Une approche pour des capteurs d'alarmes intelligents dans les réseaux

Renée Boubour, Claude Jard

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Une approche pour des capteurs d'alarmes intelligents dans les réseaux

Renée Boubour et Claude Jard

N° 2982

Septembre 1996

THÈME 1

ISSN 0249-6399

INRIA
RENNES

Une approche pour des capteurs d'alarmes intelligents dans les réseaux

Renée Boubour et Claude Jard

Thème 1 — Réseaux et systèmes
Projet Pampa

Rapport de recherche n° 2982 — Septembre 1996 — 16 pages

Résumé : Dans le cadre de la gestion des fautes dans les réseaux de télécommunication, nous proposons une approche nouvelle, utilisant des outils et méthodes développés pour l'observation et la vérification dans le domaine des systèmes répartis. Nous utilisons notamment les réseaux de Petri et les ordres partiels pour exprimer les causalités existantes entre pannes et alarmes. Nous exposons notre démarche et définissons un modèle de propagation des pannes et des alarmes.

Mots-clé : réseaux de télécommunication, gestion des fautes, corrélation d'alarmes, ordres partiels, réseaux de Petri.

(Abstract: pto)

Ce travail a bénéficié du soutien de France Télécom/CNET.

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu, 35042 RENNES Cedex (France)
Téléphone : (33) 99 84 71 00 – Télécopie : (33) 99 84 71 71

Towards intelligent sensors in networks

Abstract: This paper presents a new approach to fault management in telecommunication networks. It is based on distributed system experience. We define a model of faults and alarms propagation, using partial orders and Petri nets.

Key-words: telecommunication network, fault management, alarm correlation, partial orders, Petri nets

1 Introduction

La croissance actuelle, en taille et en complexité, des réseaux de télécommunication explique l'intérêt grandissant pour les questions de gestion. Parmi les différentes fonctions d'un système de gestion, nous portons une attention particulière à la question de gestion des alarmes et au diagnostic des pannes, qui apparaît une des plus délicates. Les notions de causalité et de corrélation d'alarmes, dans une acception large, y jouent un rôle central et sont actuellement abordées sous divers angles. Au vu de l'importance d'une prise en compte du caractère réparti des phénomènes, nous proposons ici un éclairage nouveau, à travers des outils et méthodes développés pour l'observation et la vérification dans le domaine des systèmes répartis. L'objectif visé est la distribution de la fonction de diagnostic sur les capteurs d'alarmes.

Il s'agit essentiellement dans cet article d'exposer une démarche, originale à notre connaissance, par le traitement des aspects dynamiques liés à l'occurrence des pannes et des alarmes, sans avoir à manipuler explicitement un temps global physique. Les algorithmes et expériences d'utilisation sont en cours d'étude et ne sont pas décrits ici. Nous présentons le contexte de gestion de réseaux et un état de l'art essentiellement axé sur la corrélation d'alarmes. Cela permet, dans le paragraphe suivant, de situer le travail et de présenter l'approche choisie. Enfin, nous exposons les modélisations proposées et les solutions envisagées.

2 Contexte et état de l'art

2.1 Gestion des pannes et alarmes

La gestion de réseaux est actuellement admise comme étant fonctionnellement indépendante et logiquement séparée de la transmission des données proprement dite, même si elle peut utiliser les mêmes ressources physiques. Cinq aires fonctionnelles de gestion sont définies ; à savoir la gestion des fautes (ou pannes), de la sécurité, des configurations, des performances, et de la comptabilité. Nous nous intéressons ici à la gestion des pannes.

C'est une question complexe. L'aspect intrinsèquement réparti, à la fois dans l'espace et dans le temps, des manifestations de pannes dans les réseaux, augmente la combinatoire des problèmes. Par ailleurs, il faut prendre en compte des phénomènes de déformations des pannes lors des signalisations.

Les travaux actuels sur le sujet font apparaître plusieurs préoccupations. D'abord, l'importance de tenir compte des cas de pannes générant des occurrences d'alarmes potentiellement indépendantes entre elles. Ensuite, le besoin de manipulation du temps, sous forme de dates d'occurrences, d'intervalles ou de précédence dans un temps logique. Le besoin de distribuer la gestion revient aussi souvent, dû à la taille de plus en plus grande des réseaux, ainsi qu'à la variété grandissante des fonctions.

2.2 Corrélation d'alarmes

Une panne est susceptible de déclencher une cascade d'alarmes. [14] souligne que, typiquement, plusieurs problèmes peuvent apparaître simultanément dans un réseau, engendrant une grande quantité d'alarmes. Le grand volume de données, leur fréquence de consultation et la complexité des réseaux modernes rend difficile le traitement efficace et adéquat de ces alarmes.

Ainsi, pour leur traitement, il est intéressant de réduire le nombre d'alarmes. [14] considère que l'ensemble des alarmes générées est fonction de la nature des problèmes, de leur localisation et de leur occurrence dans le temps, ainsi que de la configuration du réseau. La corrélation d'alarmes, qui permet de structurer dans le temps la collection des alarmes observées, est alors considérée comme une opération préliminaire à la détection de pannes dans les réseaux.

Des techniques diverses sont alors envisagées sur le thème de la corrélation d'alarmes, issues, entre autres, de manipulations de bases de données ([15]), de l'intelligence artificielle ([9]), de manipulations de graphes ([12]), de calculs de probabilités ([11]) ou de l'utilisation de réseaux de Petri ([5, 8]).

3 Principe de l'approche

3.1 Hypothèses de travail

Nous nous situons principalement dans la phase de détection des pannes à travers la corrélation d'alarmes. Le principe général de diagnostic adopté est de modéliser les observations du système en cas de mauvais fonctionnement. Il s'agit de reconnaître parmi les situations observées, celles qui correspondent à des situations répertoriées. L'expression doit être assez souple pour prendre en compte diverses incertitudes (temporelles, de connaissance, d'observation).

Dans le but d'analyser les alarmes et de diagnostiquer les pannes, il est nécessaire de fixer une représentation du réseau de télécommunication ainsi que celle du réseau de gestion associé. Le principe de diagnostic étant observationnel, nous faisons un minimum d'hypothèses sur les aspects fonctionnels du réseau. Nous nous attachons davantage à des définitions aussi précises que possible des notions de pannes et alarmes et des liens existant entre elles.

Un réseau est considéré comme un ensemble de composants matériels et logiciels interconnectés, appelés de façon générique « éléments de réseaux ». Il est représenté par un graphe dont les nœuds sont les composants et les arcs leurs interconnexions.

Nous faisons l'hypothèse qu'existe un ensemble de moyens, dans le réseau de gestion des télécommunications, permettant la gestion centralisée des alarmes (avant d'aborder une phase distribuée). Nous appelons « capteur » un agent du réseau de gestion (cf [1]),qui reçoit

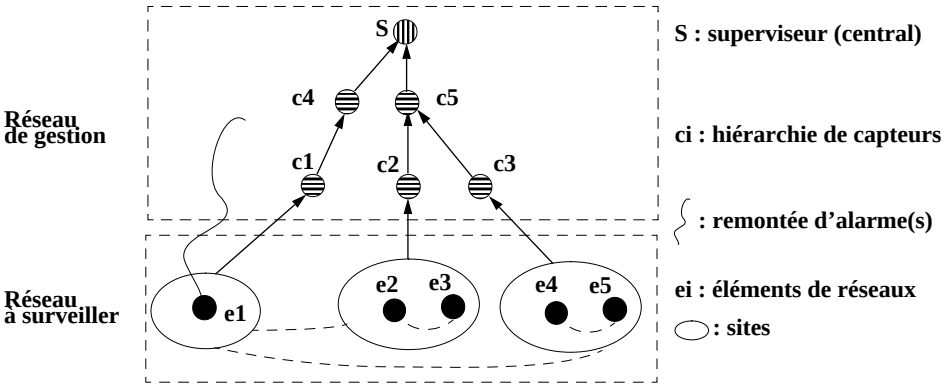

FIG. 1 – *Exemple de configuration de sites et de capteurs*

les notifications d'alarmes, ce qui permet de stocker des alarmes dans les bases d'informations de gestion. Notre mécanisme de corrélation a naturellement sa place dans les discriminateurs de retransmission d'événements de la fonction de gestion des rapports d'événements ([3]), qui est utilisée pour la fonction de signalisation d'alarmes ([2]). Nous appelons « superviseur » un gestionnaire capable de traiter les sorties des discriminateurs du réseau de gestion.

Le réseau de gestion est alors vu ici comme un ensemble de capteurs d'alarmes et de chemins de remontées des alarmes entre ces capteurs et vers un superviseur central. Les capteurs peuvent être des timers, des compteurs d'occurrences qui positionnent des attributs dans la base d'informations de gestion. Ces capteurs peuvent aussi envoyer spontanément des messages signalant les alarmes, entre eux ou à un superviseur. Nous considérons connu un ensemble de capteurs et leur placement sur le réseau de trafic de données. Un capteur est associé à un site ; un site représentant un élément de réseau ou un groupe d'éléments de réseaux proches physiquement.

La figure 1 donne un exemple de configuration de sites et de capteurs. Les rectangles pointillés délimitent le niveau de transmission de données et celui de la gestion du réseau. Les éléments de réseau sont numérotés e1 à e5 et les ovales noirs font apparaître les sites considérés. Les capteurs sont numérotés de c1 à c5 et le superviseur est dénoté par S.

3.2 Démarche

L'idée de base est d'exploiter des méthodes déterministes développées dans le domaine des applications réparties, puis de les étendre avec des méthodes probabilistes. Nous ne traitons, dans cet article, que le cas déterministe. C'est notamment dans le cadre de l'observation de comportements et de la vérification de propriétés d'exécutions réparties que ces techniques ont été explorées. Elles offrent des moyens de modéliser des comportements répartis, à l'aide d'ordres partiels, et d'effectuer des traitements algorithmiques distribués et à la volée sur des observations [7, 10].

Les apports espérés pour le diagnostic de pannes dans les réseaux de télécommunication sont de deux ordres. Tout d'abord, une prise en compte de l'aspect intrinsèquement réparti des réseaux à travers la notion de causalité. Celle-ci va faire explicitement partie du modèle, au lieu du résultat d'un effet de bord, dû à des relations temporelles exprimées dans un temps physique global, comme c'est généralement le cas dans les approches actuelles. Ensuite, il existe des techniques permettant de distribuer la fonction du superviseur sur les capteurs répartis ; ceux-ci se coordonnent pour émettre un diagnostic. L'intérêt de la décentralisation est de rendre la supervision moins dépendante de l'état de fonctionnement global du système. C'est ce que nous exprimons par le terme « capteurs intelligents ».

En plus de la notion de causalité, nous prenons explicitement en compte les éventualités de pannes multiples à travers la concurrence. De même, il semble intéressant de prendre en compte d'emblée l'aspect ordre partiel sur les alarmes, qui reflète ici la notion de précédence dans un temps logique. Nous nous fondons pour cela sur des réseaux de Petri et des ordres partiels étiquetés. Une probabilisation du modèle permet d'affiner la modélisation des phénomènes et de prendre en compte les aspects aléatoires.

Nous souhaitons développer une détection à la volée, par la reconnaissance incrémentale de motifs appartenant à une famille d'ordres dans l'observation. La distribution de la détection sur les capteurs du réseau de gestion est ensuite envisagée. Ces capteurs seront ainsi capables, en coopérant, de réaliser une partie du processus d'analyse d'alarmes et de diagnostic de pannes.

Les incertitudes les plus importantes, à la fois en terme de fréquence et d'impact, sur les pannes sont liées aux masquages et pertes d'alarmes. Nous indiquons sous quelle forme est envisagé le diagnostic, notamment avec l'utilisation d'algorithmes probabilistes basés sur le modèle.

4 Description des pannes et alarmes

4.1 Alarmes

Une alarme désigne un symptôme de dysfonctionnement ou de déviation, elle est observable et peut être associée à plusieurs pannes.

Les alarmes peuvent se propager. C'est-à-dire qu'une signalisation faite par un élément de réseau va déclencher potentiellement d'autres signalisations, à plus forte raison si l'état de panne sous-jacent se propage. Nous utilisons alors le terme de dépendances entre alarmes. Ces dépendances sont interceptées au niveau du système de gestion, à l'aide des capteurs placés sur le réseau.

Un ensemble d'alarmes et leurs dépendances sont représentées à l'aide d'un d'ordre partiel étiqueté sur les alarmes, soit un « motif d'alarmes ».

La figure 2 donne six exemples de motifs d'alarmes. Un motif peut contenir des alarmes toutes indépendantes (comme A_8), ou dépendantes (comme A_5), ou être vide (comme A_2)

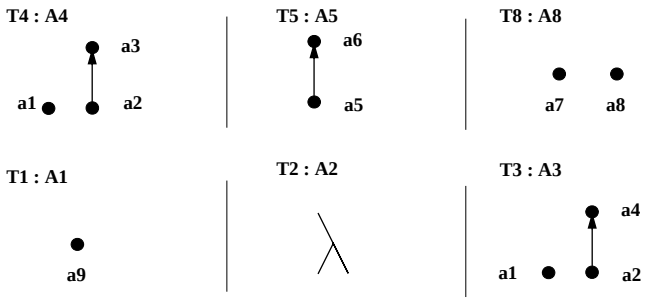

FIG. 2 – *Six exemples de motifs d'alarmes*

noté alors λ. Deux motifs peuvent également avoir des alarmes en commun (comme A_3 et A_4).

4.2 Pannes

Une panne désigne un dysfonctionnement ou une déviation de bon fonctionnement, elle n'est pas observable directement mais peut provoquer plusieurs (voire beaucoup) d'alarmes dispersées dans le réseau.

Les pannes peuvent se propager. C'est-à-dire qu'un dysfonctionnement sur un élément de réseau donné peut causer un dysfonctionnement sur des éléments de réseau qui lui sont connexes pour une raison quelconque (jeu de pile de protocoles, processus pair, relation de contenance par exemple). Nous utilisons alors le terme de causalité entre pannes. Nous considérons également qu'il peut exister une causalité entre deux pannes sans que des alarmes n'apparaissent entre elles.

Les réseaux de Petri permettent d'exprimer des liens de causalité de natures diverses entre les pannes La relation de causalité entre pannes est alors représentée à l'aide d'un « réseau de pannes ». Les configurations élémentaires de liens de causalité possibles entre pannes sont répertoriées dans la figure 3, où les pannes sont représentées par les cercles et les transitions entre pannes par des rectangles

La figure 4 donne un exemple de réseau de pannes. La présence de cycles dans le réseau de pannes représente le retour spontané du réseau de télécommunication à une situation plus normale.

Les réseaux de pannes sont donc des réseaux de Petri finis, ordinaires, c'est-à-dire qu'il n'y a pas de pondération de la dépendance, et étiquetés sur les transitions par un alphabet (de motifs d'alarmes).

Nous considérons qu'un lien de causalité entre pannes, soit une transition, est identifié par un ensemble d'alarmes (éventuellement vide) et que cet ensemble est structuré et forme

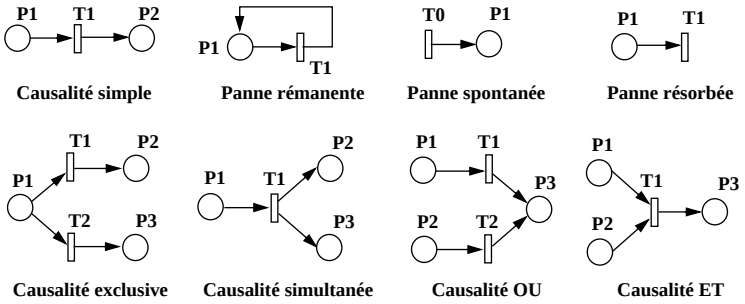

FIG. 3 – *Configurations élémentaires de liens de causalité*

un « motif d'alarmes ». Nous notons A_i le motif d'alarmes associé à la transition T_i. Par ailleurs, nous faisons l'hypothèse qu'un ensemble d'alarmes donné répertorie les phénomènes observables lors d'une transition entre pannes.

4.3 Pertes et masquages d'alarmes

Dans un réseau non sécurisé, les mêmes ressources physiques peuvent être utilisées à la fois pour l'écoulement du trafic et pour la gestion du réseau. Dans un tel réseau, lorsqu'un composant tombe en panne, il est susceptible de bloquer la remontée de paquets d'alarmes, provoquant ainsi des « masquages d'alarmes ». C'est le mode de fonctionnement du réseau qui provoque le masquage. Cela porte d'autant plus à conséquence que le réseau de gestion est organisé de façon hiérarchique et que la gestion est centralisée.

En cas de saturation du réseau de télécommunication (voire du réseau de gestion), des tampons pleins peuvent provoquer des pertes d'alarmes. Cela s'explique notamment par

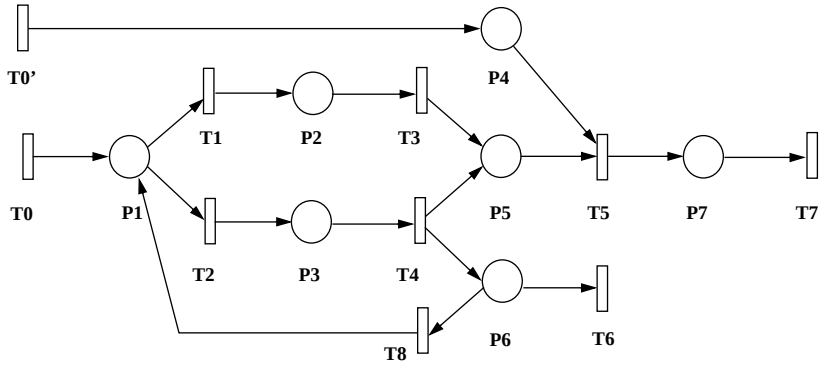

FIG. 4 – *Exemple de réseau de pannes*

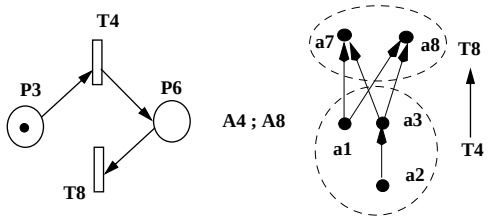

FIG. 5 – *Concaténations de motifs d'alarmes*

le fait que les informations de gestion ont généralement une priorité moindre sur le trafic de données. Ces pertes d'alarmes induisent des « trous » dans les observations. Les pertes d'alarmes sont considérées comme étant indépendantes les unes des autres. Elles sont en revanche naturellement dépendantes de l'état de fonctionnement du réseau.

5 Utilisation du réseau de pannes étiqueté

Le réseau de pannes représente les causalités entre les pannes susceptibles de se produire dans le réseau de télécommunication. Les motifs d'alarmes qui étiquettent les transitions du réseau de pannes représentent les symptômes attendus, avec leurs dépendances et indépendances.

5.1 Dynamique et sémantique du réseau de pannes

En appliquant la dynamique standard des réseaux de Petri au réseau de pannes, nous décrivons les observations attendues, lors de dysfonctionnements du réseau de télécommunication.

L'enchaînement de pannes dans un réseau de télécommunication implique l'enchaînement des alarmes dans le réseau de gestion. Cela induit des dépendances entre les alarmes des motifs concernés. La figure 5 donne un extrait du réseau de pannes et la concaténation de deux motifs : les motifs A_4 et A_8 associés respectivement aux transitions t_4 et t_8 qui peuvent se déclencher en séquence.

La notion de sémantique de réseau considérée ici est celle de sémantique comportementale, c'est-à-dire qu'elle se définit par une description des exécutions que peut effectuer le réseau. Le sens donné au réseau de pannes étiqueté est alors défini par la famille d'ordres partiels sur les alarmes qu'il décrit, elle est notée $\mathcal{F}_{oa}$.

Nous avons besoin d'exprimer explicitement la concurrence entre pannes. Pour définir la sémantique de réseau de pannes, nous nous appuyons donc sur les sémantiques d'ordres partiels des réseaux de Petri, et non sur les sémantiques d'entrelacements généralement considérées. La figure 6 illustre cela par l'exemple de deux réseaux de Petri qui sont équiva-

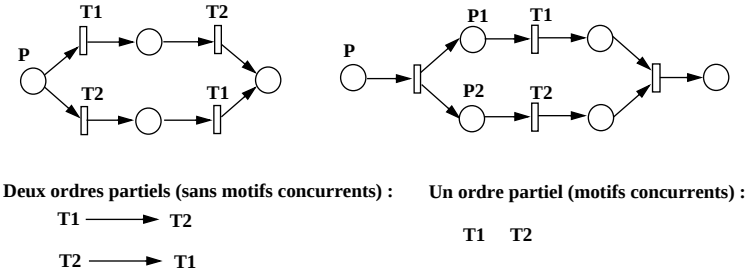

FIG. 6 – *Illustration de sémantique d'ordres partiels de réseaux de Petri*

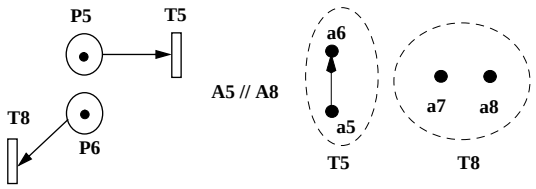

FIG. 7 – *Illustration de l'entrelacement de motifs d'alarmes*

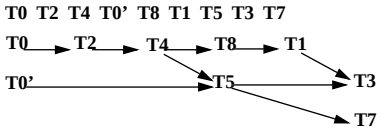

FIG. 8 – *Séquence de transitions et ordre partiel associé*

lents du point de vue des séquences de transitions, mais qui sont distingués par les ordres partiels sur les transitions qu'ils admettent.

La concurrence de pannes signifie que les alarmes des motifs concernés se produisent de façon indépendante. Les motifs concurrents seront donc observés « entrelacés ». La figure 7 présente un extrait du réseau de pannes et la composition parallèle représentant l'entrelacement de deux motifs d'alarmes associés à des transitions qui peuvent être tirées simultanément dans le réseau.

La famille $\mathcal{F}_{oa}$ est alors décrite grâce à un algorithme de construction d'exécutions de réseau de Petri, qui prend en compte explicitement la structure du réseau. On associe pour cela au réseau de pannes un réseau de Petri équivalent qui est sauf et T-restreint. Pour ce type de réseaux, la constuction d'exécutions est connue et prouvée correcte ([4]). Cette construction associe à une séquence de transitions un ordre partiel sur ces transitions.

La figure 8 donne un exemple de séquence et l'ordre partiel associé.

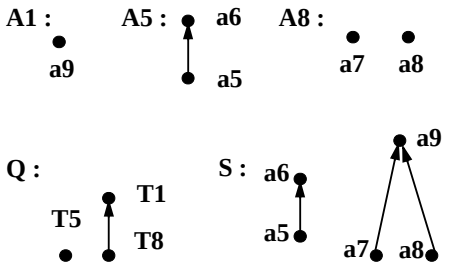

FIG. 9 – *Exemple de substitution de transitions par leur motif d'alarmes*

L'ordre partiel sur les alarmes associé à une exécution est obtenu en substituant les transitions par les motifs d'alarmes. La figure 9 illustre la substitution des éléments T_1, T_5 et T_8 de Q respectivement par les ordres partiels A_1, A_5, A_8 pour obtenir S.

Le modèle ainsi établi permet de synthétiser l'ensemble des spécifications données par l'utilisateur. C'est-à-dire qu'il contient à la fois l'ensemble des pannes, et leur relation de causalité, à travers les places et transitions ; et les motifs d'alarmes, avec leurs dépendances et indépendances, sur les transitions.

Cet exemple fait apparaître également du non-déterminisme entre des évolutions possibles à partir d'un même état de panne, par exemple pour la panne P_1 et les cas de pannes multiples, comme P_5 et P_6.

5.2 Prise en compte des masquages d'alarmes

La prise en compte des masquages se fait directement au niveau du modèle de propagation, en y intégrant des évolutions du réseau en fonction de ses modes de fonctionnement possibles. Cela permet, à partir d'un état de panne donné, d'exprimer plusieurs observations attendues selon que des masquages peuvent se produire ou non. La probabilisation du réseau de pannes permet de discriminer, lors de la détection de pannes, entre les évolutions possibles selon les alarmes observées.

6 Détection de pannes

Le principe est de placer en entrée du superviseur des informations (ici des occurrences d'alarmes et des dépendances), obtenues par des capteurs placés sur le réseau, pour fournir des diagnostics de pannes.

En utilisant des techniques développées dans le cadre d'exécutions réparties [6, 13], nous pouvons envisager la capture d'informations de précédence causale, par estampillage dans la couche de gestion par exemple. Nous excluons d'emblée l'intrusion dans le trafic du réseau de

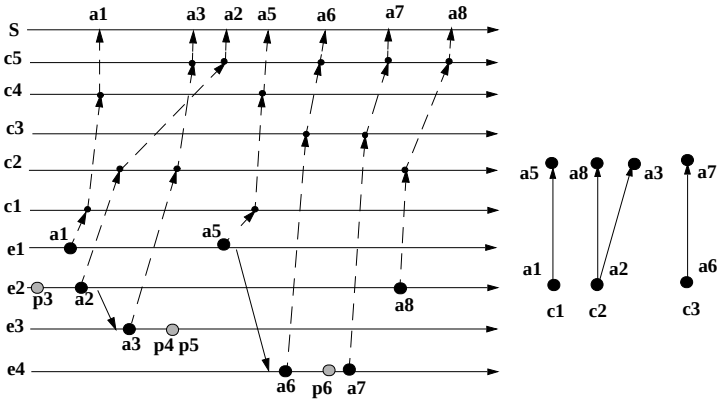

FIG. 10 – *Exemple d'observation fournie par les capteurs*

télécommunication, pour des raisons de coût ; c'est pourquoi nous nous basons uniquement sur les informations que peut apporter la couche de gestion.

6.1 Observations

Pour chaque site (un élément de réseau ou un groupe d'éléments de réseau) un capteur observe les alarmes produites. Les capteurs produisent chacun un ordre, contenant des alarmes produites sur le site associé. C'est cet ensemble d'ordres qui est fourni en entrée du superviseur. Nous notons $Y = \{C_k\}$ l'ensemble des ordres fournis par les capteurs.

La figure 10 présente un résultat possible d'observation par les capteurs c1, c2 et c3 de la figure 1. Les éléments de réseaux (e1 à e4) et le superviseur (S) sont figurés par des horizontales. Les ronds noirs figurent des alarmes produites. Les ronds grisés figurent des pannes, non observables. Les flèches obliques figurent des échanges de messages entre les éléments de réseau. On a $Y = \{C_1, C_2, C_3\}$. Nous faisons l'hypothèse que les alarmes sont observées par les capteurs c1, c2 et c3 dans un ordre cohérent avec l'ordre dans lequel elles se sont produites sur chaque site. Dans le cadre d'un système de gestion centralisée, elles sont ensuite transmises au superviseur S par l'intermédiaire des capteurs c4 et c5.

Sous l'hypothèse que les capteurs ordonnent correctement les alarmes, l'ensemble des ordres observés est inclus dans l'ordre qui contient toutes les dépendances entre alarmes, telles qu'elles se sont produites. Cette inclusion est généralement stricte, puisque les dépendances entre alarmes se produisant sur différents sites du réseau de télécommunication ne peuvent pas raisonnablement être observées par les capteurs du réseau de gestion.

6.2 Reconnaissance

Le principe de la reconnaissance consiste à déterminer si les observations d'alarmes et de leurs dépendances révèlent l'occurrence d'un (ou de plusieurs) ordres partiels sur des alarmes défini(s) par le réseau de pannes, à travers les motifs d'alarmes. Dans le cas d'une spécification parfaite et d'une observation idéale, la relation entre un ordre défini par le réseau de pannes et l'ensemble d'ordres fourni par les capteurs est une relation d'extension d'ordre. En effet, la spécification peut contenir des dépendances entre des alarmes de sites distincts. En revanche, pour les raisons évoquées ci-dessus, les capteurs ne pourront pas fournir d'information de dépendance pour des alarmes de sites distincts. Cela induit que les ordres observées contiennent moins de relations de dépendance que les ordres spécifiés à travers le réseau de pannes.

L'occurrence d'un ou de plusieurs ordres partiels de motifs d'alarmes dans un ensemble d'ordres fourni par les capteurs se traduit alors en terme d'extension d'ordre.

La question de la reconnaissance est alors :

Étant donné Y, $\exists$? $X \in \mathcal{F}_{oa}$ tel que X étend Y.

La réponse est non dès que l'observation Y contient une dépendance contradictoire avec la spécification. Cela permet de discriminer les motifs d'alarmes.

Il s'agit alors de retrouver à quel ordre partiel sur des étiquettes de transitions du réseau de pannes l'ensemble Y des alarmes observées correspond potentiellement. La connaissance d'une séquence de transitions correspondante permettrait de retrouver, grâce à l'algorithme de construction d'exécution, l'élément X de la famille $\mathcal{F}_{oa}$.

Cette reconnaissance peut alors se baser sur l'algorithme de construction d'exécution, en recherchant des occurrences de motifs d'alarmes.

Nous pouvons envisager un traitement efficace des observations reçues, en exploitant la forme de l'information disponible. En effet, les dépendances entre capteurs ne seront pas observées, nous pouvons donc en faire abstraction lors de la recherche de motifs. La décomposition, en une portion par capteur, d'un motif permet d'extraire, pour chaque capteur, la partie du motif qui le concerne. Nous pouvons alors projeter le réseau de pannes sur les capteurs. Pour cela, la structure du réseau de pannes est dupliquée sur les capteurs ; et chacun des capteurs ne conserve pour chaque motif que la portion qui le concerne. Suite à cette projection, une synchronisation des capteurs est nécessaire pour la reconnaissance de motifs. En effet, pour un motif donné, chaque portion du motif doit être observée par le capteur concerné. Cela signifie que chacun de ces capteurs doit observer toutes les alarmes de « sa » portion du motif. Ensuite, un test de terminaison entre les capteurs leur permet de se mettre d'accord pour la détection du motif.

6.3 Prise en compte des pertes d'alarmes

Les alarmes sont susceptibles d'être perdues lors de la remontée dans le réseau de gestion. Ces pertes d'alarmes induisent des « trous » dans les ordres fournis par les capteurs, ce qui

se traduit par la notion de sous-ordre sur l'observation Y. Nous notons $Y' = \{C_k^{'}\}$ où les $C_k^{'}$ sont des observations à « trous ». La question de la reconnaissance se traduit alors par :

Étant donné Y', $\exists$? $Y, \exists$? $X \in \mathcal{F}_{oa}$ tel que
Y' est un sous-ordre de Y et X étend Y.

La question de reconnaissance est ici transformée par l'ajout d'une quantification permettant de prendre en compte toutes les pertes possibles. Nous pouvons noter que, dans le cas général, la relation entre Y' et X n'est ni une relation de sous-ordre, ni une relation d'extension d'ordre.

Par ailleurs, cette transformation de la question de reconnaissance peut aussi se ramener à une transformation du réseau de pannes. En effet, les pertes d'alarmes peuvent être exprimées en dédoublant les transitions de façon à prendre en compte les sous-ordres possibles dus aux pertes d'alarmes. La mise au point de cette transformation est en cours d'étude, car elle n'est pas ordinaire du fait qu'il faut travailler l'intérieur des étiquettes des transitions. Par ailleurs, de même que pour la perte d'alarmes, la probabilisation du modèle permet de traiter de façon souple ces approximations.

7 Diagnostic

Le diagnostic doit au minimum fournir un état courant de fonctionnement du réseau. Celui-ci est en général constitué d'un ensemble d'états courants d'éléments du réseau. De plus, nous avons vu que le non-déterminisme peut amener à considérer un ensemble d'états courants potentiels et plusieurs évolutions possibles.

L'idée est alors de fournir un graphe correspondant au dépliage de la partie du réseau de pannes parcourue lors de la reconnaissance. Nous obtenons potentiellement une succession d'états de pannes ou dégradations. En effet, il est intéressant, pour la gestion de réseaux, de connaître quels enchaînements de phénomènes ont conduit à l'état courant.

Les techniques de diagnostic utilisant les probabilités permettent de fournir un degré de validité d'un diganostic pour une observation donnée ; ainsi qu'un degré de confiance accordée au modèle vis à vis de cette observation.

Deux niveaux au moins sont envisageables pour l'introduction de probabilités dans le modèle ; à la fois pour mieux résister aux bruits (masquages et pertes d'alarmes) et mieux discriminer. D'une part, la connaissance des phénomènes du réseau permet de pondérer les liens de causalité entre pannes par la probabilité pour chaque causalité de se produire. Cette pondération de la relation de causalité permet de raffiner la discrimination entre les évolutions possibles pour le réseau. Cela permet de plus de traiter des situations dans lesquelles des masquages sont susceptibles de se produire. D'autre part, la perte d'alarmes produit une déformation de l'observation, dont il faut tenir compte lors du processus de discrimination de pannes. Cette déformation peut être s'exprime par exemple en associant à chaque alarme une probabilité d'être perdue. Lorsqu'une alarme distinguant deux motifs est perdue, la probabilité pour cette alarme d'être effectivement perdue permet de choisir le comportement effectif le plus probable du réseau. Enfin, lorsqu'une extension linéaire est

commune à deux motifs, la probabilité d'occurrence de cette extension pour chacun des motifs permettent de choisir l'évolution la plus vraissemblable.

8 Conclusions et perspectives

Nous avons proposé une vision précise des notions de pannes et alarmes dans les réseaux de télécommunication. Nous proposons une modélisation dans le cadre d'utilisation de méthodes formelles, cette approche ayant également pour but la spécialisation de savoir–faire développé dans le domaine des systèmes répartis. Cela permet notamment de considérer la notion de précédence causale dans un temps logique. Des méthodes probabilistes sont de plus utilisées pour affiner le modèle et les mécanismes.

L'algorithme de reconnaissance de motifs d'alarmes est en cours d'élaboration. Il s'appuiera sur une adaptation de l'algorithme de Viterbi au cas des pannes dans les réseaux de télécommunication.

Cet algorithme fonctionnera au vol, lors de l'observation des alarmes. Il pourra être distribué par projection sur les capteurs, par exemple en utilisant une décomposition des motifs selon les capteurs. Une synchronisation entre capteurs sera alors utilisée pour le diagnostic de pannes.

Références

[1] *X.701 - Aperçu général de la gestion des systèmes.* UIT, 1992.

[2] *X.733 - Fonction de signalisation des alarmes.* UIT, 1992.

[3] *X.734 - Fonction de gestion des rapports d'événements.* UIT, 1992.

[4] E. Best and R. Devillers. Sequential and Concurrent Behaviour in Petri Nets Theory. *Theoretical Computer Science*, (55):87–136, 1987.

[5] R. Valette et L.A. Künzle. Réseaux de petri pour la détection et le diagnostic. In GDR automatique, editor, *Journées Sûreté, surveillance, supervision : détection et localisation des défaillances*, novembre 1994.

[6] J. Fidge. Timestamps in Message Passing Systems that Preserve the Partial Ordering. In *Proc.* 11$^{\text{th}}$ *Australian Computer Science Conference*, pages 55–66, February 1988.

[7] E. Fromentin, C. Jard, G.-V. Jourdan, and M. Raynal. On-the-fly Analysis of Distributed Computations. *Information Processing Letters*, (54):267–274, 1995.

[8] M.Z. Hasan. An Active Temporal Model for Network Management Databases. In Sethi, Raynaud, and Faure-Vincent, editors, *Integrated Network Management*, number 4, pages 266–277. IFIP, Chapman and Hall, may 1995.

[9] G. Jakobson and M. D. Weissman. Real-time Telecommunication Network Management: Extending Event Correlation with Temporal Constraints. In Sethi, Raynaud, and Faure-Vincent, editors, *Integrated Network Management*, number 4, pages 266–277. IFIP, Chapman and Hall, may 1995.

[10] C. Jard, T. Jéron, G.-V. Jourdan, and J.-X. Rampon. A General Approach to Trace-Checking in Distributed Computing Systems. In 14^{th} *International Conference on Distributed Computing Systems, Poznan, Pologne*, pages 396–403. IEEE Computer Society Press, June 1994.

[11] I. Katzela, A.T. Bouloutas, and S.B. Calo. Centralized vs Distributed Fault Localisation. In Sethi, Raynaud, and Faure-Vincent, editors, *Integrated Network Management*, number 4, pages 266–277. IFIP, Chapman and Hall, may 1995.

[12] S. Kliger, S. Yemini, Y. Yemini, D. Ohsie, and S. Stolfo. A Coding Approach to Event Correlation. In Sethi, Raynaud, and Faure-Vincent, editors, *Integrated Network Management*, number 4, pages 266–277. IFIP, Chapman and Hall, may 1995.

[13] F. Mattern. Virtual Time and Global States of Distributed Systems. In Cosnard, Quinton, Raynal, and Robert, editors, *Proc. Int. Workshop on Parallel and Distributed Algorithms Bonas, France, Oct. 1988*. North Holland, 1988.

[14] Y.A. Nygate. Event Correlation using Rule and Object Based Techniques. In Sethi, Raynaud, and Faure-Vincent, editors, *Integrated Network Management*, number 4, pages 266–277. IFIP, Chapman and Hall, may 1995.

[15] O. Wolfson S. Sengupta and Y. Yemini. Managing Communication Network by Monitoring Databases. *IEEE Transactions on Software Engineering*, 17(9), Septembre 1991.

Unit´e de recherche INRIA Lorraine, Technopôle de Nancy-Brabois, Campus scientifique,
615 rue du Jardin Botanique, BP 101, 54600 VILLERS LÈS NANCY
Unit´e de recherche INRIA Rennes, Irisa, Campus universitaire de Beaulieu, 35042 RENNES Cedex
Unit´e de recherche INRIA Rhône-Alpes, 655, avenue de l'Europe, 38330 MONTBONNOT ST MARTIN
Unit´e de recherche INRIA Rocquencourt, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex
Unit´e de recherche INRIA Sophia-Antipolis, 2004 route des Lucioles, BP 93, 06902 SOPHIA-ANTIPOLIS Cedex

Éditeur
INRIA, Domaine de Voluceau, Rocquencourt, BP 105, 78153 LE CHESNAY Cedex (France)
ISSN 0249-6399