Qualité de service et systèmes contrôlés en réseau Qds & SCR

Jean-Philippe Georges

Qualité de service et systèmes contrôlés en réseau

Jean-Philippe Georges
Centre de Recherche en Automatique de Nancy
Nancy-Université, CNRS
Campus Sciences, BP 70239, 54506 Vandœuvre lès Nancy cedex
Email : jean-philippe.georges@cran.uhp-nancy.fr

***Résumé*—Les systèmes de contrôle-commande industriels et embarqués se caractérisent par l'interconnexion en réseau de multiples équipements via des réseaux non plus dédiés, mais partagés avec d'autres applications. Dans ces systèmes contrôlés en réseau, il est nécessaire que la Qualité de Service du réseau ait un impact limité sur la Qualité de Performance du système. Pour les réseaux basés sur des équipements sur étagère, il s'agit donc d'adresser les scénarios pour lesquels les protocoles de communication communs échouent à la satisfaction des exigences de par de longs délais ou la rupture de la connectivité de bout-en-bout. La problématique générale vise à doter les applications distribuées des moyens en communication qu'elles requièrent, et/ou définir leur commande en fonction du service offert par le réseau. Il s'agit donc de contrôler et/ou adapter le système de communication (qualité de service) et/ou l'application. Cette présentation s'intéresse plus particulièrement aux travaux concernant la commande dynamique (réservation de mémoire, contrôle d'admission, ordonnancement, etc.) de la qualité de service réseau (disponibilité, délais, pertes, etc.) en fonction des exigences du système contrôlé.**

I. Systèmes contrôlés en réseau (SCR)

A. Introduction

Un système contrôlé en réseau (SCR) (ou *networked control systems* dans la littérature anglophone) correspond à un système de contrôle/commande distribué *via* un réseau pouvant être partagé avec d'autres applications non impliquées dans la commande du système. Plus précisément, un SCR est un système de contrôle à asservissement dans lequel les boucles de régulation sont fermées au moyen d'un réseau de communication [1], [2] comme le montre la figure 1.

Le domaine des systèmes contrôlés en réseau est relativement nouveau dans la communauté académique du contrôle (nouveau Technical Committee 1.5 de l'IFAC), mais il ne l'est pas dans l'industrie. On les retrouve notamment dans les systèmes de production, mais aussi dans les systèmes embarqués comme les avions ou les automobiles. Historiquement les SCR s'appuient sur l'implémentation des contrôles distribués définis au travers du Distributed Control System (DCS) de Honeywell dans les années 70. L'introduction d'un réseau dans la boucle de commande vise notamment à la réduction des coûts de câblage, l'aide au diagnostic et à la maintenance des systèmes, l'amélioration de la modularité et de la flexibilité dans la conception des systèmes. Aujourd'hui, plusieurs compagnies comme Rockwell Automation, ABB, Siemens proposent des équipements intégrant leur propre coupleur de communication réseau, si bien que plusieurs réseaux sont des composants naturels des SCR actuellement en service comme DeviceNet, Fip, CAN, Profibus, Modbus, etc.

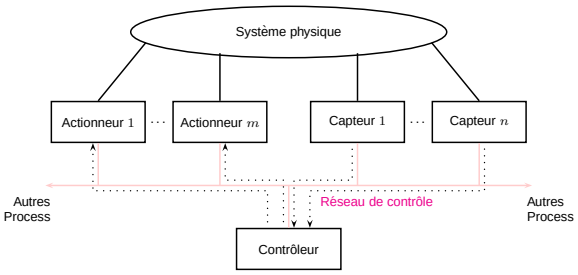


FIGURE 1. Vue traditionnelle des systèmes contrôlés en réseau [1]

L'insertion du réseau de communication dans la boucle de contrôle rend l'analyse et la conception des SCR relativement complexe. Les théories de contrôle conventionnelles qui comportent plusieurs hypothèses idéales telles la synchronisation de la commande et de l'observation ainsi que la capacité de réaction sans retard doivent être réévaluées avant de pouvoir être appliquées aux systèmes contrôlés en réseau. Les points critiques mis en avant par [1] sont :

- le délai induit par le réseau (du capteur vers le contrôleur et du contrôleur vers l'actionneur) lors de l'échange de données entre les équipements connectés au médium partagé. Ce délai, qu'il soit constant ou variable, peut dégrader la performance d'un système de contrôle qui ne le prendrait pas en compte, voire même le rendre instable,
- le réseau fournit un ensemble de chemins non fiables. Il faut donc prendre en compte le fait que des paquets peuvent être perdus, dupliqués, désordonnés,
- l'information peut être contenue dans plusieurs messages. Les chances que la totalité, une partie ou aucun des paquets arrivent doivent alors également être étudiées.

Les systèmes informatiques distribués (calculateurs interconnectés à travers un réseau de communication qu'il soit local ou réseau de terrain) sont aussi de plus en plus utilisés pour réaliser des applications de contrôle commande et en particulier de type bouclé. Ces systèmes sont des systèmes temps-réel, c'est-à-dire que la maîtrise temporelle du service fourni est essentielle pour garantir les performances des applications. Cette maîtrise temporelle dépend, non seulement, de l'exécution des tâches concernées (début, durée) mais aussi des échanges à travers le réseau (délai de transmission, perte).

Compte tenu des particularités de la ressource

≪ réseau ≫ (délais, gigues, pertes, protocoles), il est nécessaire que les différents équipements prennent notamment en compte les problèmes suivants :

- cohérences spatiales et temporelles de l'information
- production (conditions) et fraîcheur de l'information
- priorité de l'information
- disponibilité de la ressource
- autonomie des sous-systèmes

Toutes ces notions mettent l'accent sur la vérification formelle et l'évaluation de performances des caractéristiques temps-réel de l'application. Et comme chaque type de réseau répond à des critères de performances différents tels la vitesse de transfert, la taille des messages, des majorants du délai et la disponibilité, l'analyse d'un SCR est implicitement liée au protocole de communication mis en œuvre.

B. Présentation générale des travaux de recherche

La problématique des SCR s'inscrit dans le cadre général des *systèmes à retard* (ou *time-delay systems* en anglais). Les systèmes contrôlés en réseau sont des systèmes à retard pour lesquels le retard est introduit par le réseau. Un tutoriel des travaux et des problématiques est donné dans [3]. Les points clés des systèmes à retard sont la modélisation des délais, le contrôle optimal, et la robustesse de la stabilité. La collecte des informations relatives au comportement du délai est alors primordiale. Par exemple, si des observateurs pour les systèmes à retard ont été proposés, ces travaux s'appuient sur des mesures supposées du retard. Le délai est supposé connu ou calculable, de sorte que cette connaissance nécessite d'être fournie par une étape d'identification ou d'analyse des limites technologiques. Ce problème est alors d'autant plus délicat que le retard est produit par un réseau dont le comportement peut être difficilement analysable.

Les systèmes contrôlés en réseau partagent également la problématique du contrôle des retards induits par le réseau avec les systèmes téléopérés comme le contrôle d'un robot à distance qui sont très sensibles à la fluctuation des délais de transmission. Des travaux montrent qu'une solution est que le retard soit constant. Des techniques informatiques peuvent alors être utilisée pour assurer cette hypothèse. Ainsi que ce soit dans le cadre de la téléopération d'un robot [4], [5] ou pour les applications distribuées [6], la régulation des retards variables par bufferisation peut être utilisée. L'information est volontairement retenue de façon à pouvoir la restituer avec un retard le plus constant possible (annulation de la gigue).

Cette prise en compte des délais liés à la traversée du réseau se matérialise alors dans les boucles de régulation par l'ajout de blocs retardateurs. Cette intégration peut alors se traduire comme dans le modèle de l'asservissement présenté à la figure 2.

Ce modèle est établi dans le cadre d'une architecture producteur / consommateur semblable à la figure 1, mais où le contrôleur est directement intégré à l'actionneur. Dans cette architecture, la boucle de retour tient compte de l'influence du réseau. Dans un premier temps, le bloc $e^{-\tau_d p}$ introduit le retard issu de la traversée du réseau qui dépend de divers

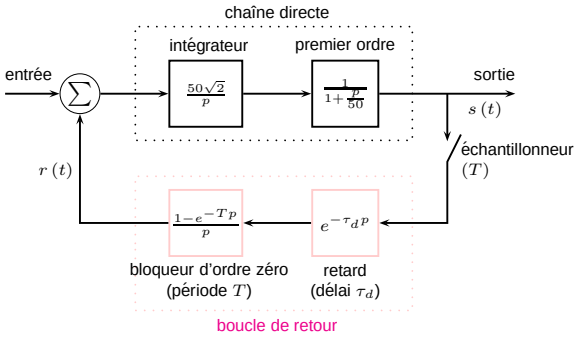


FIGURE 2. Asservissement distribué [7]

paramètres tels que le protocole de transfert ou les politiques d'ordonnancement. Dans un second temps, le bloqueur d'ordre zéro matérialise une probabilité de perte non nulle des paquets. Dans ces travaux, il est admis que la dégradation de la périodicité d'émission des paquets due aux pertes peut être approximée par une période T plus large que la période initiale (ceci n'est toutefois pas juste si l'on considère des rafales de pertes). La fonction de transfert du bloqueur d'ordre zéro est ainsi approximée par celle d'un retard pur. Notons que s'il n'y a ni pertes ($T = T_0$) ni retard ($\tau_d = 0$), on retombe dans le schéma classique d'un asservissement échantillonné.

La figure 2 permet d'introduire différents indicateurs de performance du réseau dans le modèle d'asservissement d'une application distribuée. Dans ce modèle, le réseau est simplement utilisé pour l'échange des mesures effectuées en sortie du système. La figure 3 élargit le champ d'utilisation du réseau puisqu'il intègre cette fois les communications du capteur au correcteur ainsi que du correcteur à l'actionneur.

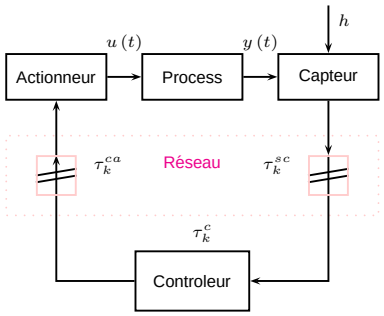


FIGURE 3. Modèle d'asservissement distribué [8]

Contrairement au premier modèle, celui de la figure 3 n'intègre que le retard issu de la traversée du réseau. Toutefois, le système est ici totalement distribué : le contrôle se fait sur un équipement distribué. Ce modèle intègre trois délais : le temps de calcul au niveau du contrôleur ainsi que les temps de traversée du réseau du capteur au contrôleur et du contrôleur à l'actionneur. La distinction des retards suivant l'échange considéré est essentielle lorsque le système à retard est un réseau (notamment en raison des chemins multiples). Si bien que comme le montre la figure 4, ce modèle doit

être complété lorsque l'application intègre plusieurs entrées et plusieurs sorties.

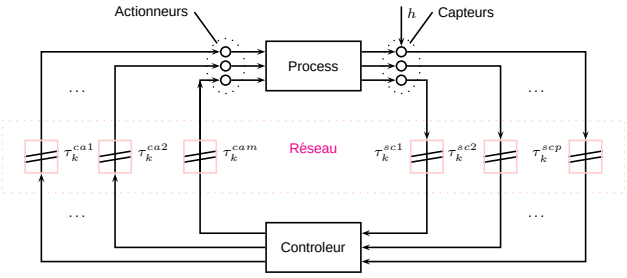


FIGURE 4. Modèle d'asservissement distribué à multiples entrées et sorties [8]

La figure 4 introduit un aspect supplémentaire de la difficulté d'analyse des SCRs. Outre l'influence du réseau pouvant rendre le contrôle du système instable, le réseau est un système à part entière et les caractéristiques telles que le retard dépendent de nombreux paramètres (chemins, taille des messages, ordonnancement, protocole ...) et peuvent fortement varier. Il sera donc nécessaire de formuler une analyse des retards dédiée pour chaque application et plus particulièrement pour chaque échange.
Les paragraphes suivants présentent les différents axes d'étude des systèmes contrôlés en réseau tels la commandabilité et la stabilité du contrôle ainsi que l'intégration des niveaux de performance du réseau dans le contrôle de l'application.

Le lecteur intéressé par la recherche dans le domaine des SCR pourra consulter les papiers introductifs [9], [10], [11], [2] et le dernier état de l'art publié dans [12]. Plus globalement, deux grandes directions peuvent être distinguées selon que le SCR est étudié du point de vue de la commande du système ou alors du point de vue réseau.

Dans la première approche généralement appelée « commande en réseau », la commande s'adapte aux perturbations induites par le réseau. Dans ce contexte, le réseau est une ressource passive apportant différentes contraintes exprimées en termes de Qualité de Service. Le réseau est ainsi vu comme une « boîte noire » associée à un système à retard variable. En fonction des informations disponibles concernant la QdS offerte par le réseau, plusieurs stratégies de compensation ont été proposées : cela va de l'adaptation traditionnelle du gain PID, la synthèse de commande prédictive ou encore de commande robuste. L'enjeu majeur porte généralement sur la stabilité du système. Ces résultats relevant de la problématique des systèmes à retard, [3] présente un état de l'art des derniers développements dans ce domaine.

Dans le second cas, le réseau est désormais une ressource « active » et commandable. Cette approche qui sera détaillée dans la suite, est appelée « contrôle de réseau » [12]. L'adaptation du réseau aux exigences de la commande du système vise à optimiser les performances que ce soit de manière endogène (paramètres de QdS) ou exogène, c'est-à-dire relativement à la Qualité de Performance (état courant du système comme sa stabilité ou l'erreur). La caractéristique fondamentale des travaux relatifs à cette approche est d'être profondément marqués par le type de réseau étudié puisque celui-ci restreint les possibilités d'optimisation. Ainsi lorsque [13] relie différents panels de priorité sur CAN à la marge de phase, [14] présente une fonction de dégradation des performances pour différentes architectures. De même lorsque [15] propose un nouveau protocole *try-once-discard*, [16] propose une nouvelle politique d'ordonnancement type TDMA pour Profibus.

Dans cet article, l'étude des SCR se focalisera sur les réseaux filaires, et plus particulièrement le réseau Ethernet dont l'indéterminisme, et donc son incapacité à satisfaire des exigences temps-réel, le rend a priori inadapté comme support aux SCRs. L'utilisation de la Classification de Service et de politiques d'ordonnancement équitables seront alors utilisées en vue de répondre à ces exigences. Par la suite, l'impact sur le système de la disponibilité fournie par un réseau commuté. Cet article reprendra les travaux menés dans [17] concernant une stratégie permettant d'améliorer la disponibilité du réseau.

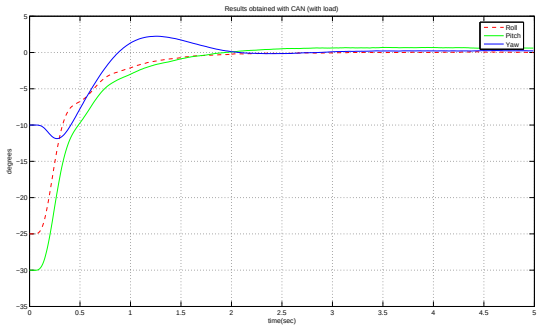
II. CAS DE RÉSEAUX FILAIRES À BASE D'ETHERNET

Le recours à l'utilisation de réseaux dans la commande en boucle fermée de systèmes s'est initialement tournée vers les réseaux locaux industriels classiques, comme le réseau CAN. La raison principale s'explique naturellement par le comportement déterministe de ces réseaux, les rendant adaptés aux SCRs. Cependant, de nouvelles exigences sont apparues comme de nouvelles fonctionnalités (e-maintenance, téléopération), mais aussi la volonté de partager le médium avec d'autres applications. Face à cette intensification de l'utilisation de la bande passante et la multitude des messages supportés, le protocole Ethernet apparaît alors comme une solution pour les SCRs. Les intérêts majeurs sont donc liés au support de débits largement supérieurs (jusqu'au Gb/s) aux réseaux locaux traditionnels et à la standardisation effective d'Ethernet [18]. C'est ainsi qu'Ethernet est aujourd'hui de plus en plus implanté dans les systèmes temporellement contraints (citons par exemple l'Airbus A380 d'EADS).

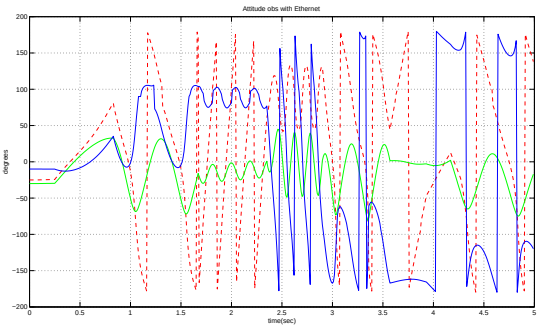
Néanmoins, l'utilisation d'Ethernet comme support de SCR pose différentes problématiques. Dans un premier temps, en termes de sûreté de fonctionnement, différentes précautions doivent être prises afin de faire face notamment à la défaillance d'un lien, ou même du bus. Il s'agit donc de construire des topologies redondantes (par exemple, redondance de liens, d'équipements d'interconnexion, etc). La gestion de cette redondance physique doit également être accompagnée d'une topologie logique (algorithmes d'arbre couvrant comme STP ou RSTP) optimisant les temps de détection de défaillance et de reconfiguration de la topologie. Cette problématique est notamment abordée dans [19].

Dans un second temps, l'augmentation de la bande passante ne solutionne pas tous les problèmes. En effet, le protocole CSMA/CD utilisé par Ethernet conduit à un accès au médium non déterministe du fait de la probabilité d'occurrence de collisions [20]. L'occurrence de ces collisions est d'autant plus grande lorsque le réseau est partagé par différentes applications (qu'elles soient ou non impliquées dans la commande du

système). Ce phénomène est ainsi mis en exergue dans [21] pour la commande en réseau d'un drone hélicoptère à quatres rotors développé par le GIPSA-lab dans le cadre du projet ANR SafeNecs [1]. Pour ce système, le réseau embarqué doit supporter le trafic généré par 17 flux périodiques, où la période d'échantillonnage est fixée à $10\ ms$. La figure 5 présente les résultats de simulation conjointe (système, commande et réseau) du SCR réalisé via la librairie TrueTime sous Matlab/Simulink. L'étude considère tour à tour le réseau Ethernet et le réseau CAN (comme référence). Ethernet peut réussir à fournir des performances du même niveau que CAN pour la commande du système, notamment dans le contexte d'un réseau dédié (sans trafic annexe). Néanmoins, la figure 5(b) montre ensuite que si le réseau est partagé avec d'autres applications, Ethernet, malgré sa bande pasante de $10\ Mb/s$, impacte sensiblement la commande puisque cette fois le système est instable. Le problème pour la commande de systèmes industriels ou embarqués est lié au fait qu'aucune garantie de performance n'est fournie aux messages à fortes contraintes temporelles.



(a) CAN 1 Mb/s avec charge



(b) Ethernet 10 Mb/s, avec charge

FIGURE 5. Problématique d'Ethernet dans les réseaux partagés *(les graphes réprésentent l'évolution des angles au cours du temps en seconde)*

L'instabilité observée à la figure 5(b) s'explique par le fait que le trafic réseau va induire une charge (congestion) du commutateur et en conséquence une augmentation des délais. L'ordonnancement utilisé par le standard [22] étant de type FIFO, il n'existe aucune différentiation de service entre le trafic de commande et le trafic non temps-réel. À l'inverse, le réseau CAN de la figure 5 intégrant un ordonnancement de type priorité stricte, reste capable de fournir un service suffisant bien que le débit soit plus faible. L'utilisation d'Ethernet comme support au SCR passe donc dans le cas d'un réseau partagé, par l'utilisation de mécanismes d'ordonnancement plus avancés comme décrit ci-dessous.

Au niveau d'Ethernet, il est à noter que l'on ne parle pas de qualité de service mais simplement de classification de service. Cette différence suggère déjà le fait que l'on ne va pas chercher à satisfaire des besoins prédéfinis mais plutôt à privilégier le traitement de certaines trames sans pour autant garantir un niveau de service. Dans ce cadre, cela sous entend également une première étape qu'est la prioritisation du trafic. Phase qui par nature sera arbitraire.

Comme il a déjà été indiqué, il y a une différence fondamentale entre les concepts de Classe de Service (CdS) et de Qualité de Service (QdS). La QdS se définit par la garantie que donne le réseau à une application en terme de contrat de services au travers de la session de l'application. L'application requiert explicitement ou implicitement (*via* un gestionnaire de politique) un niveau de service d'utilisation du réseau. Le réseau réserve alors les ressources (mémoires, canaux ...) appropriées pour la durée de la session applicative. La QdS implique une connexion et une réservation des ressources réseau de façon à fournir une garantie d'un niveau de service minimum.

La CdS est plus simple. Le réseau fournit un niveau de service supérieur pour les applications prioritaires, mais ne garantit explicitement rien d'autre. Il n'y a aucune garantie d'un service minimum. Ni la mémoire ni les canaux n'ont besoin d'être réservés. Il n'y a pas besoin d'autres protocoles. Cette approche suppose que la capacité du réseau est en moyenne suffisante pour l'ensemble des applications, mais que temporairement des phénomènes de congestion peuvent apparaître. Une justification possible est qu'il est plus simple et par conséquent moins cher de surestimer quelque peu les capacités du réseau et d'utiliser la CdS pour améliorer les surcharges spécifiques que d'invoquer les mécanismes complexes de QdS.

Nativement, Ethernet n'implémente pas de mécanisme de priorité. Les priorités vont intervenir lors de la gestion de la congestion d'un commutateur, gestion qui est réalisée au travers de l'implémentation de buffers. Pour les flux les plus importants (plus sensible aux délais), un traitement préférentiel sera accordé au vu du niveau d'importance codé à travers le niveau de priorité. La standardisation de la classification de service couvre actuellement deux standards. 802.1D/p précise les questions de priorité, à savoir la détermination, la regénération et l'association des ressources mémoires entre les différentes classes de service. 802.1Q inclut quant à lui l'étiquetage de la priorité d'une trame dans l'étiquette VLAN.

L'instanciation de plusieurs files en sortie d'un commutateur nécessite d'adopter une stratégie d'ordonnancement. Les standards [23], [22] précisent alors que la discipline de service

1. `http://safe-necs.cran.uhp-nancy.fr/`

définie par défaut est la politique à priorité stricte. Néanmoins, ils laissent la possibilité à l'utilisation d'autres politiques, sous réserve que la discipline de service d'une seule file doit rester FIFO. Toutefois, une étude des produits actuellement commercialisés montre que seule la discipline WFQ (*weighted fair queueing*) est implantée. Aussi seules ces 2 politiques seront considérées.

Finalement, le recours à la Classification de Service se justifiera donc dans les cas suivants :

- on cherche à minimiser des bornes temporelles délivrées par le réseau qui ne satisfont pas les besoins applicatifs,
- on veut privilégier des trafics lorsque temporairement il existe des points de congestion du réseau pour lesquels la bande passante disponible est insuffisante.

En résumé, si la Classification de Service ne permet pas de rendre Ethernet déterministe, elle contribue à la réduction des délais subis par les informations critiques. Cet apport a été ainsi illustré dans différents travaux comme [24], [25] ou [26] qui présentent une optimisation des différents paramètres de la CdS.

III. Contrôle *équitable* de réseau pour SCR

L'objectif de cette section est d'illustrer l'apport de la Classification de Service pour Ethernet, et plus particulièrement de l'ordonnancement WRR dans le contexte de SCR reposant sur un réseau partagé. Par rapport aux deux approches d'étude d'un SCR identifié dans [12], cet article détaille la stratégie « commande de réseau » permettant de répondre aux exigences requises par l'application (ici, la commande du système). De manière générale, il s'agit, relativement à une QdS souhaitée, de gérer au mieux les ressources de communication (réservation de ressources, contrôle dynamique de leur allocation, flexibilisation de l'offre de service, etc.) [27]. Dans le cadre d'un SCR à base d'Ethernet, les solutions suivantes visent à agir explicitement sur l'affection des poids de l'ordonnancement WRR, soit implicitement sur la bande passante offerte à chaque trafic, et *in fine* sur les délais de bout-en-bout. À titre de comparaison, [28] présente une approche de commande en réseau basée sur la synthèse d'une commande robuste à partir de majorants des délais de bout-en-bout.

La particularité des approches suivantes est de développer un *co-design*, où les paramètres de Qualité de Service (ici, les délais de bout-en-bout) exigés du réseau sont exprimés en fonction d'indicateurs de Qualité de Performance (QdP) du SCR. La QdP d'un SCR peut être exprimée de différentes manières : stabilité du système, temps de réponse, dépassement maximal, marge de phase ou de retard, ou encore la position des pôles. Il s'agit ensuite de traduire cette QdP en QdS. Dans la suite, nous considérerons que la QdS exigée du réseau correspond à des retards maxima.

Enfin, dans la mesure où le réseau support au SCR est un réseau partagé avec d'autres applications non temps-réel, le but est aussi de maximiser le service offert au trafic non temps-réel. Ce dernier point reflète l'originalité des ordonnancements de type *fair queueing* pour les SCR : assurer une bande passante au trafic de fond, et éviter ainsi de se retrouver dans la configuration d'un réseau dédié. Deux approches d'optimisation des poids ϕ_j sont alors proposées : soit de manière dynamique avec un objectif de flexibilité maximale, soit de manière statique avec une contrainte de robustesse [29].

Les résultats suivants s'appuient sur une plateforme expérimentale présentée dans [29]. Sur cette plateforme, 4 stations sont interconnectées *via* un commutateur à politique d'ordonnancement WRR (figure 6). Les deux premières stations exécutent des codes C/Posix simulant respectivement la partie process et commande du SCR. Le système étudié est le suivant :

$$P(s) = \frac{2}{(s+5)(s+0,2)}, \quad C(s) = \frac{K_p s + K_i}{s}$$

avec $K_p = 0,5508$ et $K_i = 0,4529$ les paramètres de commande minimisant l'erreur quadratique.

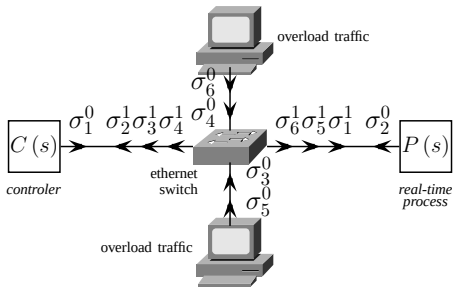
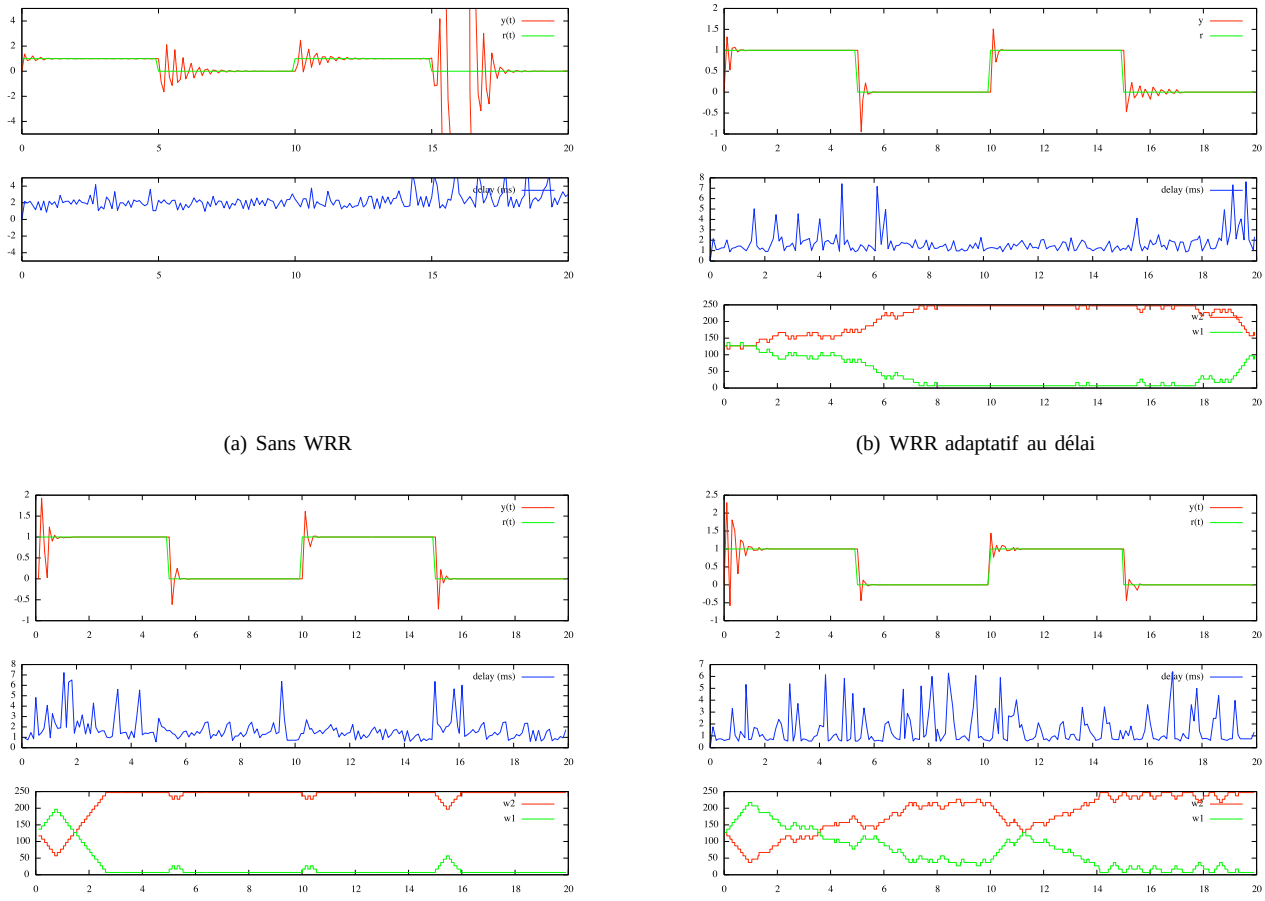


FIGURE 6. Plateforme expérimentale (les paramètres σ_i^j représente l'avalanche maximale de données pour un flux i après la traversé de j commutateurs)

Les deux autres stations sont responsables d'un flux de charge. Enfin, la plateforme est enrichie d'agents de mesure des délais uni-directionnels basés sur la synchronisation d'horloge selon le standard IEEE PTP 1588 et d'un agent de reconfiguration en-ligne des poids attribués à chaque classe du WRR. Le débit du réseau est fixé à $10\ Mb/s$ et la charge de fond introduite par les deux stations est approximativement de $8\ Mb/s$. Comme précédemment, la figure 7(a) montre alors que si la bande passante peut apparaître en moyenne suffisante, de grands retards peuvent apparaître et se traduire en phase transitoire par des dépassements, voire engendrer une instabilité du système.

Compte tenu des indications de la figure 7(a), une première utilisation de l'ordonnancement équitable du WRR est proposée dans le but d'adapter les poids de chaque classe de trafic conformément à l'évolution du délai de commande. L'adaptation expérimentale proposée est la suivante : lorsque le délai des messages temps-réel augmente, le poids (allant de 1 à 255) de la classe temps réel est augmenté. La valeur des poids est alors gérée de deux manières. Tout d'abord, comme les paramètres du système impliquent un retard de $2\ ms$ (plus petite constante de temps de la fonction de transfert $P(s)$), si le retard observé est supérieur à ce seuil, alors le poids de la classe temps réel est incrémenté de 10 et celui de la classe basse priorité décrémenté d'autant. Ensuite, dans le cas où les délais mesurés sont inférieurs à ce seuil, le processus



(a) Sans WRR

(b) WRR adaptatif au délai

(c) WRR adaptatif à l'erreur

(d) WRR adaptatif au délai et à l'erreur

FIGURE 7. Adaptation en ligne des poids d'un WRR *(le graphe du haut représente la consigne et la sortie du système, l'intermédiaire le délai et celui du bas, l'évolution des poids ω_1 et ω_2 en fonction du temps en s)*

est inversé de manière à offrir le service maximum au flux de fond. La figure 7(b) présente les résultats obtenus. Elle montre alors clairement que cette stratégie a permis de maîtriser les délais, et ainsi les dépassements.

Pour éviter les oscillations observées en fin de figure 7(b), une seconde stratégie basée sur le signal d'erreur de commande a été étudiée. La figure 7(c) donne les résultats. La procédure est la même que précédemment, excepté l'identification du seuil. Dans cette approche, le seuil est déterminé suivant que l'erreur est supérieure à $5\ \%$ du signal de référence. L'originalité ici consiste donc à consolider la commande du système et celle du réseau, ce qui permet comme observé à la figure 7(c), de limiter les dépassements et les oscillations. Au final, ces deux stratégies peuvent alors être rassemblées en une seule, c'est-à-dire où l'adaptation est basée à la fois sur l'erreur et le délai. Le délai apporte ici une indication de prédiction de l'état du réseau, permettant d'anticiper des phases de congestions progressives. Dans ce cas, la procédure est redéfinie telle que l'augmentation des poids du flux temps-réel intervient dès que l'un des deux seuils définis est atteint. La figure 7(d) présente les résultats.

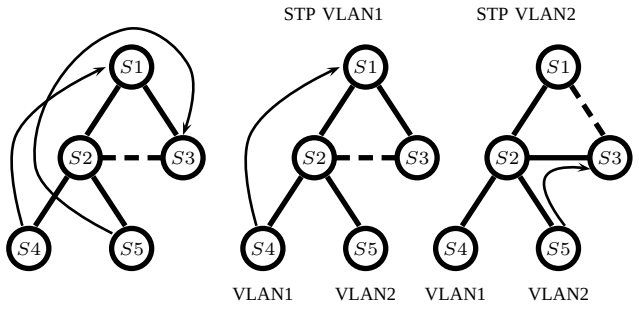
Au final, l'adaptation en ligne des poids du WRR (c'est-à-dire la maîtrise de la bande passante) a ici permis :

- de réduire le dépassement maximal puisque l'on passe de près de $800\ \%$ dans le cas sans WRR à 94, 72 et finalement $44\ \%$ pour l'approche combinée
- de réduire les délais moyens ($1,52$ contre $2,27\ ms$ initialement)
- tout en augmentant et garantissant la bande passante offerte aux autres flux circulant sur le réseau partagé support du SCR.

IV. DISPONIBILITÉ D'UN RÉSEAU & SCR

Dans le domaine des réseaux, la redondance se traduit par la mise en place d'un certain nombre de boucles, posant alors des problèmes de retransmissions infinies, qui congestionnent le réseau. Des protocoles existent et permettent de remédier à ces problèmes, ils consistent à mettre en place des arbres couvrants sur le réseau. Par exemple le protocole Spanning Tree (STP) a pour but d'analyser le câblage du réseau, puis d'inhiber un certain nombre de liens de façon à éliminer les boucles du réseau, tout en assurant l'interconnexion de tous les nœuds. La fonction du protocole ne se limite pas à cela, elle surveille en permanence l'état des liens et des équipements du réseau.

Lorsqu'une anomalie se produit (défaillance d'un câble, port, etc.), le protocole STP cherche à maintenir la connectivité de l'ensemble des nœuds du réseau en réactivant des liens qu'il avait préalablement inhibés. Le protocole RSTP (Rapid-STP, IEEE 802.1w), évolution de STP permet également, mais plus rapidement (de l'ordre de 1 à 5 secondes contre 30 secondes pour STP), de réaliser ces fonctions. Pour limiter les problèmes de congestion sur un chemin donné, il est possible en activant des protocoles tels que MSTP (Multiple STP, IEEE 802.1s), ou encore PVST (Per-VLAN STP, protocole propriétaire Cisco), de définir non pas un arbre sur le réseau Ethernet mais un arbre par VLAN (Virtual LAN, 802.1Q). Le but est de pouvoir répartir la charge en utilisant les liens redondants du réseau pour éliminer les goulots d'étranglement. En effet, basiquement les VLAN s'appuient sur l'arbre unique définit par le protocole STP pour acheminer leurs messages, c'est-à-dire que toutes les communications, quelque soit le VLAN, passent par les mêmes chemins pour aller d'un point vers un autre. Cette configuration peut avoir comme incidence d'amplifier ou de générer de la congestion sur certains chemins. La figure 8 montre la différence entre une gestion unique et multiple du STP. Sur le graphe figure 8(a), un seul arbre est défini pour acheminer tous les messages. Dans ce cas, lorsque le sommet S4 envoie des messages typés VLAN1 vers S1 et le sommet S5 envoie des messages typés VLAN2 vers S3, alors le lien entre S1 et S2 est sollicité à chaque fois. Sur les deux autres graphes figure 8(b), le protocole MSTP est activé et propose d'inhiber le lien entre S2 et S3 pour l'arbre de VLAN1 et d'inhiber le lien entre S1 et S3 pour le VLAN2. Cette configuration permet de répartir les charges puisque le lien entre S1 et S2 est utilisé pour transporter le message typé VLAN1, alors que le message typé VLAN2 passe directement via le lien entre S2 et S3.



(a) STP unique (b) Multiple STP

FIGURE 8. Configuration STP unique vs Multiple STP

Dans le cadre des SCRs, l'objectif est de proposer une méthode permettant de minimiser la probabilité qu'une déconnexion intervienne entre le(s) contrôleur(s), les capteurs et les actionneurs.

A. Arbres couvrants

Le problème du protocole STP, ainsi que de son évolution RSTP, concerne les temps de reconfiguration pour proposer de nouveaux arbres. En effet, STP nécessite une trentaine de secondes et RSTP en moyenne cinq secondes, des durées non adaptées aux environnements temps-réel. On constate alors que l'utilisation d'un seul arbre se révèle être une configuration critique, puisque la présence d'un dysfonctionnement d'équipement au sein du réseau a pour conséquence d'interrompre les communications entre les équipements du SCR. La société MOXA a mis en place un nouveau mécanisme nommé Turbo-ring afin de résoudre ce problème. Ce dernier assure une reconfiguration aux alentours des 20 ms, mais cette solution n'est pas normalisée, utilise une architecture particulière dite en anneau et peut se révéler trop longue.

Plusieurs stratégies peuvent être proposées afin d'éviter ou minimiser cette situation. Dans [30], un nouvel algorithme de routage multi-chemins disjoints est défini. Ces travaux se basent sur la théorie des arbres colorés et ont pour but de prendre en compte la défaillance des nœuds, dans le cadre d'un maintien de la communication entre un nœud et un puits. La spécificité de ces travaux concerne la minimisation des échanges sur le réseau. C'est-à-dire qu'il s'agit d'une approche en ligne permettant l'amélioration des performances de reconfigurations. Une autre approche consiste à anticiper de manière hors-ligne la défaillance d'un chemin. Ainsi [31] propose de dupliquer le médium afin de mettre en place une redondance concernant l'acheminement des trames. Cette solution est basée sur une architecture non commutée et présente une limitation en débit.

La solution présentée dans ce papier [17] utilise le protocole MSTP afin de définir plusieurs parcours possibles pour relier différents points du réseau, nous utiliserons alors la notion de chemin lors de notre étude. L'intérêt de cette approche est de définir un niveau de redondance adapté aux contraintes de l'application. On propose que le nombre d'équipements redondants soit fonction d'un niveau de SIL (Safety Integrity Level, IEC 61508) prédéterminé. Aussi, la stratégie vise à mettre en place une procédure passive en envoyant autant de messages que d'arbres définis. Le but est que si un chemin est défectueux, le destinataire reçoit les informations par au moins un des autres chemins. De cette manière, les communications entre équipements réseau seront interrompues uniquement si les chemins sur la totalité des arbres subissent une défaillance simultanée.

B. Analyse de fiabilité pour des chemins indépendants

La fonction objectif définie dans [17] correspond à la probabilité que le système (le réseau) soit défaillant. Nous allons analyser la fiabilité du réseau en considérant dans un premier temps des chemins indépendants. Pour cela, définissons α_i comme étant le nombre de branches composant le chemin c_i et λ le taux de défaillance pour tout équipement réseau. La probabilité de défaillance concernant un chemin est donnée par (1). La probabilité de défaillance du système, c'est-à-dire que tous les chemins soient défaillants est donnée par (2), avec j représentant le nombre de chemins ($j \geq 1$).

$$P_{D_1} = 1 - (1 - \lambda)^{\alpha_1} = 1 - \omega^{\alpha_1} \quad (1)$$

$$P_{D_j} = \prod_{i=1}^{j} 1 - \omega^{\alpha_i} \quad (2)$$

La probabilité de défaillance est sélectionnée à partir des spécifications SIL de la norme IEC 61508 selon un fonctionnement en mode continu. Le contexte de ce travail est de fiabiliser une architecture Ethernet industriel. Le niveau de SIL dépend des contraintes applicatives. On utilise généralement pour un SCR des niveaux de SIL d'ordres 3 ou 4 (aviation, plate-forme nucléaire, etc.). Nous nous placerons dans le cas où les équipements réseau seront SIL 4 (avec $\lambda = 10^{-8}$). Le but est alors d'évaluer l'architecture globale du réseau en fonction du niveau de SIL retenu. La figure 9 présente les probabilités de défaillances estimées par (2) en fonction du nombre d'équipements composant les chemins et ce, pour 3 niveaux de redondance. A noter que pour l'étude, nous avons pris une symétrie parfaite concernant la longueur des différents chemins.

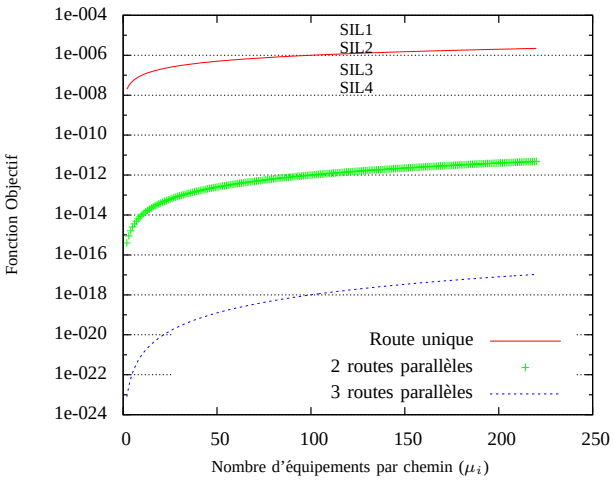


FIGURE 9. Analyse de fiabilité pour des chemins indépendants

La première observation qui peut être faite, est que la probabilité de fonctionnement du réseau se dégrade rapidement avec l'utilisation d'un chemin unique. La seconde remarque est qu'il n'est pas nécessaire de définir plus d'un chemin redondant (soit deux au total), puisque nous respectons les conditions définies par le niveau SIL 4 et ce, jusqu'à atteindre 10001 équipements sur les chemins respectifs. Ce nombre semble largement suffisant pour l'interconnexion de SCR. De plus, multiplier les routes a un impact sur le coût de la solution mise en œuvre (bande-passante, liens, etc.) La conclusion est telle qu'une architecture réseau implémentant deux chemins parallèles est un compromis acceptable fiabilité/coût.

C. Contiguïté entre chemins

Dans cette section, l'impact de la contiguïté sur le réseau est étudié. Pour cela, nous considérons un réseau composé de deux chemins non indépendants. Définissons α_i comme étant le nombre d'équipements réseau composant le chemin c_i et non communs à l'autre chemin, et β comme étant le nombre d'équipements communs aux deux chemins. La longueur totale d'un chemin c_i sera ainsi équivalente à $\mu_i = \alpha_i + \beta$. En nous appuyant sur l'équation (2), il est possible de déterminer la probabilité de dysfonctionnement du système, représenté par (3), avec P_S correspondant à la probabilité de succès du système (le réseau).

$$P_D = 1 - P_S = 1 - \left[1 - \left[1 - \omega^{\alpha_1}\right]\left[1 - \omega^{\alpha_2}\right]\right]\omega^{\beta} \quad (3)$$

La figure 10 illustre les probabilités de défaillances estimées par notre fonction objectif (3) en fonction de la longueur des chemins et de la proportion d'équipements en commun entre chemins (β/μ). L'observation qui peut-être faite ici est qu'il suffit d'un équipement en commun sur les deux chemins, pour que la probabilité de défaillance soit d'ordre SIL 3 environ. La conclusion est qu'il est impératif d'éviter toute contiguïté entre chemins.

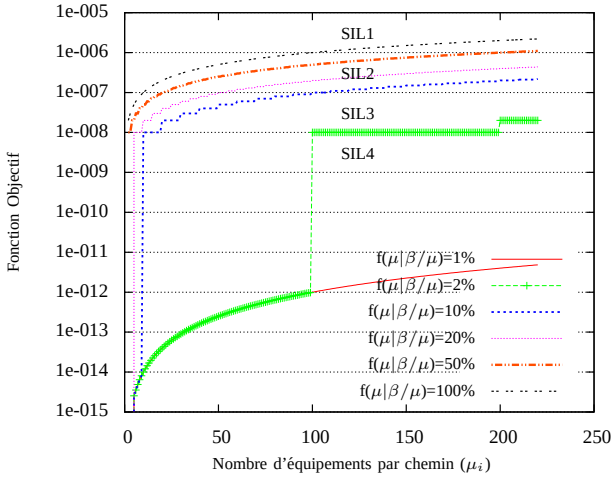


FIGURE 10. Analyse de fiabilité pour deux chemins (*non indépendants*)

D. Critère d'optimisation

Le problème à résoudre consiste à trouver la paire d'arbre permettant de minimiser la fonction objectif (3), c'est-à-dire de minimiser la probabilité de défaillance de la paire de chemins. L'analyse développée dans [30], nous amène à écarter les approches dites exhaustives car elles posent le problème de l'explosion combinatoire. Nous allons plutôt nous pencher sur des heuristiques.

E. Simulations

Le but de ce paragraphe est de montrer l'intérêt de nos travaux sur un SCR simulé sous Opnet. Un module permettant de réaliser la partie contrôleur, actionneur, capteur a été développé sous Opnet. Il s'agit du même système qu'étudié précédemment à la figure 6. Les équations caractéristiques sont ainsi :

$$P(s) = \frac{2}{(s+5)(s+0,2)}, \qquad C(s) = \frac{0.5508s + 0.4529}{s}$$

La plate-forme réseau étudiée est illustrée à la figure 11, elle est composée de 31 nœuds et 56 branches. Les équipements du SCR (contrôleur, capteur, actionneur) sont respectivement reliés aux commutateurs 20, 5 et 11. Le temps de cycle automate est de 2 ms, les équipements envoient des paquets de 64 octets toutes les 1 ms. L'étude se décompose en deux phases, la première sera dédiée à l'analyse de la plateforme via une solution classique (STP). Puis on procédera à la mise en place de la meilleure paire de chemins sur nos VLAN respectifs. Il est à noter que nous utiliserons le protocole RSTP lors de l'étude. Par nécessité de clarté concernant les arbres couvrant, nous représenterons uniquement les liens faisant partie des chemins reliant nos équipements du SCR.

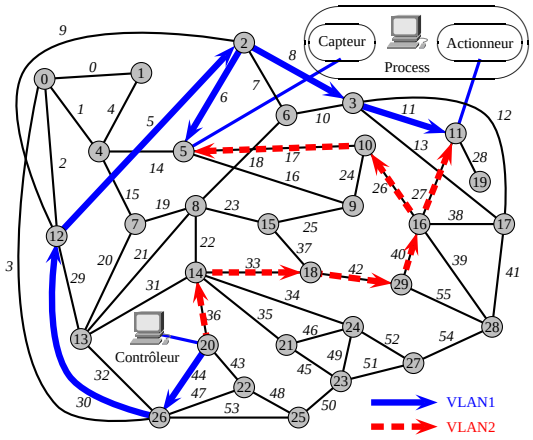


FIGURE 11. Plate-forme de l'étude

L'arbre couvrant défini par défaut par STP utilise les liens $3, 2, 5, 8, 11, 1, 14$ afin de relier le contrôleur, l'actionneur et le capteur. Nous procédons à $t = 115s$ à une défaillance du lien 8. La figure 12 représentative du SCR, montre que la réponse du système $y(t)$ ne suit plus la consigne du fait des informations non reçues par l'actionneur. Le SCR redevient stable lorsque le réseau a terminé la reconfiguration d'un nouvel arbre, c'est-à-dire à $t = 120s$.

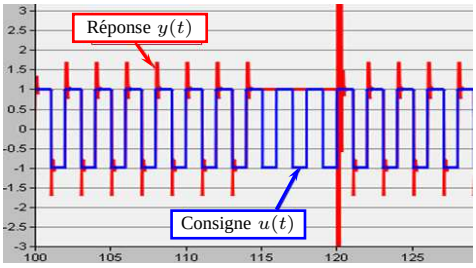


FIGURE 12. Solution classique (Sans Multi-VLAN)

Cette nouvelle étude se base sur la technique de duplication de paquets sur une paire de chemins obtenue *via* une heuristique basée sur les algorithmes génétiques [17]. La figure 11 présente la paire retenue. Nous procédons dans un premier temps à une défaillance sur le lien 6 à $t = 110s$. Cette dernière empêche alors les messages envoyés par le capteur de parvenir jusqu'au contrôleur via le VLAN1. La figure 13 montre que cela ne perturbe nullement le système du fait que l'acheminement de ces mêmes messages peut se faire via le VLAN2. Nous remettons dans un second temps le lien 6 en fonctionnement, les arbres vont ainsi redevenir tels qu'ils étaient initialement. Nous procédons alors à $t = 140s$ à une rupture du lien 33 qui lui, appartient au VLAN2, coupant ainsi toute communication entre contrôleur/actionneur et capteur/contrôleur de ce VLAN. On constate encore une fois que le SCR ne s'en trouve pas perturbé du fait que les messages sont acheminés via le VLAN1. Nous remettons ensuite le lien 33 en fonctionnement, les arbres redeviennent tels qu'ils étaient initialement. Nous procédons pour finir à une rupture des liens 6 et 33 à $t = 170s$, ce qui a pour conséquence de rendre un lien de chaque VLAN défaillant en même temps. La réponse du SCR $y(t)$ devient alors instable du fait du non retour des informations du capteur au contrôleur, mais aussi du contrôleur à l'actionneur et ce, jusqu'à ce qu'un des arbres (STP) soit reconfiguré, ce qui se produit à $t = 173s$. Nous avons finalement constaté que pour rendre le SCR instable avec la solution de "duplication de paquets", il faut simultanément une rupture sur chaque VLAN, d'où l'intérêt d'avoir deux chemins les plus disjoints possibles.

Nous allons maintenant montrer l'incidence des retards sur les VLAN. Rappelons le principe de base de la méthode passive, qui est de dupliquer un message envoyé par un équipement sur les différents VLAN (VLAN1 et 2). Nous avons mis en place un trafic sur le lien 42 à $t = 130s$, afin de générer de la congestion sur le VLAN2. Cette congestion génère des retards plus importants sur les messages empruntant le chemin VLAN2 par rapport aux messages du VLAN1. Des mêmes informations sont alors reçues et traitées à des instants différents, entraînant ainsi une instabilité du SCR comme le montre la figure 14. Il faut donc ajouter des dates ou numéros à chaque message de façon à éliminer les informations "périmées". Nous avons choisi dans cette étude de numéroter les paquets. La figure 15 montre qu'avec cette solution le SCR reste stable, du fait que les équipements du SCR ne prennent plus en compte des informations dites "périmées".

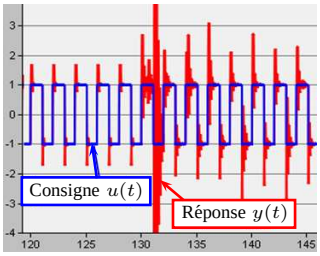


FIGURE 14. Sans numérotation

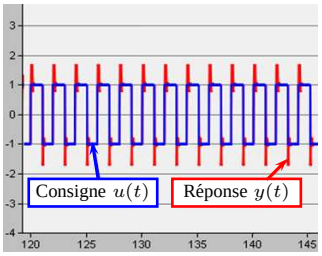


FIGURE 15. Avec numérotation

V. CONCLUSION

Parmi les différentes stratégies d'adaptation des SCR aux influences de la Qualité de Service du réseau, la « commande de réseau » est une approche pouvant permettre de

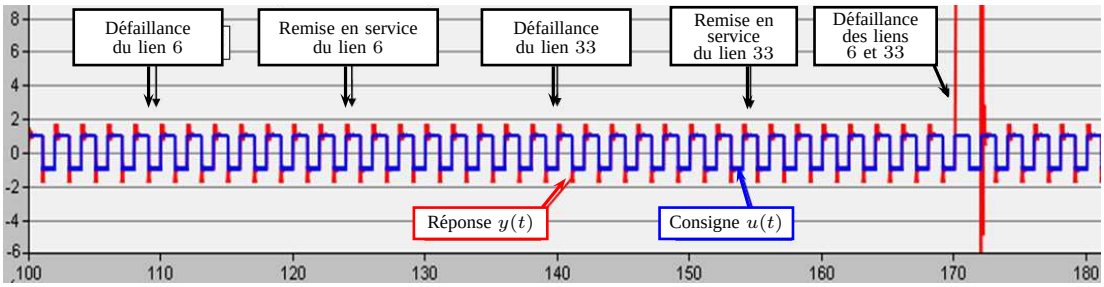


FIGURE 13. Solution Multi-VLAN

prévenir toute dégradation de performances du système. Elle a pour objectif, relativement à une QdP souhaitée, de gérer au mieux les ressources de communication (réservation de ressources, contrôle dynamique de leur allocation, flexibilisation de l'offre de service, etc.). Chaque réseau apportant ses propres caractéristiques de contrôle d'admission, d'accès et de régulation, cela implique la nécessité de développer des approches spécifiques au réseau utilisé par le SCR.

Dans cet article, des stratégies de reconfiguration d'un ordonnancement de type *weighted round robin* sont proposées pour des SCRs à base d'architectures Ethernet commutées. L'apport de cette technique d'ordonnancement équitable est de valider l'utilisation d'un réseau non déterministe comme Ethernet tout en favorisant le service rendu aux trafics non impliqués dans la commande du SCR. Cette configuration des poids, qu'elle soit adaptative ou robuste, passe par un *co-design* entre les disciplines de la commande et du réseau. Une méthode permettant d'améliorer la continuité de service sur Ethernet a été développée, basée sur une méthode passive mettant en œuvre deux arbres couvrants sur le réseau. Ces arbres couvrants sont déterminés à l'aide d'une méthode basée sur les algorithmes génétiques, pour laquelle une fonction objectif a été définie. Cette fonction évalue des paires d'arbres couvrants, d'une part en calculant le nombre de sauts de chaque chemin et d'autre part, en évaluant le nombre d'équipements communs aux deux chemins. Cette solution permet de réduire la probabilité que les applications critiques subissent des coupures de communication entraînant de longues phases de reconfiguration. À noter que l'étude menée ici peut s'étendre au cas des architectures sans fil et hybrides.

RÉFÉRENCES

[1] W. Zhang, S. Branicky, and S. Phillips, "Stability of networked control systems," *IEEE Control Systems magazine*, vol. 21, pp. 84–89, Feb. 2001.

[2] J.-P. Richard and T. Divoux, Eds., *Systèmes commandés en réseau*, ser. Traité IC2. Hermès Lavoisier, Feb. 2007.

[3] J.-P. Richard, "Time-delay systems : an overview of some recent advances and open problems," *Automatica*, vol. 39, no. 10, pp. 1667–1694, Oct. 2003.

[4] A. Lelevé and P. Fraisse, "Teleoperation over ip network : Network delay regulation and adaptive control," *Journal of Autonomous Robots, special issue "Internet and online robots"*, vol. 15, no. 3, pp. 225–235, Nov. 2003.

[5] F. Lepage, T. Divoux, and F. Michaut, "Adaptation of control parameters based on qos monitoring," in *17th International Symposium on Mathematical Theory of Networks and Systems (MTNS'06)*, Kyoto, Japan, Jul. 2006, pp. 1753–1758.

[6] R. Luck and A. Ray, "An observer-based compensator for distributed delays," *Automatica*, vol. 26, no. 5, pp. 903–908, 1990.

[7] G. Juanole and I. Blum, "Influence de fonctions de base (communication-ordonnancement) des systèmes distribués temps-réel sur les performances des applications de contrôle-commande," in *7ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'99)*, Nancy, France, Apr. 1999, pp. 217–232.

[8] J. Nilsson, "Real-time control systems with delays," Ph.D. dissertation, Lund Institute of Technology, Department of Automatic Control, Feb. 1998.

[9] Z. Huo, H. Fang, and C. Ma, "Networked control system : state of the art," in *Fifth World Congress on Intelligent Control and Automation (WCICA'04)*, vol. 2, Hangzhou, China, Jun. 2004, pp. 1319–1322.

[10] S. Li, Z. Wang, and Y. Sun, "Fundamental problems of networked control system from the view of control and scheduling," in *28th IEEE Conference of the Industrial Electronics Society (IECON'02)*, vol. 3, Séville, Espagne, Nov. 2002, pp. 2503–2508.

[11] Y. Tipsuwan and M.-Y. Chow, "Control methodologies in networked control systems," *Control Engineering Practice*, vol. 11, pp. 1099–1111, 2003.

[12] S. Zampieri, "Trends in networked control systems," in *Proceedings of the 17th IFAC World Congress*, Séoul, Corée du Sud, Jul. 2008, pp. 2886–2894.

[13] G. Juanole and G. Mouney, "Real time distributed systems : Qos and impact on the performances of process control applications," in *Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems*, Kyoto, Japan, Jul. 2006, pp. 1739–1746.

[14] J. Yook, D. Tilbury, and N. Soparkar, "A design methodology for distributed control systems to optimize performance in the presence of time delays," *International Journal of Control*, vol. 74, no. 1, pp. 58–76, Jan. 2001.

[15] G. Walsh, H. Ye, and L. Bushnell, "Stability analysis of networked control systems," *IEEE Transactions on Control Systems Technology*, vol. 10, no. 3, pp. 438–446, May 2002.

[16] K. Lee, S. Lee, and M. Lee, "Qos-based remote control of networked control systems via profibus token passing protocol," *IEEE Transactions on Industrial Informatics*, vol. 1, no. 3, pp. 183–191, Aug. 2005.

[17] S. Kubler, E. Rondeau, and J.-P. Georges, "Dependability of switched network architectures for Networked Control Systems," in *Dependability of switched network architectures for Networked Control Systems*, Istanbul, Turquie, Apr. 2011, p. CDROM. [Online]. Available : http ://hal.archives-ouvertes.fr/hal-00586758/en/

[18] IEEE Computer Society, "Ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 3 : Carrier sense multiple access with collision detection (csma/cd) access method and physical layer specifications," IEEE standard 802.3, Edition 2002, 2002.

[19] S. Kubler, "Continuité de service sur ethernet industriel," Master's thesis, Université Henri Poincaré, Nancy 1, Centre de Recherche en Automatique de Nancy, 2009.

[20] M. Alves, E. Tovar, and F. Vasques, "Ethernet goes real-time : a survey on research and technological developments," Groupe de recherche IPP-HURRAY, Polytechnic Institute of Porto (ISEP-IPP), Tech. Rep. HURRAY-TR-2K01, Jan. 2000.

[21] I. Diouri, C. Berbra, J.-P. Georges, S. Gentil, and E. Rondeau, “Evaluation of a switched ethernet network for the control of a quadrotor,” in *16th Mediterranean Conference on Control and Automation (MED’08)*, Ajaccio, France, Jun. 2008, pp. 1112–1117.

[22] IEEE Computer Society, “Ieee standards for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - common specifications - part 3 : Media access control (mac) bridges,” ANSI/IEEE Std 802.1D, Edition 1998, Dec. 1998.

[23] ——, “Ieee standards for local and metropolitan area networks - virtual bridged local area networks,” IEEE standard 802.1Q, Edition 2003, 2003.

[24] J. Jasperneite, P. Neumann, M. Theis, and K. Watson, “Deterministic real-time communication with switched ethernet,” in *4th IEEE International Workshop on Factory Communication Systems (WFCS’02)*, Västerås, Suède, Aug. 2002, pp. 11–18.

[25] J.-P. Georges, T. Divoux, and E. Rondeau, “A formal method to guarantee a deterministic behaviour of switched Ethernet networks for time-critical applications,” in *IEEE Conference on Computer Aided Control Systems Design (CACSD’04)*, Taipei, Taiwan, Sep. 2004, pp. 255–260.

[26] J. Grieu, “Analyse et évaluation de techniques de commutation ethernet pour l’interconnexion des systèmes avioniques,” Ph.D. dissertation, Institut National Polytechnique de Toulouse, Ecole doctorale informatique et télécommunications, Sep. 2004.

[27] C. Aubrun, B. Brahimi, J.-P. Georges, G. Juanole, G. Mouney, X. Nguyen, and É. Rondeau, *Co-design approaches for dependable networked control systems*. ISTE Ltd et John Wiley & Sons, Apr. 2010, ch. QoC-aware dynamic network QoS adaptation, pp. 105–147.

[28] N. Vatanski, J.-P. Georges, C. Aubrun, E. Rondeau, and S.-L. Jämsä-Jounela, “Networked control with delay measurement and estimation,” *Control Engineering Practice*, vol. 17, no. 2, pp. 231–244, Feb. 2009.

[29] I. Diouri, J.-P. Georges, and E. Rondeau, “Adaptation of scheduling policy parameters to control networked systems,” in *3nd International NeCST IFAC Workshop on Networked Control Systems : Tolerant to Faults (NECST’07)*, Nancy, Jun. 2007.

[30] G. Jayavelu, S. Ramasubramanian, and O. Younis, “Maintaining colored trees for disjoint multipath routing under node failures,” *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 346–359, 2009.

[31] S. Limal, S. Potier, B. Denis, and J.-J. Lesage, “Formal verification of redundant media extension of ethernet powerlink.” in *Proceedings of 12th IEEE Conference on Emerging Technologies and Factory Automation*, Patras, Grèce, 2007.