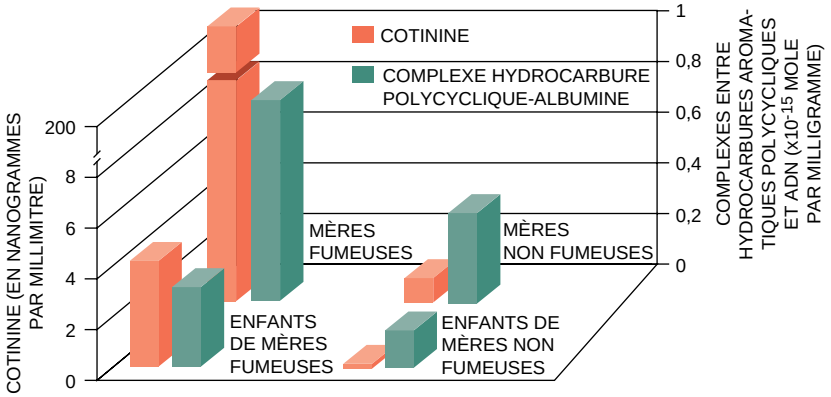


3. LE TABAGISME PASSIF augmenterait le risque que les jeunes enfants aient, un jour, un cancer pulmonaire. L'auteur et ses collègues ont montré que les concentrations en cotinine (un dérivé de la nicotine, qui est un marqueur de l'inhalation de fumée) et en complexes hydrocarbures aromatiques polycycliques-albumine (un marqueur indirect des lésions de l'ADN) étaient plus élevées chez les mères fumeuses que chez les mères non fumeuses, mais aussi chez les enfants des mères fumeuses *(histogramme de droite)*. Ces femmes fumaient moins d'un paquet de cigarettes par jour, ce qui prouve que la fumée de cigarette – même en faible quantité – est une menace pour les enfants.

fréquence des caractères génétiques qui favorisent un type particulier de cancer varie d'une population à l'autre.

De surcroît, l'âge d'une personne au moment de son exposition à un agent cancérogène est essentiel : le risque est supérieur pour les fœtus, les bébés et les enfants exposés aux agents cancérogènes de l'environnement. Toutes les études réalisées sur la pollution atmosphérique, la fumée de cigarette, les hydrocarbures aromatiques polycycliques, les pesticides, les nitrosamines, l'aflatoxine B1 et les rayonnements montrent que le risque de cancer augmente quand l'exposition aux agents cancérogènes commence au stade utérin ou pendant l'enfance. C'est sans doute parce que la période d'incubation est plus longue et que la multiplication cellulaire augmente : or, les cellules qui prolifèrent risquent plus de subir des dommages génétiques que les cellules au repos. Chez les jeunes enfants, les mécanismes d'inactivation des agents cancérogènes et de réparation des anomalies moléculaires sont moins efficaces que chez l'adulte. De plus, les enfants absorbent souvent des quantités d'agents cancérogènes plus importantes que les adultes, si l'on rapporte ces quantités à leur poids.

Ainsi, on estime que les bébés ingèrent 10 à 20 fois plus de dioxine en une journée que les adultes (par rapport à leur poids). Nous avons récemment montré que, chez des nouveau-nés d'une zone polluée de l'Europe de l'Est, la concentration sanguine en complexes ADN-hydrocarbures aromatiques polycycliques est supérieure à celle de leur mère, bien que le fœtus ne soit exposé qu'au dixième de la dose d'hydrocarbures aromatiques polycycliques absorbée par la mère. Nous avons également montré que de jeunes enfants dont les mères fumaient une dizaine de cigarettes par jour avaient des concentrations sanguines en protéines complexes hydrocarbures aromatiques polycycliques supérieures à celles des enfants nés de mères non fumeuses.

Ces études sur le cancer ont mis en évidence deux points qui auront des conséquences notables en santé publique. Tout d'abord, la plupart des cancers sont partiellement dus à l'environnement ; pour s'en protéger, on devra modifier les comportements à risques et prendre des mesures visant à réduire les expositions involontaires aux substances cancérogènes présentes dans l'air, dans l'eau, dans la nourriture et sur les lieux de travail. On estime qu'en l'absence de facteurs cancérogènes dans l'environnement, l'incidence du cancer diminuerait de 80 à 90 pour cent.

D'autre part, les agents cancérogènes présents dans l'environnement sont plus nocifs pour certains individus que pour d'autres ; pour améliorer la prévention, on devra protéger ces sujets plus vulnérables par diverses mesures, telles que des campagnes d'information ou des lois.

Aujourd'hui, les pouvoirs publics ne prennent pas en considération la disparité des susceptibilités individuelles face aux agents cancérogènes. Pour déterminer les doses d'agents cancérogènes qui entraîneraient un nombre «inacceptable» de cancers, on utilise un facteur de risques global, en admettant que toutes les personnes réagissent de la même façon à ces agents. Cette hypothèse est fausse, et la méthode actuelle sous-estime les risques pour certains groupes de la société. Ainsi, les personnes qui ont des facteurs de susceptibilité présentent dix fois plus de risques d'avoir un cancer que la population supposée «standard» et homogène.

Pour éviter d'exposer excessivement les populations sensibles (certaines ethnies, les femmes, les enfants, les vieillards), on devrait les avertir et rechercher des normes environnementales et des programmes de santé publique qui ne fassent pas courir les plus grands risques aux personnes les plus sensibles de la population.

Le meilleur traitement du cancer est sa prévention. En évitant ne serait-ce que 20 cancers sur 100, plus de 50 000 vies seraient épargnées, chaque année, en France. Les spécialistes de l'épidémiologie moléculaire pourraient faciliter l'élaboration de mesures préventives, et insister sur la nécessaire protection des plus vulnérables.

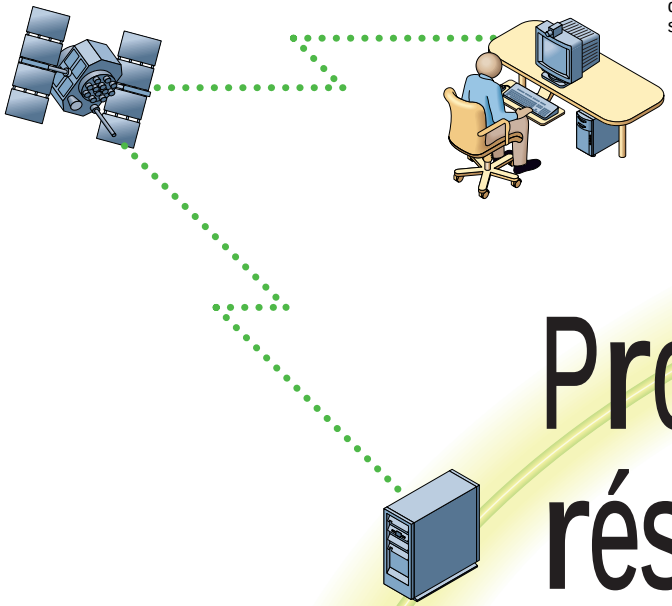
Frederica PERERA est directeur adjoint du Centre de cancérologie presbytérien, à Columbia.

F.P. PERERA et I.B. WEINSTEIN, *Molecular Epidemiology and Carcinogen-DNA Adduct Detection : New Approaches to Studies of Human Cancer Causation*, in *Journal of Chronic Diseases*, vol. 35, pp. 581-600, 1982.

Molecular Epidemiology, sous la direction de P.A. Schulte et F.P. Perera, Academic Press, 1993.

C.C. HARRIS, *p53 : At the Crossroads of Molecular Carcinogenesis and Risk Assessment*, in *Science*, vol. 262, pp. 1980-1981, 24 décembre 1993.

J.D. GROOPMAN et al., *Molecular Biomarkers for Aflatoxins and Their Application to Human Cancer Prevention*, in *Cancer Research*, vol. 54, n° 75, pp. 1907S-1911S, 1er avril 1994.



LA CONSULTATION À DISTANCE
Les serveurs de vidéoconférences permettent aux médecins de consulter des confrères, afin d'obtenir plus d'informations sur certains cas.

Programmes pour réseaux fiables

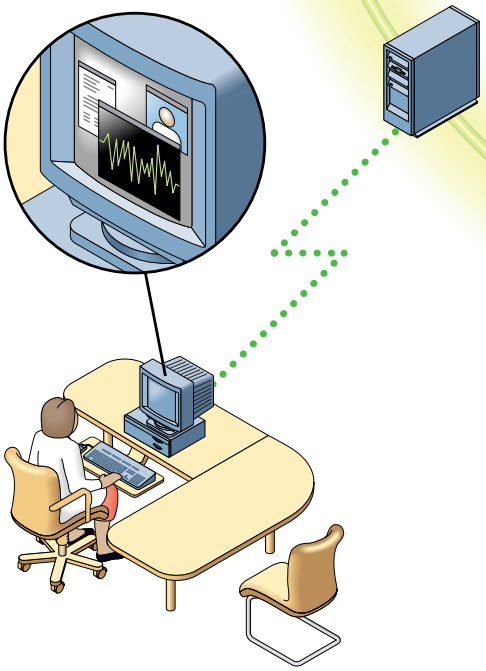
KENNETH BIRMAN • ROBBERT VAN RENESSE

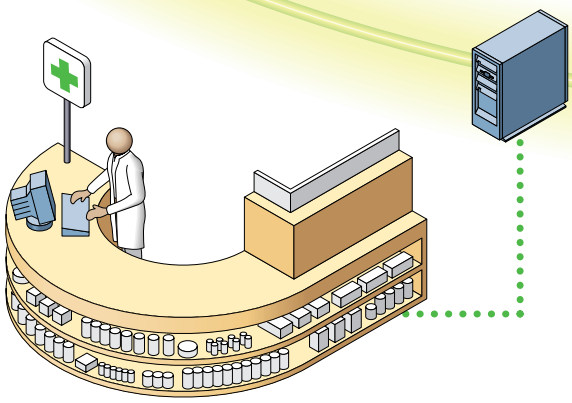
Les techniques qui permettent aux réseaux d'ordinateurs de se réorganiser peuvent rétablir le fonctionnement d'un réseau quand une partie de celui-ci tombe en panne.

La navigation sur le réseau *Internet* n'est plus uniquement un passe-temps ludique : un nombre croissant d'entreprises utilisent des services en ligne analogues à ceux qui sont accessibles par le réseau *Internet*. Ces services facilitent la gestion d'informations importantes et accélèrent les prises de décision. Cependant, les entreprises qui se fondent sur ces systèmes se préoccupent des pannes éventuelles des réseaux. Les plus inquiets sont les utilisateurs des systèmes informatiques répartis, c'est-à-dire les systèmes qui relient des programmes, des serveurs et des fichiers de données disséminés à travers un vaste réseau d'ordinateurs et de terminaux.

Tous ceux qui utilisent des réseaux savent, ô combien, que les programmes qui opèrent à travers les réseaux sont faillibles. Leslie Lamport, de la Société *Digital Equipment*, définit, avec humour, un système informatique réparti comme «un système où la défaillance d'un ordinateur dont vous ignoriez jusqu'à l'existence peut rendre votre propre ordinateur inutilisable». Cette «toile d'araignée mondiale» qu'est le *World Wide Web* (un réseau de serveurs qui couvre le monde) n'est évidem-

LE MÉDECIN
D'un cabinet privé, dans un autre immeuble que l'hôpital, un médecin peut surveiller des patients hospitalisés. Il accède ainsi aux rythmes respiratoire et cardiaque, aux résultats des analyses de laboratoire et aux dossiers médicaux mis à jour.



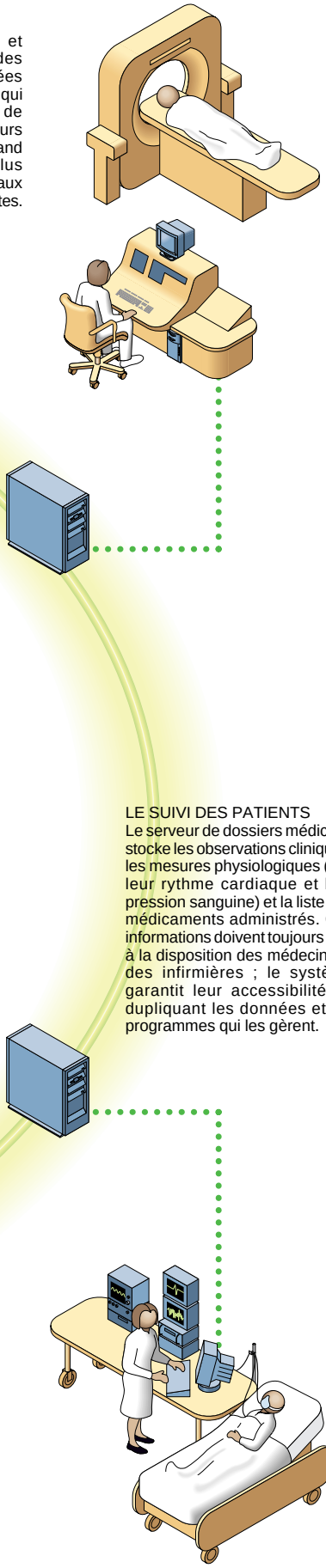


LA PHARMACIE
Le pharmacien hospitalier complète aussi le dossier médical des patients en notant quand les traitements prescrits ont été administrés. En enregistrant avec précision tous les médicaments que prend un malade, on évite les interactions médicamenteuses dangereuses.

ment pas à l'abri *(voir l'encadré de la page 84)* : en 1995, plusieurs coupures ont bloqué toutes les communications. On a attribué ces défaillances à des erreurs dans les programmes, à l'engorgement du trafic sur les lignes de transmission, à des surcharges des machines ou à des pannes des serveurs, c'est-à-dire les ordinateurs qui stockent les documents auxquels accèdent les utilisateurs ; une combinaison de ces facteurs a vraisemblablement contribué à ces coupures partielles. Sans aucun doute, les blocages se multiplieront à mesure que se développeront les réseaux informatiques, *Internet* lui-même ainsi que tous les autres réseaux informatiques desservant les banques, les universités ou les sociétés.

Une panne d'ordinateur n'a pas toujours de conséquences dramatiques : quand un distributeur de billets ne fonctionne pas, on traverse la rue et l'on s'approvisionne au distributeur voisin. En revanche, l'interruption du fonctionnement de réseaux complexes peut avoir des conséquences désastreuses. Le 15 juillet 1994, le NASDAQ (un marché boursier exclusivement électronique destiné aux entreprises de haute technologie) ouvrit avec deux heures de retard en raison d'un problème mystérieux qui avait bloqué le fonctionnement du système tout entier. Initialement, les opérateurs du système pensèrent qu'une erreur de programme avait déclenché l'arrêt, mais ils identifièrent que celui-ci résultait du dysfonctionnement d'un disque dur. Comme le début des échanges n'avait été retardé que de quelques heures, peu d'argent fut perdu, mais le marché aurait dû faire face à d'énormes pertes si les échanges n'avaient repris si vite.

Dans un autre exemple datant de janvier 1990, le réseau téléphonique de la compagnie américaine *AT&T* a connu un dérangement de grande envergure lorsqu'un central électronique du système tomba en panne. Les appels furent automatiquement transférés à un central de secours, mais ce dernier tomba en panne à son tour en raison d'une erreur logicielle. La défaillance se propagea à travers tout le réseau et aboutit à une interruption des communications à l'échelle nationale : neuf heures durant, 60 000 personnes furent privées du téléphone. Pour tous ceux qui sont familiarisés avec la difficulté que représente la gestion d'un réseau même simple, l'étonnant n'est pas que ces incidents surviennent, mais plutôt qu'ils ne soient pas plus fréquents. La France n'a jamais connu de problèmes de ce genre grâce à une mise en place progressive du réseau et à des tests draconiens.



AU LABORATOIRE
Pour s'assurer que médecins et infirmières ne prennent pas des décisions fondées sur des données périmées, les fichiers du serveur qui stocke les résultats d'analyses de laboratoire sont copiés sur plusieurs serveurs dans tout le système. Quand le serveur principal n'est plus accessible, les requêtes d'accès aux dossiers sont dirigés vers d'autres sites.

LE SUIVI DES PATIENTS
Le serveur de dossiers médicaux stocke les observations cliniques, les mesures physiologiques (tels leur rythme cardiaque et leur pression sanguine) et la liste des médicaments administrés. Ces informations doivent toujours être à la disposition des médecins et des infirmières ; le système garantit leur accessibilité en dupliquant les données et les programmes qui les gèrent.

LE PERSONNEL SOIGNANT
Le personnel soignant met fréquemment à jour les dossiers des patients, entrant de nouvelles informations dans le système à partir d'un des terminaux de l'hôpital ou d'un bloc-notes électronique.

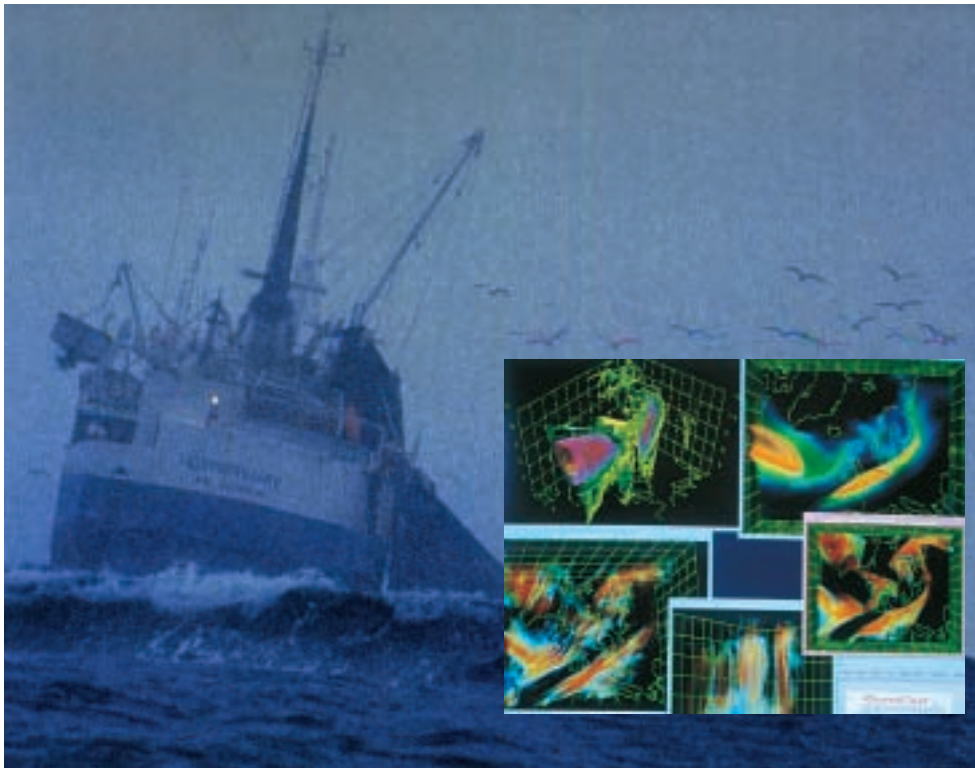
1. DANS LES HÔPITAUX, les réseaux relieront bientôt les patients au personnel médical de l'ensemble de l'hôpital ou de quelque lieu que ce soit dans le monde. Afin que des pannes informatiques ne mettent pas en danger les patients, les réseaux devront utiliser la technique de duplication active décrite dans cet article.

Des passerelles fiables

Même une brève défaillance des systèmes répartis est grave quand les programmes utilisés doivent fonctionner en permanence. Ainsi, les réseaux qui gèrent le trafic aérien ou les opérations bancaires doivent être extrêmement fiables et constamment remis à jour : un message tel que «l'ordinateur central ne répond pas» ou l'affichage d'informations périmées sur le trajet d'un avion en vol ou la cote de valeurs boursières risqueraient de provoquer des accidents ou des désastres financiers. Or les systèmes informatiques répartis se multiplient ; leur fiabilité devient vitale tant pour les entreprises que pour les particuliers. On vante aujourd'hui les avantages considérables des autoroutes de l'information, mais on n'obtiendra les avantages rêvés que si les liaisons entre les ordinateurs sont étudiées de près. Depuis la fin des années 1970, de nombreux informaticiens recherchent des programmes qui rendraient les réseaux plus sûrs et plus fiables, bref plus «robustes».

Pourquoi les réseaux tombent-ils en panne? Habituellement, un problème isolé en un site quelconque se propage dans le réseau, ce qui provoque l'interruption en chaîne des programmes, ordinateur après ordinateur. Il serait vain de renforcer les composants individuels, par exemple en introduisant des ordinateurs et des disques spécialement conçus pour tolérer les erreurs, car on ne parerait pas aux incidents imprévisibles tels qu'une fuite d'eau dans la salle informatique ou une panne de courant ; de surcroît, les communications peuvent être coupées par inadvertance ou par sabotage. Même si les ingénieurs et les programmeurs améliorent sans cesse les matériels et les logiciels, les ordinateurs ne sont jamais totalement fiables.

En outre, des ordinateurs fiables interconnectés et des programmes sans erreur ne conduisent pas nécessairement à des systèmes répartis robustes ; ils constituent seulement des réseaux qui fonctionnent correctement dans la plupart des conditions. Les programmes de gestion du courrier électronique, les tribunes de discussion et le *Web* ont été réalisés à partir de composants individuellement très fiables. Néanmoins, ces systèmes se bloquent fréquemment lorsqu'un événement inattendu survient dans l'un des composants du système. Le système tombe en panne lorsqu'une machine ou une ligne de transmission est surchargée. D'autres formes de protection sont donc nécessaires.



2. UN RÉSEAU DE SURVEILLANCE MÉTÉOROLOGIQUE alerte les pêcheurs norvégiens en cas de tempêtes dangereuses *(à gauche)* ou de marée noire *(à droite)*. Le système informatique *StormCast* relie des caméras éloignées, des stations météorologiques et des

Depuis 20 ans, les programmeurs fiabilisent les réseaux en mettant au point des logiciels qui tolèrent les erreurs : ces programmes permettent aux systèmes informatiques de quitter une tâche quand un blocage survient. Plus généralement, on cherche à éliminer les chaînes de dépendance internes qui subordonnent le fonctionnement d'un système réparti au fonctionnement de tous ses composants. Les systèmes qui en résultent continuent à fonctionner même lorsque certains sites sont déconnectés : le système change sa configuration de manière à contourner les serveurs indisponibles.

Sauvés par les sauvegardes

Les systèmes qui possèdent cette aptitude sont des systèmes répartis à haute disponibilité. En dupliquant en permanence les informations critiques et en distribuant les multiples copies de sauvegarde à leurs ordinateurs individuels, ces systèmes s'adaptent à des aléas de fonctionnement tels qu'un lecteur de disque défectueux en un site, une surcharge dans un autre, une connexion coupée, etc. Tant que les défaillances surviennent à un rythme qui laisse aux programmes le temps de s'adapter, ces systèmes peuvent répondre aux requêtes en extrayant d'un site opérationnel une copie du fichier vital ou la copie d'un programme utilisé en ligne. Le système tout entier reste ainsi opérationnel et, dans l'idéal, fournit un service ininterrompu aux utilisateurs connectés.

On obtient, de manière simple, un système réparti à haute disponibilité en associant une machine principale et une machine de secours. Lorsque la machine principale tombe en panne, la machine de secours prend la relève. La commutation d'un système à l'autre est facile lorsque les données ne changent jamais. En revanche, la commutation est difficile lorsque les données ou les fichiers changent alors que le système fonctionne. De plus, dans les grands réseaux, on distingue difficilement les systèmes en panne des systèmes qui n'ont que des difficultés avec les transmissions.

Supposons que, lors de la mise à jour des informations du serveur principal et du serveur de secours, l'un des deux ne réponde plus. Si le problème

satellites pour fournir des données mises à jour. On accède à *StormCast* par le *World Wide Web* (la «toile d'araignée mondiale» véhiculée par le réseau *Internet*) à l'adresse http://www.cs.uit.no/

ne provient que des lignes de communication, la mise à jour finira par se faire. En revanche, si le serveur qui ne répond plus est hors service, l'ordinateur qui fait la mise à jour attendra indéfiniment ; pendant ce temps, le système sera indisponible. Si l'on se contente d'ordonner à l'ordinateur de cesser l'attente et de ne mettre à jour que le serveur qui fonctionne, le système principal et celui de secours ne seront plus identiques : des erreurs surviendront si le système tente d'utiliser le serveur périmé.

Le marché financier NASDAQ résout ce problème grâce à deux serveurs centraux d'échanges boursiers. Pour éviter toute confusion, un seul des deux serveurs est actif à un instant donné. Les administrateurs du NASDAQ décident eux-mêmes quand basculer sur le serveur de remplacement. Malheureusement, très peu de systèmes distribués peuvent compter sur la sagesse d'un opérateur humain pour détecter les pannes et décider le changement d'un serveur ; les programmeurs doivent généralement automatiser cette décision, afin que la transition survienne sans heurts.

En outre, les systèmes répartis à haute disponibilité gèrent souvent un grand nombre de serveurs et de programmes. Pour ce faire, les systèmes tiennent à jour la liste de leurs membres et gardent ainsi la trace de chaque programme et de son état d'activité. Un programme qui, pour quelque raison que ce soit, ne répond pas est jugé défectueux. En reconnaissant une défaillance en un site, le système change alors sa configuration et redistribue le travail vers les sites opérationnels.

Le système NASDAQ illustre également un second problème de fiabilité des systèmes distribués. Le retard de deux heures dans le début des échanges financiers, en 1994, aurait été évité si les opérateurs avaient immédiatement enclenché le système de secours. Ils choisirent pourtant d'attendre, car ils craignaient qu'une erreur logicielle n'ait causé le mauvais fonctionnement du système principal. Dans ce cas, la panne se serait produite également sur le système de secours, comme ce fut le cas en 1994 pour la panne du système de la compagnie de téléphone *AT&T*, mentionnée auparavant. Comme il est impossible de garantir qu'un logiciel soit exempt d'erreurs, on doit trouver des moyens de réduire le risque que les versions de secours d'un serveur critique ne tombent en panne à leur tour après la défaillance du serveur principal.

À cette fin, les programmeurs ont inventé la duplication active : un programme fait des copies de secours des programmes et des fichiers vitaux en utilisant des «groupes de processus». Un groupe de processus est un ensemble de programmes qui coopèrent. Un système réparti peut comporter plusieurs groupes de processus, et les programmes peuvent appartenir à plusieurs de ces groupes. Chaque groupe est identifié par un nom semblable à un nom de fichier et possède sa propre liste actualisée de participants (l'ensemble des programmes qui coopèrent). En outre, le groupe de processus permet d'envoyer des messages à ses membres. Cette fonction de transmission des messages garantit que chaque membre du groupe reçoit chaque message dans le même ordre, même si l'émetteur tombe en panne pendant la transmission, ce qui est vital pour de nombreuses applications.

Lorsqu'un programme particulier est vital pour maintenir la disponibilité du système, ce dernier crée un groupe de programmes qui sont, chacun, une copie de l'original. Pour garder à jour les données manipulées par le programme dupliqué, le système envoie un message au groupe de programme. Chaque membre réagit en mettant à jour sa copie du programme. Comme tous les programmes «voient» les mêmes mises à jour dans le même ordre, ils restent dans des états cohérents.

La duplication active permet à un système de tolérer les erreurs, car n'importe quel membre du groupe peut traiter n'importe quelle requête : quand une machine tombe en panne, la tâche est confiée à un site opérationnel. En outre, quand une requête ne modifie pas les données, elle est satisfaite par un site unique au lieu de mettre tout le système à contribution. De cette façon, de multiples tâches sont menées en même temps par différents programmes, ce qui accélère l'application en utilisant le traitement parallèle.

Naturellement, si tous les membres d'un groupe de processus traitaient de manière erronée un message, ils tomberaient tous en panne simultanément. Toutefois, les erreurs de ce genre sont exceptionnelles, car les programmeurs ont observé que les erreurs qui passent le plus facilement inaperçues lors des tests du logiciel sont plutôt celles où intervient l'ordre de réception des données. Ces erreurs sont provoquées uni-

quement par des séquences d'événements improbables. Lorsqu'un système utilise la duplication active, les différentes copies voient les mêmes mises à jour dans le même ordre ; toutefois, les mises à jour sont seulement une petite partie des requêtes reçues par un programme. La plupart du temps, les programmes dupliqués travaillent en parallèle, chaque programme traitant son propre ensemble de requêtes dans un ordre spécifique. Dès lors, même si une erreur logicielle échappait aux tests et interférait avec un membre d'un logiciel réparti, il serait improbable qu'elle mette hors service tous les membres d'un groupe de traitement en même temps.

L'idée de la duplication active est simple, mais sa mise en œuvre est difficile. La gestion dynamique des listes de participants, qui changent continuellement, et les communications avec les groupes de processus sont sujettes aux erreurs systèmes et à la perte de messages. Bien que l'informatique répartie se soit imposée au cours de la dernière décennie, la duplication active n'est sortie que récemment des laboratoires de recherche.

La boîte à outils des réseaux robustes

Durant ces dernières années, plus d'une dizaine d'équipes d'ingénieurs ont mis au point des logiciels qui assurent la robustesse des systèmes répartis. Tous offrent une haute disponibilité grâce à la duplication active, mais ils diffèrent sur leurs priorités : les uns privilégient la rapidité ; d'autres, la sécurité.

À l'Université Cornell, nous avons réalisé deux logiciels. L'un d'entre nous (K. Birman) a dirigé l'équipe qui a produit le logiciel *Isis* en 1987 ; puis, ensemble, nous avons construit le logiciel *Horus*, achevé en 1994. Les noms de ces programmes indiquent leurs propriétés : la déesse égyptienne Isis ressuscita le dieu Osiris après qu'il avait été tué, lors d'un duel, par Seth, dieu de la guerre ; Horus, fils d'Isis, vainquit finalement Seth. De même, les logiciels *Isis* et *Horus* établissent le fonctionnement d'un système distribué interrompu par une défaillance.

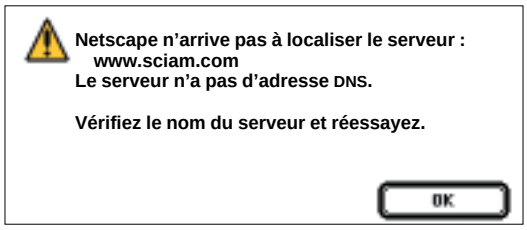
Des logiciels comme *Isis* utilisent un assortiment de fonctions logicielles, ou «outils», qui dupliquent et mettent à jour les données, gardent la trace des groupes de processus et aident à gérer l'appartenance de ces groupes. *Isis* peut aussi répartir le traitement des données entre les serveurs (une procédure nommée partage des tâches). Les systèmes répartis qui utilisent le partage des tâches présentent la plupart des avantages du parallélisme sans recourir à des ordinateurs parallèles spécialisés. En divisant le travail entre de nombreux serveurs fonctionnant de concert, *Isis* permet aux systèmes d'effectuer rapidement de lourdes tâches. De même, lorsqu'une application particulière nécessite davantage de puissance de calcul, on peut ajouter un serveur, en conservant la technique de partage des tâches pour le nouveau groupe. Les performances d'*Isis* et d'*Horus* surprennent souvent les programmeurs, qui considèrent qu'un système robuste est nécessairement lent et onéreux.

La duplication active a été utilisée pour de nombreuses applications : télécommunications, marchés financiers, banques... En Norvège, des informaticiens ont mis au point un système de surveillance de l'environnement

Le *Web* s'emmêle

La majeure partie du *World Wide Web* est invisible. De nombreux utilisateurs ne voient qu'un programme de navigation et des serveurs distants, où les documents à charger sont stockés. Cependant les sites du réseau et le réseau lui-même, qui relie ces sites, est composé de millions d'autres programmes et de serveurs ; des dizaines d'entre eux coopèrent pour fournir un seul document. Par exemple, quand on cherche une information dans un serveur du centre de coordination européen du réseau à l'Institut national de recherche en informatique et en automatique, le nom «www.inria.fr» doit être converti en une adresse numérique que les logiciels reconnaissent. Cette tâche est effectuée par une série de programmes de conversion d'adresses avant que l'adresse correcte soit localisée. En outre, toute requête d'accès à un site du réseau passe normalement par un certain nombre de relais, qui sauvegardent une copie des documents fréquemment demandés, afin de diminuer la charge de travail des serveurs *Web* distants. Ainsi, quand un intermédiaire proche a stocké une copie du document recherché, l'utilisateur évite un long transfert de fichier à travers le réseau.

Ce système de relais est classique dans les réseaux, mais c'est une source de défaillances : quand un serveur de nom ne répond pas, ou quand un relais échoue, ou quand le serveur *Web* tombe en panne, la requête initiale n'aboutit pas. Aussi l'incontournable message d'erreur du *Web* qui signale qu'un serveur est bloqué ou occupé *(ci-dessous)* peut-il être trompeur : la surcharge ou la panne d'un nombre quelconque de programmes intermédiaires peut aussi conduire à ce message.



Le réseau *Internet* dans sa globalité peut connaître des pannes partielles assez semblables à celles des réseaux téléphonique et électrique. Ainsi, fin 1995, l'un des principaux serveurs de temps du réseau *Internet*, à Atlanta, fut surchargé de façon intermittente. Pendant ce temps, personne sur le *Web* ne pouvait obtenir de documents de serveurs dont l'adresse n'était pas déjà connue du système local. Ce type de pannes gêne un grand nombre de personnes dans le monde entier. Même si une connexion avec un serveur réussit, cela n'exclut pas des erreurs ultérieures. Les copies faites par les programmes intermédiaires du *Web* ne sont pas actualisées lorsque le document original l'est. Aussi les utilisateurs n'ont-ils aucune garantie que la version qu'ils consultent est la dernière mise à jour. Si les documents nécessaires ne sont pas gardés à jour, certaines applications dépendantes du temps perdent alors leur fiabilité. D'un côté, les programmes mandataires du *Web* améliorent la fiabilité du réseau *Internet* en diminuant sa charge de travail, mais, de l'autre, ils diminuent la fiabilité en créant l'éventualité de l'obtention d'informations périmées.

Les projets vitaux, sur le réseau *Internet* ou sur d'autres systèmes informatiques répartis, requerront la garantie que les informations extraites du système soient précises, mises à jour et toujours disponibles. On peut éviter des problèmes en sauvegardant les informations vitales par le biais de la duplication active décrite dans l'article.

fondé sur cette technique *(voir la figure 2)*. L'organisme français de contrôle du trafic aérien expérimente également cette technique pour l'appliquer à une nouvelle génération de logiciels de contrôle du trafic. Des usines de production ont utilisé les groupes de processus pour coordonner les tâches et pour reconfigurer les chaînes d'assemblage lorsque certains équipements de ces chaînes sont retirés pour être révisés.

Toutefois, à mesure que la complexité des applications augmente, les informaticiens découvrent que la duplication active a des limitations. Le partage des tâches n'est ni toujours possible, ni désirable : certains systèmes (notamment ceux où les données stockées dans un serveur changent très rapidement) ralentissent quand leurs éléments sont dupliqués. Par exemple, pour les vidéoconférences, la duplication active améliore la tolérance aux pannes du réseau de serveurs qui doivent continuer de fonctionner même quand certains participants sont déconnectés. En revanche, appliquée à la transmission de données vidéo à distance, cette technique ralentira le système sans améliorer sa fiabilité.

Le besoin de flexibilité nous a conduits à mettre au point *Horus*. *Horus* utilise à la fois la technique de duplication active et un traitement modulaire des tâches : un peu comme avec des *Lego*, les différentes pièces de construction, ou modules, d'*Horus* peuvent s'assembler selon n'importe quelle combinaison pour répondre aux besoins spécifiques d'un groupe de processus particulier. Un module chiffre les données, afin de fermer le réseau aux pirates ; un autre module identifie les erreurs de communication potentielles pouvant survenir lorsque des messages sont perdus ou altérés. Les programmeurs qui utilisent *Horus* décident des propriétés nécessaires à leur système et adaptent le système à l'usage projeté. En outre, *Horus* est extensible à l'aide de modules faits sur mesure pour des besoins spécifiques que nous n'avons pas rencontrés ni imaginés.

Horus a un nombre croissant d'utilisateurs dans le monde. À l'Université Cornell, Brian Smith l'a utilisé pour construire un système de vidéoconférences associé à des groupes de discussion et à des outils de travail coopératif assisté par ordinateur.

3. CES PASSAGERS, qui attendent leurs avions à l'aéroport de La Guardia, à New York, sont victimes d'une panne du système local de contrôle de trafic aérien faisant suite à une coupure de courant, en mai 1995. Les efforts pour rajeunir les logiciels américains vieillissants de contrôle de trafic aérien utilisant des systèmes répartis remontent aux années 1980.

Un manque de volonté?

Notre travail sur *Isis* et sur *Horus* nous a convaincus qu'une étude soignée assure la fiabilité d'un réseau informatique. Toutefois, la réalisation d'autoroutes de l'information robustes coûtera plus cher et prendra plus de temps que ne le voudraient les fabricants et les utilisateurs. Les logiciels de gestion des systèmes répartis sont habituellement construits avec la technique existante, qui n'a pas été conçue pour être fiable. En outre, les informaticiens doivent trouver des techniques nouvelles pour les très gros réseaux : un système extrêmement robuste lorsque 50 utilisateurs y accèdent simultanément peut se révéler trop lent, et donc non fiable, lorsque 5 000 personnes s'y connectent.

Bien que les programmeurs aient appliqué la technique de l'informatique répartie robuste avec succès dans certains cas, le public entend plus souvent parler des défaillances des systèmes non robustes. Ainsi, ces dernières années, des dizaines de rapports ont fait état de problèmes du système de contrôle du trafic aérien américain. Fin 1995, le système de Los Angeles tomba en panne, mettant les contrôleurs dans l'impossibilité de communiquer avec les avions ; une collision en plein ciel fut évitée de justesse.

Pis encore, les mises à jour des logiciels de contrôle de trafic aérien commandées, en 1982, par le ministère américain de l'aviation ont été retardées et les logiciels finalement proposés sont moins performants que ceux qui avait été initialement choisis : les aspects «haute disponibilité» et «distributivité» ont été presque éliminés. Pourtant, les contrôleurs aériens considèrent que le système existant est inapproprié, notamment parce qu'il lui manque une architecture de logiciel distribué et qu'il a perdu de sa fiabilité avec l'âge.

L'industrie logicielle est-elle en crise? Si une crise existe, c'est peut-être autant par manque de volonté que par manque de moyens. Tous les ingénieurs n'ont pas besoin de rendre robustes leurs logiciels réseaux : la pression du public pour accroître la fiabilité ne semble pas s'étendre au-delà de quelques applications particulièrement sensibles. Les sociétés qui commercialisent les logiciels d'informatique répartie précisent souvent, dans les garanties de leurs produits, que la technique de programmation employée n'est pas assez fiable pour un usage dans des applications critiques, avouant implicitement que la fiabilité n'est pas un objectif. C'est un peu comme si un constructeur d'automobiles vendait ses voitures en prévenant que les véhicules pourraient ne pas