment la suivante : « En fonctionnement normal, le temps de réponse de bout-en-bout d'un paquet quelconque ne doit pas dépasser l'échéance du flux ». Ce réseau est composé d'une centaine de commutateurs identiques connectés en ligne (voir Fig. 1.1).

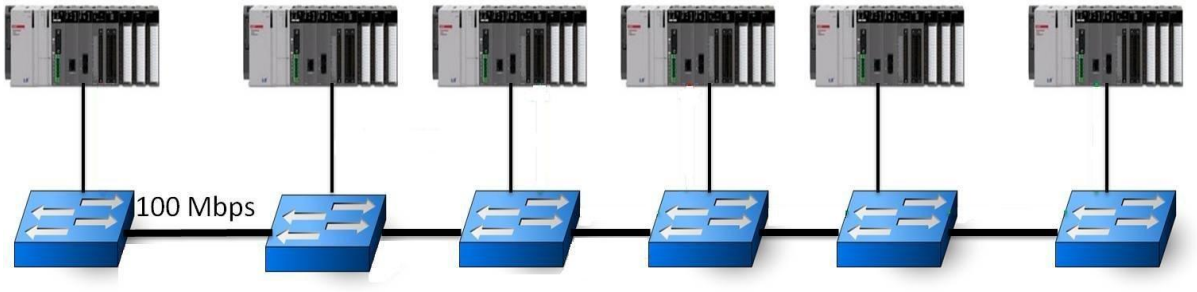

Figure 1: Topologie du réseau étudié

Chaque commutateur est relié à un nœud unique qui peut être soit un capteur soit un actionneur. Les nœuds sont connectés par des liens full-duplex et les commutateurs comprennent huit ports de type « store & forward ».

Comme illustré dans la figure. 1.2, à chaque port de sortie est dédiée une fille d'attente de taille 1 Mo. La politique d'ordonnancement utilisée est First In First Out (FIFO). Par conséquent, les paquets sont servis en fonction de leur instant d'arrivée. Chaque commutateur maintient à jour une table dite « forwarding table ». Il associe à chaque adresse MAC le port sur lequel le paquet doit être envoyé pour atteindre sa destination. En outre, le délai de commutation incluant la consultation de la table et l'envoi du paquet dans la file d'attente en sortie est considéré constant et égal à 3µs.

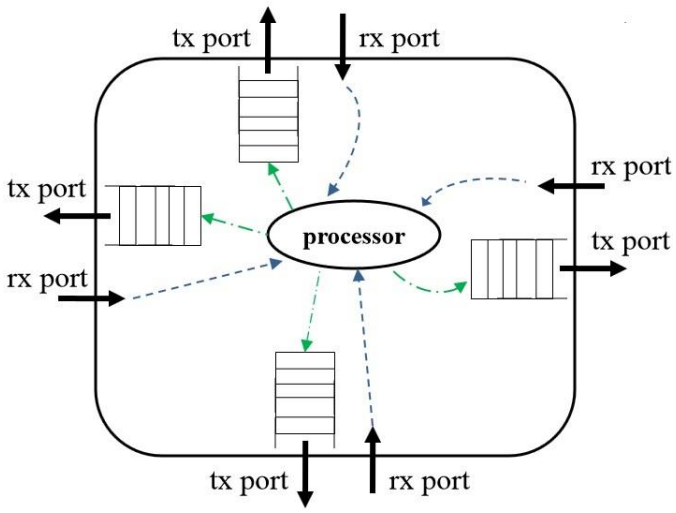

Figure 2: Structure interne des commutateurs

L'objectif de cette thèse est d'établir des bornes déterministes, mathématiquement calculables, sur les délais de bout-en-bout des paquets transitant dans un réseau Ethernet commuté de configuration donnée. Parmi les principales techniques proposées dans la littérature, nous nous sommes intéressés à celle appelée "approche par trajectoire", ou TA (Trajectory Approach). Ce choix s'explique par différentes raisons explicitées dans le chapitre 2.

Cependant, l'approche par trajectoire souffre du même problème de passage à l'échelle que les autres techniques existantes. Cette complexité est due au caractère itératif et récursif de la formule permettant d'établir les bornes sur les délais de bout-en-bout des différents flux transitant dans le réseau. Ce problème est étudié et illustré dans le chapitre 3.

Pour permettre le dimensionnement ou la certification de grands réseaux industriels comptant plus d'une centaine de nœuds et des milliers, voire des dizaines de milliers de flux, il est donc nécessaire d'éliminer cette complexité afin de déterminer, dans un temps raisonnable, des bornes sur les temps de réponse pire cas de l'ensemble des flux du réseau considéré. L'approche proposée, intitulée STA (Scalable Trajectory Approach), se concentre sur l'effet de sérialisation, les gigues de certains flux et les instants à tester. Cette solution est décrite en détail dans le chapitre 4 et les performances de notre proposition sont présentées. Nous montrons notamment que STA permet le passage à l'échelle pour la détermination de bornes déterministes dans de grands réseaux temps-réel critiques, sans perte significative de précision.

Chapitre 2 : Garanties temporelles

La technologie Ethernet est largement utilisée dans le secteur industriel. Depuis quelques années, elle est également utilisée dans les domaines temps-réel critiques tels qu'à bord des avions, dans les centrales nucléaires, etc. Cependant, le problème majeur lors de l'utilisation de cette technologie dans les applications temps-réel distribuées est sa propriété stochastique qui est généré par le mécanisme de gestion de collision. Pour se débarrasser de ce problème, les infrastructures basées sur les ponts ont été simplement remplacés par des commutateurs Ethernet fonctionnant en Full Duplex. En fait, l'Ethernet commuté crée des connexions point-à-point entre les entités communicantes, éliminant ainsi tout type de collisions. Ainsi, l'utilisation de l'Ethernet commuté a permis de surmonter le problème résultant du partage du medium entre les différentes entités. Néanmoins, un autre problème survient : puisque les paquets sont désormais en concurrence sur les ports de sortie des commutateurs, ces derniers doivent être bien dimensionnés pour éviter tout débordement possible.

Par définition, dans les systèmes temps-réel critiques, tout comportement défectueux peut avoir des conséquences désastreuses (danger de mort, …). Ainsi, la vérification et la validation d'un tel système sont indispensables avant son déploiement. En fait, les autorités de sûreté demandent notamment d'assurer des garanties déterministes. En d'autres termes, le temps de réponse pire cas d'un paquet doit être inférieur à l'échéance du flux auquel il appartient. Par conséquent, il est nécessaire de prouver que le temps de réponse de bout-en-bout de chaque flux est borné. Ce sujet a été largement abordé ces dernières années et plusieurs approches ont été développées.

Ce chapitre présente brièvement les méthodes présentes dans la littérature répondant à cette problématique. La simulation ou les tests, la méthode de vérification du modèle (*Model Checking*, ou MC) et le calcul du réseau (*Network Calculus*, ou NC) ont été utilisés pour estimer le temps de réponse de bout-en-bout. Plus récemment, une autre méthode appelée l'approche par trajectoire (*Trajectory Approach*, ou TA) traite la même problématique.

SI l'analyse du réseau en utilisant la simulation et/ou les tests n'est pas exhaustive, le scénario pire cas, parfois rare, peut ne pas être considéré, conduisant à une sous-estimation de la borne (intolérable dans le contexte de réseaux temps-réel critiques). Si l'analyse prend en compte tous les scénarios possibles, le temps nécessaire pour les tester tous peut s'avérer irraisonnable, ce délai pouvant aller jusqu'à plusieurs années. Pour toutes ces raisons, les approches fondées sur la simulation ne parviennent pas à répondre à nos exigences.

La deuxième approche utilisée est le Model Checking. Cette méthode, présentée par Alur et Dill, est une approche formelle se basant sur les automates temporisés. Une fois le système modélisé et la propriété formulée, le MC vérifie d'une manière exhaustive si la propriété

étudiée est satisfaite dans chaque état du modèle du système. Si une erreur se produit, l'approche génère le scénario exact qui l'a causée, fournissant ainsi une preuve que le système est défectueux et doit être révisé. Le MC permet d'obtenir le scénario pire cas et le temps de réponse pire cas exact. Néanmoins, cette approche ne permet d'obtenir des résultats que sur des configurations réseaux dont la taille est limitée, en raison du problème d'explosion combinatoire.

La troisième approche est le calcul réseau. Celle-ci est la plus utilisée. La certification de l'avion A380, par exemple, s'est appuyée sur une approche fondée sur NC. Dans le cas général, cette approche donne des bornes supérieures déterministes sur le délai (ou temps de réponse) et la gigue d'un flux transmis sur un réseau. Cette théorie se base sur l'algèbre (min,+). Un flux est représenté par une fonction *R*, telle que *R*(*t*) est le nombre de bits émis par le flux à l'instant *t*. La définition des courbes d'arrivée et de service peuvent cependant être difficile à établir ou conduire à des bornes particulièrement pessimistes.

La méthode par trajectoire offre également des bornes déterministes, mathématiquement calculables, sur les temps de réponse de flux sporadiques coexistant dans un réseau. Elle s'applique dans le cadre d'un fonctionnement sans collision, ni perte de paquets. Elle a été développée pour des ordonnancements non-préemptifs et offre des résultats pour des algorithmes à base de priorités fixes (FP) et/ou dynamiques (DP). Pour les algorithmes FP, les paquets appartenant au même flux ont tous le même niveau de priorité, tandis que pour les algorithmes DP, la priorité des paquets dépend de leurs instants d'activation. L'approche a été notamment formalisée pour la politique d'ordonnancement FIFO (First In First Out).

Plus précisément, chaque flux τ_i est défini par une durée minimum d'inter-arrivée T_i, une gigue d'activation J_i, une échéance sur le temps de réponse de bout-en-bout D_i et une durée d'exécution C_i^h sur chaque nœud *h*. L'ensemble des nœuds sur lequel τ_i a été traité forme sa trajectoire et est noté $\mathcal{P}_i$. Le délai de commutation dans les commutateurs est compris entre L_{min} et L_{max}.

Le temps de réponse de bout-en-bout d'un paquet est la somme des délais de commutation sur les commutateurs (au plus L_{max} par commutateur) et des durées passées dans chacun des nœuds visités (voir Fig. 3), fonction des temps d'attente dans les files.

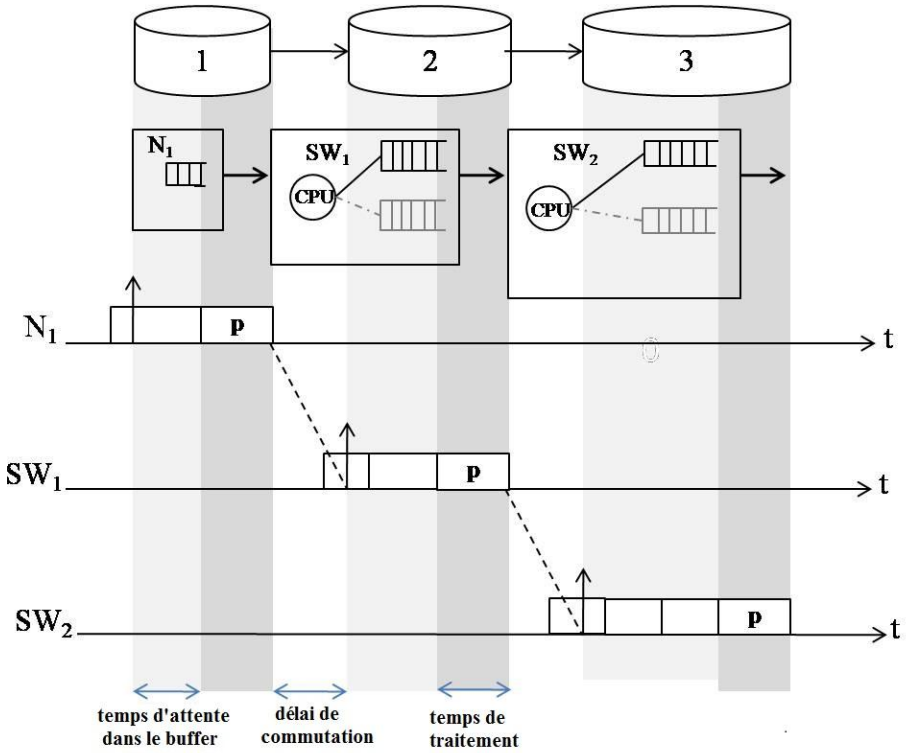

Figure 3 : Décomposition du délai de bout en bout d'un paquet *p*

L'approche par trajectoire est basée sur l'analyse du scénario pire cas expérimenté par un paquet p du flux τ_i tout au long de sa trajectoire $\mathcal{P}_i$. Sur l'ensemble de ces nœuds, en partant de la destination et en remontant à la source du flux étudié, l'approche détermine les paquets affectant l'exécution de *p*. La somme des temps de traitement des paquets identifiés et des délais de commutation permet de déduire une borne supérieure sur le temps de réponse de bout en bout.

Certaines études se sont intéressées à la précision des approches NC et TA sur des configurations données. Il a été montré que TA offrait de meilleurs résultats en termes de précision. La figure 4 schématise les bornes obtenues par les différentes méthodes.

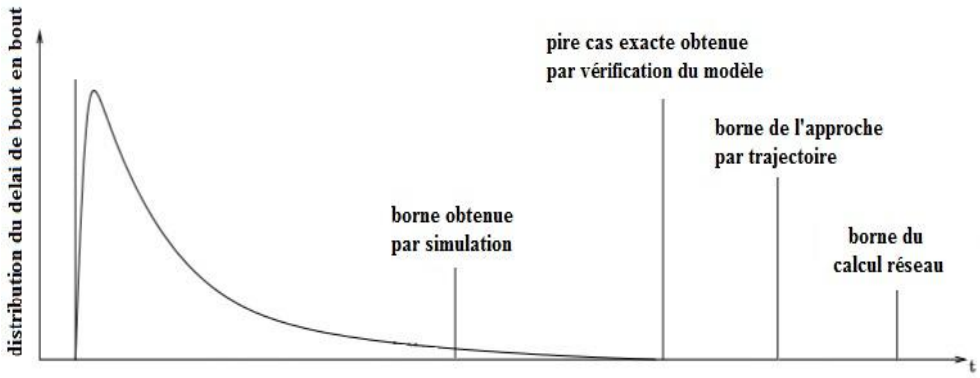

Figure 4 : Bornes sur le temps de réponse (ou délai) de bout en bout

Chapitre 3 : Limitations de TA en FIFO

Ce chapitre s'intéresse plus en détail à l'application de l'approche par trajectoire avec la politique d'ordonnancement FIFO dans un réseau Ethernet commuté en ligne.

Tout d'abord, l'expression permettant de calculer une borne supérieure telle que présentée par l'approche par trajectoire est introduite. Puis, sur un exemple simple, nous illustrons comment l'approche procède pour calculer les bornes. Nous présentons ensuite les différents problèmes rencontrés lors de l'application de cette méthode sur de grandes configurations industrielles. Finalement, pour des raisons de simplicité et sans perte de généralité, nous illustrons ces limitations sur de petites configurations.

Lors de l'application de l'approche par trajectoire sur des réseaux de grande taille, nous avons étudié deux aspects principaux : la précision de la borne supérieure du temps de réponse de bout-en-bout et passage à l'échelle. En effet, la notion de précision est particulièrement importante puisque les flux échangés doivent respecter leurs échéances. Or l'obtention de bornes trop pessimistes ne permettrait pas de conclure sur la faisabilité du système si ces bornes venaient à dépasser ces échéances. Cela conduirait alors à un surdimensionnement du réseau, impliquant des coûts naturellement plus élevés. Quant au passage à l'échelle, il est tout aussi important de pouvoir l'assurer pour valider des réseaux de grande taille en un temps acceptable.

De notre analyse, le pessimisme de l'approche par trajectoire est due à :

- Une surestimation des paquets de jonction [ARTICLE SARA]
- Une surestimation du nombre de paquet retardant l'exécution du flux étudié. Cette surestimation est due à deux effets : la sérialisation des flux [BAUER] et à la présence des flux quittant la trajectoire [SARA]. L'approche par trajectoire avait déjà été améliorée ces dernières années afin de prendre en compte les effets de la sérialisation. Cette solution est notée par la suite *Enhanced Trajectory Approach* (ETA).

Tout d'abord, nous avons comparé le temps de calcul total mis par ETA et TA pour une petite configuration formée de 10 commutateurs. Le temps de traitement des flux est égal à $C = 26\mu s$ et la période à $T = 100ms$. Le délai de commutation est de $3\mu s$. En augmentant le nombre de flux, nous déduisons que le temps de calcul mis par ETA augmente de manière exponentielle par rapport à TA (voir figure 5).

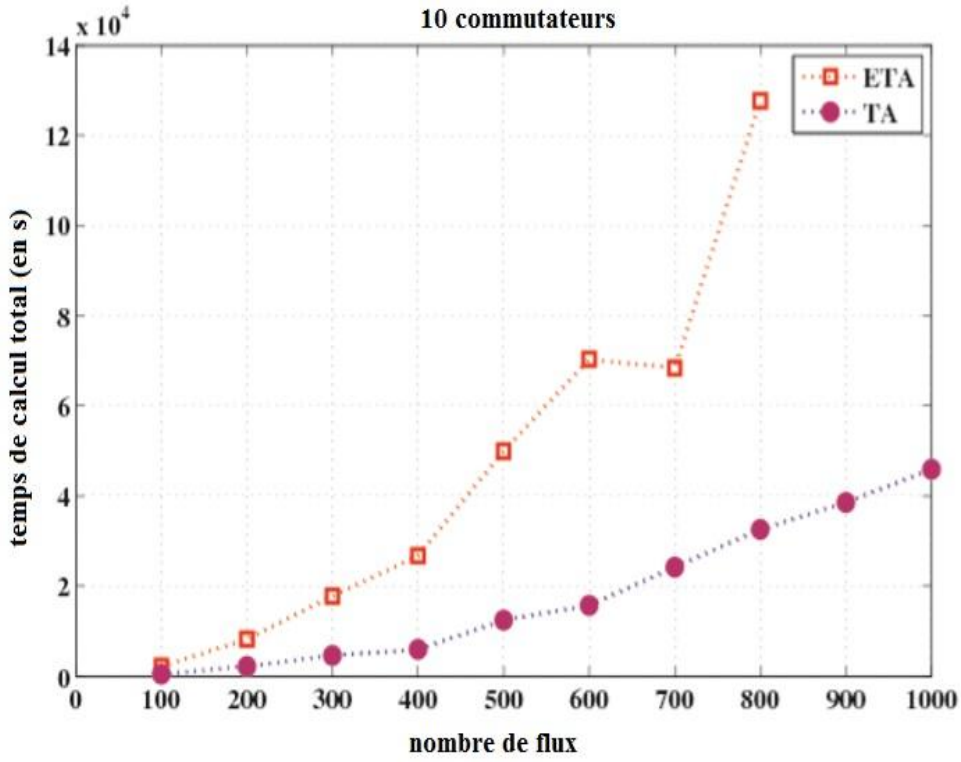

Figure 5: Temps de calcul en fonction du nombre de flux transmis

Ensuite, nous avons appliqué TA sur une configuration industrielle de grande taille (i.e. composée de 100 commutateurs). Nous désirons l'évolution du temps de calcul moyen en fonction du nombre de commutateurs et de flux. Nous considérons que les flux ont le même temps de traitement et la même période. Les valeurs de ces deux paramètres sont $C = 1\mu s$ et $T = 1000\mu s$ Pour un nombre de flux et de commutateurs fixes, nous générons 50 configurations avec les sources et les destinations choisies aléatoirement. Les résultats illustrés par la figure 6 montrent que les temps de calcul des flux augmentent aussi exponentiellement en fonction du nombre de flux et du nombre de commutateurs.

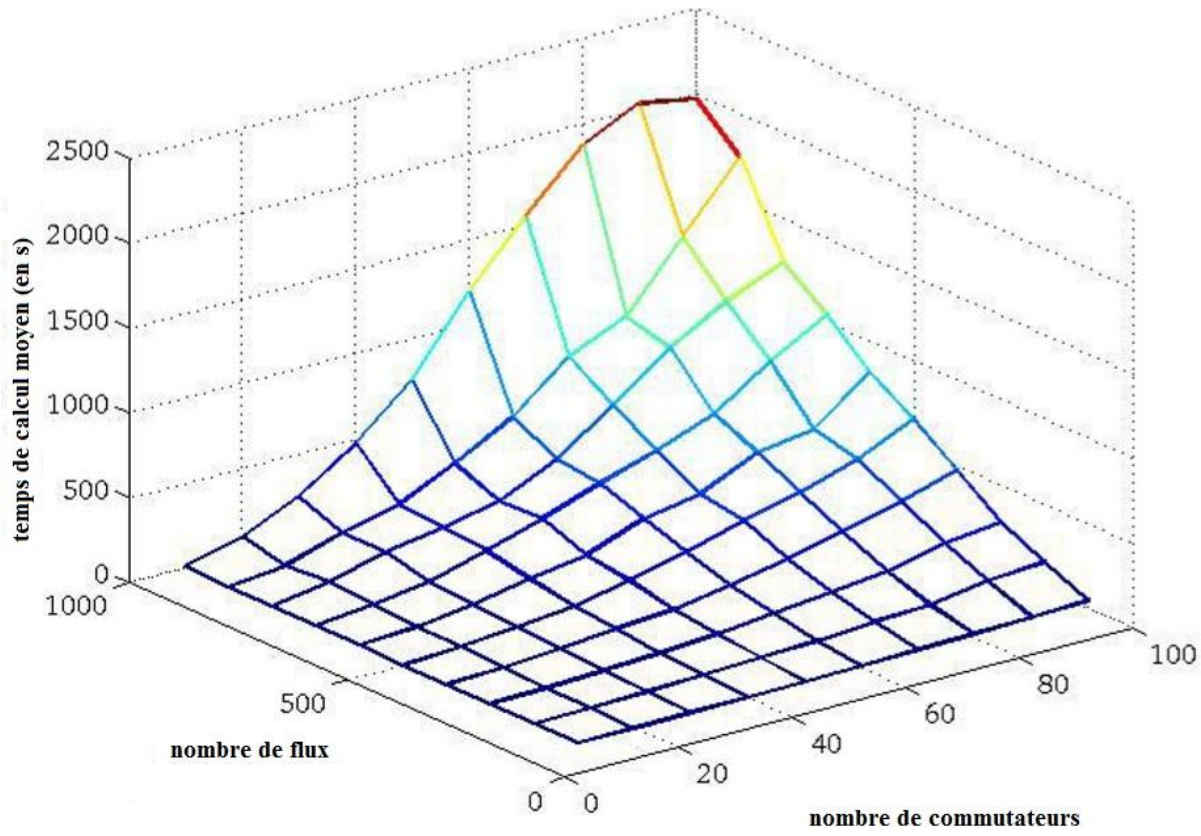

Figure 6: Temps de calcul moyen en fonction du nombre de commutateurs et de flux

Pour conclure, nous avons montré que les approches TA et ETA prennent énormément de temps pour analyser tous les flux transmis sur un réseau de grande taille (formé par exemple de cent nœuds et comportant un millier de flux).

Chapitre 4 : Approche par trajectoire scalable

Le chapitre 4 présente une solution qui se base sur l'approche par trajectoire et qui permet de calculer une borne supérieure en un temps de calcul acceptable. L'approche proposée est nommée *Scalable Trajectory Approach*.

Comme indiqué dans le chapitre précédent, les principales raisons pour lesquelles le calcul de la limite supérieure peut être complexe sont la récursivité et le processus itératif de la formule permettant d'obtenir la borne supérieure. La récursivité présente en particulier sur le premier commutateur d'un flux est éliminée. Ensuite, nous montrons que pour les flux vérifiant des conditions spécifiques, l'ensemble des instants à tester peut être réduit à un seul instant. Le processus itératif est ainsi éliminé. De plus, nous avons également étudié le cas où les flux ont tous le même temps de traitement et la même période. Dans ce cas particulier, nous avons prouvé que la condition devient simplement une condition de charge. Enfin, nous comparons les résultats obtenus en utilisant notre proposition et l'approche de la trajectoire améliorée ETA et nous montrons que notre proposition permet d'obtenir des résultats sur les grands réseaux industriels dans un délai acceptable.

Nous avons appliqué cette approche sur un réseau industriel de taille limitée composé de 10 commutateurs dans lequel 1000 flux sont transmis, sachant que les sources et les destinations sont choisies aléatoirement. Nous considérons que les flux ont tous le même temps de traitement ($C = 26\mu s$) et la même période ($T = 100ms$). De plus, le délai de commutation est de $3\mu s$. Dans un premier temps, nous avons utilisé ETA pour borner le temps de réponse des flux. Ensuite, STA est utilisée : nous rappelons que pour les flux vérifiant une certaine condition, la borne est obtenue quasi instantanément. Pour les autres flux, la formule d'ETA est utilisée pour obtenir la borne. Les résultats sont illustrés à la figure 7.

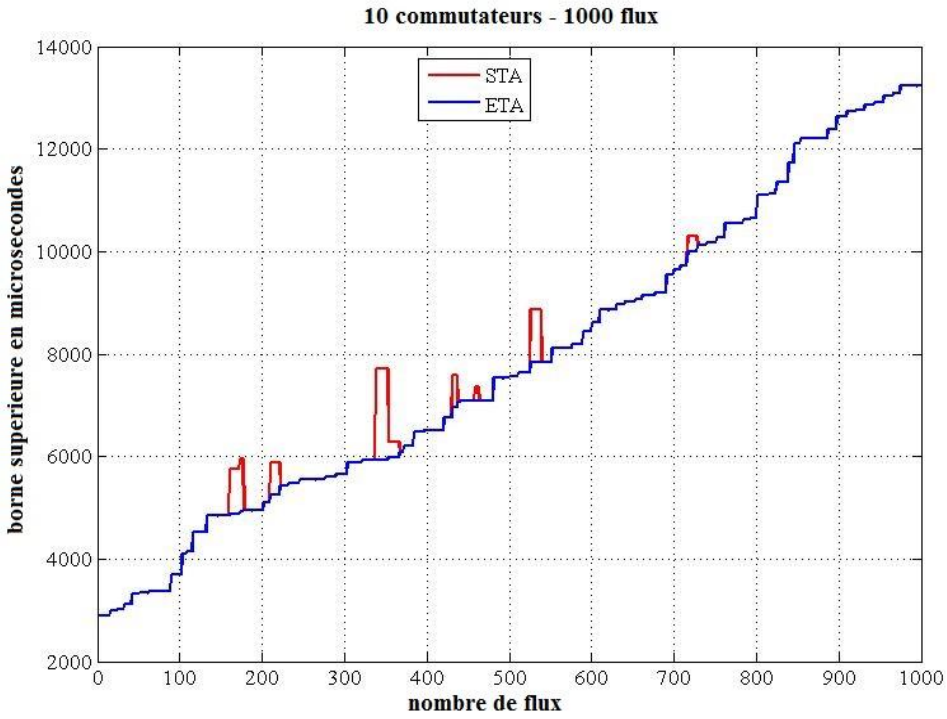

Figure 7: bornes supérieures du temps de réponse de bout-en-bout (en micros)

Ces résultats montrent que le calcul des bornes déterministes sur les temps de réponse pire cas des flux est plus rapide en utilisant notre solution, sans perte significative en termes de précision. Le temps de calcul moyen des bornes de tous les flux est à peu près 4 jours en utilisant ETA. Cette durée se réduit à 15 secondes avec STA.

Ensuite, nous avons comparé les trois approches (TA, ETA et STA) en termes de temps de calcul. Nous avons utilisé la première configuration du chapitre précédent ayant permis de comparer ETA et TA. Les résultats sont illustrés à la figure 8.

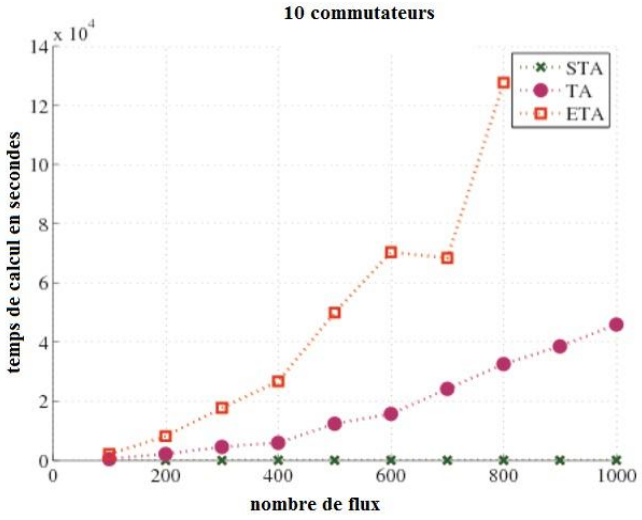

Figure 8: les bornes supérieures des méthodes TA, ETA et STA

Chapitre 5 : Conclusions et perspectives

La vérification et la validation des réseaux temps-réel critiques est un sujet abordé depuis de nombreuses années. Le réseau investigué se base sur de l'Ethernet commuté qui permet d'éliminer le caractère stochastique dû aux collisions. Cependant l'indéterminisme est présent au niveau des commutateurs où les flux concurrents partagent les ressources (en particulier les files d'attente des ports en sortie). La validation du système impose de prouver que le temps de réponse de bout-en-bout de chacun des flux temps-réel transmis sur le réseau est borné et que cette borne ne dépasse pas l'échéance correspondante. Le problème consiste donc essentiellement à déterminer le temps passé par un paquet dans les buffers des commutateurs. Par conséquent, cette thèse porte sur l'analyse temporelle du réseau étudié.

Tout d'abord, les méthodes qui peuvent être utilisées pour effectuer l'analyse temporelle ont été brièvement examinées dans le chapitre 2. Ces méthodes peuvent être divisées en deux groupes: les approches fondées sur la simulation et les méthodes formelles. Nous rappelons que, lors du calcul des garanties déterministes, les méthodes de simulation ne répondent pas à nos exigences. Par conséquent, les approches basées sur des modèles mathématiques (ou connu comme méthodes formelles) sont de bons candidats. Parmi ces approches, nous citons le Model Checking (MC), le calcul réseau (NC) et l'approche par trajectoire (TA). Le MC calcule le temps de réponse pire des cas exact et offre le scénario correspondant. Cependant, cette méthode est toujours incapable d'analyser les grands réseaux. D'autre part, bien que le NC soit utilisé dans la vérification et la validation de systèmes et réseaux, les bornes sur les temps de réponse sont parfois très pessimistes, ce qui conduit à un surdimensionnement du réseau. Enfin, l'approche par trajectoire se base sur la théorie de l'ordonnancement et offre des bornes plus précises que le calcul réseau. Nos travaux se sont donc axés sur l'approche de la trajectoire.

Par la suite, les limitations de l'application de l'approche par trajectoire, avec comme politique d'ordonnancement FIFO, ont été discutées. Après nous être intéressés aux raisons conduisant à des bornes pessimistes, nous avons considéré le problème du passage à l'échelle de l'approche par trajectoire. Nous avons montré que TA, telle qu'elle a été formalisée initialement, prend énormément de temps pour analyser tous les flux transmis sur un réseau de grande taille (e.g. formé d'une centaine de nœuds et comportant à peu près un millier de flux).

Enfin, le problème du passage à l'échelle lors de l'application de l'approche par trajectoire sur une grande configuration industrielle a été abordé dans le chapitre 4. Nous avons proposé une méthode permettant de calculer quasi instantanément des bornes supérieures sur les temps de réponse de certains flux satisfaisant des conditions spécifiques. Nous avons également étudié le cas particulier où tous les flux ont le même temps de traitement et la même période. Nous avons alors prouvé que la contrainte devient simplement une condition de charge, condition nécessaire pour la faisabilité de l'ordonnancement.

Nous avons appliqué cette approche sur un réseau industriel limité. Le calcul des bornes déterministes s'est avéré beaucoup plus rapide en utilisant notre solution. Nous avons montré par la suite que notre approche permettait d'obtenir des résultats sur de grandes configurations industrielles où le nombre de paramètres à déterminer est particulièrement élevé, sans perte significative de précision. STA répond donc à la problématique posée portant sur la détermination de bornes déterministes en un temps raisonnable et avec une précision fine sur de larges réseaux.

Plusieurs perspectives du travail effectué sont envisageables :

- L'approche STA a été appliquée sur une topologie en ligne. Il serait intéressant, avec les résultats obtenus dans cette thèse, de l'étendre sur d'autres topologies (e.g. un réseau en arbre).

- Il serait également intéressant de comparer les résultats obtenus en utilisant l'approche STA avec ceux obtenus en utilisant le Network Calculus. Ce travail a été entamé durant la thèse et semble confirmer pour l'instant que notre approche offre de meilleurs résultats en termes de précision, avec une plus faible complexité.

- Un autre axe consisterait à appliquer STA sur des réseaux avec des flux de priorités différentes. Dans ce cas, les flux pourront se voir attribuer des priorités fixes en plus des priorités dynamiques affectées dans leurs files d'attente. Cela étendrait davantage notre approche à celle originelle basée sur des ordonnancements FP/DP.

- Un autre sujet de recherche serait de trouver un compromis entre complexité du temps de calcul et précision de la borne obtenue. Plus précisément, pour les flux qui ne rempliraient pas la condition définie dans STA, il serait intéressant de calculer des bornes en dégradant l'approche de base. Si ces bornes ne respectaient pas les échéances fixées, alors elles pourraient être affinées de manière optimisée jusqu'à la faisabilité de l'ensemble des flux.