Sécurisation des infrastructures critiques : modélisation des interdépendances, étude des pannes en cascade et recherche d'une méthodologie de détection des propagations des défaillances

Alpha-Amadou Diallo

THÈSE

Présentée

pour obtenir le grade de

Docteur de l'École Nationale Supérieure des Télécommunications de Paris

Spécialité : INFORMATIQUE ET RÉSEAUX

par

Alpha Amadou DIALLO

Sécurisation des infrastructures critiques : modélisation des interdépendances, étude des pannes en cascade et recherche d'une méthodologie de détection des propagations des défaillances

---

Soutenue le 1er septembre 2010 devant la Commission d'examen :

Maryline Laurent	Président
Nouredine Hadjsaid	Rapporteur
José Araujo	Examinateur
Ghislain du Chéné	Examinateur
Claude Chaudet	Encadrant
Michel Riguidel	Directeur de Thèse

Je dédie cette thèse à la mémoire de ma belle-mère, à celles de mon père et de ma sœur disparus trop tôt. J'espère que, du monde qui est le leur maintenant, ils apprécient cet humble geste comme preuve de reconnaissance et de remerciement de la part de celui qui ne cesse de penser à eux et de prier pour le repos de leur âme !

Remerciements

Au terme de ce doctorat, je tiens tout d'abord à remercier Michel Riguidel, directeur du département Informatique et Réseaux de l'École Nationale Supérieure des Télécommunications pour m'avoir accueilli au sein de son département ainsi que pour avoir accepté d'être mon directeur de thèse.

Mes plus vifs remerciements s'adressent à mon encadrant Claude Chaudet sans qui cette thèse ne serait pas ce qu'elle est. Je le remercie pour sa disponibilité, ses conseils et son aide inestimable tout au long du déroulement de cette thèse.

Je tiens également à remercier l'ensemble des chercheurs du département INFRES pour leur accueil et leur soutien scientifique. Je souhaite évidemment remercier les différentes personnes qui ont accepté d'être les membres du jury, particulièrement le Prof. Maryline Laurent qui a assuré la présidence.

Il m'est également impossible d'oublier toute ma famille avec une dédicace spéciale à ma mère et à ma femme sans qui ce travail n'aurait pas été possible.

Enfin, merci à toutes les personnes que je n'ai pas citées ici et qui se reconnaîtront dans ces quelques lignes.

Résumé

Au cours de ces dernières décennies, les infrastructures critiques comme les réseaux électriques, les réseaux de transport, les réseaux de télécommunications, les infrastructures des services de santé et des services de secours se sont de plus en plus modernisées et ont largement profité des progrès des technologiques de l'information et de la communication. Cet essor a fortement contribué à l'efficacité de ces infrastructures en favorisant l'automatisation de certaines tâches, l'accès à distance à certains composants clefs, le télétravail et l'utilisation optimale des ressources. Pour profiter au mieux de tous ces avantages, ces infrastructures, à travers leurs réseaux informatiques locaux se sont largement connectées au réseau Internet. Or le réseau Internet est un réseau public accessible à tout le monde, donc aux attaquants mal intentionnés. C'est aussi une infrastructure vulnérable, constituée de logiciels standards et bien connus de la plupart des spécialistes. Ce qui rend tous les réseaux qui forment Internet des cibles potentiels pour les nombreuses attaques lancées fréquemment contre le réseau Internet et visant à dégrader ou interrompre des services. De nos jours, les réseaux informatiques et les systèmes d'informations constituent une vulnérabilité commune pour l'ensemble des infrastructures modernes. Aussi, les infrastructures critiques sont interdépendantes et les défaillances de l'une d'entre elles peut se propager pour toucher d'autres infrastructures soit parce que ces infrastructures se situent à proximité les unes des autres ou parce que l'interruption du service (l'électricité par exemple) fourni par l'une d'entre elles peut engendrer des pannes d'autres infrastructures. Compte tenu de tous ces facteurs, il est devenu inefficace de protéger une infrastructure unique sans se préoccuper des autres infrastructures qui sont interdépendantes avec celle-ci.

Dans le cadre de cette thèse, nous proposons différentes techniques et architectures pour améliorer la compréhension des interdépendances et lutter contre les phénomènes de propagation des défaillances résultant des interdépendances. La première contribution de cette thèse définit un simulateur des propagations des défaillances entre les réseaux électriques et de télécommunications. Ce simulateur est fondé sur la répartition des charges entre les différents composants du réseau électrique et sur le fonctionnement des protocoles de routage pour le réseau de télécommunications. Le calcul de la répartition de charge est réalisé avec la méthode *DL Load Flow*. Dans le simulateur, les topologies des réseaux sont représentées par des graphes, ce qui permet d'intégrer plusieurs infrastructures hétérogènes dans un simulateur unique. Différentes simulations ont été réalisées avec des graphes représentant le réseau 400 kV du Réseau de Transport d'Électricité (RTE[1]) et le réseau du fournisseur d'accès Internet Free[2]. Les résultats de ces simulations valident notre simulateur et montrent qu'il est possible de développer un modèle des interdépendances et un simulateur des propagations des défaillances suffisamment génériques pour permettre d'intégrer plusieurs infrastructures hétérogènes tout en offrant la possibilité de prendre en compte les principaux facteurs qui influent la propagation des défaillances. Ils montrent aussi qu'un réseau de télécommunications performant permet de réduire l'ampleur des propagations des pannes dans les réseaux électriques en mettant à disposition des opérateurs les informations temps réel sur l'état du réseau électrique nécessaires pour entreprendre des actions appropriées pour rééquilibrer la production et

[1] http://www.rte-france.com
[2] http://www.free.fr

la consommation de l'énergie électrique après une panne. Ces différentes simulations ont aussi fait surgir le besoin de disposer des topologies réalistes et en nombre suffisant pour obtenir des résultats pertinents. D'où la deuxième contribution faite dans le cadre de cette thèse qui propose une technique de génération des topologies réalistes et adaptées aux études des interdépendances. Cette technique se base sur les règles de déploiement des réseaux et tient compte des contraintes techniques et économiques liées à la conception et au déploiement des réseaux. Elle concerne principalement les réseaux de télécommunications de type Internet, mais nous avons aussi présenté quelques topologies de réseaux électriques générées par la technique proposée pour montrer qu'elle est suffisamment générique et peut être facilement adaptée pour générer des topologies représentant des infrastructures autres que des réseaux de télécommunications. Pour distinguer les différents nœuds d'un réseau, nous utilisons des paramètres pour les identifier et leur attribuer des poids et des coordonnées. Ces différentes caractéristiques permettent de différencier les nœuds BGP (*Border Gateway Protocol*) et OSPF (*Open Shortest Path First*) par exemple) et les différents liens (intra et inter-AS) constituant les graphes générés. Différents niveaux d'interconnexions sont offerts pour générer des topologies des réseaux de télécommunications de type Internet, il s'agit de l'interconnexion de nœuds formant un point de présence, l'interconnexion des points de présence et, enfin l'interconnexion des systèmes autonomes. L'interconnexion des nœuds formant un point de présence est fondée sur la distance euclidienne, celle des points de présence se base sur les poids des nœuds qui représentent les différents points de présence et la distance euclidienne. Enfin l'interconnexion des différents AS est réalisée sur la base d'un système de préférence fondé sur le degré de connectivité des AS. La technique proposée permet de générer des graphes plus réalistes et mieux adaptés aux simulations des interdépendances. Plusieurs graphes ont été générés et différentes études comparatives ont été effectuées pour valider la technique et évaluer la pertinence des graphes générés. Un autre volet de nos travaux concerne la simulation des propagations des défaillances dans les réseaux de télécommunications de type Internet. Le simulateur proposé est fondé sur la théorie des graphes et un modèle de propagation d'épidémie modifié pour mieux prendre en compte la particularité des réseaux de télécommunications. Ce choix nous a permis de développer un simulateur générique qui peut être adapté pour simuler les propagations des défaillances dans une grande variété d'infrastructures. Cette adaptation du modèle épidémiologique de base permet de prendre en compte les principaux facteurs qui influent les propagations des défaillances dans les réseaux de télécommunications comme les différents temporisateurs des protocoles de routage et la taille des tables de routage. Ce simulateur permet d'étudier différentes défaillances qui se propagent dans les réseaux Internet comme la corruption des tables de routage, les attaques de déni de service, la propagation des virus informatiques et les pannes des routeurs. Plusieurs simulations ont été réalisées avec le simulateur proposé pour évaluer l'impact des propagations des défaillances dans les réseaux en terme de l'existence des fausses routes, de déconnexion du graphe, du nombre de composants touchés et de la durée de vie des défaillances. Enfin, notre dernière contribution définit une architecture client-serveur permettant de détecter des pannes dans un environnement hétérogène et distribué. L'architecture proposée permet de réutiliser les outils de supervision existants et offre des moyens pour assurer le contrôle d'accès aux informations lorsque l'environnement est constitué de plusieurs réseaux gérés par différents opérateurs qui doivent échanger des informations sur l'état de leurs infrastructures. Cette architecture a été conçue avec une attention particulière sur sa ca-

pacité de fonctionner avec des environnements hétérogènes, de réduire le trafic supplémentaire engendré et son aptitude à détecter des propagations des pannes qui peuvent résulter des inter-dépendances entre infrastructures hétérogènes. Plusieurs scénarios de test ont été réalisés avec l'architecture proposée sur un réseau virtuel constitué de 5 systèmes autonomes de 6 routeurs chacun construit avec le logiciel de virtualisation Netkit[3]. Le logiciel Nagios[4] a été déployé sur chaque système autonome. Les différents scénarios de tests réalisés ont permis, notamment d'évaluer la variation du délai de détection des pannes, de la période d'échange d'informations et de l'évolution du trafic engendré. Les résultats ont, enfin permis d'identifier, pour le réseau de test utilisé, une valeur qui constitue un bon compromis entre la nécessité de réduire le trafic et celle de diminuer la période d'échange d'informations afin de réduire le délai de détection des pannes.

[3] http://www.netkit.org
[4] http://www.nagios.org

Table des matières

Chapitre 1

Introduction générale

La société moderne repose, dans une très large mesure sur un ensemble d'activités d'importance vitale (AIV) telles que l'électricité, les transports, les télécommunications, les systèmes d'information, la santé, l'agriculture, l'administration, les réseaux d'adduction d'eau, les banques et la finance, l'énergie, les services d'urgence, l'éducation, l'industrie, la défense et les monuments [103]. Ces AIV s'appuient sur des installations, des services, des actifs et des systèmes appelés infrastructures critiques. Ces infrastructures jouent un rôle déterminant dans le bien être des citoyens et tout dysfonctionnement de l'une d'entre elles peut avoir des conséquences graves sur la vie économique et sociale de la société. Les infrastructures critiques sont composées d'un ensemble de technologies, d'installations et des processus complexes.

Conscients de leur importance, les États s'emploient, depuis de nombreuses années à l'identification et à la protection de ces infrastructures. Aux États-Unis, par exemple, en 1996, le président Clinton signe une circulaire (Executive Order 13010 [8]) établissant la PCCIP (*President's Commission on Critical Infrastructure Protection*) chargée de définir et d'établir une liste et une classification de ces infrastructures critiques selon leur importance nationale. En 2004 l'IAIP (*Information Analysis and Infrastructure Protection Directorate*) dresse une liste de 1700 infrastructures considérées comme critiques [104]. Plusieurs travaux de recherche consacrés à ce sujet montrent que la liste des infrastructures critiques varie en fonction des pays et évolue avec le temps. Les centrales nucléaires, par exemple sont des infrastructures critiques pour certains pays alors que ces infrastructures sont inexistantes pour d'autres. L'évolution de la liste des infrastructures critiques avec le temps est principalement liée à l'influence du développement technologique, économique et géo-politique sur la politique de sécurité publique. Dans le document [104] qui synthétise les listes des infrastructures critiques de plusieurs rapports techniques, on trouve ainsi plusieurs secteurs qui apparaissent dans ces listes ou qui disparaissent en fonction de la date et des organismes établissant les rapports. Par ailleurs, les interconnexions nécessaires aux interactions entre les infrastructures et l'influence que l'état d'une infrastructure peut avoir sur les états des autres rendent ces infrastructures dépendantes entre elles et favorisent les propagations des pannes entre ces infrastructures. L'importance du rôle de ces **interdépendances!** dans la propagation des défaillances a été mentionnée dès 1997 dans le premier rapport publié par PCCIP.

D'autre part, la plupart de ces activités d'importance vitale nécessitent le concours de plu-

sieurs infrastructures qui, parfois interagissent entre elles pour assurer ces services. Le transport ferroviaire, par exemple, s'appuie conjointement sur le réseau électrique et celui de télécommunications. Le premier assure l'alimentation en électricité de l'ensemble des installations et des locomotives et le deuxième fournit les services de télécommunications nécessaires au fonctionnement des systèmes de signalisation et de coordination de la circulation. En outre ces deux réseaux s'appuient, chacun sur des services fournis par l'autre réseau pour son propre fonctionnement. Le réseau électrique fournit l'énergie électrique au réseau de télécommunications et ce dernier fournit des services réseaux nécessaires au fonctionnement du système de supervision du réseau électrique. Quant au réseau d'approvisionnement en gaz et de pétrole, il fournit le combustible nécessaire au fonctionnement des stations de production de l'énergie électrique et le réseau électrique assure la fourniture de l'électricité aux stations de pompage de pétrole et de gaz. Par conséquent, chacune de ces infrastructure est dépendante d'une ou de plusieurs infrastructures et une panne d'une d'entre elles provoque souvent la défaillance d'autres infrastructures. Après l'ouragan Katrina, l'approvisionnement en produits pétroliers a été interrompu [111] en raison d'une coupure électrique dans les stations de pompage pour trois pipelines : les pipelines *Colonial*, *Plantation* et *Capline*.

Les interdépendances résultent, le plus souvent, de la nécessité d'interactions entre deux ou plusieurs infrastructures et de leurs actions conjointes pour délivrer certains services. Les multiples interconnexions entre ces infrastructures matérialisent ces interdépendances, contribuent au renforcement de la complexité du système résultant de ces interconnexions et favorisent la propagation des pannes d'une infrastructure à une autre. Il devient alors, de plus en plus inefficace de sécuriser une infrastructure singulière, isolée de l'ensemble des autres infrastructures interdépendantes. En plus du besoin de protéger les infrastructures singulières, les interdépendances et les propagations des pannes constituent, aujourd'hui un enjeux de sécurité majeur. La protection du système résultant de l'interconnexion de plusieurs infrastructures critiques reste, cependant, une tâche difficile compte tenu de la taille, de la complexité et du nombre d'entités impliquées.

Par ailleurs, la protection des infrastructures critiques nécessite du temps et des ressources, le défi consiste donc à réduire, avec des ressources limitées, l'impact des pannes de ces infrastructures sur le bien être de la société. Une allocation éfficace ces ressources limitées nécessite une classification de ces infrastructures. Cette classification peut être faite à partir des conséquences économiques, sociales, politiques ou la combinaison d'autres critères de ces pannes et permet d'allouer les ressources en fonction des priorités. Bien que toutes ces infrastructures soient critiques, certaines sont plus vitales que d'autres et au sein d'une même infrastructure, différents éléments peuvent être plus critiques que d'autres, soit parce que les pannes de ces dernières ne provoquent que des impacts minimes ou parce qu'ils sont redondants et que la panne des uns n'empêche pas les autres de fonctionner. Un autre type de classification consiste à privilégier les infrastructures dont des pannes ont des impacts de plus grandes ampleurs à cause, notamment des interdépendances qui font que la panne d'une infrastructure peut se propager pour toucher un nombre plus ou moins important d'infrastructures. Le réseau électrique est un exemple de ce type d'infrastructure. Une panne électrique de grande ampleur peut affecter simultanément un nombre important d'infrastructures critiques comme les transports et les télécommunications. On peut aussi considérer comme prioritaire les systèmes comme les infrastructures d'information et de communication qui introduisent des vulnérabilités communes

à plusieurs infrastructures. Dans le cadre de cette thèse, le travail réalisé est principalement axé sur les interdépendances relatives aux technologies de l'information et de la communication. Car les interdépendances entre les infrastructures critiques est un sujet vaste qui comporte plusieurs axes de recherches. La compréhension de ces infrastructures et leurs interdépendances constitue, à elle seule, un sujet de recherche dans de nombreux secteurs, notamment l'urbanisme, l'environnement, le génie civil et les services d'urgence [55]. Les auteurs de [128], par exemple identifient 7 pistes qui doivent être explorées pour bien cerner la propagation des défaillances dans les infrastructures critiques. Ces pistes comprennent, notamment, la conception des techniques de modélisation consacrées aux interdépendances. Compte tenu du nombre élevé de pistes à explorer et celui des sujets qui peuvent être considérés comme prioritaires dans l'étude des interdépendances des infrastructures critiques, le travail exposé dans ce manuscrit est centré sur la modélisation et la simulation des interdépendances relatives aux technologies de l'information et de la communication.

Aujourd'hui la plupart des infrastructures modernes ont une forte dépendance aux systèmes d'information et aux réseaux de télécommunications. A cause de cette dépendance, les systèmes d'information et de la communication occupent une place décisive dans la protection des infrastructures critiques contre les propagations des pannes. Le fonctionnement et l'état des infrastructures modernes deviennent fortement dépendants des systèmes de contrôle informatisés comme des logiciels de l'architecture SCADA (*Supervisory Control And Data Acquisition*). De ce fait, le système d'information et de communication se retrouve au cœur des activités de toutes les entreprises, il devient essentiel pour l'économie et les services d'urgence, il constitue une base fondamentale pour le système éducatif, sanitaire et administratif. En effet, les réseaux de télécommunications ont connu, ces dernières années, des progrès fulgurants en terme de débits et de diversité des services offerts. Aujourd'hui, les services (voix, données, vidéos) des réseaux de télécommunications sont essentiellement numériques, ce qui permet de les traiter et de les acheminer conjointement par la même infrastructure dans le cœur des réseaux. Cette convergence des services présente de nombreux avantages en terme de coût et de confort d'utilisation. En plus des avancés liées à la convergence des services réseaux, les progrès des réseaux en terme de bande passante et l'émergence des offres hauts débits mobiles (*business everywhere*) ont fortement contribué à l'explosion de l'utilisation des réseaux, notamment de l'Internet dans les entreprises et les infrastructures critiques.

L'utilisation accrue des technologies de l'information et de la communication durant ces dernières décennies a contribué de manière significative à l'amélioration de l'efficacité de l'ensemble des infrastructures modernes et de la qualité des services offerts par celles-ci en automatisant la plupart des opérations liées à leur gestion et à leur exploitation. Ces services ont considérablement contribué à l'informatisation, à l'efficacité et à l'amélioration de la qualité des services offerts par ces infrastructures. Les bénéfices de l'utilisation des technologies de l'information et de la communication (TIC) dans les infrastructures modernes ont largement dépassé ses coûts et des nouveaux avantages continuent à faire leur apparition. L'augmentation des débits et le développement des solutions de sécurité informatique ont encouragé le télétravail, l'accès à distance aux systèmes de contrôle de infrastructures critiques, l'externalisation des systèmes d'informations et l'accès à des ressources informatiques (infrastructures, réseaux, stockage) extérieures aux entreprises utilisatrices (*cloud computing*). Pour profiter de tous ces avantages, les entreprises se sont fortement inter-connectées à l'Internet et ce phénomène est

accentué par les ouvertures des marchés, les fusions des entreprises, la concentration des populations dans les centres urbains et l'opportunité qu'offre Internet pour faire connaître une entreprise. Selon l'INSEE (Institut National de la Statistique et des Études Économiques)[1], en janvier 2008, entre 57% et 75% des entreprises françaises utilisent l'Internet dans leurs relations avec les autorités publiques, 22% d'entre elles ont recours au télétravail.

Or les interconnexions nécessaires à la mise en réseaux et les dépendances mutuelles entre infrastructures qu'elles engendrent font apparaître des nouvelles vulnérabilités à cause des propagations des pannes qui peuvent résulter de ces interconnexions. Le déploiement massif des infrastructures de l'information et de la communication dans les entreprises renforce ces vulnérabilités car elle rend possible l'accès à distance à des entités névralgiques de ces infrastructures critiques avec des faibles ressources informatiques et en un temps relativement court. Les technologies de l'information et de la communication constituent une source d'interdépendances pour l'ensemble des infrastructures modernes. Par ailleurs, à cause de ces interconnexions, la complexité des réseaux s'intensifie et rend possible l'apparition des phénomènes inattendus capables de s'amplifier de façon incompréhensible. Maintenant la défaillance de l'une de ces infrastructures peut se propager à d'autres infrastructures et entraîner des conséquences graves sur l'économie, la santé, la sécurité, en un mot le bien être de la société. Les réseaux dédiés aux infrastructures pourraient être moins vulnérables s'ils étaient déconnectés du réseau Internet, mais rares sont désormais les entreprises qui utilisent des réseaux totalement déconnectés de l'extérieur à cause, notamment du manque d'expertise, du besoin de reduire les coûts opérationnels et les avantages liés à l'utilisation des réseaux publics pour interconnecter différents sites d'une société.

Le télétravail, la télémaintenance, la densification des échanges d'information et les autres procédés de gestion à distance vont à l'encontre du cloisonnement censé protéger les réseaux locaux des entreprises des attaques extérieures. Les externalisations des systèmes d'information conduisent à ce que des systèmes d'informations de plusieurs sociétés soient hébergés par une seule entreprise dont la défaillance (panne électrique par exemple) rend inaccessible l'ensemble des systèmes d'informations qu'elle héberge. Aussi, pour des raisons économiques, certaines entreprises ne déploient pas leurs propres réseaux pour interconnecter leurs sites et font transiter leurs données, parfois sensibles, via le réseau Internet. Ceci rend ces données plus vulnérables aux attaques. L'interconnexion des réseaux dédiés à ces infrastructures avec le réseau Internet accessible à l'ensemble des individus connectés à l'Internet ouvre de nombreuses failles permettant à des individus non autorisés à accéder aux systèmes de contrôle de ces infrastructures et à des attaquants de pouvoir altérer simultanément un grand nombre d'infrastructures essentielles et dissimuler la responsabilité.

En effet, l'Internet est une interconnexion de plusieurs réseaux hétérogènes appelés systèmes autonomes (*Autonomous System* AS). Au début de l'Internet, cette interconnexion était fondée sur un système hiérarchique simple où des réseaux de petite taille (réseaux des campus par exemple) sont connectés à des réseaux régionaux qui, à leur tour, sont connectés à un réseau backbone national. A partir du milieu des années 90, des nouveaux enjeux financiers ont émergés et ont conduit à l'apparition de réseaux géographiquement très étendus (Cogent[2]

[1] http://www.insee.fr/fr/themes/document.asp?ref_id=ip1228
[2] http://www.cogentco.com

par exemple) avec des points de présence dans la majorité des continents et interconnectant plusieurs réseaux fournisseurs de services Internet de différents pays. Et ces réseaux fournisseurs de services Internet (*Internet Services Provider ISP*) se sont connectés à plusieurs réseaux backbones avec des interconnexions essentiellement basées sur des contrats commerciaux. Cette évolution favorisée par les progrès en terme de performance des protocoles et de capacités des liens et de commutation a conduit à une architecture complexe, fortement décentralisée. Avec cette nouvelle architecture décentralisée et complexe, l'Internet avec ses millions d'utilisateurs (plus $1,7$ milliards d'utilisateurs en 2009[3]) dispersés partout dans le monde est devenu difficile à contrôler et à sécuriser. Dans une telle situation, l'interconnexion de l'Internet avec les réseaux d'entreprises, notamment des réseaux dédiés des infrastructures critiques rendant possible l'accès à des informations sensibles et aux systèmes de contrôles de ces infrastructures critiques à partir du réseau Internet constitue un enjeux de sécurité majeur. Aussi, le réseau Internet est une concentration d'une multitude de technologies émergentes, complexes et standardisées, donc accessibles et connus par un grand nombre de personnes. Par conséquent, il reste aussi très vulnérable aux attaques. Pour toutes ces raisons, l'interconnexion des réseaux dédiés des infrastructure critiques à l'Internet exposent ces infrastructures de plus en plus aux menaces émanant de l'Internet.

En mai 2008, par exemple, la société d'audit *Core Security* de la ville de Boston découvre une vulnérabilité du logiciel *Suitelink* largement utilisé dans les stations de transformation électrique et les raffineries d'hydrocarbure. Cette vulnérabilité permettait de mettre ce logiciel hors service par un simple envoi d'un paquet de données avec une taille excessive à l'ordinateur sur lequel tourne ce logiciel[4]. Ce qui aurait permis à un attaquant de mettre ce logiciel hors service et ainsi de causer des dommages aux installations concernées à partir d'un réseau externe comme Internet.

Aussi, la plupart des infrastructures critiques ont des systèmes de contrôle avec des logiciels conçus selon l'architecture SCADA. Un logiciel conçu sur la base de cette architecture est constitué de plusieurs entités qui communiquent grâce aux réseaux. Ces entités comprennent, entre autres, les stations maîtres qui permettent de piloter, à distance, différents autres stations et capteurs et de collecter les données transmises par ces capteurs. L'interconnexion des réseaux dédiés à ces systèmes de contrôle avec les réseaux accessibles à tous, comme Internet, ouvre de nombreuses failles permettant à un attaquant de causer des dommages à ces systèmes de contrôle. En janvier 2003, par exemple, le ver informatique Slammer avait provoqué la désactivation du système de surveillance de la sécurité de la centrale nucléaire de Davis-Besse de l'opérateur *FirstEnergy* [91]. Il a aussi réussi à toucher le système SCADA d'un autre opérateur dont le nom n'a pas été révélé dans le document du NERC (*North American Electric Reliability Council*), en s'introduisant dans le réseau local de l'opérateur via les interconnexions avec d'autres opérateurs. Enfin, il a causé le blocage du trafic du système SCADA de certains réseaux électriques qui utilisaient le réseau Internet pour acheminer leurs trafics [42].

Par ailleurs, les technologies de l'information et de la communication ont contribué à optimiser les processus dans les infrastructures qui, par conséquent opèrent avec des charges de plus en plus proche de leurs capacités maximales. En France, par exemple, RTE (Réseau de

[3] http://www.internetworldstats.com/stats.htm
[4] http://www.newscientist.com/article/mg19826566.200-power-plants-open-to-hacker-attack.html

Transport d'Électricité)[5] avait enregistré 5 jours de consommation record en électricité les 5, 6, 7, 8 et 9 janvier 2009 avec des valeurs estimées respectivement à 90200MW, 91500MW, 92400MW, 91402MW et 91239MW. Ces charges record réduisent les marges de manœuvre en terme de solution de secours à cause de l'utilisation maximale des ressources des infrastructures, donc la diminution des réserves en ressources. La réduction de la marge entre la charge et la capacité de plusieurs infrastructures aggrave leur vulnérabilité car cette marge constitue un facteur de sécurité pour certaines infrastructures comme le réseau électrique.

Malgré une prise de conscience très ancienne des menaces liées aux phénomènes des interdépendances (théorie du *industrial web* de l'école militaire américaine *Air Corps Tactical School* en 1930), l'intérêt des chercheurs à ce sujet est relativement récent. Ces dernières décennies, les interdépendances des infrastructures critiques et les propagations des pannes qu'elles peuvent engendrer ont suscité, pour la recherche, un grand intérêt et de nombreux travaux scientifiques ont été menés sur ce sujet. Étant donné le faible niveau de compréhension des interdépendances des infrastructures, la plupart de ces travaux concerne la modélisation des interdépendances. L'attention sur les aspects de sécurité liés aux interdépendances a été notamment attirée par des organismes comme CIAO (*Columbia International Affairs Online*) [6] et par des projets comme PCCIP et EPCIP (*European Programme for Critical Infrastructure Protection*). A la suite du premier rapport de la PCCIP dont la principale recommandation était la mise en place d'un système d'échange d'informations entre les pouvoirs publics et les secteurs privés qui détenaient environ 80% des infrastructures critiques nationales des Etats-Unis, plusieurs projets ont été initiés et des fonds conséquents ont été alloués aux universités, laboratoires et compagnies privées menant des travaux sur ce sujet pour permettre d'identifier les vulnérabilités auxquelles ces infrastructures sont exposées et d'évaluer les risques liés aux interdépendances. En Europe, l'émergence des travaux consacrés à ce sujet a été matérialisée par le programme européen EPCIP démarré en juin 2004 qui a été suivi par des projets comme CI2RCO (*Critical Information Infrastructure Research Co-ordination*) en 2004, IRRIIS (*Integrated Risk Reduction of Information-based Infrastructure Systems*) en 2005 et ReSIST (*Resilience for Survivability in Information Society Technologies*) en 2006.

L'intérêt récent des chercheurs pour les interdépendances des infrastructures critiques s'explique par le risque des pannes généralisées qui peuvent survenir à cause des propagations des pannes à travers ces interdépendances et le manque de compréhension des interdépendances qui empêche de prévoir l'évolution des pannes dans ces infrastructures pour pouvoir les prévenir. Pour améliorer la compréhension des interdépendances, les chercheurs ont principalement consacré leurs premiers travaux sur les interdépendances à leur modélisation et à leur simulation afin de faciliter la mise en œuvre des techniques qui permettent de lutter contre les pannes en cascade des infrastructures critiques. Le document [114] donne la liste des principaux projets et logiciels consacrés à la modélisation et à la simulation des interdépendances avant 2006. Ces différents projets ont permis de concevoir de nombreuses techniques de modélisation et de simulation.

Les résultats des travaux actuels sur ce sujet montrent qu'il existe, en général, deux approches pour aborder le problème de la modélisation et de la simulation des interdépendances.

[5] http://clients.rte-france.com/lang/fr/visiteurs/vie/vie_stats_jour_rem.jsp
[6] http://www.ciaonet.org

La première consiste à fédérer des logiciels de modélisation des infrastructures déjà existants et la deuxième utilise les graphes pour représenter l'ensemble des infrastructures impliquées et la théorie des graphes pour caractériser les interdépendances. La principale limite de la première approche est la complexité de sa mise en œuvre et l'impossibilité d'étudier les interdépendances entre un grand nombre d'infrastructures. La seconde approche permet de surmonter la plupart des limites de la première, mais son inconvénient est le niveau d'abstraction qu'elle nécessite, donc ses résultats approximatifs. Ces deux approches seront présentées de manière détaillée plus loin dans ce manuscrit.

Dans le cadre de cette thèse, nous nous intéressons aux cyber-interdépendances et aux pannes en cascade qui peuvent se propager entre différentes infrastructures par l'intermédiaire des réseaux de télécommunications et toucher des systèmes d'informations sensibles des infrastructures critiques. La notion des pannes en cascade utilisée dans ce manuscrit désigne l'ensemble des défaillances susceptibles de se propager d'une infrastructure à une autre, quelque soit la cause de cette défaillance (panne ou attaque). Ces défaillances regroupent toutes les dégradations ou interruptions de service en rapport avec les interdépendances, c'est à dire tous les défauts qui se propagent au sein d'une même infrastructure ou d'une infrastructure à une autre. De ce fait, nous utiliserons, dans ce mémoire, aussi bien le terme de propagation des pannes que celui de propagation de défaillances ou pannes en cascade pour désigner la transmission d'une dégradation ou d'une interruption du fonctionnement d'une infrastructure à une autre, suite à leurs interactions ou à l'influence que l'état de l'une peut avoir sur l'état de l'autre infrastructure. Donc, dans ce manuscrit, les pannes en cascade désignent, toute incapacité (accidentelle ou intentionnelle) d'un système ou d'un composant d'assurer sa fonction avec les performances requises et capable de se propager. La propagation des virus, les annonces des fausses routes (*IP Hijacking*) par les protocoles de routage, les attaques par déni de service (*Denial Of Service - DOS*), les pannes électriques, ... sont, entre autres, des exemples des pannes dont il est question dans ce mémoire. Tous ces types de pannes sont capables de se propager et de causer, instantanément, des dommages à différents réseaux. Par exemple, l'annonce des fausses routes conduit souvent à des pertes des paquets, ce qui peut entraîner une mauvaise estimation de l'état d'une infrastructure. Les attaques DOS (*Denial-Of-Service*) provoquent la surcharge, et, comme les pannes électriques, la panne de certains équipements comme les routeurs, ce qui peut conduire, par effet domino à des pannes d'autres routeurs, puis à des pannes à grande échelle des réseaux. En revanche, nous ne nous intéressons pas, dans ce mémoire, à tous les phénomènes qui ne sont pas susceptibles de se propager entre différents réseaux, par exemple, les attaques qui visent à voler des mots de passe.

Les cyber-interdépendances ont déjà fait l'objet de nombreux travaux de recherche. Ces travaux, comme ceux des auteurs de [64] qui ont étudié la propagation des défaillances sur plusieurs types de graphes montrent que ces propagations dépendent fortement de la topologie du réseau impliqué. Par conséquent, à cause de l'interconnexion des réseaux dédiés et de l'Internet, il est devenu approximatif de mener des études d'évaluation des robustesses des réseaux dédiés aux infrastructures critiques sans inclure le réseau Internet. Or les travaux menés jusqu'à maintenant dans ce domaine s'intéressent à des topologies de niveau AS ou à des échantillons topologiques représentant uniquement des réseaux dédiés. Dans l'un ou l'autre cas, les topologies considérées sont donc loin de représenter fidèlement la structure actuelle de ces réseaux. La première méthode ignore complètement les réseaux dédiés car ils sont noyés

dans le système autonome auquel ils sont connectés et l'ensemble constitue un nœud du graphe considéré. Dans le second cas, les auteurs de ces travaux considèrent une topologie partielle de la structure réelle et s'intéressent, le plus souvent, uniquement aux impacts de la défaillance d'un composant sans s'occuper des événements et des conditions qui conduisent à ce défaut. Par exemple, des travaux comme ceux de [127] et [77] évaluent l'impact de la panne d'un ou de quelques nœuds du réseau de télécommunications sur les performances du réseau électrique, mais n'étudient pas les conditions qui provoquent les défaillances de ces composants du réseau de télécommunications. Avec les travaux présentés dans ce mémoire, nous essayons de pallier ces insuffisances en concevant des modèles et des simulateurs permettant de caractériser et d'étudier la succession des événements qui conduisent aux défaillances d'un composant de l'infrastructure, en appliquant ces simulateurs sur des topologies qui peuvent représenter, de manière réaliste les réseaux intra et inter AS formant l'Internet et en méttant en œuvre les caractéristiques des protocoles de routage qui influent la propagation des défaillances dans les réseaux de télécommunications.

Dans la suite de ce manuscrit, le chapitre 2 est consacré à une présentation générale du contexte où nous décrivons les architectures des réseaux impliqués dans les modèles développés et les différents sujets traités, notamment les interdépendances et les pannes en cascade. Ensuite, nous présentons, au chapitre 3, un simulateur des interdépendances entre les réseaux électriques et de télécommunications permettant de simuler la propagation des pannes entre ces deux infrastructures. Ce simulateur est fondé sur la théorie des graphes pour étudier les interdépendances entre les réseaux électriques et les réseaux de télécommunications et permet d'évaluer les propagations des pannes entre ces deux réseaux. Pour répondre aux carences liées à l'abstraction des modèles et simulateurs fondés sur cette approche, notre simulateur met en œuvre les principaux facteurs qui influent la propagation des pannes dans les réseaux électriques et de télécommunications, notamment la distribution des charges pour le réseau électrique et le routage pour le réseau de télécommunications.

Ensuite, nous concentrons notre étude sur les réseaux de télécommunications et développons un simulateur de propagation des pannes fondé sur des techniques issues de l'épidémiologie ou le modèle d'épidémie [45, 21, 98], classiquement utilisé pour étudier la propagation des vers informatiques et virus informatiques dans l'Internet. Pour mettre en œuvre ce simulateur, nous développons des modules spécifiques pour caractériser les rôles des protocoles des réseaux dans les propagations des pannes au sein des réseaux de type Internet, comme les propagations des virus informatiques. Compte tenu de l'importance du rôle de la topologie dans les phénomènes dynamiques des réseaux comme les propagations des pannes [117] pour lesquelles le réseau représente la trame, nous proposons un algorithme de génération de topologie inspiré du principe de déploiement des réseaux. Cet algorithme est présenté dans le,chapitre 4 et permet de générer des topologies ayant toutes les caractéristiques nécessaires aux études des phénomènes liés aux interdépendances, notamment l'identification des nœuds des graphes représentants les topologies pour offrir la possibilité d'appliquer des traitements spécifiques à certaine catégorie de nœuds. Par exemple les nœuds représentant les routeurs BGP. La validation des topologies générées est réalisée par une comparaison de ces topologies avec des topologies réelles et des topologies obtenues par d'autre technique de génération. Ensuite, le simulateur de propagation des défaillances proposé est appliqué à une des topologies générées par notre algorithme pour étudier les pannes en cascade et évaluer les risques liés à l'intercon-

nexion des réseaux publics et des réseaux internes des infrastructures critiques. Ce simulateur de propagation des pannes fait l'objet du chapitre 5. L'impact des défaillances de ces réseaux est évalué et les résultats de nos simulations exposés de manière à permettre la comparaison des différentes techniques de dimensionnement des réseaux.

Enfin, nous proposons, dans le chapitre 6, un système de détection des pannes fondé sur l'échange d'informations entre opérateurs de différents réseaux. En effet, dans la lutte contre les propagations des défaillances conduisant à des pannes généralisées, le délai de détection des événements de risque par les opérateurs des réseaux exposés constituent un facteur déterminant pour la vitesse de propagation et l'ampleur des pannes. Or de nombreux rapports [63, 41, 62] d'experts qui enquêtent sur ces types de pannes indiquent qu'à cause du manque d'échange d'informations entre les opérateurs des infrastructures concernées, ces pannes sont, le plus souvent, détectées tardivement. Aussi, pour certaines infrastructures, comme les réseaux de télécommunications, la propagation des défaillances est tellement rapide qu'elle ne laisse pas le temps aux opérateurs de prendre les mesures appropriées permettant d'arrêter ces propagations avant qu'elles ne prennent des proportions importantes. Le seul moyen efficace de lutter contre ces phénomènes est de mettre en place des dispositifs techniques capables de détecter automatiquement ces pannes. L'Internet étant une interconnexion de plusieurs réseaux gérés par plusieurs opérateurs, ces dispositifs doivent être déployés sur des réseaux administrés par différents opérateurs. Or certains de ces opérateurs peuvent être des concurrents, favoriser l'échange d'informations entre plusieurs concurrents est un exercice très délicat. Pour faire face à cette contrainte, la plateforme proposée est basée sur des accords, à l'image du fonctionnement du protocole BGP, et permet un échange automatique et sécurisé d'informations entre les opérateurs des réseaux impliqués.

Pour terminer, nous présentons, dans la dernière section de ce manuscrit, l'intérêt de nos résultats pour les opérateurs des réseaux en terme de réduction des pannes en cascade, de conception et de dimensionnement des réseaux d'opérateurs et, enfin notre conclusion et les perspectives.

Chapitre 2

Contexte : Architectures et Interdépendances des réseaux électriques et de télécommunications

Pour faciliter la compréhension du sujet traité dans ce manuscrit, nous exposons dans cette section une présentation générale des interdépendances des infrastructures critiques, principalement celles entre les réseaux électriques et de télécommunications. Puis, nous décrivons les pannes en cascade qui peuvent découler de ces interdépendances, énumérons quelques exemples de pannes liées aux interdépendances et présentons une synthèse des enjeux de sécurité liés aux propagations des défaillances.

2.1 Interdépendances des infrastructures critiques

Dans ce mémoire le terme d'interdépendance désigne l'interconnexion explicite entre les entités (composants, environnement et activités des composants) des différentes infrastructures susceptibles de favoriser la propagation des défaillances entre ces infrastructures. De par leurs caractéristiques, les interdépendances des infrastructures critiques se matérialisent de différentes manières, certaines sont purement matérielles alors que d'autres font intervenir des facteurs plus abstraits comme l'opinion publique, par exemple la dimunition de la fréquentation du transport aérien suite à un accident d'avion. Ainsi, dans le but d'améliorer la compréhension, Dudenhoeffer et Perman [53] classent les interdépendances en cinq catégories :

– Les interdépendances physiques : sont celles où l'influence entre les états des infrastructures interdépendantes est de nature physique ou matérielle. Prenons l'exemple des réseaux électriques et des réseaux de télécommunications. Les premiers fournissent les moyens de pilotage et de supervision des réseaux électriques qui, à leur tour alimentent en électricité les commutateurs et autres équipements nécessaires au fonctionnement des réseaux de télécommunications. L'état d'une infrastructure influence directement celui de l'autre infrastructure et vice-versa, donc les conséquences des changements d'état d'une infrastructure touchent directement les infrastructures interdépendantes. De ce fait,

les risques de propagation des pannes est élevé et la vulnérabilité d'une infrastructure dépend fortement de celle des autres infrastructures interdépendantes.

– Les interdépendances géographiques : Lorsque différentes infrastructures ou des équipements appartenant à différentes infrastructures sont à proximité les uns des autres, on parle d'interdépendances géographiques. Dans ce cas, un événement local peut provoquer des changements d'état pour l'ensemble de ces infrastructures. Dans les interdépendances géographiques, les propagations des pannes ont lieu lorsque des désastres affectent l'endroit où se situent les équipements en question, c'est par exemple une explosion d'une conduite de gaz qui provoque des dégâts sur les conduites d'eau et les fibres optiques qui passent à proximité de l'endroit de l'explosion. Dans cet exemple, les défaillances qui touchent les infrastructures concernées sont dues uniquement à leur proximité géographique, les changements d'état d'une infrastructure n'ont pas d'influence sur les autres et tout événement qui survient à cet endroit touche simultanément l'ensemble des infrastructures. Les interdépendances géographiques peuvent concerner plusieurs infrastructures à cause de leur promiscuité. Ce type d'interdépendance peut entraîner simultanément des multiples pannes qui ne sont souvent pas pris en compte dans les analyses de sécurité. On s'aperçoit donc qu'il est possible d'avoir en même temps des interdépendances physiques et géographiques.
– Les interdépendances logiques : Ce sont toutes les interdépendances où l'état de chaque infrastructure dépend des états des autres infrastructures via des influences liées à des procédures ou politiques, mais aussi à des facteurs sociaux en rapport avec ces changements d'état. C'est dans ce type d'interdépendances qu'intervient le plus le facteur humain. Comme exemple d'interdépendances liées aux procédures, on peut prendre la fermeture d'une route suite à un accident par exemple. Cette décision peut augmenter le trafic ferroviaire suite à la hausse de la fréquence qui fait suite à la baisse de l'utilisation des véhicules personnels. L'accroissement du trafic ferroviaire qui demande plus d'énergie électrique peut provoquer une surcharge du réseau électrique et éventuellement une panne de ce dernier. L'opinion publique, l'actualité sont, entre autre, les facteurs sociaux déterminants pour la catégorie des interdépendances sociales. Par exemple les attaques de septembre 2001 ont engendré des pertes financières considérables pour le transport aérien liées à la baisse de la fréquentation du public [114].
– Le dernier type d'interdépendance est celui des interdépendances relatif aux technologies de l'information et de la communication désigné, le plus souvent par le terme de cyber-interdépendance. Une infrastructure est cyber-dépendante si l'état de celle-ci est dépendante des informations numériques transitant par une infrastructure de télécommunications. Les cyber-interdépendances seront largement décrites dans la suite de ce manuscrit car elles constituent l'axe principal des sujets traités dans le cadre de cette thèse.

Selon l'objectif visé, d'autres critères peuvent servir de base pour la classification des interdépendances. Par exemple, pour une modélisation destinée à faciliter leur compréhension, les interdépendances peuvent être classées en fonction des facteurs déterminants qui influent la manière dont les infrastructures interagissent entre elles. Ainsi, l'article [124] classe les interdépendances en fonction du degré, de l'ordre et de l'intensité du couplage des infrastructures et de la complexité des interactions. Le degré des interdépendances d'une infrastructure ca-

ractérise le nombre d'infrastructures avec lesquelles elle a des relations d'interdépendances. À titre d'exemple les réseaux électriques et de télécommunications ont des degrés d'interdépendance élevés car ils fournissent des services à la plupart des autres infrastructures contrairement au réseau d'approvisionnement de gaz qui ne fournit de service qu'au réseau électrique pour les générateurs et au réseau de télécommunication pour le système de refroidissement. L'ordre indique si les interdépendances sont directes ou indirectes. Dans le cas des interdépendances indirectes, l'influence d'un changement d'état d'une infrastructure sur une autre se fait par l'intermédiaire d'une infrastructure tierce. Le couplage est dit fort lorsque l'une des infrastructures est indispensable au fonctionnement de l'autre. Par exemple, les transports ferroviaires modernes sont fortement dépendants du réseau électrique car les chemins de fer cessent de fonctionner dès que le réseau électrique tombe en panne. En revanche, la dépendance du réseau électrique au réseau ferré est moins forte. En effet le transport ferroviaire assure le transport de câbles de remplacement pour le réseau électrique, mais une défaillance du transport ferroviaire n'entraîne pas directement la défaillance du réseau électrique. Quant aux interactions, elles peuvent être linéaires ou complexes. Les interactions dites linéaires sont celles qui sont usuelles et bien connues des opérations de production et de maintenance, tandis que les interactions complexes sont non familières, non prévues, parfois inattendues et difficilement compréhensibles. Les interactions complexes se manifestent lorsque des composants d'une infrastructure interagissent avec ceux d'une autre infrastructure en dehors des séquences normales des opérations.

2.2 Architecture et Modélisation des réseaux de télécommunications de type Internet

L'Internet est une large interconnexion d'une multitude de réseaux qui échangent du trafic à l'aide d'un protocole unique, IP (*Internet Protocol*) qui permet à des ordinateurs hétérogènes de communiquer entre eux. Chacun des réseaux est géré par une structure administrative appelée système autonome ou AS (*Autonomous System*). Un AS est un ensemble de réseaux IP contrôlés par une même entité administrative et identifié par un nombre entier. Un AS fournit une interconnexion entre un ou plusieurs réseaux et l'Internet en appliquant ses propres politiques aux trafics entrant et sortant de son domaine. De nombreux AS sont des fournisseurs de services Internet (*Internet Services Provider - ISP*), mais on trouve aussi des entreprises, des institutions publiques, d'enseignements et de recherche, des fournisseurs de contenus comme Yahoo et Google et des réseaux de distribution de contenus (*Content Delivery Network - CDN*) comme Akamai et Limelight [39]. Chacun de ces AS gère de manière autonome ses réseaux et ses plages d'adresses, mais doit être physiquement connecté aux autres AS pour pouvoir recevoir le trafic destiné à ses clients et acheminer le trafic de ses clients à l'ensemble des destinataires potentiels connectés à l'Internet.

Chaque réseau met à disposition des utilisateurs différents services avec différents niveaux de qualité de service. La connectivité globale entre les AS est assurée par des accords entre opérateurs pour acheminer le trafic émis par leurs clients ou destinés à ces derniers. Ces interconnexions physiques et logiques influent fortement les chemins suivis par les paquets IP, la qualité et les types de service supportés par le réseau Internet.

Au début de l'Internet ces interconnexions étaient relativement simples, mais l'accroisse-

ment des enjeux économiques et financiers de l'Internet a conduit à des contrats entre opérateurs très variés, donc à des interconnexions très complexes. Cette augmentation de la complexité a fait l'objet de nombreux travaux de recherche, notamment celui des auteurs de [57] qui ont étudié l'augmentation de la complexité des interconnexions à cause de l'inégalité des trafics des différents réseaux. Ils ont démontré, entre autres, que l'assymetrie du trafic entre les réseaux spécialisés dans la distribution du contenu comme Google et de ceux spécialisés dans l'interconnexion des utilisateurs qui, eux sont des consommateurs de contenu comme Cogent aggrave cette complexité.

Aujourd'hui ces interconnexions ont conduit à un immense maillage qui repose sur des infrastructures disséminées à travers le monde : serveurs DNS (*Domain Name System*) [9], centres hébergeurs et des millions de routeurs permettant d'aiguiller le trafic sur les différents réseaux, via des câbles terrestres et sous-marins ou encore par voie satellitaire. Il existe plusieurs dispositifs permettant d'assurer les liaisons physiques et logiques de cet ensemble très massif, mais le plus important est l'infrastructure de routage. Les protocoles de routage maintiennent la connectivité au sein et entre les AS et sont conçus pour calculer les routes et mettre à jour automatiquement les tables de routage après une défaillance. On distingue deux principales catégories de protocoles de routage : les protocoles de routage intra-domaine qui sont utilisés pour le calcul des routes à l'intérieur d'un AS et les protocoles de routage inter-domaine qui sont dédiés au routage entre les AS. Les protocoles les plus utilisés pour le routage intra-AS sont les protocoles RIP (*Routing Information Protocol*) [11] et OSPF [10] alors que BGP [122] est, lui utilisé pour le routage inter-domaine. Ces protocoles calculent les chemins que les paquets émis ou transitant par un nœud doivent suivre pour atteindre leurs destinations. Les protocoles de routage intra-domaine sélectionnent le plus court chemin pour atteindre chaque destination, ils utilisent des algorithmes comme *Bellman-Ford* pour le protocole RIP et *Djikstra* pour le protocole OSPF. Quant au protocole BGP, il utilise, en plus de la longueur des chemins, de nombreux critères pour prendre en compte les politiques du domaine impliqué et pour permettre à chaque AS de configurer ses préférences et d'appliquer ses politiques de routage.

Les informations sur ces chemins sont regroupées dans une table de routage, elles indiquent, notamment les prochains routeurs à utiliser pour acheminer des paquets destinés aux réseaux accessibles au nœud en question. Cette table de routage est mise à jour à chaque modification des routes causée, notamment par la découverte des meilleurs routes ou des défaillances de liens ou de routeurs. À chaque modification, l'ensemble des routeurs impliqués échangent leurs tables de routage (les informations sur les réseaux accessibles par chacun des routeurs), effectuent de nouveaux calculs avec les nouvelles informations reçues et mettent à jour ces tables de routage. Pour limiter le trafic lié à l'échange des informations de routage lorsque le réseau devient instable, ces protocoles peuvent êtres configurés à l'aide des paramètres (comme *InfTransDelay* pour OSPF[1], *MinRouteAdvertisementIntervalTimer* pour BGP) pour fixer un intervalle de temps minimum entre deux annonces successives de modification ou de suppression d'une route. Les paquets transitant par un réseau peuvent donc être acheminés plus ou moins vite en fonction des configurations des protocoles de routage. Par conséquent, la performance de ces protocoles, leurs configurations et l'état du réseau (réseau congestionné ou non) ont

[1] urlhttp ://www.ietf.org/dyn/wg/charter/ospf-charter.html

une incidence non négligeable sur tout acheminement d'information dans les réseaux et, par conséquent sur les propagations des défaillances.

Les informations collectées à l'aide de ces protocoles et stockées dans les tables de routage concernent, en plus des routes, les métriques et les politiques des AS associées à chaque route [17]. Ces informations permettent, non seulement de suivre l'évolution de l'architecture de l'Internet grâce aux données relatives aux politiques de routage et des métriques fournies par les différents AS, mais aussi d'évaluer la consommation des ressources [78] car la taille des tables de routage a une répercussion sur la consommation CPU (*Central Processing Unit*) et mémoire des routeurs et la bande passante absorbée par le trafic des protocoles de routage.

Pour le réseau Internet, la propagation des virus informatiques et vers informatiques, la surcharge des liens et des serveurs appelée aussi attaque par déni de service (*Denial Of Service - DOS*), la corruption des tables de routage par l'annonce des fausses informations (*Prefix hijacking*) ou les pannes des composants matérielles comme les routeurs ou les liens constituent l'essentiel des facteurs conduisant à des pannes en cascade.

L'ensemble de ces facteurs sont liés à du trafic réseau acheminé de la même manière que le trafic normal. Par conséquent, les protocoles de routage et les informations qu'ils collectent sont déterminantes pour toute étude portant sur les pannes en cascade dans le réseau Internet. Par exemple, la taille des tables de routage, la performance des routeurs et la capacité des liens du réseau influent fortement la vitesse des propagations des pannes. Par conséquent, les modèles et simulateurs destinés à l'étude des propagations des défaillances doivent prendre en compte l'ensemble de ces facteurs pour pouvoir fournir des résultats pertinents.

2.3 Architecture et Modélisation des réseaux électriques

Les réseaux électriques font partie des grandes réalisations techniques accomplies par l'humanité dans les 100 dernières années. Ils constituent une ressource essentielle et sont impliqués dans toutes les activités de la société moderne, la santé, la sécurité, les administrations, les transports, les communications, le commerce, etc.

A la différence du réseau Internet où tous les éléments terminaux peuvent être à la fois producteurs et consommateurs de flux, le réseau électrique est constitué d'un ensemble d'éléments producteurs, transporteurs et consommateurs de l'énergie électrique.

Les stations de production comprennent les générateurs (machines synchrones), les turbines et les circuits de contrôle qui permettent de maintenir l'amplitude et la fréquence de la tension constantes.

Pour acheminer l'énergie électrique entre les centres de production et les consommateurs, le flux électrique emprunte successivement le réseau de transport, destiné à transporter des quantités importantes d'énergie sur de longues distances, le réseau de répartition, destiné à répartir l'énergie en quantité moindre, sur de courtes distances et le réseau de distribution qui achemine l'énergie électrique vers les consommateurs.

Le réseau de transport assure le transport de l'électricité à l'échelle nationale, voire internationale, principalement en haute et très haute tension (400000 volts par exemple) sur des très longues distances. Ce niveau de tension permet de réduire les pertes en ligne (chaleur dissipée par effet Joule dans les conducteurs). Sa principale fonction est d'assurer l'équilibre entre la

production et la consommation d'électricité à l'échelle nationale et de compenser les déséquilibres intra-régionaux, inter-régionaux et internationaux.

Le réseau de répartition assure le transport de l'électricité à l'échelle régionale ou locale en haute tension (225000, 90000 et 63000 volts). Il achemine l'énergie électrique vers les postes sources des réseaux de distribution et les grands clients industriels.

Les réseaux de transport et de répartition ont une topologie fortement maillée pour permettre au flux électrique de transiter par différents chemins et d'assurer ainsi l'alimentation des postes sources du réseau de distribution, même au cas où certaines parties du réseau tombent en panne. Les réseaux de transport et de répartition sont constitués de lignes de transport de l'énergie et des transformateurs. Ces transformateurs se rencontrent aux deux extrémités du réseau de transport : les transformateurs élévateurs de tension augmentent la tension à la sortie des centres de production et les transformateurs abaisseurs de tension qui réduisent la tension destinée aux consommateurs.

Du point de vue des réseaux de transport et de répartition, les charges représentent les réseaux de distribution et les gros consommateurs.

Le réseau de distribution est consacré au transport de l'électricité à l'échelle locale en moyenne tension (20000 volts) et basse tension (380 et 220 volts). La topologie du réseau de distribution a une structure en arbre.

L'électricité ne se stocke pas à l'échelle industrielle : à tout instant, la production d'électricité doit être égale à celle qui est consommée. Les opérateurs doivent donc assurer, en permanence, un équilibre entre les offres de production et les besoins de consommation qui varient avec la saison, la météo du jour, etc. Les opérateurs ont donc besoin de faire des prévisions fiables qui leur permettent de définir les besoins théoriques nécessaires et procéder de manière permanente à des ajustements pendant la journée.

Ils doivent aussi maîtriser la gestion des risques comme les brusques réductions de la production et les augmentations de la consommation pour éviter les pannes en cascade qui conduisent le plus souvent à des pannes généralisées (*blackout*). En effet, comme décrit dans [76], les pannes en cascade dans les réseaux électriques se déroulent en plusieurs phases :

Durant la première phase, une panne matérielle (coupure de ligne, perte d'un générateur, ...) provoque la surcharge des composants adjacents qui peuvent, à leur tour tomber en panne ou être déconnectés du réseau par les systèmes de protection. Puis, au fur et à mesure que le nombre d'équipements touchés par la panne augmente, l'intervalle de temps entre deux pannes successives se réduit. Cet intervalle peut varier de 5 à 20 minutes durant la première phase à seulement 30 secondes lorsque de nombreuses lignes de haute tension du réseau de transport sont touchées et le peu de lignes restantes deviennent fortement surchargées pour compenser la perte de puissance causée par ces pannes. Ensuite, le déséquilibre entre les zones surchargées et des zones en surproduction provoque une instabilité significative de la fréquence causée par l'agmentation de la fréquence des générateurs des zones en sous-production et la dimunition de celle des zones en surproduction. Ce qui peut donner comme résultat l'isolation rapide (10 à 30s) de plusieurs générateurs par les systèmes de protection dont les décisions sont basées sur la fréquence, la phase et la tension. Enfin, l'ensemble des phénomènes décrits ci-dessus conduisent à l'apparition des zones isolées et à une panne généralisée.

Le modèle de propagation des défaillances proposé dans le chapitre 3 est basé sur la répartition des charges (transfert de la charge des composants en pannes sur les composants adjacents)

du modèle standard des réseaux électriques, précisément sur la technique de l'écoulement du flux (*Power Flow*).

Ce modèle standard est fondé sur un système d'équations différentielles non linéaires [100]. Une description détaillée de ce modèle et les principales techniques de simulation numérique du réseau électrique est exposée dans [31]. Pour faciliter la compréhension du modèle du réseau électrique présenté dans le chapitre 3 de ce manuscrit, nous présentons dans cette section une synthèse de la méthode de l'écoulement du flux (*Power Flow*) qui permet d'analyser un réseau électrique à l'état stable. Cette méthode permet de déterminer, notamment l'amplitude et la phase de la tension de chaque nœud et les puissances active et réactive de chaque ligne du réseau afin de pouvoir, par exemple estimer l'état du réseau ou planifier son extension.

Les systèmes d'équations décrivant le système électrique dans la méthode *Power Flow* représentent la variation de la puissance (ΔP) de l'ensemble du système, c'est à dire les générateurs, le réseau (ligne et transformateurs) et les charges. Avec cette méthode, les puissances active et réactive injectées par les générateurs et celles consommées par les charges sont connues et sont constantes, on parle de « *PVbuses* » et « *PQbuses* » pour désigner les générateurs et les charges. La modélisation du système à l'état stable revient donc à représenter la variation des puissances de chaque nœud du réseau de transport (des lignes électriques, des transformateurs) avec des fonctions de la forme :

$$f(x) = 0$$

où la fonction $f(x)$ représente cette variation qui est égale à 0 lorsque le système est à l'état stable. Pour rappel, la puissance électrique P d'un appareil est le produit de la tension électrique aux bornes de laquelle est branchée l'appareil et de l'intensité du courant qui le traverse. Elle se calcule avec la relation $P = UI$ lorsque la tension et l'intensité sont continues et $p(t) = u(t)i(t)$ lorsque ces deux grandeurs varient avec le temps.

$$\begin{gathered} i(t) = \sqrt{2}Isin(\omega t + \theta_I) \\ v(t) = \sqrt{2}Isin(\omega t + \theta_V) \\ \Rightarrow p(t) = P + Acos(2\omega t + \theta_P) \\ \text{où } \theta \text{ est la phase initiale, } \omega = 2\pi f \text{ avec } f \text{ la fréquence} \end{gathered}$$

Pour obtenir la valeur de la puissance pour chaque élément du modèle, il est nécessaire de calculer la tension et l'intensité de cet élément. Ce calcul se fait avec un système de 2 équations à 2 inconnues obtenues à partir de la loi d'Ohm : la tension U aux bornes d'un conducteur de courant continu est égale au produit de la résistance électrique R du conducteur et de l'intensité I du courant qui traverse ce conducteur : U = RI. En courant alternatif sinusoïdale, on ne parle pas de résistance, mais d'impédance Z et la loi d'Ohm s'écrit : U = ZI. Une impédance ($Z = R + jX$) est l'association d'une résistance R et d'une réactance électrique qui peut être capacitive ($X_c = -j\frac{1}{\omega C}$) ou inductive ($X_l = j\omega L$) où C est la capacité et L est l'inductance.

Pour réduire les pertes lors du transport énergétique, le réseau est constitué, en général, des circuits triphasés à courant alternatif, la relation utilisée est donc $U = ZI$ qui est équivalente à $I = Y$U où $Y = G + jB$ est l'admittance, G et B sont respectivement la conductance et la susceptance. Pour rappel, l'admittance est l'inverse de l'impédance $Y = \frac{1}{Z}$, la conductance est l'inverse de la résistance $G = \frac{1}{R}$ et la susceptance ($\frac{1}{X}$) est la réciproque de la réactance.

Pour modéliser un système avec N éléments, l'intensité du courant de chacun de ces éléments est exprimée en fonction de la tension avec le relation $I = YU$ qui permet de représenter l'ensemble du système par la matrice suivante :

$$\begin{bmatrix} I_1 \\ I_2 \\ . \\ . \\ . \\ I_i \\ . \\ . \\ . \\ I_N \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} & . & . & . & Y_{1i} & . & . & . & Y_{1N} \\ Y_{21} & Y_{22} & . & . & . & Y_{2i} & . & . & . & Y_{2N} \\ . & . & & & & . & & & & . \\ . & . & & & & . & & & & . \\ . & . & & & & . & & & & . \\ Y_{i1} & Y_{i2} & . & . & . & Y_{ii} & . & . & . & Y_{iN} \\ . & . & & & & . & & & & . \\ . & . & & & & . & & & & . \\ . & . & & & & . & & & & . \\ Y_{N1} & Y_{N2} & . & . & . & Y_{Ni} & . & . & . & Y_{NN} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ . \\ . \\ . \\ V_i \\ . \\ . \\ . \\ V_N \end{bmatrix}$$

où $Y_{ii} = \sum_{k=1}^{N} (\frac{1}{Z_{ik}})$ est la somme des admittances de tous les éléments connectés au nœud i et $Y_{ij} = \frac{-1}{Z_{ik}}$ est l'admittance de la ligne interconnectant les nœuds i et j. L'obtention des valeurs de l'intensité du courant de chaque nœud permet, ensuite de calculer la puissance complexe ou puissance apparente ($S_i = P_i + jQ_i$) d'un nœud comme suit :

$$S_i = U_i I_i^* = U_i \Sigma_{k=1}^{N} (Y_{ik}^* U_k^*)$$

A l'état stable $\Delta S_i = 0$, donc

$$\Delta P_i(\delta, U, P_i) = P_i - \sum_{k=1}^{N} U_i U_k [G_{ik} \cos(\delta_i - \delta_k)) + B_{ik} \sin(\delta_i - \delta_k)] = 0$$
$$\Delta Q_i(\delta, U, Q_i) = Q_i - \sum_{k=1}^{N} U_i U_k [G_{ik} \sin(\delta_i - \delta_k)) + B_{ik} \cos(\delta_i - \delta_k)] = 0$$

où P_i est la puissance active et Q_i la puissance réactive du nœud i.

Pour chaque nœud, on obtient donc 2 équations non linéaires dont les inconnues sont l'amplitude U_i et la phase δ_i de la tension. Pour un réseau de N nœuds, le modèle est constitué d'un système de $2N$ équations à $2N$ inconnues. La résolution numérique de ce système d'équations non linéaires est complexe et nécessite l'utilisation des techniques spécifiques comme celles de *Gauss-Seidel* [31], de *Newton-Raphson* [31] ou encore la méthode dite *Fast Decoupled Load Flow* [19].

La méthode de *Gauss-Seidel* permet la résolution d'un système d'équations non linéaires, à partir d'une valeur initiale et un calcul itératif pour se rapprocher graduellement de la solution du système d'équations. La méthode de *Newton-Raphson* utilise aussi une valeur initiale et des calculs itératifs, mais elle se fonde sur le calcul des racines des dérivées partielles de la matrice correspondante au système d'équations. La méthode *Fast Decoupled Load Flow* est une amélioration de la technique de *Newton-Raphson*.

Le modèle présenté ci-dessus est utilisé par de nombreux logiciels de simulation des réseaux électriques pour étudier leur stabilité transitoire. Parmi ces logiciels on peut citer TEFTS (*Transient Stability Program to Study Energy Functions*)[2], PSAT (*Power System Analysis Toolbox*)[3]. Le logiciel TEFTS, par exemple lie dans un fichier les données au format WSCC (*Wes-*

[2] http://thunderbox.uwaterloo.ca/~claudio/software/tefts.htm
[3] http://www.power.uwaterloo.ca/~fmilano/psat.htm

tern Systems Coordinating Council) [5] ou IEEE (*Institute of Electrical and Electronics Engineers*) [4] ou encore EMTP (*ElectroMagnetic Transients Program*) [6] pour obtenir la fréquence du flux électrique du réseau, les valeurs de l'inertie, de l'amortissement, de la réactance de chaque générateur du réseau simulé, mais aussi l'inductance et le gain de chacune des lignes. Ensuite, il évalue l'état du réseau simulé en calculant le système d'équations ci-dessus à l'aide la méthode de Newton-Raphson à chaque étape de la simulation.

Selon les contraintes et l'objectif des modèles, il existe une simplification de ce modèle appelée *DC Load Flow* qui néglige la puissance réactive et les composantes résistives et capacitives du modèle des lignes. Cette simplification est possible lorsqu'on ne dispose pas des données complètes du réseau ou lorsqu'on veut réduire le temps de calcul ou encore lorsqu'on s'intéresse qu'à la puissance active. Pour la simulation des pannes en cascade dans les réseaux électriques fondée sur la répartition des charges, la puissance active d'un nœud est suffisante pour estimer la variation de puissance de ce nœud suite à des défaillances des lignes ou des défaillances d'autres nœuds. Nous utilisons donc cette simplification pour mettre en ouvre, dans le chapitre 3, un simulateur unique de propagation des pannes entre les réseaux électriques et de télécommunications.

Pour faciliter la compréhension de l'approche utilisée dans les modèles et simulateurs des pannes en cascade présentés dans le chapitre 3, nous présentons dans les sections suivantes quelques exemples de pannes en cascade dans les réseaux électriques et de télécommunications

2.4 Exemples de pannes en cascade

Avant de présenter quelques exemples de propagations des pannes ayant touché les réseaux électriques et de télécommunications ces dernières années, nous procédons à la définition de certains termes utilisés dans les sections suivantes.

Pannes en cascade : Dans ce manuscrit, les pannes en cascade désignent les pannes au cours desquelles la défaillance d'une infrastructure provoque le dysfonctionnement d'un composant d'une autre infrastructure qui, à son tour provoque la panne de cette infrastructure. Par exemple une panne électrique locale (à cause d'une coupure de câble haute tension par exemple) peut entraîner l'arrêt des services de télécommunications à cet endroit qui provoque l'accroissement du trafic, puis la panne du reste du réseau de télécommunication. Enfin cette panne du réseau de télécommunications peut, à son tour provoquer des défaillances pour d'autres infrastructures à la suite de la perte de leurs systèmes de contrôle SCADA.

L'escalade des pannes : L'escalade des pannes a lieu lorsqu'une panne dans une infrastructure s'aggrave à cause d'une défaillance sans lien direct dans une autre infrastructure, mais en rapport avec la gravité ou le délai de réparation de la panne de la seconde infrastructure. Par exemple une panne électrique peut s'aggraver à cause d'un dysfonctionnement du réseau de transport qui retarde la livraison des équipements de remplacement.

Pannes de cause commune : Les composants de deux ou plusieurs infrastructures peuvent être affectés simultanément par une panne. Ces pannes peuvent se produire soit parce que les composants sont proches géographiquement (interdépendances géographiques)

ou bien parce que l'étendue de la défaillance est très vaste (tremblement de terre, inondation).

La modélisation des pannes de cause commune et celles en aggravation fait intervenir de nombreux facteurs extérieurs et complexes comme les facteurs sociaux et les catastrophes naturelles. Ce type de modélisation est donc, en général abstrait et aléatoire. Dans le cadre de cette thèse, nous nous intéressons essentiellement aux pannes en cascade dont la propagation est essentiellement liée aux caractéristiques des infrastructures et à leur fonctionnement. C'est à dire que les transmissions des défaillances d'un composant à un autre ou d'une infrastructure à une autre se fait exclusivement dans le cadre de leur interaction (par exemple, un routeur qui annonce des fausses routes à un autre) ou des services que ces composants ou ces infrastructures se rendent entre elles (par exemple, une panne électrique qui provoque une panne de serveur).

Dans ce manuscrit, les pannes en cascade désignent toutes les défaillances qui se propagent instantanément pour toucher plusieurs infrastructures. Ainsi nous ne distinguons pas les défaillances causées par des attaques à celles dont les causes ne sont pas intentionnelles. Cependant, nous ne considérons que celles qui sont susceptibles de se propager au sein d'une infrastructure, voire à d'autres infrastructures. Cette propagation peut se faire à cause des transferts de charge entre les composants, à cause de l'influence des infrastructures entre elles ou encore à cause des services que les entités impliquées se rendent mutuellement.

2.4.1 Exemples de propagation des défaillances entre les réseaux électriques et de télécommunications

Les informations précises sur les défaillances des réseaux sont rares et en dépit du fait que les opérateurs de certaines infrastructures (réseaux de télécommunications par exemple) aient l'obligation de communiquer aux autorités publiques de contrôle les informations sur les pannes de celles-ci ayant touché un certain nombre de clients, il reste difficile pour le milieu de la recherche d'accéder à ces informations. Les rapports sur les incidents, souvent classés confidentiels ne sont accessibles qu'à un nombre limité de personnes et à l'administration publique. Les travaux de recherche dans ce domaine se tournent, le plus souvent, vers les rapports publics ou les informations de la presse. Par exemple, les auteurs de [120] utilisent les rapports publics sur les défaillances des réseaux entre 1994 et 2005 pour étudier leur origine et les phénomènes de propagation de pannes liés à ces défaillances et pour évaluer l'impact des pannes des réseaux de télécommunication sur les autres infrastructures.

Les rapports d'enquête sur les grandes défaillances accessibles au public constituent nos principales références pour les exemples des pannes cités ci-dessous. Ces rapports existent en grand nombre et sont, très souvent, disponibles sur les sites Web des organismes qui mènent ces enquêtes malgré la réticence des opérateurs de rendre public les informations relatives aux incidents survenus aux infrastructures pour éviter de dévoiler les vulnérabilités de leurs infrastructures et d'exposer leurs faiblesses à leurs concurrents. Nous nous limiterons donc à un tour très bref de la longue liste des défaillances liées aux interdépendances et connues du public avant de se focaliser sur celles qui concernent les réseaux de télécommunications.

Ces dernières années, de nombreuses pannes généralisées (*blackouts*) ont été causées ou aggravées par les interdépendances entre les infrastructures touchées et les réseaux de télécommunications. Ainsi les États-Unis et le Canada ont été frappés par une panne électrique de

grande ampleur le 14 août 2003[4]. Cette panne a été provoquée, d'après le rapport [63] élaboré par les experts désignés pour l'enquête, par la perte de certains générateurs de l'opérateur *FirstEnergy* suite à une augmentation brusque de la consommation. La succession des évènements inattendus ont provoqué l'apparition d'un bogue du logiciel de supervision XA/21[5] utilisé dans le système de gestion de l'énergie (*Energy Management System - EMS*) du centre de contrôle de Akron dans l'Ohio dont le système d'alarme a cessé de fonctionner. Les opérateurs ne recevant plus d'alarme n'ont pas pris les mesures appropriées et la panne s'est propagée et a provoqué la coupure de certaines lignes haute tension d'un autre opérateur (*Cinergy*) conduisant à une panne généralisée touchant environ 50 millions de personnes et entraînant des pertes estimées à 10 milliards de dollars pour les États-Unis et $2,3$ milliards de dollars pour le Canada. En Europe, les *blackouts* de ces dernières années ont touché entre autre, l'Italie et la partie sud de la Suisse le 28 septembre 2003 [41] et plus récemment la plupart des pays de l'Europe occidentale le 4 novembre 2006 [62]. Les rapports [41, 62] de l'UCTE (*Union for the Co-ordination of Transmission of Electricity*)[6] rédigés suite à ces pannes indiquent que des coupures de lignes haute tension sont à l'origine de ces pannes dont la première a été causée par une chute d'arbre et la deuxième par une coupure accidentelle causée par un navire. Les événements qui se sont succédés par la suite ressemblent à ceux qui se produisent en général lors des pannes de grande ampleur des réseaux électriques. La coupure d'une ligne provoque la surcharge des lignes adjacentes et la coupure en cascade des lignes surchargées conduit à une perte de synchronisation des générateurs, à des oscillations (instabilité de puissance), à des variations anormales des fréquences qui passent en dessous ou en dessus de la fréquence nominale ($50Hz$ en Europe et $60Hz$ en Amérique du Nord) et enfin à la perte de tension. Si la panne de 2006 est principalement due au non respect du critère $N-1$ (critère qui permet de maintenir le fonctionnement de l'infrastructure après la panne d'un de ses composants) et au manque de coordination entre les opérateurs, celle de 2003 qui a touché l'Italie a été considérablement aggravée par les interdépendances. En effet, la panne prolongée a causé l'épuisement des sources d'alimentation de secours des systèmes de contrôle et de communication dont l'indisponibilité a fortement allongé le temps de restauration du réseau électrique.

Ces exemples montrent que l'identification et la caractérisation des propagations des pannes dans les infrastructures critiques sont des tâches loin d'être intuitives, surtout lorsque ces propagations impliquent différentes infrastructures hétérogènes, c'est à dire des infrastructures de différents secteurs. Comme le montrent les exemples ci-dessus, il n'existe pas de lien direct et évident entre les pannes d'un réseau de télécommunications et celle d'un réseau électrique. Ceci est dû principalement au fait que les liens entre ces deux infrastructures sont essentiellement fonctionnels. La panne du réseau de télécommunications n'entraîne pas systématiquement la panne du réseau électrique, mais une dégradation des services essentiels au bon fonctionnement du réseau électrique comme le système de supervision. En revanche, ces propagations deviennent nettement plus évidentes lorsque les infrastructures sont homogènes, par exemple la propagation des pannes entre différents systèmes autonomes.

Puisque les derniers chapitres de ce mémoire sont essentiellement consacrés aux propagations des pannes dans les réseaux de télécommunications, nous présentons dans la section

[4] http://www.nerc.com/filez/blackout.html
[5] http://www.gepower.com/prod_serv/products/scada_software/en/xa21.htm
[6] http://www.ucte.org

suivante quelques exemples des propagations des défaillances ayant touché les réseaux de télécommunications.

2.4.2 Exemples de propagation des défaillances dans les réseaux des télécommunications

L'attaque informatique d'envergure dirigée contre l'Estonie au printemps 2007 [18] est la première de son genre. Les attaquants avaient pu toucher des sites gouvernementaux, ceux des banques, des sites d'information et des opérateurs de téléphonie mobile. Tous les services en ligne ont été interrompus au cours de ces attaques par déni de service distribué(*Denial Of Service - DOS*). Plus récemment, plusieurs sites Web stratégiques des États-Unis et la Corée du Sud ont été victimes d'attaques informatiques le dimanche 5 juillet 2009 [138]. Aux États-Unis, il s'agit, entre autres des sites des départements de la Sécurité intérieure, de la Défense, du Trésor, des Transports et des Services secrets, mais aussi des sites non gouvernementaux comme ceux de la Bourse de New York, du NASDAQ et du Washington Post. En Corée du Sud, c'est le site de la présidence et ceux des ministères de la Défense et des Affaires étrangères qui ont été visés. Les attaquants ont lancé des attaques DOS aux serveurs cibles, occasionnant des indisponibilités dont la durée varie de quelques heures à plusieurs jours. Par exemple le site de la présidence sud-coréenne à été indisponible pendant 4 heures, alors que celui du département américain des Transports a été complètement inaccessible pendant 48 heures.

Ces attaques, le plus souvent par déni de service visaient à saturer les serveurs par des multitudes de demandes de connexions simultanées et utilisaient des réseaux de robots (*botnets*) pour accentuer l'ampleur des dégâts et rendre l'identification de leurs origines particulièrement difficile. Les auteurs de ce type d'attaques se cachent derrière des ordinateurs appartenant à des utilisateurs tiers pour ne pas être démasqués par les services de sécurité. Le prise de contrôle de ces ordinateurs se fait, très souvent, par la diffusion des virus informatiques qui fournissent les informations nécessaires pour accéder aux des ordinateurs victimes. On estime actuellement à plus de 150 millions [33] le nombre de machines passées sous le contrôle des attaquants informatiques. Aujourd'hui il existe un véritable commerce autour de ces réseaux clandestins car leurs propriétaires ne sont, en général pas les véritables commanditaires des attaques, mais ils monnayent leur capacité de génération massive de trafic. Ces réseaux servent aussi à envoyer des courriers électroniques non désirés pour des fins publicitaires (*spams*) ou pour dérober des informations. Les attaques dites « chinoises » [138] dont plusieurs gouvernements occidentaux déclarent avoir été victimes en 2006 et 2007 avaient opté pour une autre technique qui consiste à envoyer des mails avec des pièces jointes piégées comportant des « chevaux de troie » à des hauts responsables ou fonctionnaires. Aux États-Unis ces attaques ont touché principalement les serveurs de messagerie du département de la défense.

Les exemples ci-dessus montrent bien la banalisation de l'usage des outils informatiques et des réseaux comme arme pour mener des attaques coordonnées, simultanées et transfrontalières. Or, avec les réseaux, il est possible, parfois avec une simple authentification virtuelle, d'ouvrir et de fermer rapidement des commutateurs et des clapets, de transférer des fonds à des grandes distances aussi facilement que si le donneur d'ordre se situait dans le même endroit. Aussi, l'uniformisation des architectures comme SCADA pour les systèmes de contrôles des infrastructures, notamment les réseaux électriques et l'interconnexion de ces systèmes de

contrôle au réseau Internet offrent aux cyber-attaquants la possibilité de causer des dommages importants à ces infrastructures. Donc, les cyber-menaces des infrastructures critiques sont liées à celles de l'Internet et regroupent les menaces externes (menaces liés aux réseaux externes) et internes, c'est à dire celles liées aux individus internes à l'infrastructure concernée avec des motivations diverses comme les vengeances et les infiltrations (volontaires et involontaires) par des groupes bien organisés. La prise de contrôle du *Rome Laboratory* par un attaquant adolescent en 1994 [7] en est un exemple frappant. Les défaillances énumérées dans le rapport [120] ainsi que les dégâts causés par les vers informatiques CODE RED et NIMDA en 2001 montrent la fragilité de l'infrastructure des réseaux de télécommunications. La rapidité de propagation et le nombre de composants victimes de ces attaques, environ 360000[7] serveurs IIS (*Internet Information Services*) pour CODE RED II[8], 500000[9] postes Windows pour BLASTER[10] montrent toute la difficulté de la mise en place des outils permettant de lutter contre les phénomènes de propagation des défaillances dans les réseaux de télécommunications.

Aussi plusieurs simulations d'attaques informatiques [7] menées, notamment aux États-Unis contre le département de la défense américaine et des systèmes de contrôle des réseaux électriques et de télécommunications ont montré qu'il est possible de pénétrer ces systèmes avec parfois des privilèges d'administrateur. Ces attaques de test menées, notamment contre les réseaux informatiques du département de la défense américaine et des sociétés privées de l'électricité et des télécommunications montrent qu'il existe des possibilités pour endommager ces infrastructures à partir des cyber-attaques. L'organisme CyberCom[11] (*US Cyber Command*) mis en place par l'administration américaine et chargé de lutter contre ces attaques évalue, en milliers par jour le nombre de tentatives d'intrusion sur les réseaux sensibles américains.

2.5 Résumé du chapitre 2 et synthèse des enjeux de sécurité liés aux interdépendances entre les infrastructures pour la recherche

Suite aux différentes interconnexions, aux politiques d'exploitation et à la proximité géographique, la plupart des infrastructures critiques interagissent entre elles. Ces interactions entraînent souvent des relations complexes, des dépendances et des interdépendances conduisant à des systèmes complexes et dynamiques avec des vulnérabilités plus importantes. Ces interdépendances constituent un facteur idéal pour les propagations des défaillances au cours desquelles une infrastructure victime d'une défaillance peut provoquer des effets de cascade qui affectent d'autres infrastructures.

Ces dernières décennies, comme le montre la figure 2.1, la modernisation des infrastructures et les progrès des technologies de l'information et de la communication ont conduit à l'interconnexion du réseau public Internet avec la plupart des réseaux dédiés aux infrastructures critiques. Or le réseau Internet est une infrastructure complexe et vulnérable, cette interconnexion expose les réseaux et les systèmes d'information des infrastructures aux nombreuses

[7] http://www.thlab.net/~lmassoul/quarantine.pdf
[8] http://www.cert.org/incident_notes/IN-2001-09.html
[9] http://www.thlab.net/~lmassoul/quarantine.pdf
[10] www.cert.org/advisories/CA-2003-20.html
[11] http://www.globalresearch.ca/index.php?context=va&aid=14186

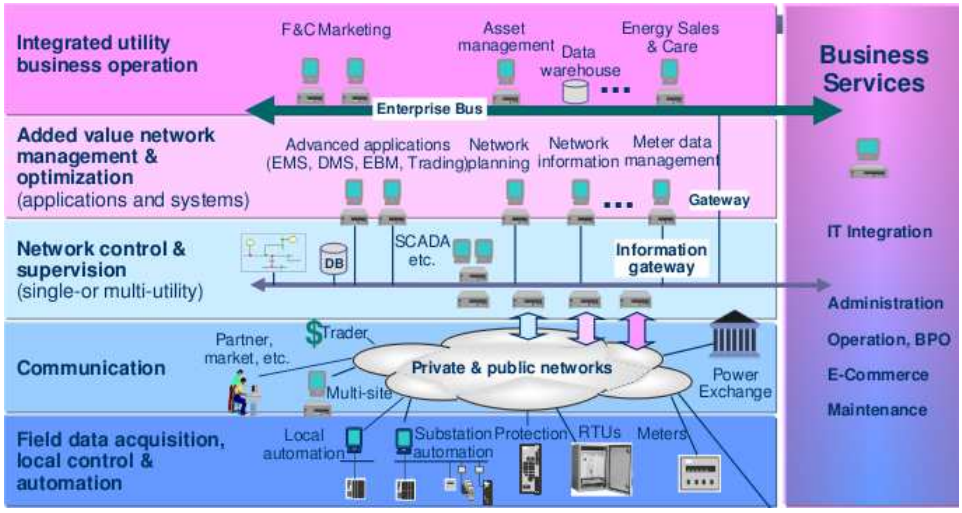


FIG. 2.1 – *Interconnexion des réseaux dédiés et des réseaux publics (crédit Grupo AIA)*

menaces liées à l'Internet. Aujourd'hui, on peut résumer la problématique de sécurité liée aux interconnexions entre les réseaux dédiés et l'Internet comme le présente la figure 2.2.

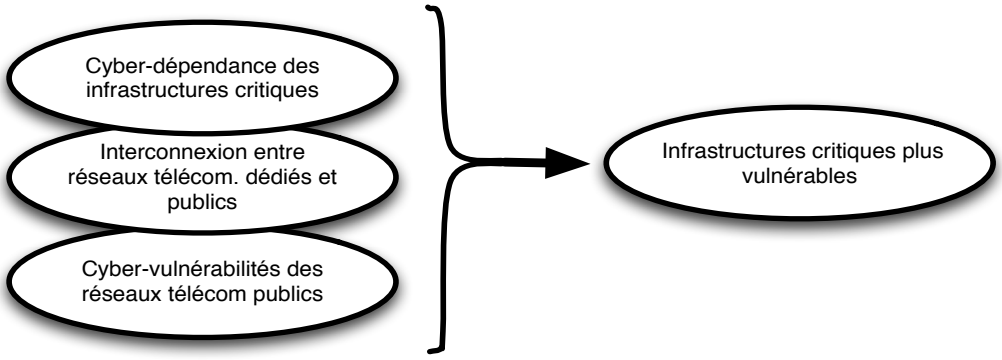


FIG. 2.2 – *Vulnérabilité des infrastructures critiques*

Les infrastructures critiques dépendent fortement des technologies de l'information et de la communication et leurs réseaux dédiées sont de plus en plus interconnectés à l'Internet qui est une infrastructure exposée aux pannes en cascade. Ce qui contribue à augmenter les risques des pannes de grande ampleur pour les infrastructures critiques. Par conséquent, la sécurisation de ces infrastructures passe nécessairement par la mise en place des dispositifs qui tiennent compte du reste de l'Internet.

Plusieurs travaux de recherche sur la propagation des défaillances menés sur plusieurs types de graphes par les auteurs de [64] montrent que ces propagations dépendent fortement de la topologie du réseau en question. Comme on le voit avec le schéma 2.1, il est quasiment impos-

sible d'assurer une protection fiable aux réseaux dédiés des infrastructures critiques en ignorant l'Internet. A cause de l'interconnexion des réseaux dédiés et de l'Internet, il serait trop approximatif de mener des études d'évaluation des robustesses des réseaux dédiés aux infrastructures critiques sans inclure le réseau public faisant partie de l'infrastructure Internet qui constitue la source des menaces potentielles. Or les travaux menés jusqu'à maintenant dans ce domaine s'intéressent à des topologies de niveau AS ou des échantillons topologiques représentant uniquement des réseaux dédiés. Dans l'un ou l'autre cas, les topologies considérées sont donc loin de représenter fidèlement la structure actuelle de ces réseaux. La première méthode ignore complètement les réseaux dédiés car ils sont noyés dans l'AS auquel ils sont connectés et l'ensemble constitue un nœud du graphe considéré. Dans le second cas, les auteurs considèrent une topologie partielle de la structure réelle et s'intéressent, le plus souvent, uniquement aux impacts de la défaillance d'un nœud sans s'occuper des événements et des conditions qui conduisent à ce défaut. A titre d'exemple, des travaux comme ceux de [127] et [77] évaluent l'impact de la panne d'un ou de quelques nœuds du réseau de télécommunications sur les performances du réseau électrique, mais n'étudient pas les conditions qui provoquent les défaillances de ces nœuds du réseau de télécommunications. Dans le cadre de cette thèse, nous essayons de pallier ces insuffisances, en concevant des simulateurs permettant d'étudier la succession des événements qui conduisent aux défaillances d'un composant de l'infrastructure, en appliquant ces simulateurs sur des topologies qui peuvent représenter toutes les composantes de l'infrastructure Internet (réseaux intra et inter AS) et en prenant en compte les caractéristiques des protocoles de routage qui sont déterminantes pour la propagation des défaillances dans les réseaux de télécommunications. La topologie utilisée dans le cadre de nos expérimentations représente un réseau de niveau routeur interconnectant des réseaux locaux au réseau Internet et l'environnement de simulation reproduit toutes les fonctionnalités déterminantes (topologie, protocoles de routage, ...) pour les propagations des défaillances dans le réseau résultant de ces interconnexions.

Chapitre 3

Modélisation et Simulation des propagations des pannes dans des réseaux électriques et de télécommunications interdépendants

3.1 Introduction

L'un des premiers défis dans la lutte contre les effets néfastes des interdépendances des infrastructures critiques est leur compréhension. Les infrastructures impliquées étant, très souvent, de grande taille et d'une complexité importante, la compréhension et la prévention des propagations des défaillances liées à ces interdépendances constituent un enjeu technique majeur. Dans un contexte où la faible compréhension constitue l'une des plus importantes lacunes dans la lutte contre les propagations des défaillances dans les infrastructures critiques, la modélisation et la simulation apparaissent comme une première étape pour étudier les propagations des défaillances, identifier les vulnérabilités de ces infrastructures et améliorer leur protection. Les résultats de ces simulations peuvent être exploités, notamment par les opérateurs des infrastructures pour améliorer la robustesse, élaborer des plans d'extension, réduire les coûts et faciliter la prise des décisions durant les situations d'urgence.

Cependant, les défis liés à la modélisation et à la simulation des interdépendances des infrastructures critiques sont nombreux. En effet, pour un modèle des interdépendances, l'accès à des données réalistes, la conception d'un modèle unique et adéquat pour différentes infrastructures et la validation des modèles soulèvent plus de difficultés que lorsque le modèle concerne une seule infrastructure. L'implication de plusieurs infrastructures renforce ces difficultés à cause de la complexité liée à l'harmonisation des données issues de plusieurs variétés d'infrastructures. Par ailleurs, la nécessité de disposer des données réalistes sur les topologies des infrastructures impliquées et les défaillances de celles-ci constitue une autre source de difficultés non négligeable. En effet pour diverses raisons, ces données, même si elles existent restent le plus souvent confidentielles et il devient alors difficile pour les chercheurs extérieurs de mener leurs travaux en se basant sur des données réalistes et suffisamment précises. Le fait que

certaines de ces infrastructures soient privées complique davantage le problème à cause des difficultés liées à l'interprétation de ces données qui nécessite un certain niveau d'expertise et à la réticence des opérateurs de rendre public des données sur les défaillances de leurs infrastructures. Dans ce contexte l'obtention des données crédibles sur chacune des infrastructures concernées, leur fusion et leur harmonisation constitue une tâche complexe. L'ensemble de ces difficultés et la complexité des interdépendances font apparaître plusieurs interrogations sur le type de simulateur (intégration, fédération, etc.) qui convient le plus aux interdépendances des infrastructures critiques.

La modélisation et la simulation sont des techniques largement utilisées pour étudier des systèmes et des phénomènes complexes, ces techniques ont fait l'objet de nombreux travaux scientifiques qui ont permis de développer des outils capables de modéliser et de simuler avec précision le fonctionnement de nombreuses infrastructures singulières. Les modèles et les simulateurs résultants de ces travaux (analyse du flux et de stabilité transitoire pour les réseaux électriques, simulation des protocoles et de la congestion pour les réseaux IP) sont, à ce jour, largement utilisés comme outils d'aide à la prise de décision concernant chaque infrastructure. Les enjeux de la modélisation et de la simulation des interdépendances consistent à étendre ces outils ou à développer de nouveaux qui permettent de modéliser et de simuler conjointement de multiples infrastructures afin de mieux comprendre les interdépendances et les chaînes de propagation des défaillances entre ces infrastructures.

Ces dernières décennies, les interdépendances des infrastructures critiques et les propagations des pannes qu'elles peuvent engendrer ont suscité, pour la recherche, un grand intérêt. Malgré ce regain d'intérêt, les travaux scientifiques consacrés à la modélisation et à la simulation des interdépendances sont toujours embryonnaires. La diversité et la complexité des infrastructures concernées engendrent des contraintes considérables pour le développement des modèles et des simulateurs des interdépendances. Les outils actuellement utilisés pour la simulation des infrastructures singulières sont aussi diverses et variés que les infrastructures concernées et ces caractéristiques disparates constituent un facteur qui freine le développement des outils de modélisation et de simulation des interdépendances.

Par ailleurs, les caractéristiques des interdépendances présentées dans le chapitre 2 montrent que le développement des outils de modélisation et de simulation des interdépendances doit inclure un nombre important de paramètres pour pouvoir couvrir la totalité des besoins relatifs à la caractérisation des interdépendances. Ils doivent aussi pouvoir manipuler des données de formats différents dont l'harmonisation peut se révéler complexe. Ce qui peut engendrer un volume important de données dont la gestion et la maintenance peuvent s'avérer délicates. Aussi, l'évaluation des interdépendances nécessite des métriques clairement définies. Ces métriques constituent un moyen efficace pour la validation des modèles car elles permettent de faire des comparaisons avec des données réelles des infrastructures, mais elles restent difficiles à définir surtout lorsqu'elles doivent couvrir l'ensemble des facteurs essentiels pour la modélisation et la simulation des interdépendances. En outre les caractéristiques dynamiques des interactions entre les infrastructures et les différences des échelles temporelles et spatiales du fonctionnement des différentes infrastructures impliquées doivent être prises en compte dans la conception des simulateurs des interdépendances. Cette différence d'échelle est un facteur important pour la simulation des phénomènes dynamiques comme la propagation des défaillances dont l'échelle du temps peut fortement varier d'une infrastructure à une autre. À titre exemple,

cette échelle est de l'ordre de quelques secondes pour les réseaux de télécommunications alors qu'elle peut varier de plusieurs minutes à quelques heures pour le réseau électrique. Les difficultés liées à l'harmonisation de ces échelles de temps et la diversité des techniques de simulation des différentes infrastructures constituent un facteur qui explique, en partie, le faible succès de la fédération des logiciels de simulation existant car chaque logiciel a ses propres caractéristiques liées à l'échelle du temps et à l'algorithme utilisé qui sont souvent incompatibles entre elles.

Malgré ces difficultés, les travaux de recherche sur la modélisation et la simulation des interdépendances ont permis d'obtenir des modèles divers et variés. Ainsi, aujourd'hui, on trouve des modèles basés sur les systèmes multi-agents (*agent-based model*), la théorie des jeux, les réseaux de Pétri, les opérations (modèles fonctionnels), les chaînes de Markov, les modèles *input-output*, etc. Ces modèles sont applicables à des systèmes de tailles très variables allant des réseaux des campus à ceux des grands opérateurs Internet ou encore à des réseaux électriques et d'adduction d'eau. Mais, compte tenu des caractéristiques multidimensionnelles, dynamiques et complexes des interdépendances, les modèles existants ne couvrent pas la totalité des phénomènes résultants des interdépendances, ce qui conduit très souvent à des modèles trop génériques ou des modèles spécifiques qui caractérisent une infrastructure singulière en considérant les autres infrastructures interdépendantes comme des boîtes noires. Ces modèles conviennent, le plus souvent, à des modélisations avec des objectifs précis (évaluer les risques liés à la défaillance d'un composant, par exemple) sans offrir la possibilité d'analyser les conditions et les événements qui favorisent l'apparition de ces risques.

Dans le cadre de la protection des infrastructures critiques contre les propagations des pannes, l'enjeu pour la modélisation des interdépendances consiste donc à développer des outils capables, sur la base des données réalistes, de modéliser et de simuler toutes les caractéristiques déterminantes pour la compréhension des interdépendances des infrastructures impliquées afin de fournir des résultats les plus pertinents possibles. Cette technique permettrait, à l'aide de la modélisation et de la simulation, de découvrir de nouvelles vulnérabilités et de pouvoir évaluer de nouveaux systèmes au lieu de se limiter à l'évaluation de l'influence du changement de l'état d'une infrastructure sur une autre infrastructure.

L'un des premiers modèles consacrés aux infrastructures critiques est celui de Dudenhffer, Permann et Manic [53] qui représente, de manière très simple, une infrastructure par un graphe dont les nœuds représentent les composants et les arrêtes les interconnexions entre les composants par lesquelles transitent les flux de services ou d'influence. Pour un tel modèle, les interdépendances peuvent être représentées simplement par des arrêtes entre des nœuds appartenant à des infrastructures différentes et ces arrêtes peuvent être bidirectionnelles. Ce type de modèle permet de donner une représentation visuelle des interdépendances, mais doit être complété par des fonctions caractérisant tout le dynamisme de ces interdépendances pour offrir des moyens permettant de simuler un fonctionnement réaliste des infrastructures et leurs interactions, donc leurs interdépendances. Avec la représentation des interdépendances par un graphe constitué de plusieurs nœuds et arrêtes, l'enjeu de la simulation consiste à offrir les fonctionnalités nécessaires pour :

- Analyser l'impact d'un événement ou d'une succession d'événements sur un ensemble de composants des réseaux interdépendants représentés par des nœuds et des liens.
- Connaître les événements qui conduisent à l'état stable d'un ensemble de composants

donné.
- Déduire, à partir d'une succession d'événements les interdépendances d'un ensemble de composants.
- Identifier les composants critiques d'un ensemble de réseaux interdépendants à partir d'une fonction critique donnée, c'est à dire l'ensemble des composants qui interagissent directement ou indirectement à travers un ou plusieurs réseaux pour assurer cette fonction.
- Évaluer l'ampleur des conséquences de l'interruption d'un service sur le bien-être des personnes et la durée de cette interruption en analysant l'ensemble des composants impliqués. Il faudra donc être capable de déterminer la valeur du MDT (*Mean Down Time*) des composants de tous les réseaux participant à la fourniture de ce service et de caractériser leurs interactions complexes. Ce qui peut être délicat à cause de la nécessité de définir clairement la correspondance entre un service et les composants qui le fournissent.

Pour répondre aux besoins ci-dessus, il est indispensable de compléter les modèles par des simulateurs afin d'étudier les caractéristiques dynamiques de ces infrastructures. Actuellement, deux principales approches sont utilisées pour concevoir et développer des outils permettant de modéliser et de simuler conjointement plusieurs infrastructures : la fédération des logiciels de simulation existants et le développement de nouveaux logiciels de simulation multi-infrastructures offrant des fonctionnalités pour simuler conjointement plusieurs infrastructures.

3.2 Modélisation et Simulation des interdépendances : fédération des simulateurs et simulateur multi-infrastructures

Pour mieux appréhender les critères qui nous ont conduits à choisir une de ces approches, nous exposons, dans cette section, une description des deux approches fréquemment utilisées pour la mise en œuvre des simulateurs des interdépendances ainsi que leurs principaux avantages et leurs inconvénients.

Le développement des simulateurs des interdépendances par fédération consiste à coupler deux ou plusieurs logiciels de simulation spécifiques aux infrastructures impliquées à l'aide des techniques standards comme DDS (*Data Distribution Service for Real-time Systems*) [75], SIMNET [101], DIS (*Distributed Interactive Simulation*) [2], HLA (*High Level Architecture* (IEEE-1516)) [12] ou les communications multi-agents utilisant des langages spécifiques comme AML (*Agent Modeling Language*) [140] pour concevoir un environnement de simulation unique. DDS est une spécification permettant de développer des intergiciels d'échanges de données basés sur un système de producteur/consommateur. SIMNET, DIS, HLA sont des architectures standardisées qui permettent de mettre en œuvre des simulations distribuées. Ils ont tous été initiés dans le cadre des projets DARPA (*Defense Advanced Research Projects Agency*). HLA est la dernière version et intègre la plupart des fonctionnalités de ses prédécesseurs (SIMNET et DIS) avec quelques améliorations comme la possibilité d'intégrer des simulateurs à évènements discrets [51] qui n'étaient pas supportés par DIS.

Outre les standards énumérés ci-dessus et le couplage multi-agents avec le langage AML [140], Strassburger [135] identifie quatre techniques pour adapter un logiciel de simulation à une fédé-

ration basée sur l'approche RTI (*RunTime Infrastructure*). Ces différentes techniques consistent à ré-implémenter un logiciel pour ajouter les nouvelles extensions, à ajouter un module intermédiaire, à utiliser une interface de programmation extérieure ou un programme passerelle pour coupler les logiciels impliqués dans la fédération. La ré-implémentation consiste à modifier le code source du logiciel pour ajouter les fonctionnalités nécessaires et lui permettre de communiquer avec les autres logiciels. Cette méthode nécessite l'accès au code source, ce qui peut s'avérer difficile lorsque des logiciels non libres sont utilisés. La deuxième approche consiste à ajouter des modules pour les nouvelles fonctionnalités, typiquement par l'appel des fonctions au sein du code source du logiciel. Cette méthode s'adapte bien aux logiciels offrant la possibilité d'appeler des programmes ajoutés par l'utilisateur (Opnet[1], NS-2[2], ...), même si sa mise en place reste délicate à cause de la nécessité de modifier le code source des logiciels. L'interface de communication externe utilisée par la troisième approche se base sur l'utilisation d'intergiciel qui consiste à mettre en place un module jouant le rôle d'interface et permettant la communication entre plusieurs programmes. La dernière méthode est bien adaptée aux programmes mettant en œuvre des outils de communications externes (les fichiers, les tubes, les sockets, etc.) qui permettent aux programmes de communiquer entre eux localement ou à distance (utilisation des programmes passerelles spécifiquement développés pour assurer cette communication).

La technique de fédération permet d'effectuer des simulations très affinées car les logiciels couplés sont, le plus souvent conçus pour être capables de couvrir la plupart des besoins de simulations des infrastructures pour lesquelles ils ont été développés (par exemple, NS-2[3] pour les réseaux de télécommunications, EMTP-RV[4] pour les réseaux électriques), mais elle comporte de nombreuses faiblesses. En effet, outre la limite en terme de nombre de logiciels par fédération, certaines techniques de cette approche nécessitent l'accès aux codes sources qui peut s'avérer délicat dans le cas des logiciels propriétaires et surtout ceux qui sont développés uniquement pour un usage interne. Aussi cette technique ne peut convenir que pour certains types de simulations d'interdépendances, notamment ceux dont le temps de calcul d'un modèle est relativement bas, c'est à dire qu'il n'excède pas la valeur du temps réel des simulateurs. Elle implique aussi des difficultés relatives à la non maîtrise par les personnes extérieures des technologies développées exclusivement en interne. Toute fédération de logiciels de simulation requiert une synchronisation dont la mise à en œuvre peut se révéler délicate lorsqu'elle implique des logiciels de modélisation à évènements discrets ou à temps continu et discret.

La fédération des simulateurs ne peut être réalisée de manière aisée que si la différence de l'échelle temporelle d'apparition des évènements simulés par ces logiciels n'est pas trop importante ou si la synchronisation des simulateurs n'est pas indispensable, c'est à dire lorsque les événements des différents simulateurs ne sont pas synchrones. Ces deux conditions ne peuvent être satisfaites dans le cas des simulations des interdépendances car la première condition oblige à limiter la simulation des interdépendances à des infrastructures de même domaine (différents réseaux de télécommunications par exemple) et la deuxième suppose que les évènements simulés sont totalement indépendants alors que les pannes qui se propagent sont forte-

[1] http://www.opnet.com/
[2] http://www.isi.edu/nsnam/ns/
[3] http://www.isi.edu/nsnam/ns/
[4] http://www.emtp.com/software/emtp_rv.html

ment dépendantes les unes des autres.

La deuxième approche de la modélisation et de la simulation des interdépendances consiste à intégrer dans un modèle unique l'ensemble des modèles des infrastructures impliquées à l'aide, notamment, de la théorie des graphes. Cette approche permet de surmonter la plupart des difficultés de la fédération des logiciels évoquées ci-dessus car elle permet d'harmoniser les caractéristiques topologiques et fonctionnelles de l'ensemble des infrastructures impliquées. Cependant, elle peut s'avérer inefficace, lorsque l'objectif de la modélisation ou de la simulation nécessite des analyses très fines de chacune des infrastructures car l'intégration de l'ensemble des paramètres pertinents pour cet affinement dans un seul modèle peut conduire à des modèles extrêmement complexes, coûteux et quasi-impossibles à utiliser. En effet, la diversité des infrastructures, la complexité des caractéristiques de chacune d'entre elles et les différences liées à leur fonctionnement conduisent très souvent à ce que des modèles des interdépendances utilisant cette technique soient conçus avec un niveau d'abstraction qui ignore la plupart des aspects fonctionnels (algorithme de routage pour les réseaux de télécommunications et répartition de charge pour les réseaux électriques par exemple) qui, pourtant constituent des facteurs déterminants pour les propagations des défaillances. Par exemple, il est possible de trouver certains de ces travaux qui évaluent la résistance des infrastructures aux pannes en cascade en se basant uniquement sur le cœfficient de *clustering* du graphe représentant l'infrastructure en question. Ainsi, pour un réseau de télécommunications, une telle étude de résistance aux pannes se limiterait simplement à une évaluation de la topologie.

Que ce soit la fédération ou l'intégration dans un modèle ou simulateur unique, la modélisation et la simulation des interdépendances comportent un défi technique et conceptuel de taille qui consiste à caractériser techniquement les influences entre les différents composants des infrastructures concernées dans les modèles en question. Par exemple, comment traduire l'influence de la défaillance d'un composant du réseau électrique sur le composant correspondant du réseau de télécommunications dans le cas d'une modélisation des interdépendances entre les réseaux électriques et de télécommunications ? L'impact d'une défaillance électrique sur une autre infrastructure, en l'occurrence le réseau de télécommunications fait intervenir de nombreux paramètres extérieurs notamment l'utilisation ou non de sources d'alimentation électrique de secours (groupes électrogènes, batteries) dont l'autonomie peut atteindre plusieurs jours (environ 34 heures [110]). La prise en compte de ces facteurs dans un modèle d'interdépendance avec les réseaux de télécommunications où l'unité de temps est inférieure à la seconde est particulièrement difficile à cause de la différence d'échelle de temps. Quant à la défaillance d'un composant du réseau de télécommunications sur un réseau électrique, elle n'entraîne pas directement un défaut du réseau électrique, mais une perte de son système de contrôle dont le réseau électrique peut se passer dans des conditions normales pendant une durée qui peut être suffisante pour la remise en état du réseau de télécommunications. Cet exemple montre que la fédération des logiciels de simulation nécessite la prise en compte de nombreux facteurs et fait apparaître des difficultés liées à la limite en nombre de simulateurs qui peuvent être couplés et à la caractérisation de la correspondance entre les composants des différentes infrastructures à cause des caractéristiques abstraites des rapports entre ces composants.

Les obstacles liés à la différence d'échelle temporelle des propagations des pannes dans les différentes infrastructures, à la synchronisation des évènements et à la caractérisation de l'impact de la défaillance d'un composant d'une infrastructure sur un composant d'une autre

infrastructure surgissent à chaque fois que les interdépendances simulées concernant des infrastructures de différents domaines et que la simulation implique des phénomènes dynamiques comme les propagations des pannes.

Le dernier aspect des défis de la modélisation des interdépendances abordés dans cette section est celui de la qualité des données utilisées dans la modélisation qui constitue un facteur déterminant pour fournir des résultats pertinents et éviter le phénomène de GIGO (*Garbage In - Garbage Out*). Des donnés crédibles et traçables sont des facteurs clés pour des modélisations réalistes fournissant des résultats séants. Pour le cas spécifique de la modélisation des interdépendances, ces données doivent être issues de plusieurs infrastructures de secteurs très divers et gérées par des opérateurs privés, ce qui rend la tâche de collectes d'informations plus complexe. Aussi, l'analyse et le traitement des informations issues de ces différentes infrastructures demandent un certain niveau d'expertise pour identifier et valider les caractéristiques et les relations entre les infrastructures que ces données reflètent. La taille des infrastructures impliquées est un autre facteur déterminant à cause de la diversité et la quantité des données à collecter. Pour les réseaux de télécommunications par exemple, les relations entre systèmes autonomes suffisent pour une analyse au niveau national alors que des informations intra-AS (niveau routeurs) sont indispensables lorsque l'analyse concerne une ville. Pour faire face à ces différents défis, de nombreux projets se sont attelés à rendre disponible les informations nécessaires à la modélisation et à la simulation. Certaines données sont rendues publiques gratuitement alors que d'autres comme celles fournies par ESRI[5] et Platts[6] sont payantes. Plusieurs autres laboratoires maintiennent des données détaillées sur des infrastructures des domaines particuliers, mais considérées comme confidentielles qui, par conséquent, ne sont pas rendues publiques. A titre d'exemple, on peut citer le Laboratoire National d'Idaho (*Idaho National Laboratory - INL*) qui fournit des informations SCADA sur les réseaux électriques, le Laboratoire National d'Oak Ridge pour le secteur des transports aux États-Unis.

3.3 État de l'art de la modélisation et de la simulation des propagations des pannes et des interdépendances entre les réseaux électriques et de télécommunications

Bien que l'intérêt des chercheurs vis-à-vis de la modélisation des interdépendances soit relativement récent, un nombre important de travaux scientifiques consacrés à ce sujet a été réalisé. Ces dernières années, de nombreux projets de recherche sur la modélisation des interdépendances ont été initiés. Dans un rapport technique consacré à la modélisation des interdépendances des infrastructures critiques, les auteurs de [114] recensent environ 30 projets initiés avant 2006 et portant sur le développement des logiciels dédiés à la modélisation et la simulation des interdépendances des infrastructures critiques. Les modèles présentés dans cette liste utilisent différentes approches pour modéliser les interdépendances, notamment la communication multi-agents, le langage UML (*Unified Modeling Language*), la théorie des graphes, des modèles Monte Carlo, des modèles fonctionnels (*Input-Output*), des modèles mathématiques

[5] http://www.esri.com
[6] http://www.platts.com

(équations différentielles, événements) ou des systèmes de jetons qui, elles, nécessitent un développement de fonctions complexes pour caractériser les interdépendances grâce à l'échange des jetons entre les différentes entités impliquées. La simulation de Monte Carlo permet d'introduire une approche statistique par le calcul des valeurs numériques à partir d'un certain nombre de variables-clés de l'entité simulée affectées à des distributions de probabilités.

3.3.1 Modélisation et Simulation basées sur l'approche multi-agent

Les simulateurs fondés sur cette approche comportent des modules de programmes destinés à reproduire le fonctionnement d'une entité (composant matériel ou logiciel) ou à faciliter la communication entre différents logiciels de simulation. Dans [139], les auteurs proposent un modèle fondé sur la technique multi-agents pour modéliser les interdépendances techniques des infrastructures. Le modèle proposé est conçu sur la base des différents types d'interdépendances dont la classification est fondée sur différents niveaux d'abstraction (applications, processus) ou du type de liaisons (pair-à-pair, aiguillée) entre les différentes entités modélisées. Dans le modèle, des modules de programme déployés sur chacune des entités transmettent les informations sur les changements d'état de celle-ci aux autres agents. Pour valider leurs modèles, les auteurs les appliquent sur les réseaux électriques et de gaz dans une ville fictive et simulent l'impact d'une défaillance du réseau électrique sur le réseau de gaz.

La technique de modélisation et de simulation proposée par les auteurs de [22] est fondée sur les agents et des techniques de simulations à évènements discrets. Ils ont développé un simulateur à évènements discrets permettant de simuler les interdépendances entre des infrastructures représentant un hôpital, un réseau de chemin de fer, un réseau de transport public et un réseau électrique. Ensuite, ils simulent l'impact d'une panne électrique sur ces infrastructures et démontrent que cette panne peut avoir des conséquences plus ou moins graves en fonction, notamment de l'impact de la panne initiale sur le réseau de transport.

AIMS (*Agent-Based Infrastructure Modeling and Simulation*) [66] est un simulateur développé à partir du langage UML sur la base d'une approche orientée services. Il a été utilisé par ses auteurs pour modéliser les interdépendances des réseaux de télécommunications, électriques et d'adduction d'eau de la région de New Brunswick (Canada).

Le simulateur CISIA (*An Agent Based Simulator for Critical Interdependent Infrastructures*) proposé par les auteurs de [112] est réalisé avec une approche multi-agents où le comportement de chaque agent reflète le fonctionnement et la dynamique des défaillances de l'entité modélisée par l'agent. Le simulateur est destiné spécifiquement à l'évaluation des effets à court-terme d'une panne et l'identification des éléments critiques des infrastructures simulées. Avec une étude de cas portant sur un réseau de télécommunications, un réseau électrique et une infrastructure d'air conditionné, les auteurs montrent comment une défaillance de l'une de ces infrastructures peut se propager sur les autres infrastructures et conduire à une dégradation de performance des infrastructures simulées.

3.3.2 Modélisation et Simulation basées sur les graphes

Les modèles basés sur les graphes demande-approvisionnement (*supply-demand graph*) ou sur la théorie des graphes représentent les infrastructures modélisées par un ensemble de

nœuds, de liens et de flux. Les modèles avec les graphes demande-approvisionnement comportent 3 types de nœuds qui sont des nœuds fournisseurs, consommateurs et de transit qui ne produisent pas et ne consomment pas de flux. Les liens représentent les connexions par lesquelles transitent les flux entre les nœuds producteurs et consommateurs. Certains de ces modèles définissent des valeurs pour les quantités produites et consommées par les nœuds et les capacités des liens. Par exemple l'article [92] présente un modèle de graphe demande-approvisionnement avec un algorithme de retour sur trace[7] (*backtracking algorithm*) pour déterminer la probabilité qu'un service ne soit pas fourni à un nœud à cause d'une défaillance. Cette méthode peut aussi être utilisée pour identifier les composants vulnérables lors d'une conception d'un système et d'évaluer une nouvelle technique de conception.

Le modèle présenté dans [126] est un modèle unique intégrant les modules de simulation des réseaux électriques, des réseaux de télécommunications et les interdépendances dans un même environnement de modélisation et de simulation. Ce modèle est basé sur la théorie des graphes et simule les propagations des pannes entre le réseau de télécommunications et le réseau électrique par une approche simple dans laquelle la panne d'un composant du réseau électrique entraîne la panne du composant du réseau de télécommunications qui est attaché à celui-ci et vice-versa. Ce modèle s'intéresse essentiellement au réseau électrique, il considère le réseau de télécommunications comme une simple boîte noire et évalue uniquement l'influence du réseau de télécommunications sur la robustesse du réseau électrique sans s'intéresser aux propagations des défaillances dans le réseau de télécommunications.

Dans [136], les auteurs définissent un ensemble d'algorithmes qui permettent de caractériser les interdépendances et identifier les caractéristiques clefs de ces interdépendances, notamment la nature de ces dépendances (fortes ou faibles) et des possibilités de boucles et de cycles cachés. Le modèle est réalisé à l'aide d'un graphe orienté où les liens sont caractérisés par le type de dépendance entre ses 2 nœuds d'extrémité et sa capacité. Un nœud est caractérisé par la quantité de ressource qu'il délivre, la ressource disponible à un temps t et le type de stockage (fixe, non fixe, éphémère ou sans stockage). Des « supernodes » sont reliés aux nœuds sources et permettent d'étudier les interdépendances à l'aide de la technique de recalcul de flux ou *multiflow*.

Le modèle des interdépendances des infrastructures critiques proposé dans [83] utilise des graphes orientés pour caractériser les interdépendances avec pour objectif principal de trouver un compromis entre la réduction de la complexité, donc le temps de calcul et la capacité du modèle à couvrir l'ensemble des caractéristiques à modéliser. Les interactions entre les infrastructures sont modélisées par plusieurs graphes orientés. Les nœuds sont modélisés comme des producteurs ou des consommateurs de plusieurs services avec une dépendance définie pour chacun des services. Une fonction de réponse est définie pour modéliser chaque service échangé entre deux nœuds à travers une arrête du graphe. Avec ce modèle, les auteurs évaluent l'impact d'une panne d'un réseau électrique sur les réseaux de gaz et de télécommunications en calculant la proportion des nœuds impactés des graphes qui représentent les réseaux modélisés.

[7] Le retour sur trace désigne, en programmation, une stratégie pour trouver des solutions à des problèmes de satisfaction de contraintes

3.3.3 Modélisation et Simulation basées sur la fédération des logiciels de simulations

HLA [12] est l'un des rares standards dédiés au couplage de simulateurs, il a été initié par le DMSO (*Defense Modeling and Simulation Office*) et a été standardisé par l'IEEE [80]. Il est conçu pour faciliter l'interopérabilité entre différents logiciels de simulation et leur réutilisation. Pour assurer l'inter-opérabilité, HLA distingue les fonctionnalités de base des différents simulateurs et les services d'échanges des données entre les simulateurs, leurs communications (utilisant une RTI) et leurs synchronisations. Les entités de la simulation distribuée sont appelées des « fédérés » qui coopèrent sur une base commune et pour un objectif précis et qui forment une fédération. La communication entre les entités de la fédération et la RTI est assurée par une interface bidirectionnelle. L'un des principaux inconvénients de cette approche est la nécessité de modifier l'ensemble des logiciels participant à la fédération pour les adapter au standard HLA, ce qui nécessite des ressources et de temps très importants.

Mais, en plus des standards de fédération de logiciels comme HLA, certains chercheurs utilisant cette technique effectuent des modifications des logiciels couplés avec l'une des techniques définies par Strassburger [135] ou développent des techniques spécifiques pour assurer la communication entre les différents logiciels impliqués dans la simulation.

Le logiciel SimCIP proposé dans [25] est fondé sur une fédération des logiciels de simulation PSS-SINCAL[8] pour la simulation des réseaux électriques et NS-2[9] pour celle des réseaux de télécommunications. SimCIP permet un couplage des logiciels fondé sur les services et offre la possibilité de modéliser et de simuler avec précision les infrastructures impliquées car les logiciels couplés sont développés pour couvrir l'ensemble des caractéristiques de ces infrastructures.

L'article [77] décrit un environnement de simulation constitué par le couplage des logiciels de simulation électromagnétique (PSCAD/EMTDC) et électromécanique (PSLF[10]) des réseaux électriques et de simulation à évènements discrets des réseaux de télécommunications NS-2. Les auteurs développent avec le langage Java une interface et une RTI. L'interface assure les communications entre les modules logiciels déployés sur les simulateurs des différents capteurs IED (*Intelligent Electronic Device*) du réseau électrique et les autres composants (NS-2, PSLF (*Positive Sequence Load Flow Software*), PSCAD/EMTDC[11]) via la RTI qui assure la synchronisation entre les différents composants. Avec cet environnement de simulation, les auteurs démontrent comment un réseau de télécommunications fiable peut contribuer à réduire l'impact d'une panne électrique en réduisant le temps nécessaire à la détection de cette panne grâce à l'isolement des entités du réseau électrique qui sont vulnérables.

Les auteurs de l'article [125] exposent l'objectif du projet DIESIS (*Design of an Interoperable European federated Simulation network for critical InfrStracture*) qui consiste à concevoir, en réutilisant des standards comme HLA [12], BPEL (*Business Process Execution Lan-*

[8] http://www.simtec-gmbh.at/sites_en/sincal_updates.asp
[9] http://www.isi.edu/nsnam/ns/
[10] http://www.gepower.com/prod_serv/products/utility_software/en/ge_pslf/index.htm
[11] https://pscad.com/index.cfm

guage)[12] et WSRF (*Web Services Resource Frame-work*)[13] une architecture qui permet à des simulateurs de communiquer via un réseau IP. Pour le couplage des logiciels, les auteurs proposent une caractérisation des interdépendances fondée sur les interactions des infrastructures liées à l'échange des données, aux liaisons matérielles et aux synchronisations.

CERTI[14] (Centre d'Etude et de Recherche de Toulouse RTI) développé par l'ONERA (Office National d'Etudes et de Recherches Aérospatiales) est une infrastructure d'exécution des simulations distribuées fondée sur des inter-fédérations. Une fédération est constituée d'un ensemble de simulateurs dont le couplage est fondé sur le standard HLA. La communication entre les fédérations est assurée par une interface appelée « *federation bridge* ». La conception et l'implémentation de CERTI sont décrites dans [26] et les résultats présentés dans cet article montrent que l'ajout d'un *bridge* nécessaire à la communication inter-fédération réduit considérablement la performance.

Le co-simulateur des interdépendances entre les réseaux électriques et de télécommunications développé lors des travaux réalisés dans le cadre de cette thèse et dont les résultats ont été publié [54] en 2007 à la *2nd International Conference on Dependability of Computer Systems* est fondé sur le couplage des logiciels POWER DESIGNER[15] et Sgoose[16] avec pour objectif l'évaluation de la variation de l'énergie consommée par une station de base et un commutateur en fonction du nombre de paquets traités. POWER DESIGNER est un logiciel gratuit développé par Baghli dans le carde de son mémoire [20] de fin de cycle Ingénieur. Il permet la simulation de l'écoulement de puissance, de la stabilité transitoire et de différents défauts des réseaux électriques et utilise les techniques de Gauss-Seidel, de Newton-Raphson ou de *Fast Decoupled Load Flow* largement détaillées dans [20]. Sgoose permet de simuler toutes les couches des protocoles GSM (*Global System for Mobile Communications*) et GPRS (*General Packet Radio Service*). L'interdépendance entre les réseaux électriques et de télécommunications dans le carde de l'émission des données est modélisée par l'évaluation de l'énergie supplémentaire consommée par une station de base pour émettre les paquets de données. Ce co-simulateur a permis, notamment d'évaluer la quantité d'énergie consommée par un émetteur en fonction des débits de données.

3.3.4 Autres types de modélisation et de simulation

Möbius[17] est un logiciel de simulation des systèmes complexes et des interdépendances développé par des chercheurs de l'Université de l'Illinois avec l'objectif de permettre l'intégration de plusieurs modèles avec des formalismes différents et pour l'extension de ces formalismes en fonction des besoins [40]. Il supporte, entre autres les modèles fondés sur les réseaux de pétri, les chaînes de Markov et les processus stochastiques. Möbius offre un niveau d'abstraction qui permet la construction des modèles pour de nombreuses infrastructures, notamment les technologies de l'information, l'aéronautique et la biologie. Mais il nécessite de décrire

[12] http://www.oasisopen.org/committees/tc_home.php?wg_abbrev=wsrf
[13] http://www.openmi.org/
[14] http://www.cert.fr/CERTI/index.fr.html
[15] http://www.baghli.com/
[16] http://www.aixcom.com
[17] http://www.mobius.illinois.edu

les caractéristiques fonctionnelles de chacune de fonctionnalité du modèle pour que le logiciel puisse générer un code correspondant aux fonctionnalités. Pour des fonctionnalités plus complexes non prises en charge par le logiciel, l'utilisateur doit les développer lui-même.

Les auteurs de [110] utilisent le simulateur vensim[18] pour simuler les effets de cascade d'une panne électrique de plus de 4h sur le fonctionnement d'un réseau de télécommunications et les services d'urgences 911 et 112. Leur modèle est basé sur des méthodes empiriques et des données obtenues suite à des pannes qui se sont déjà produites et permet de montrer qu'une panne électrique électrique dont la durée est supérieure à 4h mettrait hors service le réseau mobile. Ils montrent aussi à travers un modèle simple qu'une panne électrique de 34h provoquerait des pertes économiques importantes et des augmentations des coûts non négligeables.

L'article [88] utilise les réseaux de Pétri pour modéliser la propagation des pannes dans les infrastructures en se basant sur des facteurs qui conduisent aux pannes en cascade identifiés à partir des pannes du réseau électrique, notamment celle du 10 août 1996 aux USA. Ils utilisent ensuite les réseaux de Pétri avec un système de jetons pour effectuer la modélisation des propagations des pannes (les jetons d'un équipement en panne sont transférés vers le voisin en bon état et si le total des jetons est supérieure à un seuil, cet équipement tombe à son tour).

Le modèle de Permann [89] décrit une technique de modélisation qui combine le système CIMS (*Critical Infrastructure Modeling System*) [44] développé par le laboratoire INL (*Idaho National Laboratory*) et un algorithme générique (*Generic Algorithm - GA*). CIMS est un logiciel de simulation des interdépendances qui permet d'analyser les interactions causes-à-effets des infrastructures à partir d'une représentation graphique 3D. L'Algorithme Générique (GA) définit un ensemble de méthodes d'optimisation probabilistes inspirées du principe de l'évolution organique [73] et de la théorie de l'évolution de Darwin. L'algorithme consiste à effectuer, à partir d'un ensemble d'entités initialement défini, des simulations itératives durant lesquelles des fonctionnalités de ces entités peuvent être détruites ou altérées aléatoirement et d'évaluer le résultat avec une analyse comparative des caractéristiques des infrastructures avant et après ces simulations.

L'article [102] propose de combiner des modèles des infrastructures singulières et un modèle dynamique fondée sur les interactions fonctionnelles pour étudier les interdépendances matérielles et économiques des infrastructures critiques. Le modèle inter-infrastructure est réalisée avec l'évaluation de ressources accumulées (*Stock*) par chaque entité participant à la modélisation et le taux d'altération (*Flow*) de ces ressources. En appliquant ce modèle sur un réseau électrique d'une région fictive, les auteurs démontrent comment il est possible de prévoir, avec le modèle proposée, la production de l'énergie en fonction de la demande et de réduire le coût par l'importation de l'énergie.

CI^3 (*Critical Infrastructures Interdependencies Integrator*) [115] est un logiciel permettant d'évaluer, à l'aide des simulations Monté Carlo, le temps nécessaire et le coût pour restaurer un composant, une infrastructure ou un ensemble d'infrastructures interdépendantes après une défaillance. Les simulations sont fondées sur des diagrammes de transitions et fournissent des résultats sous forme de courbes graphiques et de tables avec les valeurs du temps et de la distribution du côut de restauration des infrastructures simulées.

Dans [147], les auteurs proposent un modèle fonctionnel fondé sur la technique *Input-*

[18] http://www.vensim.com

output appelé IIM (*Inoperability Input-output Model*) pour évaluer l'impact, en terme économique et de dysfonctionnements, de l'attaque d'une infrastructure sur des infrastructures économiquement interdépendantes. Avec un système pyramidale, les auteurs démontrent, en utilisant des données économiques du Département du Commerce Américain comment une attaque d'un réseau de contrôle comme SCADA peut impacter économiquement d'autres secteurs de l'économie nationale. Les données d'entrée du modèle sont obtenues à partir de la traduction d'une classification des composants du réseau SCADA en fonction du risque de panne de ces composants suite à l'attaque. Comme résultat, le modèle IIM fournit une estimation des effets cumulatifs de ces pannes en terme de pertes financières et de la baisse d'activité des entreprises de la région concernée.

3.4 Limites des outils existants pour la modélisation et la simulation des interdépendances entre les réseaux électriques et de télécommunications

Après avoir analysé l'ensemble des fonctionnalités offertes par ces logiciels, nous avons constaté qu'en dépit du nombre important des outils de modélisation et de simulation proposés, les fonctionnalités offertes par la plupart d'entre eux se limitent à l'analyse de l'influence d'une défaillance sur une infrastructure particulière (les finances, l'économie par exemple). Ils n'offrent pas des possibilités qui permettent d'étudier précisément les facteurs et la succession des événements qui caractérisent la propagation des pannes. En effet, les modèles fondés sur les techniques multi-agents nécessitent la modification de l'ensemble des logiciels pour qu'ils puissent communiquer entre eux par l'intermédiaire d'agents. Quant à la fédération de logiciels à l'aide des standards comme HLA, outre la modification des simulateurs couplés nécessaire pour ajouter les interfaces de communication avec la RTI, la performance se dégrade considération avec le nombre de de simulateurs. Aussi, la RTI par laquelle transitent toutes les communications entre les simulateurs couplés constitue un goulot d'étranglement. Les techniques proposées pour pallier cette faiblesse comme l'inter-fédération décrite dans [26] sont très complexes à mettre en œuvre et introduisent d'autres problématiques comme le risque de cycles et la nécessité de mettre en œuvre des fédérés-ponts par lesquels transitent les communications entre différentes fédérations, c'est à dire entre différents groupes de simulateurs couplés. Les modèles fondés sur des techniques comme les réseaux de Pétri, de Monté Carlo ne sont adaptés que pour certaines catégories d'infrastructures.

Quant aux modèles et simulateurs fondés sur les graphes, ils se limitent, pour la plupart d'entre eux aux interdépendances fonctionnelles ou à la caractérisation limitée à une seule infrastructure en considérant les autres infrastructures comme des boîtes noires. Lorsque ces défauts sont corrigés, le niveau d'abstraction des modèles fondés sur les graphes oblige à ce que les interdépendances modélisées soient limitées à des aspects particuliers, par exemple les services, comme c'est le cas du modèle décrit dans [83]. Dans tous les cas, ils n'offrent aucun moyen d'analyser la succession des évènements qui conduisent aux pannes. Ce qui fait que ces modèles ne permettent d'étudier que des caractéristiques et des fonctionnalités connues empêchant ainsi toute découverte de phénomènes nouveaux résultant des effets des interdépendances.

Pour repousser ces limites en ce qui concerne la simulation des interdépendances, nous proposons, dans la suite de ce chapitre une technique de modélisation et simulation des interdépendances entre les réseaux électriques et de télécommunications fondée sur les graphes, capable de couvrir l'ensemble des caractéristiques des deux infrastructures impliquées et qui est axée sur la simulation des évènements dont la succession peut conduire aux pannes en cascade.

3.5 Description de la technique de modélisation et de simulation des propagations des pannes entre les réseaux électriques et des télécommunications proposée

3.5.1 Introduction

Le rôle principal du réseau de télécommunications du point du vue des interdépendances avec le réseau électrique est de fournir les services de télécommunications nécessaires pour assurer la supervision, le contrôle et l'estimation de l'état du réseau électrique à tout instant. Donc le réseau de télécommunications permet d'avoir une vision globale du réseau électrique et ceci, malgré sa taille et le nombre élevé d'équipements qui le composent. Son but est donc d'assurer une communication entre les centres de contrôle, d'une part, et entre les différents dispositifs (capteurs, microphones, accumulateurs, etc.) et les centres de contrôles en charge de leur gestion et du traitement des informations transmises par ces dispositifs, d'autre part. Le travail présenté dans ce chapitre a été réalisé en 2007 et a fait l'objet de publication à la *European Conference on Complex Systems* en 2007 [47], puis au *International Journal of Critical Infrastructure* en 2009 [46] et porte sur la modélisation des interdépendances entre les réseaux électriques et de télécommunications

L'objectif du modèle proposé dans ce chapitre est d'évaluer l'importance de la réactivité des protocoles de routage du réseau de télécommunications sur la propagation des défaillances dans les réseaux électriques. Comme le montrent les exemples de panne décrits dans la première partie de ce manuscrit, les informations temps réel sur l'état d'un réseau électrique constituent un facteur important pour limiter la propagation des défaillances dans ces réseaux. Or, lors de certaines pannes de grande ampleur des réseaux électriques, leurs systèmes et réseaux informatiques peuvent faire l'objet des dysfonctionnements causés, en général par la succession des événements inhabituels comme décrit dans le rapport [63] rédigé à la suite de la panne électrique du 14 août 2003 aux États-Unis. Par conséquent, maintenir la communication entre les centres de contrôle et tout équipement défaillant du réseau électrique est un facteur important que nous essayons de caractériser dans ce chapitre. Plus précisément, nous évaluons la capacité des protocoles de routage dynamique comme OSPF à calculer les chemins et rétablir une communication interrompue à cause d'une défaillance. Ces protocoles de routage jouent un rôle important lors des défaillances matérielles ou logicielles qui engendrent des interruptions de communications. En effet, à l'exception des interruptions physiques des communications à cause, notamment des pannes de cause commune pour lesquelles le calcul automatique de chemin devient impossible, les protocoles de routage recalculent les chemins et rétablissent les communications après chaque interruption. Ce calcul permet de remplir les tables de routage

qui fournissent, pour chaque destination le prochain routeur auquel le paquet doit être envoyé (routage dynamique). A noter que ces tables peuvent aussi être remplies à la main, mais uniquement pour les réseaux de petite taille, on parle, dans ce cas, de routage statique. Compte tenu de la taille des réseaux impliqués dans les interdépendances, nous nous intéressons uniquement au routage dynamique. Ce routage est déterminant car la restauration ou l'isolement d'un équipement défaillant du réseau électrique dépend, techniquement de l'existence d'un canal de communication entre cet équipement et le centre de contrôle. Donc, les moyens de lutte contre les propagations des défaillances dans les réseaux électriques dépendent fortement du temps de rétablissement des routes, par conséquent, l'utilisation d'un routage dynamique et rapide se révèle nécessaire.

Dans les modèles des interdépendances fondés sur la théorie des graphes, les topologies utilisées constituent un facteur déterminant. Avant de présenter les caractéristiques techniques de notre modèle, nous présentons dans les sections suivantes les topologies des infrastructures utilisées dans les simulations réalisées avec le simulateur proposé.

3.5.2 La topologie du réseau électrique

En général, les réseaux électriques sont constitués des réseaux de transport et des réseaux de distribution et sont composés des sources de production, des sous-stations de transformation, des charges et des lignes (aériennes ou souterraines) par lesquelles est acheminée l'énergie électrique. Comme décrit dans le chapitre 2, le réseau de transport électrique a une topologie fortement connectée alors que la topologie du réseau de distribution forme une structure en arbre et est, le plus souvent connecté à deux ou plusieurs sources (sous-station primaire ou poste de transformation de haute à moyenne et basse tension). De par leur architecture, les pannes des réseaux électriques ne conduisent à des pannes généralisées que lorsqu'elles touchent le réseau de transport. Une panne du réseau de distribution reste, le plus souvent, une panne locale lorsqu'elle ne provoque pas des pannes du réseau du transport. À l'inverse, une panne du réseau de transport provoque systématiquement des défaillances de postes sources pour les réseaux de distribution. Donc l'enjeu de modélisation des pannes en cascade concerne principalement le réseau de transport électrique.

Dans ce chapitre, nous appliquons nos simulations sur un graphe représentant le réseau de transport de très haute tension ($400kV$) du principal opérateur français (Réseau de Transport d'Électricité - RTE) tel qu'il est présenté sur son site Web (figure 4). Cependant, notre modèle peut s'appliquer avec n'importe quelle autre topologie représentée sous forme d'un graphe.

Pour la simulation des propagations des pannes, nous utilisons la méthode *DC Load Flow* décrite dans le chapitre 2 pour simuler la distribution des charges sur les lignes et les nœuds du réseau simulé. Pour rappel, la méthode *DC Load Flow* est une simplification du modèle standard du réseau électrique représenté par l'équation générale :

$$I = U.Y_{bus}$$

Où I est l'intensité du courant, Y_{bus} est l'admittance du bus (nœud) et U la tension.

Cette méthode consiste à négliger la puissance réactive et les composantes résistives et capacitives du modèle des lignes électriques. Dans ce mémoire, nous utilisons cette simplification

car dans la modélisation des pannes en cascade, seule la puissance active des nœuds nous intéresse pour évaluer le déficit en puissance de ce nœud suite à des défaillances des lignes ou des défaillances d'autres nœuds.

3.5.3 La topologie du réseau de télécommunications

Dans ce simulateur, nous nous intéressons à un aspect indispensable au fonctionnement des réseaux de télécommunications modernes, le routage, c'est à dire la capacité de ces réseaux d'établir des communications entre deux ou plusieurs nœuds connectés. Ce système de routage peut être victime, en plus des défaillances matérielles, de nombreux autres types de pannes, notamment des défauts logiciels, des dysfonctionnements provoqués par des mauvaises configurations et des attaques de type déni de service. Dans ce mémoire, notre modèle porte essentiellement sur des dysfonctionnements du routage provoqués par des pannes dues aux phénomènes des interdépendances avec le réseau électrique. Nos simulations portent sur un graphe représentant le réseau de Free[19] (qui a l'avantage d'être un réseau national étendu et disponible sur Internet), l'un des fournisseurs d'accès Internet français, mais il est possible de l'appliquer à n'importe quelle autre topologie. Ce choix peut être considéré, par certains comme approximatif car certains réseaux électriques ont leur propre réseau privé de télécommunications et peuvent utiliser des technologies autre que IP. En dépit de cette réalité, aujourd'hui, comme évoqué dans l'introduction générale, la tendance est plutôt à la convergence vers IP et à l'interconnexion entre les réseaux dédiés et les réseaux publics pour permettre la mise en place des services comme le télécontrôle et le télétravail. Aussi ces réseaux privés, du point de vue de la topologie, ressemblent très souvent aux réseaux publics (voir figure 3.1) puisque l'une et l'autre de ces deux catégories interconnectent, en général les mêmes sites pour un même pays et parfois ces réseaux privés deviennent même une société à part entière fournissant des services de télécommunications à des clients extérieurs. C'est le cas, par exemple, du réseau Artéria[20] appartenant à RTE et proposant à ses clients la mise à disposition de capacités inutilisées de ses fibres optiques. Nos simulations portent donc sur un graphe représentant un réseau d'opérateur où les nœuds représentent uniquement les routeurs. Nous ne reviendrons pas sur le fonctionnement de ces routeurs et des protocoles du routage décrit dans le chapitre 2. Dans nos simulations les défaillances considérées sont les interruptions de communication entre deux nœuds du réseau à cause des pannes d'un nœud ou d'un lien du graphe provoquées par des défaillances des nœuds correspondants du réseau électrique.

3.5.4 Modélisation des pannes en cascade

Les caractéristiques des propagations des défaillances varient en fonction des infrastructures. Pour le réseau des télécommunications, les transferts de charge considérés se font aussi bien entre les lignes de communications qu'entre les routeurs. En effet, lorsqu'un routeur est en panne, les préfixes annoncés par ce routeur et qui sont accessibles par d'autres routeurs sont annoncés une nouvelle fois par ces derniers et des nouvelles routes sont calculées. Dans le réseau électrique, les transferts de charge concernent les lignes et le déclenchement (coupure) de l'une

[19] http://www.free.fr
[20] http://www.arteria.fr

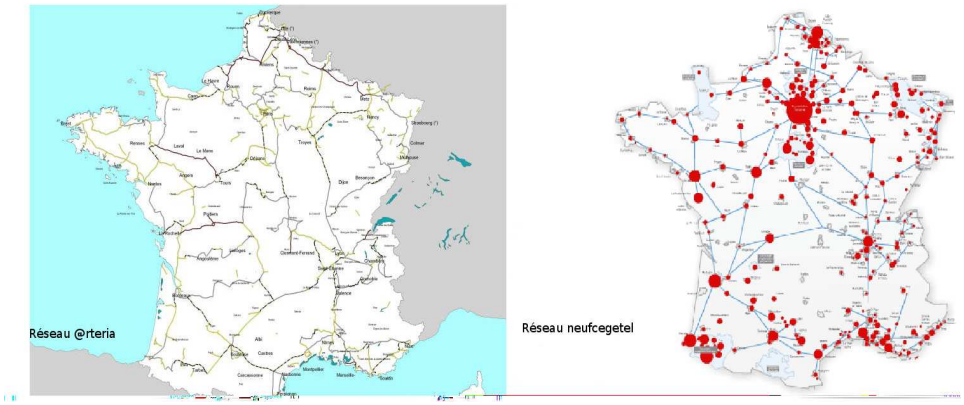


FIG. 3.1 – *Réseaux Arteria et Neufcegetel (crédits @rteria et Neufcegetel)*

d'entre elles suite à une surcharge provoquent le report de charge sur les lignes avoisinantes. Or ces lignes ont des capacités maximales, donc cette coupure de ligne peut conduire aussi à une réduction de la puissance ou à une interruption de l'alimentation électrique au niveau du nœud situé à l'extrémité vers laquelle la ligne coupée achemine l'énergie électrique. Dans notre modèle, les capacités des lignes sont fixées en début de simulation et la puissance de chacun des nœuds est calculée à l'état stable du réseau et une défaillance d'une ligne électrique peut conduire, lorsqu'il y a un dysfonctionnement du réseau de télécommunications, à un déclenchement d'autres lignes, voire une panne d'un nœud ayant enregistré un déficit de puissance important. Donc les pannes en cascade dans notre modèle concernent à la fois les lignes et les nœuds. Ce choix nous permet de prendre en compte les effets de délestage au niveau d'un nœud qui enregistre un déficit de puissance supérieur à un seuil fixé au départ. Ce délestage est effectué via le réseau de télécommunications à travers le système de contrôle et lorsque ce délestage est impossible à cause d'une défaillance du réseau de télécommunications, le nœud concerné tombe en panne avec toutes les lignes électriques connectées à ce nœud.

Dans notre scénario, la dépendance des routeurs vis-à-vis du réseau électrique est évidente et une panne du réseau électrique conduit à la panne des routeurs du réseau de télécommunications alimentés par le nœud électrique défaillant. Dans ce simulateur, nous ne prenons pas en compte les sources d'alimentation électrique de secours (batteries, groupes électrogènes). Les raisons de cette hypothèse sont la nécessite de réduire le nombre de paramètres à prendre en compte et le fait qu'il n'est pas exclu que lors des grandes pannes électriques, certaines de ces sources de secours ne puissent pas fonctionner, comme il a été constaté dans les exemples des pannes présentés dans le chapitre 2 de ce manuscrit. Aussi, avec les progrès technologies et l'optimisation des processus, la tendance est à la suppression de ces sources de secours en vue de réduire les coûts opérationnels.

Pour modéliser les interdépendances, nous considérons que le système de contrôle du réseau électrique utilise le réseau de télécommunications dont la topologie est représentée par le graphe de la figure 3.5. Ce système de contrôle permet de réguler les paramètres physiques, de superviser l'état et de reconfigurer le réseau électrique en situation d'urgence. Ces fonctions de reconfiguration comprennent, notamment le délestage lorsqu'il n'y a aucun autre recours pos-

sible après une défaillance susceptible de conduire à des surtensions ou à des sous-tentions et une perte de synchronisation du réseau. Les interdépendances sont modélisées par une association de proche en proche, c'est à dire un nœud du graphe représentant le réseau de télécommunications est attaché au nœud du réseau électrique qui est géographiquement le plus proche et vice-versa. Ce choix s'explique par le fait que nous modélisons le réseau électrique de niveau transport et un nœud de ce réseau peut représenter une sous-station qui alimente toute une ville et, par conséquent alimente tous les nœuds des réseaux de télécommunications de cette ville. Le principe de la modélisation des interdépendances est présenté sur la figure 3.2.

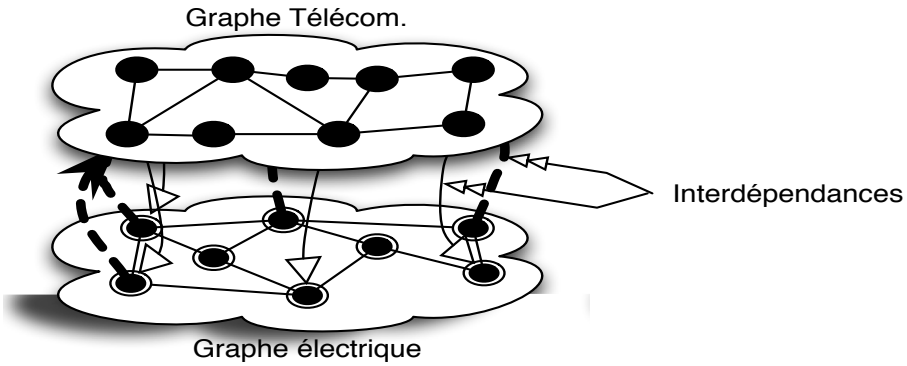


FIG. 3.2 – *Modèle des interdépendances*

3.5.5 Algorithmes

Pour développer l'ensemble des fonctionnalités qui permettent de simuler le réseau électrique, celui des télécommunications et leurs interdépendances dans un environnement unique, nous avons utilisé la librairie Boost Graph (*Boost Graph Library - BGL*), développée en C++ par l'université d'Indiana. C'est une bibliothèque évoluée permettant de manipuler les graphes. Elle fournit une interface générique ouverte permettant d'accéder à la structure du graphe sans se soucier de son implémentation et offrant des possibilités pour intégrer facilement de nouveaux programmes. Dans ce manuscrit, nous ne décrivons pas en détail cette librairie, les lecteurs intéressés peuvent visiter le site[21] Internet consacré à cette librairie. L'utilisation de BGL (*Boost Graph Library*) nous a permis de consacrer notre travail entièrement à l'implémentation des fonctionnalités de notre modèle.

3.5.5.1 Mise en œuvre du simulateur du réseau de télécommunications

Pour simuler l'influence de la performance de la reconfiguration du réseau de télécommunications sur la propagation des pannes dans le réseau électrique, nous considérons uniquement le routage dynamique et le principe de notre modèle est présenté sur la figure 3.3

[21] http://www.boost.org

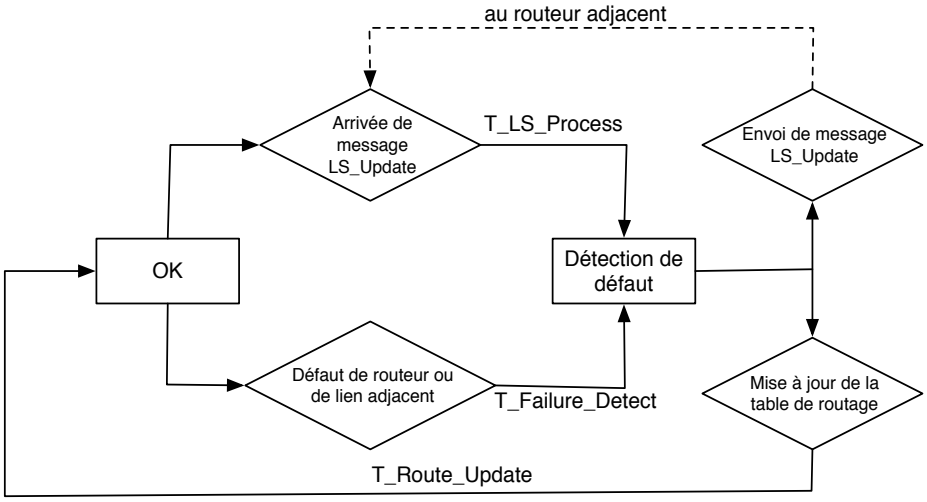


FIG. 3.3 – *Le modèle fonctionnel d'un routeur du réseau de télécommunications*

A chaque instant de la simulation le routeur peut être à l'état défaillant ou à l'état de reconfiguration ou encore en fonctionnement normal. L'état de fonctionnement normal est celui où la table du routeur contient des chemins agrégés de la topologie du réseau considéré et aucune panne de routeur n'a été détectée depuis l'instant précédent de la simulation ou une panne a été détectée, une réconfiguration a été initiée et l'ensemble des routeurs sont revenus à un état stable. Le routeur est défaillant (*Router_Failed*) lorsque le nœud du réseau électrique qui l'alimente en énergie électrique est défaillant, lorsqu'il détecte la défaillance annoncée par un autre routeur, il se met à l'état *Failure_Detected* jusqu'à la reconfiguration du réseau. Lorsqu'un routeur reçoit une notification de défaillance d'un de ses voisins directs, il se met à l'état *Failure_Detected* jusqu'à l'expiration du temporisateur *T_Failure_Detect*. Lorsque cette défaillance concerne un nœud autre que ses voisins du réseau, le routeur qui reçoit l'annonce, après un temps *T_Transmission* procède au traitement du message durant *T_LS_Process*, ensuite le routeur annonce cette défaillance à ses voisins (*LS_Update*) et recalcule les routes durant *T_Route_Update*. Donc le temps de restauration de la connectivité ($T\_Recovery(N)$) d'un routeur ayant détecté une défaillance dépend de sa distance N (en nombre de sauts) entre ce routeur et le nœud défaillant. $N = 0$ représente la situation où le nœud défaillant est directement connecté au routeur qui fait le calcul, dans ce cas $T\_Recovery(0) = T\_Failure\_Detect + T\_Route\_Update$. Ainsi pour un nœud défaillant situé à N sauts du routeur qui fait le calcul, $T\_Recovery(N) = T\_Failure\_Detect + N * (T\_Transmission + T\_LS\_Process) + T\_Route\_Update$. Une défaillance n'affecte que les routeurs qui ont dans leurs tables de routage des chemins qui passent par le nœud défaillant et le calcul d'une nouvelle route entre 2 nœuds n'est possible que lorsqu'il existe une liaison physique entre ces nœuds. Au niveau logique, chaque nœud sur le chemin d'une destination doit être capable d'acheminer du trafic vers cette destination. La table de routage de chaque nœud du chemin doit être correcte pour permettre au nœud d'acheminer du trafic. La table d'un routeur est correcte pour une destination si le prochain saut utilisé est sur

le plus court chemin entre ce routeur et la destination. Par conséquent, si après une défaillance, la table de routage d'un nœud ne change pas, nous considérons que ce nœud n'a pas été touché par cette défaillance. Pour gérer de multiple pannes, nous utilisons une liste de pannes et, pour chaque panne de cette liste, nous pouvons évaluer l'état du réseau et le comparer à son état précédent pour savoir s'il y a eu ou non une interruption de communications entre 2 nœuds du réseau. Les valeurs des paramètres sont fixées à des valeurs couramment utilisées et de manière à pouvoir évaluer l'influence du réseau de télécommunications sur le réseau électrique. En effet, des valeurs trop élevées n'auraient aucun intérêt car le réseau de télécommunications resterait défaillant à chaque anomalie du réseau électrique et les événements du réseau électrique se succéderaient comme si le réseau de télécommunications n'existaient pas. Des valeurs trop petites permettraient au centre de supervision d'effectuer des délestages à chaque surcharge d'une ligne ou d'un nœud et il n'y aurait jamais d'effets de cascade. Ces valeurs sont fixées à 1 seconde pour $T\_Transmission + T\_LS\_Process$, à 5 secondes pour *T_Route_Update* et à 60 secondes pour *T_Failure_Detect*, mais peuvent être adaptées en fonction de l'objectif du simulateur. Dans nos expérimentations, il arrive que ces valeurs varient pour évaluer certains paramètres des infrastructures simulées. Les simulations se déroulent suivant l'algorithme 1

```
input  : G : Initial network's graph, FL : Failure list, T : Current time, A Source router,
         B Destination router
output: YES (A and B are able to communicate at time T) or NO
Path = Shortest path between A and B in G without links and routers affected by the
failures of FL;
if Path does not exist then
 | Return NO;
else
 | for each router X on the Path do
 |  | for each failure F of FL do
 |  |  | G_cur = G without links and routers affected by the failures P and prior to P;
 |  |  | G_pred = G without links and routers affected by the failures earlier to P;
 |  |  | if Next_Hop(of X, to B, in G_cur) != Next_Hop(of X, to B, in G_pred) then
 |  |  |  | if T_Recovery( Distance(P , X) ) + Occuring_Time (P) > T then
 |  |  |  |  | Return NO;
 | return YES;
```

Algorithm 1: Simulation du réseau de télécommunications

3.5.5.2 Mise en œuvre du simulateur du réseau électrique

Le graphe représentant le réseau électrique est constitué de 2 catégories de nœuds, les nœuds sources qui représentent les générateurs et les nœuds puits qui regroupent les charges du réseau. Pour calculer le flux électrique arrivant au niveau d'un nœud, nous utilisons l'algorithme de flot maximum d'*Edmonds-Karp* de complexité polynomiale ($O(\mid V \mid . \mid E \mid^2)$), où V est l'ensemble des nœuds et *E* l'ensemble des arrêtes. Le choix de cet algorithme présente l'avantage d'être disponible dans la librairie BGL que nous utilisons. Pour effectuer ce cal-

cul, il est nécessaire de fixer les valeurs des capacités des arrêtes du graphe. Ces valeurs sont calculées sur la base de la tension des lignes ($400kV$) du réseau considéré et les caractéristiques fréquentes de ce type de lignes électriques (section de $500mm^2$, densité de courant de $0.75A/mm^2$). Sur la base de ces paramètres nous déterminons la capacité des lignes qui correspond à la puissance maximale les traversant. Une fois les valeurs des capacités maximales des lignes fixées pour toutes les lignes du réseau, nous calculons la quantité de flux (en puissance) arrivant à chaque nœud lorsque le réseau est à l'état stable, ce calcul nous permet de fixer les puissances produites par chacun des générateurs et celle consommée par chacun des noeuds représentant les charges.

3.5.5.3 Modèle des interdépendances et des pannes en cascade

Dans nos simulations, la première défaillance touche une ligne du réseau électrique, mais la défaillance d'un noeud, un générateur par exemple peut être facilement simulée. Le principe de fonctionnement de notre simulateur des pannes en cascade est présenté par la figure 3.4 et l'algorithme 2. La ligne déclenchée (coupée) en début de la simulation peut être sélectionnée aléatoirement, choisie ou sélectionnée à partir des critères précis, comme la charge par exemple. Après la suppression de l'arrête représentant la ligne déclenchée, nous reprenons le calcul du flot maximum décrit ci-dessus pour déterminer la puissance traversant chacune des lignes et celle délivrée à chacun des noeuds charges. Nous comparons ces valeurs à celles calculées à l'état stable du réseau et qui représentent les charges nominales des lignes et des noeuds. À l'issue de ce calcul, nous vérifions, tout d'abord si le report de charge a provoqué des surcharges à d'autres lignes. Lorsqu'il y a des surcharges, la ligne la plus surchargée est coupée s'il y a une interruption de communication, à cause d'une défaillance précédente, entre le noeud associé au centre de supervision du système de contrôle et le noeud du réseau de télécommunications associé au noeud électrique situé à l'extrémité de la ligne la plus surchargée. Si cette liaison de communication fonctionne, nous réduisons la charge de la ligne pour simuler un délestage. Lorsqu'une ligne est supprimée à cause de surcharge, nous calculons la puissance reçue par le noeud puits (noeud desservie directement par cette ligne) et nous comparons cette puissance à sa consommation normale et vérifions si ce noeud a enregistré un déficit de puissance. Si ce noeud a enregistré un déficit et si la liaison de communication entre le noeud du réseau de télécommunications associé à ce noeud déficitaire et le centre de supervision ne fonctionne pas, le noeud tombe en panne (supprimé du graphe) et le noeud correspondant du graphe du réseau de télécommunications est aussi supprimé. En revanche, si cette liaison de communication fonctionne normalement, un délestage est simulé par la réduction de la charge nominale du noeud à la puissance reçue.

Dans notre modèle, l'intervalle de temps entre 2 évaluations successives de l'état des réseaux simulés n'est pas fixe. En effet, lors des grandes pannes électriques, comme celles évoquées dans les sections précédentes, cet intervalle varie en fonction, de la durée depuis la première défaillance, donc du nombre de composants défaillants. Ces pannes ont montré que lorsqu'une première ligne déclenche, le déclenchement suivant peut survenir après plusieurs minutes, voire quelques heures. Par contre, ce temps se réduit au fur et à mesure que des lignes déclenchent et peut atteindre quelques secondes lorsque plusieurs lignes sont défaillantes. Pour tenir compte de ce phénomène dans notre modèle, nous calculons, à chaque évaluation de l'état

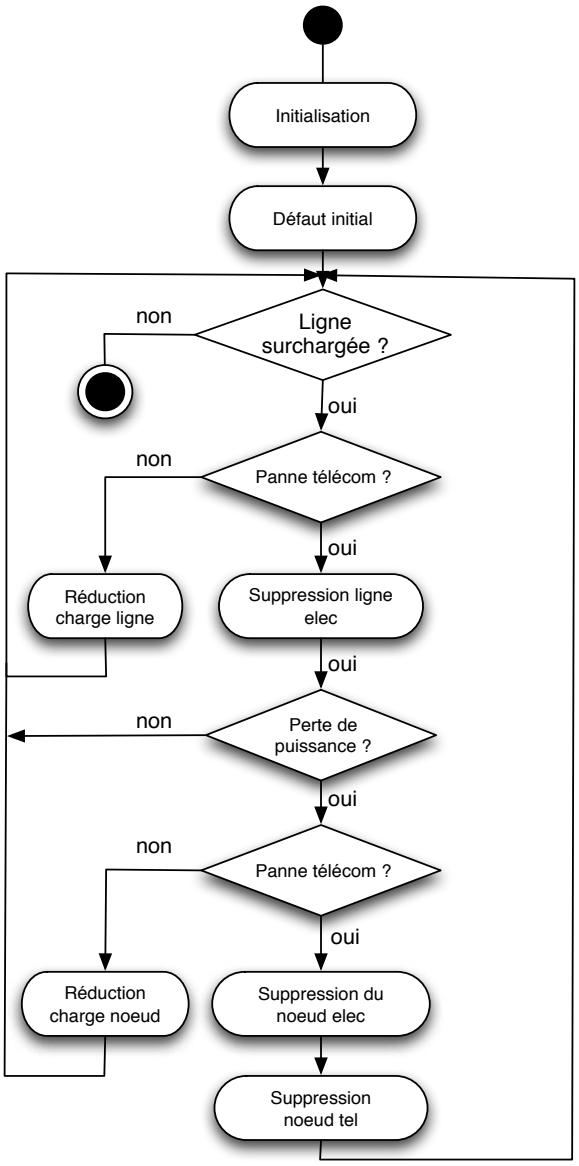


FIG. 3.4 – *Organigramme de la simulation des pannes en cascade*

du réseau, l'intervalle de temps entre 2 évaluations successives en fonction du nombre de lignes défaillantes et d'une moyenne fixée à 30 secondes.

```
input : G : Initial network's graph, LC : Links capacities, SimTime Simulation time
S = sum of all nodes representing power plants in the graph;
for each nodes in the graph do
    if Node != S then
        Demand[Node] = edmunds_karp_max_flow(G, S, node);
Choose link to cut to simulate an initial failure;
CCP = Choose the control center position;
while Time < SimTime do
    TimeStep = process the simulation time step taking into account the failed links
    number;
    Time = Time + TimeStep;
    OverloadedLink = most overloaded link in the graph;
    CO = the tail of OverloadedLink;
    A = find the router attached to CO;
    if A and CCP are able to communicate at time Time then
        Reconfigure CO's relay;
        mark OverloadedLink;
    else
        FNode = head of OvevloadedLink;
        cut OverloadedLink;
        Flow = edmunds_karp_max_flow(G, S, FNode);
        if Demand[FNode] - Flow < Seuil then
            if FNode and CCP are able to communicate at time Time then
                Demand[FNode] = Flow;
            else
                declare FNode failed;
                isolate FNode;
```

Algorithm 2: Simulation de la propagation des pannes

3.5.6 Expérimentations et résultats

Pour valider notre simulateur et étudier l'influence des protocoles de routage dans les propagations des pannes entre les réseaux électriques et de télécommunications, nous réalisons des simulations en utilisant les topologies des réseaux réels évoqués précédemment dans ce chapitre. Ces graphes sont présentés sur la figure 3.5.

Lors des simulations, les principaux paramètres évalués sont le nombre de noeuds et de lignes électriques défaillants et le nombre de reconfigurations du réseau électrique effectuées pour limiter la propagation des pannes, comme décrit dans la section précédente. Dans le premier scénario, la ligne électrique entre les noeuds 24 et 25 est coupée au début de la simulation et le centre de supervision est associé au noeud 10 du graphe de télécommunications.

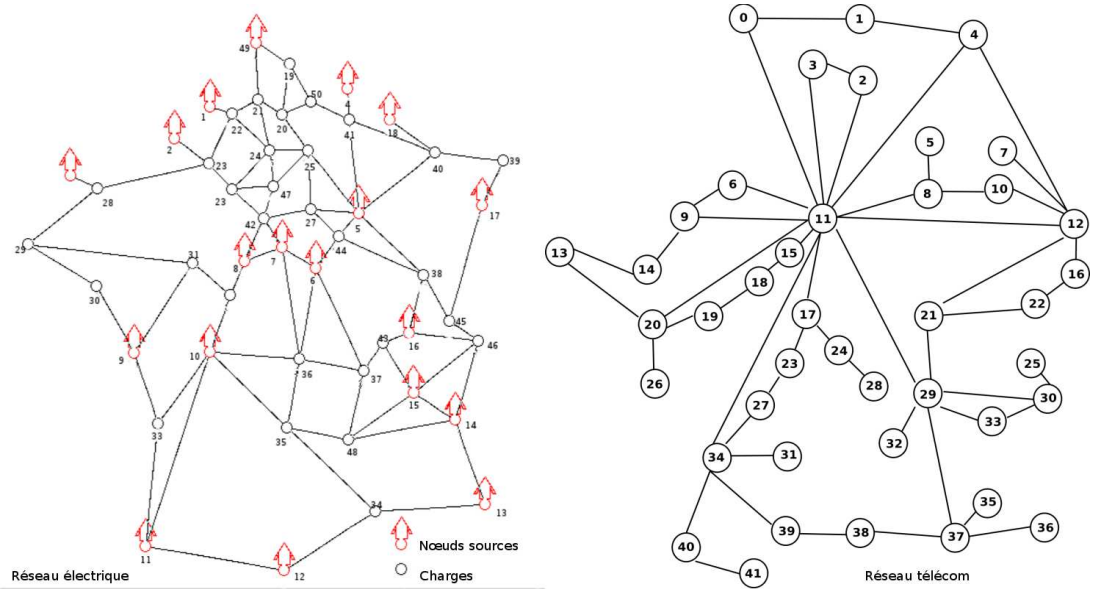


FIG. 3.5 – *Topologies utilisées pour les simulations*

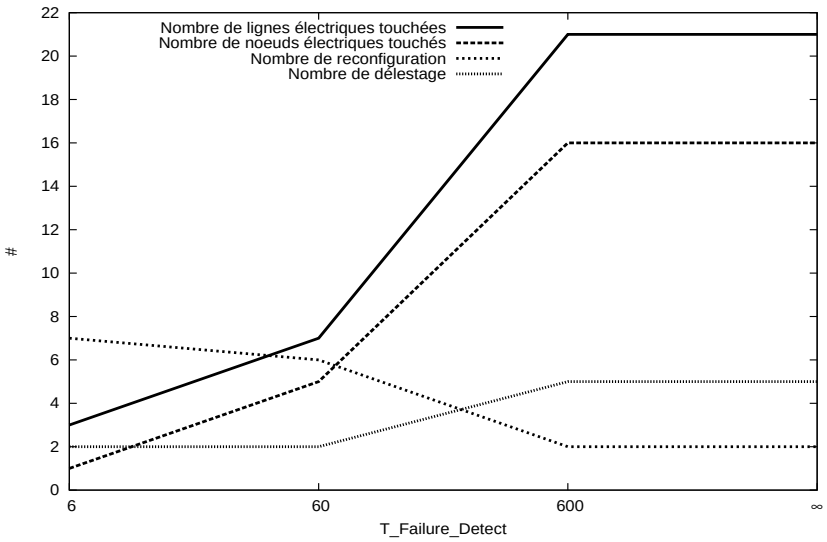


FIG. 3.6 – *Évolution du nombre de composants touchés*

Dans une première simulation, nous varions le temps de détection d'une panne par un routeur et observons l'évolution du nombre de composants du réseau électrique défaillants et du nombre de réduction de charge effectué pour éviter le déclenchement des lignes et la défaillance des noeuds. Les résultats obtenus sont présentés sur la figure 3.6. Cette figure montre qu'au fur et à mesure que le temps de détection des pannes par un routeur croît, les défaillances augmentent. On remarque, pour les valeurs des paramètres de cette simulation, une transition qui se situe entre 60 et 600*s* au cours de laquelle on observe une aggravation des pannes. Cette transition montre que lorsque le rapport du temps de détection d'une panne par un routeur sur l'intervalle moyen entre 2 pannes successives de lignes électriques atteint la valeur de 2, il y a un risque élevé de pannes en cascade pouvant conduire à un écroulement du réseau.

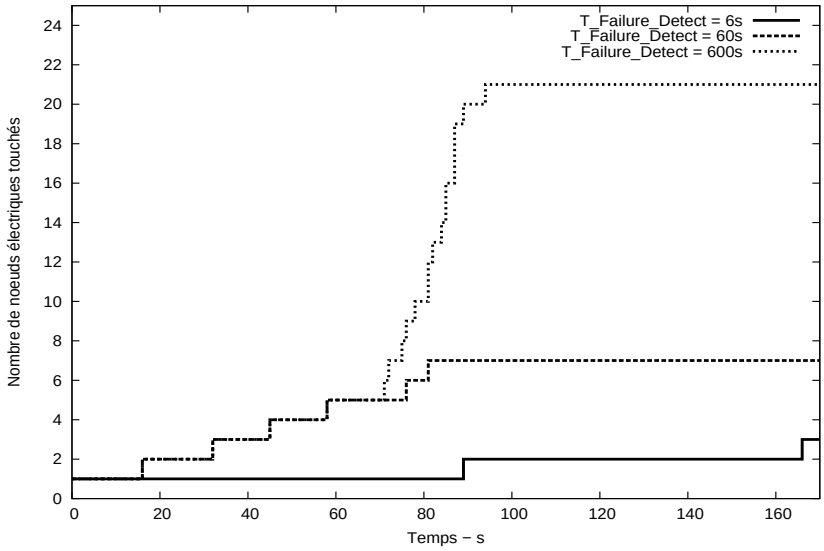


FIG. 3.7 – *Évolution des pannes en fonction du temps de la simulation*

La figure 3.7 montre l'évolution des pannes en fonction du temps de simulation. Comme dans le déroulement des pannes réelles, en début de simulation la propagation des pannes est relativement lente, puis croit fortement après que les défaillances aient touché plusieurs composants du réseau électrique. Durant toute la simulation, on constate qu'une bonne réactivité du réseau de télécommunications permet de limiter fortement les effets de cascade. Sur la figure 3.7, on constate que malgré un temps de réactivité du réseau de télécommunications très faible, la propagation des pannes ne peut être arrêté que si, à partir de l'état du réseau électrique et des pannes déjà constatées, on peut identifier les équipements vulnérables et prendre des mesures anticipées pour ne pas qu'ils soient touchés. Si les mesures sont toutes réactives, la propagation peut être atténuée par une forte réactivité du réseau de télécommunications, mais la panne continuera à survivre car des composants vulnérables peuvent toujours être touchés.

Pour montrer le rapport entre les valeurs des paramètres utilisés et les résultats présentés ci-dessus, nous présentons sur la figure 3.8 les résultats des mêmes simulations en fonction du rapport de l'intervalle moyen entre 2 pannes successives sur le temps de détection d'une panne par un routeur.

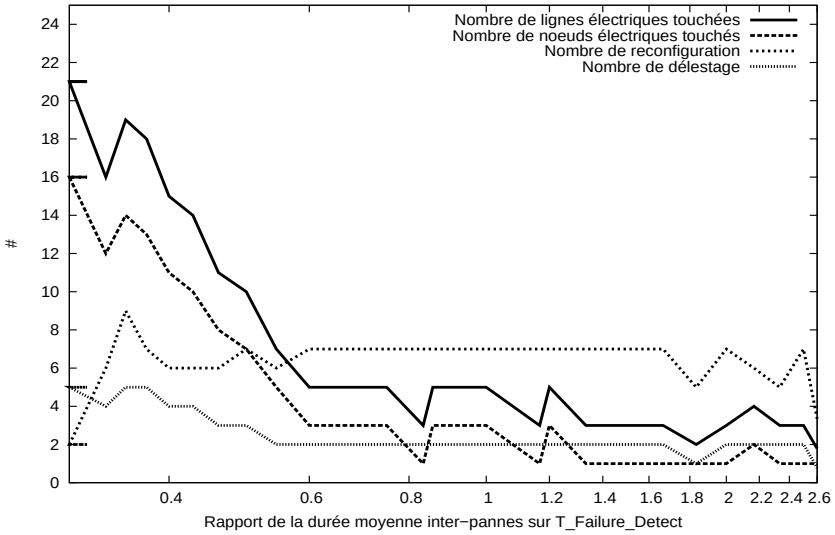


FIG. 3.8 – *Évolution de pannes du rapport de la durée moyenne inter-panne sur le temps de détection des pannes*

Lorsque le temps de détection d'une panne est inférieur à une certaine proportion ($0,6$ dans ce cas) de la valeur moyenne de l'intervalle de temps entre 2 pannes successives, le nombre décroît. Ces résultats montrent cependant, que l'évolution du nombre de réduction de charge des lignes et des noeuds ne dépend pas uniquement de ce rapport, mais aussi de la fréquence des pannes dans le réseau électrique. Ces résultats valident notre simulateur car ils sont cohérents avec les phénomènes fréquents lors des pannes en cascade. L'évolution du nombre de routeurs défaillants suit une courbe quasi-identique à celle des noeuds du réseau électrique car chacun des noeuds d'un des réseaux est associé à un et un seul noeud de l'autre réseau dans le modèle.

Dans les simulations suivantes, nous avons défini plusieurs scénarios en variant les principaux paramètres (temps de détection des pannes par les routeurs, la panne initiale, la position du centre de contrôle) pour obtenir des caractéristiques générales des pannes dans le réseau électrique en fonction de tous ces paramètres. Ceci nous a permis de simuler 14280 scénarios. Les résultats présentés dans la figure 3.9 montrent le nombre de lignes électriques défaillantes pour différentes fractions de scénarios simulés. Cette figure montre des résultats qu'on peut classer en 3 catégories. La première partie (nombre de lignes défaillantes inférieur à 6) montre que la topologie étudiée résiste relativement bien aux pannes en cascade. En effet, pour la majorité des scénarios ($92,5\%$), le déclenchement d'une ligne du réseau ne provoque qu'un nombre limité à 6 coupures de lignes et cela quelque soit le temps de réaction du réseau de télécommunications, la position du centre de supervision et la ligne coupée en début de simulation. La dernière partie montre que le risque qu'une coupure d'une seule ligne puisse provoquer des pannes en cascade très importantes existe pour $6,1\%$ du nombre total de scénarios simulés. La dernière catégorie, très intéressante pour ce travail est celle qui montre le nombre de scénarios pour lequel la réduction du temps de détection des pannes par les routeurs permet de réduire significativement la propagation des pannes. Le faible nombre de scénarios (seulement $1,4\%$)

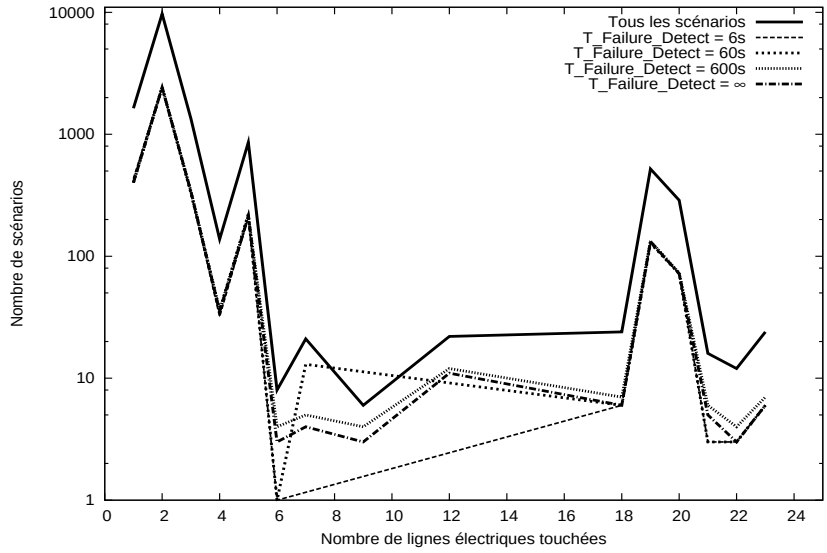


FIG. 3.9 – *Nombre de lignes défaillantes en fonction du nombre total de simulations*

de cette catégorie peut s'expliquer par la taille relativement petite du graphe simulé, du choix de l'intervalle moyen entre deux déclenchements successifs des lignes électriques et le fait que pour tous les scénarios, le réseau de télécommunications fonctionne au début de la simulation, ce qui limite le déclenchement en cascade des lignes électriques.

Dans les dernières simulations, nous avons essayé de montrer l'importance du maintien des liaisons de communication dans la lutte contre les pannes en cascade entre les réseaux électriques et les réseaux de télécommunications. Pour cela nous avons présenté sur la figure 3.10 l'évolution du nombre de lignes électriques défaillantes en fonction du degré du noeud représentant le centre de supervision. Dans notre modèle, ce noeud est un facteur fondamental car lorsqu'il est défaillant, le système de contrôle ne joue plus aucun rôle, par conséquent aucun moyen existe pour atténuer les effets de cascade.

Puisque dans nos simulations, nous évaluons à la fois la surcharge des lignes et le déficit de puissance enregistré par les noeuds, le degré des noeuds est un bon indicateur de la résistance aux pannes de ces noeuds parce que le déficit de puissance qui provoque, dans certaines conditions, la panne d'un noeud résulte d'un faible nombre de lignes connectées à ce noeud. La figure 3.10 montre les résultats obtenus qui confirment le fait que les pires situations sont celles où le centre de supervision a un degré de connectivité très faible (inférieur ou égal à 4). Le nombre des défaillances croît très rapidement lorsque le degré du noeud est inférieur à 2 pour les scénarios de la catégorie *Dependant*. Pour les valeurs supérieures à 4, le nombre des défaillances croît avec le degré du noeud du centre de supervision. Ce comportement est un cas particulier de notre modèle qui est du au fait qu'un noeud de degré élevé est plus exposé au risque de déficit de puissance, donc à la défaillance.

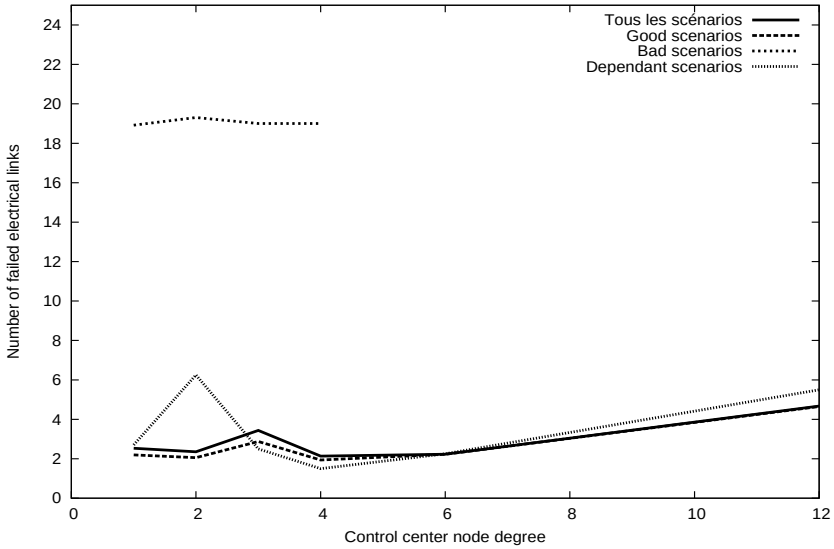


FIG. 3.10 – *Nombre de lignes défaillantes en fonction du degré du noeud du centre de supervision*

3.6 Conclusion partielle

Pour comprendre les interdépendances entre les infrastructures et les pannes en cascade qui en résultent, il est nécessaire de développer des outils de modélisation et de simulation multi-infrastructures pouvant être intégrés dans un environnement de simulation unique. Dans cet objectif, plusieurs travaux utilisent la fédération des logiciels existants. Mais cette technique présente de nombreuses limites, la faible utilisation du standard HLA, conçu pour répondre à cette attente confirme cet état de fait. C'est pourquoi nous avons choisi une nouvelle approche fondée sur la théorie des graphes capable d'intégrer dans un même modèle plusieurs infrastructures interdépendantes et de simuler leur comportement de manière réaliste. Nous avons utilisé ce modèle pour étudier les interdépendances entre les réseaux électriques et de télécommunications, particulièrement l'influence de l'intervalle moyen entre deux déclenchements successifs des lignes électriques et le temps de détection de panne par un routeur. Les expérimentations menées sur des graphes représentant des topologies réelles à l'échelle d'un pays avec un centre de supervision montrent qu'il est possible de limiter les effets de cascade par l'utilisation d'un réseau de télécommunications performant, capable de fournir aux opérateurs des informations temps réels permettant de prendre des actions appropriées pour reconfigurer les composants vulnérables du réseau électrique. Dans nos simulations, exclusivement limitées à la propagation des défaillances matérielles des composants, nous avons évalué les principaux paramètres qui favorisent ou limitent les propagations des pannes. Les résultats ont fait apparaître que certaines configurations topologiques sont moins dépendantes du réseau de télécommunications, soit parce que la défaillance initiale a un impact limité ou parce que cet impact est tellement important que la reconfiguration n'a qu'un effet très faible. En revanche, il est apparu un nombre important de scénarios pour lesquels les simulations ont montré une dépendance très forte du réseau électrique à la capacité du système de contrôle à prendre des actions appropriées au bon

moment après une défaillance, donc à la qualité des informations fournies par le système de contrôle et à la performance du réseau de télécommunications sous-jacent.

Les expérimentations menées avec notre simulateur montrent que pour obtenir des outils de modélisation des interdépendances pertinents, il est nécessaire que le modèle de chaque infrastructure soit développé de manière à pouvoir couvrir l'ensemble des caractéristiques déterminantes de cette infrastructure, mais aussi qu'il puisse être facilement intégré dans un environnement unique avec les modèles des autres infrastructures interdépendantes. Dans cette optique, nous nous sommes intéressés à l'analyse des différentes situations qui conduisent aux défaillances des composants des réseaux de télécommunications. Pour faciliter l'intégration avec d'autres outils, notre modèle utilise la théorie des graphes. Il peut ainsi être complété par des modèles développés pour d'autres infrastructures, ce qui permettra de réaliser des études plus complètes des interdépendances multi-infrastructures et de fournir des résultats plus pertinents et plus réalistes. En plus de tous les résultats présentés dans les sections précédentes, la principale contribution de ce chapitre a été de montrer qu'il est possible de concevoir un modèle et un simulateur des interdépendances suffisamment génériques pour rendre possible l'intégration des modèles et des simulateurs de plusieurs infrastructures dans un environnement unique tout en offrant la possibilité de mettre en œuvre tous les facteurs qui influent sur les propagations des pannes qui peuvent résulter de ces interdépendances. Ce modèle fondé sur les graphes peut être adapté à la plupart des infrastructures critiques et l'approche utilisée pour caractériser le rôle des protocoles de routage dans le réseau de télécommunications et le transfert des charges dans le réseau électrique montre qu'il est possible d'intégrer l'ensemble des facteurs déterminants sans rendre le modèle incalculable.

Une amélioration future de ce travail serait l'intégration d'autres infrastructures comme le réseau de transport et la caractérisation des trois scénarios résultant de ces expérimentations avec des modèles implémentant de manière plus complète les infrastructures en intégrant, par exemple, l'oscillation de la fréquence et les puissances actives et réactives pour le réseau électrique et les algorithmes réels de routage pour le réseau de télécommunications. Des simulations sur plusieurs topologies avec des données plus complètes et plus réalistes est une autre piste d'évolution qui contribuerait à obtenir des résultats plus pertinents. La simulation des topologies de taille plus importante comportant plusieurs centres de supervision peut aussi être envisagée.

La première difficulté à laquelle nous avons été confrontés lors de nos simulations des pannes en cascade est le manque de topologies réalistes pour les simulations. Nous nous intéressons donc à ce premier obstacle et exposons, dans le chapitre suivant, notre technique de génération des topologies adaptées à l'étude de la propagation des pannes dans les réseaux.

Chapitre 4

Génération des topologies des réseaux pour la modélisation et la simulation des interdépendances

4.1 Introduction

La forte croissance de l'Internet et les difficultés liées au manque de technique et de données pour la production d'une cartographie précise de l'Internet ont poussé à réfléchir à des techniques appropriées de représentation topologique du réseau. En effet, cette croissance explosive cause un certain nombre de problèmes liés au routage, à l'administration, à la réservation des ressources et au risque des pannes et attaques de grande ampleur. Le développement des outils appropriés pour faire face à ces problèmes nécessite des simulations et des modèles réalistes de la structure du réseau pour évaluer les solutions proposées. Les interconnexions des différentes infrastructures impliquées dans la cadre des études sur les interdépendances renforcent les difficultés liées à la mise à disposition des topologies qui représentent, de manière réaliste l'ensemble de ces infrastructures. Or, pour effectuer des études de modélisation et de simulation, les chercheurs ont, le plus souvent besoin de la topologie du réseau étudié. La topologie du réseau désigne la définition de l'architecture, c'est à dire de la disposition et de la hiérarchie de l'ensemble des composants du réseau et les liaisons entre ces différents composants. Selon l'objectif, cette topologie peut représenter différents niveaux des réseaux. Pour les réseaux de télécommunications, cette topologie peut représenter les interconnexions des systèmes autonomes, on parle alors de topologies de niveau AS ou les interconnexions des routeurs à l'intérieur d'un système autonome. Elle peut aussi concerner les réseaux d'accès ou les réseaux de cœur. Pour les réseaux électriques, il est possible de représenter uniquement les interconnexions entre les différents réseaux, celles d'un réseau particulier, les réseaux de distribution ou les réseaux de transport. Cette représentation topologique peut être faite à l'aide des graphes où les nœuds du graphe représentent les composants et les arrêtes représentent les liaisons entre ces composants. Actuellement, de nombreux travaux de recherche sont basés sur des topologies représentées par les graphes réguliers (topologie maillée, en anneau, en étoile, en arbre), les réseaux bien connus comme ARPANet [48] ou des topologies générées

aléatoirement.

La principale limite de ces méthodes est que les topologies générées aléatoirement et les graphes réguliers sont, le plus souvent, très loin des réseaux qu'on souhaite étudier. Les topologies représentant les réseaux bien connus ne conviennent que pour des études particulières comme l'évaluation des performances de nouveaux protocoles, elles sont souvent trop anciennes, donc inadaptées à l'étude des interdépendances des infrastructures actuelles. Par exemple, les topologies des réseaux électriques fréquemment utilisées pour des tests, comme celle du réseau électrique IEEE de 14 nœuds[1] datent des années 60.

Or les résultats des simulations varient fortement en fonction des environnements, notamment les topologies utilisées. Donc, pour obtenir des résultats pertinents avec des expérimentations basées sur des modèles et des simulations, il est indispensable de disposer, en nombre suffisant, des topologies qui représentent fidèlement les réseaux étudiés.

Par ailleurs, pour les simulations des interdépendances, la topologie utilisée doit représenter une multitude de réseaux interconnectés à des points précis suivant des accords ou des nécessités techniques. Les simulations des propagations des pannes dans les réseaux nécessitent une caractérisation de l'ensemble des événements qui conduisent à ces pannes : leur origine, leur évolution et leurs conséquences. Il est donc nécessaire de représenter l'ensemble des entités qui influent sur les propagations de ces pannes et d'utiliser des topologies qui représentent aussi bien les interconnexions au sein d'un réseau particulier que celles entre les différents opérateurs. Puisqu'il existe une différence fonctionnelle importante entre les interconnexions au sein d'un même réseau et celles entre différents réseaux liées, notamment aux accords, ces topologies doivent offrir des moyens pour identifier ces différentes interconnexions. Pour l'étude des interdépendances et les propagations des défaillances entre les infrastructures, les réseaux impliqués sont de grande taille et ont des topologies complexes.

La nécessité, pour les chercheurs de disposer de topologies en nombre suffisant pour leur simulation ont contribué à l'émergence du besoin de développer des techniques de génération automatique des topologies. Dans ce chapitre, nous présentons une technique de génération des topologies pour la modélisation et la simulation des interdépendances. La technique proposée consiste à appliquer les règles de déploiement des réseaux pour produire une topologie proche des infrastructures existantes. Ces règles sont différentes suivant les domaines, par exemple, les paramètres fondamentaux pour déployer un réseau de télécommunications diffèrent de ceux du réseau électrique. Nous prenons donc en compte ces spécificités, mais définissons un algorithme qui peut être adapté à ces spécificités. Notre algorithme utilise des paramètres d'entrée simples et réalistes couramment pris en compte pour la conception et le dimensionnement des réseaux et génère des graphes représentant des topologies qui offrent des possibilités pour identifier les interconnexions, donc les interdépendances. Ces paramètres peuvent être des résultats des mesures ou des enquêtes ou encore générés aléatoirement. La technique proposée et les résultats de l'évaluation de la qualité des topologies générées sont décrites dans les sections suivantes. Une partie du travail présenté dans ce chapitre a été publié [50] au *4th International Workshop on Critical Information Infrastructures Security* (CRITIS'09[2]) en octobre 2009.

[1] http://www.ee.washington.edu/research/pstca/

[2] http://www.critis09.org

4.2 État de l'art de la génération de topologies des réseaux de télécommunications pour des études des interdépendances

La génération automatique de topologie des réseaux a mobilisé de nombreux chercheurs et plusieurs travaux ont été faits pour fournir des outils de génération dont les plus connus sont les techniques de génération aléatoire. A titre d'exemple, on peut citer les travaux de Waxman [144] qui avait développé l'un des modèles les plus populaires. Sa technique consiste à générer des graphes probabilistes en considérant la distance euclidienne entre les nœuds. Par la suite, les auteurs de [29, 52, 149, 148] ont introduit la notion de hiérarchie observée sur Internet à l'aide des logiciels GT-ITM[3] et Inet[4] démontrant ainsi les limites du modèle de Waxman [144] pour représenter le réseau Internet, notamment sa structure hiérarchique. Le développement de ces modèles était essentiellement fondé sur des observations qui ont montré que les topologies des réseaux étaient loin d'être arbitraire et présentaient des structures hiérarchiques évidentes. L'approche de ces outils prônait aussi la prise en compte les principes de conception et de déploiement de réseaux par les générateurs de topologies. Ces outils ont été très vite suivis par l'apparition des logiciels comme BRITE[5] [99] et PLRG [15] qui, en plus de la génération des graphes hiérarchiques offrent des possibilités de produire des graphes dits sans-échelle (*scale free*) dont la distribution des degrés suit une loi de puissance. Les auteurs de [95] introduisent un modèle hybride combinant des techniques de génération aléatoires des topologies et des techniques fondées sur la distribution des degrés. Ils proposent l'utilisation des techniques aléatoires pour générer les graphes représentant les interconnexions intra-AS et la technique dont la distribution des degrés suit une loi de puissance pour générer les graphes inter-AS. Pour rappel, l'architecture Internet est constituée de différents AS hiérarchiques. Les AS de niveau 1 (*Tier-1 AS*) sont des réseaux IP qui participent à l'Internet uniquement par le biais d'interconnexions non payantes, également connu sous le nom de *peering* gratuit. Ce sont les réseaux qui peuvent atteindre tous les autres réseaux sur Internet sans avoir à payer pour des services d'un réseau de transit. Ils se situent au plus haut niveau de la hiérarchie (*Top level AS*). Il existe aussi des AS de niveaux 2 (*Tier-2 AS*) et 3 (*Tier-3 AS*). Les AS de niveau 2 sont des réseaux qui peuvent établir des liens de *peering* gratuit avec d'autres réseaux de même niveau et sont des clients des AS de niveau 1. Les AS de niveau 3 sont, en général sans lien de *peering*, ils sont des simples clients des AS de niveau 2.

Dans [28], les auteurs étudient la structure hiérarchique de l'Internet pour identifier les différentes parties du réseau qui peuvent être correctement représentées par les techniques de génération de topologie fondées sur la distribution des degrés et sur la structure hiérarchique de l'Internet. D'après leurs résultats, à l'exception des interconnexions entre les AS de niveau 1 (*Tier-1 AS*), la distribution des degrés des interconnexions entre les différents systèmes autonomes suivent une loi de puissance. Ils déduisent une technique hybride de génération permettant d'obtenir des graphes conformes à cette distribution de degrés et à la structure hiérarchique. Dans le même ordre d'idée, les auteurs de [81] proposent MAMT (*Multi-ASes and Multi-Tiers*) pour la génération des graphes représentant à la fois plusieurs systèmes autonomes

[3] http://www.isi.edu/nsnam/ns/ns-topogen.html#gt-itm
[4] http://www.isi.edu/nsnam/ns/ns-topogen.html#inet
[5] http://www.cs.bu.edu/faculty/matta/Research/BRITE/

de différents niveaux (*Tier-1*, *Tier-2* et *Tier-3*) à partir d'une technique fondée sur la structure hiérarchique du réseau Internet. Pour améliorer la qualité des topologies générées par les techniques fondées sur la structure hiérarchique, ATETEs (*Adapting Traffic Evolution Topology gEnerators*) [84] propose d'utiliser, en plus de la structure hiérarchique et de la distribution des degrés, la distribution du trafic pour générer des topologies sur la base de l'évolution du réseau. L'approche d'évolution du réseau utilisée est fondée sur l'ajout des liens et des nœuds au graphe initial de manière à réduire la charge des parties les plus congestionnées du réseau.

Une autre approche fréquemment utilisée pour la génération des topologies est celle qui consiste à générer des graphes à partir des données collectées par des moniteurs placés sur certains points du réseau Internet. Les travaux des auteurs de [145] considèrent, sur la base des données collectées en 1998, que la distribution des degrés de connectivité des liens inter-AS suivent une loi de puissance. Ils proposent une technique fondée sur cette distribution. Ces travaux ont servi de base à de nombreuses techniques de génération des topologies. Cependant, des travaux comme ceux de [109] ont démontré, par la suite que les résultats fournis par cette technique sont trop approximatifs et présentent des limites pour l'étude de la propagation des pannes à cause de la topologie incomplète du réseau qu'elle produit et l'impossibilité d'obtenir des graphes de niveau routeur nécessaires pour la modélisation des propagations des pannes. Dans [93], les auteurs proposent de combiner les données collectées à partir des réseaux existants, de la théorie des graphes et des contraintes techniques et économiques liées au déploiement des réseaux pour générer des topologies de niveau routeur. Les contraintes techniques et économiques utilisées comprennent le nombre maximum de ports d'un routeur, donc son degré de connectivité et le coût des liaisons entre les différents sites. Avec leurs résultats, les auteurs démontrent que les réseaux fortement connectés ne sont pas forcément efficaces en terme de bande passante et de coût. Les auteurs de [49] utilisent une technique de rétro-ingénierie (*reverse-engineering*) pour générer des topologies représentant des réseaux à l'échelle d'un pays à partir des données sur des réseaux de plus petite taille (à l'échelle régionale par exemple). Pour prendre en compte les contraintes techniques et de coût de déploiement des réseaux, les auteurs combinent la technique de rétro-ingénierie aux contraintes liées au coût de déploiement et à la performance, notamment la limite des routeurs et des liens en terme de bande passante. Avec leurs résultats, les auteurs démontrent que même avec une même distribution de degrés, les topologies peuvent avoir une différence importante en terme de structure lorsque la technique de génération prend en compte les contraintes d'ingénierie.

La troisième approche de génération des graphes utilise un graphe de référence, par exemple, la technique des auteurs de [96] permet de générer des graphes de différentes tailles à partir d'un graphe de base tout en conservant certaines caractéristiques du graphe réel, notamment la distribution des degrés. Cette technique utilise une méthode appelée *dK-series* décrite dans [97] et basée sur la corrélation des degrés des nœuds. Elle considère que la plupart des propriétés des graphes caractérisent leurs connectivités et par conséquent la corrélation des distributions des degrés permet de conserver les principales caractéristiques des graphes tout en offrant la possibilité de générer plusieurs graphes de taille différente. Dans le même ordre d'idées, l'auteur de [87] développe une technique semblable aux précédentes et qui permet de générer des graphes qui conservent certaines propriétés topologiques, notamment, un diamètre relativement petit, une valeur élevée du cœfficient de clustering et une distribution de degrés suivant une loi de puissance. Sa mise en œuvre consiste à générer plusieurs graphes à partir d'un graphe pris

comme référence en remplaçant certains liens des nœuds pris au hasard par des nouveaux liens connectant le nœud considéré à d'autres nœuds choisis au hasard et situés à 2 sauts de ce nœud.

Pour évaluer la qualité des différentes techniques de génération de topologie des réseaux, les auteurs de [137] effectuent une comparaison entre des graphes automatiquement générés et des graphes obtenus à l'aide des données collectées à partir des tables BGP et du projet SCAN [119]. La comparaison des graphes est basée sur 3 métriques : le nombre de nœuds accessibles par chacun des nœuds du graphe après n sauts, la résilience, c'est à dire l'existence ou non de liens redondants et la structure du graphe, déterminée par le calcul de la distance moyenne sur l'arbre couvrant (*spanning tree*) entre chaque paire de nœuds d'un graphe qui ont une arrête commune. Les auteurs démontrent, avec leurs résultats que les techniques de génération de topologie fondées sur la distribution des degrés des nœuds permettent d'obtenir des graphes plus proches des graphes utilisés comme réseaux de référence que ceux des techniques fondées sur la hiérarchie. Leurs résultats montrent que malgré la non prise en compte de la structure hiérarchique de l'Internet par les techniques fondées sur la distribution des degrés, les graphes fournis par ces techniques dont la distribution des degrés suit une loi de puissance sont plus hiérarchiques que ceux générés aléatoirement. Ils ont trouvé que cette hiérarchie « dégradée » permet d'obtenir des graphes plus proches des réseaux de référence que les graphes générés avec des techniques fondées explicitement sur une approche hiérarchique.

L'article [118] décrit le logiciel IGen[6] développé avec le langage Perl/Tk et qui permet de générer des topologies des réseaux de télécommunications sur la base des principes de conception de ces réseaux. Dans une première étape, l'IGen regroupe les nœuds au sein de différents clusters pour représenter les points de présence (*Point Of Presence - POP*). Le regroupement des nœuds dans un cluster est fondé sur la distance euclidienne ou la demande de trafic ou encore la combinaison de ces deux critères. L'interconnexion des POP est mise en œuvre avec des heuristiques comme MENTOR [27], MENTour [27], la triangulation de Delaunay [38] et la technique appelée 2-MST (*Two Trees* [68]). MENTOR permet de générer des topologies en arbre en combinant la technique du plus court chemin (*Tree/shortest-path tree - MST-SPT*) et les contraintes économiques et techniques de conception des réseaux. MENTour est une amélioration de la technique MENTOR et permet d'augmenter la connectivité du graphe généré en assurant que chaque nœud du graphe est connecté à, au moins deux de ses voisins. *2-MST* utilise la même approche que MENTOR, mais génère deux arbres au lieu d'un seul. La technique de triangulation de Delaunay [38] permet de produire des graphes avec des chemins alternatifs entre chaque paire de nœuds en minimisant le nombre de chemins redondants.

La technique de génération de topologie proposée par les auteurs de [72] utilise une distribution de degrés préalablement calculée pour générer des topologies de niveau AS et de niveau routeur. Cette distribution des degrés est calculée à partir des données sur la topologie du réseau Internet fournies, notamment par l'opérateur GEANT[7] et par le logiciel de l'analyse de la topologie et de la performance de l'Internet Skitter[8] développé par l'association CAIDA (*Cooperative Association for Internet Data Analysis*)[9]. La technique consiste à utiliser des données des réseaux spécifiques pour générer des topologies représentant plusieurs réseaux

[6] http://w3.umh.ac.be/~networks/igen/
[7] http://www.geant.net
[8] http://www.caida.org/tools/measurement/skitter/
[9] http://www.caida.org/

de différentes tailles.

L'article [121] présente une synthèse de plusieurs travaux de recherche sur la génération et la découverte de topologies du réseau Internet réalisés avant 2006. Les auteurs décrivent les fonctionnalités de certains outils qui ont été mis en œuvre par ces travaux comme BRITE[10] [99] pour la génération de topologie, Scotty [129] et NetView[11] pour la découverte de la topologie, ils exposent aussi les limites de ces différents logiciels.

Après une analyse approfondie des besoins en terme de topologies pour la modélisation et la simulation des propagations des défaillances, il ressort que les générateurs de topologie doivent prendre en compte les facteurs qui influent l'interconnexion des réseaux réels pour fournir des topologies convenables. Ces facteurs sont déterminants dans l'interconnexion des graphes et ne doivent pas être obtenues par un choix aléatoire après la génération du graphe. Dans la conception des réseaux, les points de présence (*Point Of Presence - POP*), par exemple ne sont pas choisi après le déploiement du réseau, mais ils sont pris en compte lors de cette conception et ils influent sur la manière dont le réseau est interconnecté. De même, pour le cas spécifique des modélisations et des simulations des interdépendances, les générateurs de topologies doivent répondre à un besoin spécifique de compromis entre une généricité nécessaire à l'extension du générateur à plusieurs infrastructures et une prise en compte des facteurs spécifiques à chaque infrastructure. Ils doivent aussi pouvoir générer des topologies de petite et de grande taille (adaptées aux tailles des réseaux réels) permettant de simuler de l'ensemble des caractéristiques de ces réseaux. La dernière contrainte très importante est le fait de devoir fournir des moyens permettant de caractériser ces infrastructures de la manière la plus complète possible pour faciliter les études des interdépendances. En effet, ces études nécessitent de représenter la topologie au niveau routeur de l'Internet, mais aussi de distinguer les routeurs qui sont dans un même système autonome de ceux qui ne le sont pas. Par exemple, l'outil doit permettre de savoir si un nœud du graphe généré appartient à un seul réseau ou bien s'il interconnecte deux ou plusieurs réseaux, les caractéristiques d'un lien du graphe comme sa capacité doivent aussi être définies. Ces paramètres permettent, notamment de caractériser l'importance du nœud ou du lien et différencier les nœuds (nœuds BGP et OSPF pour les réseaux de télécommunication et sources de production et charges pour les réseaux électriques).

4.3 Limites des outils existants pour la génération des topologies convenables aux modélisations et aux simulations des interdépendances

Pour répondre au besoin de disposer d'un grand nombre de topologies de réseaux pour les travaux de modélisation et de simulation, les chercheurs ont développé plusieurs techniques de génération automatique de topologies. Ces techniques utilisent différentes approches pour le choix des interconnexions. Certaines se basent sur un choix aléatoire alors que d'autres utilisent la distance euclidienne ou des lois de distributions probabilistes.

Les techniques aléatoires permettent d'obtenir des graphes qui conviennent à des travaux de

[10] http://www.cs.bu.edu/faculty/matta/Research/BRITE/
[11] http://www-306.ibm.com/software/tivoli/products/netview/

recherche spécifiques comme l'évaluation du passage à l'échelle d'un protocole, mais elles présentent plusieurs inconvénients pour l'étude des interdépendances qui nécessite des traitements spécifiques pour des nœuds ou des liens précis. Étant donné que cette technique est démunie de toute annotation, son utilisation oblige, lorsque c'est nécessaire, à choisir ces nœuds ou ces liens de manière purement aléatoire. Ce qui n'est pas convenable lorsque ces nœuds ou ces liens doivent être sélectionnés suivant des critères précis et connus à l'avance.

La deuxième catégorie des techniques utilise des informations déduites à partir des données partielles obtenues par des outils de découverte de topologie comme traceroute[12] ou des données fournies par des moniteurs placés dans différents endroits du réseau Internet pour générer des topologies représentant le réseau Internet. A cause de la difficulté liée au déploiement de moniteurs qui couvrent l'ensemble des AS du réseau Internet, ces techniques produisent des topologies, le plus souvent, très loin de la topologie réelle du réseau. Les travaux de recherche basés sur ces topologies suscitent donc de nombreuses interrogations liées à la représentativité des graphes utilisés. Les travaux des auteurs de [109] se sont justement intéressés à cette question de représentativité des graphes générés par cette technique et à l'identification de la partie de l'Internet représentée convenablement par ces graphes. Les auteurs effectuent une comparaison entre une topologie générée à partir des informations précises concernant quelques AS et une autre déduite de l'ensemble des informations accessibles au public. Avec cette comparaison, ils ont pu identifier les types de relations inter-AS fidèlement représentées par les topologies actuelles et celles qui ne le sont pas. Ils démontrent que les topologies issues des techniques de génération actuelles ne sont pas représentatives de l'ensemble des liaisons entre les AS et conduisent à des résultats erronés pour la plupart des études basées sur la théorie des graphes. En effet, il apparaît qu'avec ces topologies le taux des liens omis est de l'ordre 10 à 20% pour les AS de niveau 1 (*Tier-1 AS*) et de niveau 2. Cette omission peut atteindre 85% lorsque ces AS sont des grands réseaux avec un nombre important de liens pair à pair (*peering*). Ce taux élevé des liens non représentés est principalement dû au fait que les données soient collectées durant des périodes relativement courtes qui ne permettent pas de détecter toutes les routes BGP, mais aussi à cause de l'insuffisance du nombre de moniteurs déployés (environ 700 moniteurs déployés sur 400 AS pour plus de 26000 AS au total [109]) pour couvrir l'ensemble des liens du réseau Internet. Toutes ces difficultés conduisent à des graphes incomplets à cause des liens cachés et invisibles, mais aussi de l'omission d'un nombre important de liens pouvant aller jusqu'à 90% des liens pour un grand réseau qui ajoute des liens de peering pour une période relativement courte. En effet, les moniteurs qui fournissent les informations servant de base à ces techniques enregistrent des données obtenues à partir des annonces des autres routeurs BGP qui transitent par ces moniteurs. Or ces moniteurs ne couvrent pas tous les AS de l'Internet et il existe de nombreux cas où les routes ne sont pas annoncées, notamment certaines routes reçues des AS pairs ou des routes de secours. Les informations sur certaines routes ne transitent donc pas par ces moniteurs et les liens correspondants sont purement et simplement omis. Les auteurs de [109] ont montré, qu'en général un moniteur est déployé pour la plupart des AS de niveau 1 (*Tier-1 AS* ou *Top level AS*) et même s'il existe des AS de niveau 1 sans moniteur, leurs interconnexions directes avec d'autres AS de niveau 1 où des moniteurs sont déployés les rendent visibles, donc l'ensemble des liens des AS de niveau 1 sont relativement

[12] http://www.traceroute.org

bien représentés par les topologies générées par cette technique. Par conséquent, les moniteurs permettent d'obtenir la plupart des liens Fournisseur-Client et Client-Fournisseur, mais pas les liens pair à pair (liens de *peering*), notamment entre les AS de niveau inférieur. Ces topologies conviennent donc à des études faisant intervenir des paramètres comme le diamètre du réseau, le nombre de systèmes autonomes, mais peuvent conduire à des résultats incorrects lorsqu'elles sont utilisées pour des études basées sur d'autres paramètres (degrés des nœuds, les longueurs des chemins, le cœficient de *clustering*) et celles portant sur des relations entre AS, les chemins entre AS, la robustesse des réseaux (face aux pannes de routage), l'évaluation de nouveaux protocoles inter-AS et des problèmes comme la corruption des tables de routage par des fausses annonces (*prefix hijacking*). Pour faire face à ces limites, une alternative consiste à compléter les données fournies par les moniteurs avec des informations collectées par des outils comme les *looking glass*, la commande *show ip bgp sum*, les données fournies par certains opérateurs et les informations des fichiers de configuration et des fichiers de trace des routeurs. Cette méthode permettrait d'obtenir une topologie inter-AS plus complète de l'Internet, mais elle nécessite beaucoup de travail de collecte et de traitement de données issues de ces différentes sources et ne permet pas d'obtenir plusieurs topologies représentatives de l'Internet pour des simulations.

Quant aux techniques de génération aléatoire qui permettent de produire des topologies en nombre suffisant, leur principal défaut est le manque de pertinence, la structure du réseau Internet et son évolution ne suivent aucune logique mathématiquement établie et applicable aux techniques de génération des graphes. Les logiciels comme BRITE[13] [99] ont eu beaucoup de succès, mais révèlent des limites importantes en matière d'étude des interdépendances et des phénomènes de propagation des pannes. En effet, la nécessité de préciser le nombre de liens pour chaque nouveau nœud du graphe oblige à connaître précisément la structure du graphe à générer et la distribution des degrés des nœuds. Quant aux outils comme GT-ITM[14] et Inet[15], une description complète de la structure du graphe est nécessaire car il faut préciser, non seulement le nombre de domaines feuilles par domaine de transit et le nombre de nœuds par domaine, mais aussi les probabilités d'interconnexion de ces domaines.

Les travaux sur la génération des topologies mentionnés ci-dessus proposent plusieurs techniques plus ou moins critiquables pour la qualité des topologies qu'elles produisent. La technique utilisée par le logiciel IGen [118] est celle qui permet d'obtenir des graphes les plus convenables pour étudier les interdépendances. Ce logiciel permet de générer des graphes très proches des topologies réelles des réseaux et l'approche fondée sur la distance qu'il utilise pour la génération des topologies est un critère pertinent et fréquemment utilisé pour le déploiement des réseaux réels. Il offre aussi la possibilité d'identifier les différents nœuds et arrêtes des graphes générés, ce qui est un avantage pour des graphes destinés à l'étude des interdépendances. La technique de génération de topologie que nous proposons dans ce chapitre se base aussi sur la distance pour interconnecter les nœuds du graphe généré. Mais elle fournit, en plus, une nouvelle technique pour interconnecter les points de présence et les systèmes autonomes pour pouvoir représenter tous les niveaux d'un réseau. Une autre différence avec Igen [118] est que l'interconnexion des clusters est flexible, elle ne se limite pas aux structures en arbre

[13] http://www.cs.bu.edu/faculty/matta/Research/BRITE/
[14] http://www.isi.edu/nsnam/ns/ns-topogen.html#gt-itm
[15] http://www.isi.edu/nsnam/ns/ns-topogen.html#inet

proposée par MENTOR [27] ou MENTour [27], elle offre des possibilités pour générer des topologies pour des réseaux autres que les réseaux de télécommunications.

4.4 Description de la technique de génération de topologies proposée

4.4.1 Introduction

La modélisation des propagations des pannes requiert des informations précises sur les topologies et nécessite des analyses combinées des topologies et des principes de fonctionnement des infrastructures, c'est à dire que ces études concernent non seulement les topologies et leurs interconnexions, mais aussi les fonctionnements dynamiques des réseaux représentés par ces topologies. Les techniques de modélisation et leurs résultats sont très sensibles aux caractéristiques des topologies utilisées, comme les points d'interconnexions et des politiques de routage pour les réseaux de télécommunications. Pour les différentes raisons présentées dans la section ci-dessus consacrée aux limites des outils existants en terme de génération de topologies convenables à la modélisation et à la simulation des interdépendances, nous identifions quatre raisons principales pour concevoir une nouvelle technique de génération des topologies pour la modélisation des propagations des défaillances dans les réseaux de télécommunications :

- Nécessité de disposer des topologies de niveau routeur et de niveau AS. L'évaluation des nouvelles vulnérabilités des infrastructures critiques apparues à cause de l'interconnexion des réseaux dédiés et de l'Internet nécessite des analyses précises des réseaux dédiés, de l'Internet et de leurs interconnexions. Par conséquent une topologie de niveau routeur est indispensable. Les phénomènes de propagation des pannes entre les réseaux sont dus aux communications établies par les protocoles de routage entre les différents nœuds du réseau. Ces protocoles sont différents selon qu'ils soient intra-AS ou Inter-AS, la simulation des phénomènes de propagation des pannes nécessite la distinction entre ces protocoles, donc des topologies constituées des nœuds et des liens bien identifiés.
- Besoin d'identification et de spécification des interconnexions. L'Internet est une interconnexion, avec des nœuds et des liens précis, de plusieurs petits réseaux dont chacun a des caractéristiques particulières et ses propres politiques de management qui ont un impact important sur les propagations des pannes. Un générateur de qualité doit donc offrir la possibilité d'identifier les limites entre les différents réseaux et reproduire fidèlement les topologies individuelles et les interconnexions.
- Contrainte de flexibilité. Les topologies des réseaux varient considérablement. Certaines sont centralisées alors que d'autres sont distribuées. S'il est relativement facile de générer des graphes adaptés à ces différentes topologies, l'établissement des interconnexions matérialisant les interdépendances peut se révéler complexe lorsque les différentes topologies ne sont pas générées sur des bases communes. La possibilité de faire évoluer le générateur est aussi particulièrement importante lorsqu'on envisage d'étudier des interdépendances entre différents réseaux, par exemple les réseaux électriques et les réseaux de télécommunications.
- Besoin de préserver les identités des éléments pour les analyses post-simulations. Les

composants des réseaux interconnectant différents réseaux ont des rôles différents de ceux des composants internes à un réseau. Par conséquent ces différents éléments doivent être clairement identifiés et ces informations d'identification ne doivent pas disparaître après la construction du graphe représentant l'infrastructure globale.

Sur la base de ces différentes contraintes, nous proposons une technique de génération de topologies fondée sur un algorithme simple et qui peut être facilement adaptée pour générer des topologies représentant différents réseaux tout en offrant des possibilités pour satisfaire les différentes contraintes relatives à la spécificité de chaque réseau.

Pour concevoir cette technique, nous prenons en compte les différentes contraintes techniques et économiques pour la conception, le dimensionnement et le déploiement des différents réseaux concernés. Par exemple, dans les réseaux électriques, il y a des sources de production électrique, des nœuds d'aiguillage ou de transformation et des charges. Les interconnexions, donc la topologie dépend très fortement de l'emplacement des sources de production et des charges. Dans les réseaux de télécommunications, il n'y a pas cette notion de sources et de charges, tous les nœuds feuilles sont à la fois producteurs et consommateurs d'informations, mais à des degrés différents et les interconnexions dépendent des nœuds stratégiques comme ceux des grands serveurs de distributions de contenus et ceux des réseaux fournisseurs d'accès Internet constitués par des nœuds gros consommateurs de flux. Nous définissons donc un algorithme générique qu'il est possible d'adapter pour générer des topologies convenables pour étudier les interdépendances de différents réseaux. Pour montrer la flexibilité de l'algorithme proposé, nous générons aussi des topologies des réseaux électriques et procédons à leur validation par comparaison avec des topologies standards et largement utilisées par les chercheurs.

Dans la section suivante, nous décrivons notre algorithme pour générer séparément des topologies de différentes infrastructures, notamment des réseaux de télécommunications et des réseaux électriques avec des adaptions minimales.

Les principes de la technique proposée sont, pour certains, inverses de ceux des techniques actuellement proposées (qui consistent à générer un graphe avant de placer les nœuds particuliers représentant les serveurs, les routeurs BGP pour les réseaux de télécommunications et les générateurs, les charges pour les réseaux électriques). Ces nœuds particuliers jouent un rôle important dans l'interconnexion de ces réseaux, il est donc plus logique de placer ces nœuds avant de définir les interconnexions. Sur la base de cette observation et des contraintes techniques et économiques de déploiement des réseaux comme la distance et la situation géographique des principaux points de présence, nous déduisons les algorithmes d'interconnexion des réseaux télécommunications qui peuvent être facilement adaptés pour la génération des topologies représentant d'autres infrastructures comme les réseaux électriques. Cette technique consiste à définir un simple modèle représentant un pays ou une localité avec un certain nombre de sites à interconnecter définis par leurs coordonnées et leurs poids.

La première étape consiste donc à générer une zone et à y positionner des sites avec des coordonnées et des poids. Les valeurs des coordonnées et des poids peuvent être aléatoires ou basées sur des données réelles. A l'issue de cette étape, nous obtenons un nombre N de sites avec des coordonnées géographiques (xi, y_i) et des poids (p_i) dans un espace E de dimension 2. Ces sites peuvent représenter des villes et les poids les populations de ces villes, les activités, les opportunités de marché ou toute autre combinaison de critères déterminants pour le déploiement et l'extension des réseaux. La figure 4.1 montre un exemple de résultat obtenu à

l'issu de la première étape avec des coordonnées et des poids lus à partir d'un fichier.

L'algorithme est implémenté sous Scilab[16] qui est un logiciel libre, initialement développé par des chercheurs de l'INRIA (Institut National de Recherche en Informatique et en Automatique) et de l'ENPC (École Nationale des Ponts et Chaussées). Bien qu'il ne soit pas le plus rapide des logiciels de sa catégorie, Scilab a été choisi parce qu'il est libre, permet d'ajouter facilement des modules et offre des nombreuses possibilités pour manipuler les graphes.

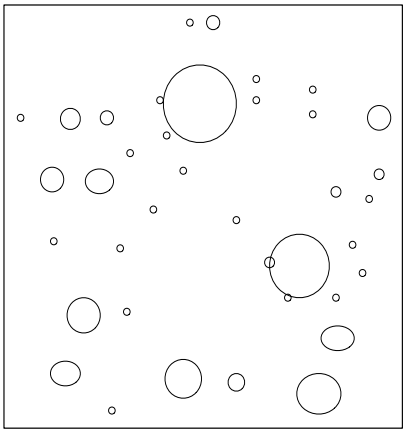


FIG. 4.1 – *Exemple d'une zone géographique avec des sites à connecter - Les diamètres représentent les poids des nœuds)*

4.4.2 Algorithme de génération des topologies des réseaux de télécommunications

La conception, le dimensionnement et le déploiement des réseaux obéissent à des contraintes économiques et techniques liées au potentiel de la clientèle, aux activités humaines, aux technologies et équipements utilisés. Les topologies des réseaux ne sont donc pas le fruit du hasard et les interconnexions qui en résultent sont plus denses dans et entre les zones où les activités sont intenses (généralement les zones très peuplées). Le déploiement de ces réseaux débutent donc de manière à couvrir les endroits stratégiques et au fur et à mesure de leur évolution, de nouveaux sites moins prioritaires sont connectés. Il y a, parfois des contraintes qui font que les opérateurs sont obligés de couvrir tout un territoire, mais le dimensionnement et le déploiement se déroulent toujours de la même manière.

L'algorithme proposé utilise donc en entrée des sites représentant différents points de présence avec des coordonnées et des poids comme présentés dans la figure 4.1. Tout d'abord, il sélectionne le site ayant le poids le plus élevé qui peut correspondre au site de potentiel le plus élevé, puis recherche les sites que nous appelons « sites secondaires » car ce sont les sites de poids inférieurs à celui du site principal, mais relativement élevés et qui se trouvent à des positions précises. En effet, selon l'étendue de la zone concernée et la densité des réseaux, on

[16] http://www.scilab.org

peut avoir une topologie avec un site principal interconnecté avec des liaisons de grande capacité avec tous les sites secondaires de la zone à couvrir (le réseau Free en France par exemple) ou une topologie avec plusieurs sites principaux situés dans différents endroits de la zone à couvrir et interconnectés entre eux par des liaisons de grande capacité (le réseau ARPANet aux États-Unis par exemple). La sélection de sites secondaires peut se faire de différentes manières. Il est possible de fixer le nombre de sites secondaires ou de choisir un seuil minimum et considérer tous les sites avec des poids supérieurs à ce seuil et situés dans les zones définies comme secondaires. Le critère sur la position de ces sites secondaires est important car dans la pratique il n'y aucune particularité pour interconnecter deux sites secondaires ou un site secondaire et le site principal lorsque ceux-ci sont situés à proximité l'un de l'autre. Pour définir ce critère de position, nous avons choisi de subdiviser la zone en 9 (3*X*3) sous-zones et de choisir un site pour chaque zone lorsque le poids de celui-ci est supérieur à un seuil que nous avons fixé sous-forme de pourcentage du plus grand poids de la zone (figure 4.2, les diamètres des cercles représentent les poids). Les 9 sous-zones constituent un nombre minimum nous permettant de pouvoir, si nécessaire, définir un site pour chaque zone représentative (centre, nord, nord-est, est, sud-est, sud, sud-ouest, ouest et nord-ouest) de l'espace *E* considéré.

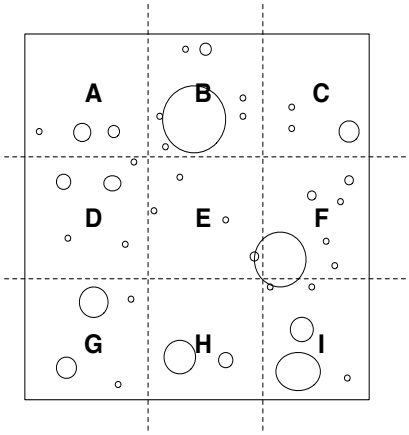


FIG. 4.2 – *Subdivision de la zone en 9 sous-zones*

Ainsi il est possible qu'une sous-zone ne contienne aucun site secondaire. Ceci permet, pour un même espace *E*, de générer plusieurs topologies avec différents nombres de sites secondaires (points de présence) comme cela se fait en réalité. En effet, dans une même zone (un même pays par exemple) il est possible d'avoir plusieurs réseaux de différentes densités d'interconnexion, les anciens réseaux interconnectent plus de sites que des réseaux récemment déployés.

Après la sélection de ces sites déterminants pour notre algorithme, celui-ci passe à la phase de la construction des liaisons de communications qui débute par l'interconnexion des sites secondaires voisins (c'est à dire ceux qui sont dans des sous-zones voisines) entre eux dans le sens des aiguilles d'une montre. Ensuite pour les réseaux contenant un site principal interconnecté avec les sites secondaires (comme celui de Free), l'algorithme interconnecte le site principal à tous les sites secondaires. Pour les réseaux constitués de plusieurs sites principaux

distribués, l'algorithme n'effectue pas cette dernière interconnexion car les sites principaux distribués sont, en réalité les sites secondaires déjà interconnectés entre eux. Dans ce cas de figure, le site principal est connecté comme un site secondaire. Pour tous les cas, les liaisons d'interconnexion de deux sites passent par tous les sites intermédiaires entre ces deux sites. Ces sites intermédiaires sont choisis en fonction de la distance par rapport à la ligne droite entre les sites des extrémités de la liaison. Cette distance est calculée en fonction de la distance entre les nœuds d'extrémités, c'est à dire la distance entre les sites secondaires à interconnecter. Le figure 4.3 présente le résultat obtenu après l'interconnexion des sites principal et secondaires. A noter que pour les réseaux avec plusieurs sites principaux distribués, il n'y a pas de liaisons entre chaque site secondaire et le site principal. Aussi pour l'exemple présenté ici, il n'y a ni site principal, ni secondaire dans la sous-zone centrale, mais le procédé fonctionnerait de la même manière si un de ces sites se trouvait dans cette sous-zone.

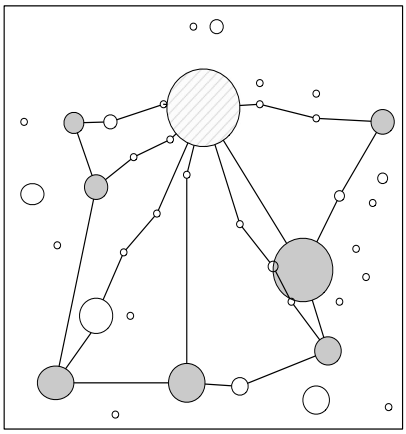


FIG. 4.3 – *Interconnexion des sites principal et secondaires*

Une fois cette étape terminée, les sites restants sont connectés au réseau par des liens directes établis de manière à réduire au minimum les longueurs des liens. Cette minimisation de la longueur des liens est réalisée de façon gloutonne en connectant en premier le site non connecté le plus proche du graphe existant et en terminant par le site le plus éloigné de ce graphe. On obtient un graphe comme celui présenté sur la figure 4.4.

Le dernière étape consiste à optimiser le réseau en construisant une topologie robuste avec un nombre de liens minimum. La résistance aux pannes nécessite l'élimination des longues branches où la coupure d'un seul lien peut déconnecter plusieurs sites. La réduction des coûts se fait en réduisant les longueurs des liens directes et le nombre de liens. Pour satisfaire ces deux contraintes, les branches trop longues (branches connectant plus d'un site) sont connectées, soit à une autre branche longue, soit à la partie du réseau fortement connectée, c'est à dire à l'un des nœuds du réseau connectés lors de la première étape de l'algorithme. La figure 4.5 montre le résultat obtenu à l'issue de cette dernière étape. On obtient ainsi un graphe maillé, à l'exception de quelques sites connectés par un seul lien, mais dont la coupure ne déconnecte qu'un seul site. Sur les figure 4.6(a) et 4.6(b), nous présentons les graphes représentant le réseau réel et celui généré par notre algorithme.

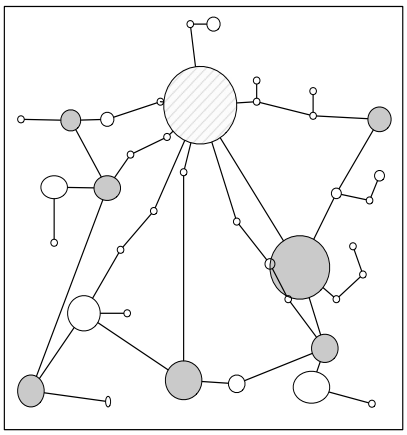


FIG. 4.4 – *Interconnexion des sites restants*

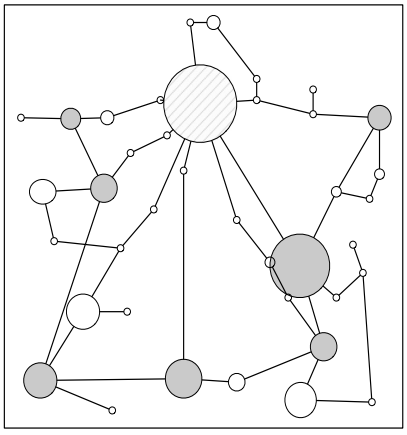
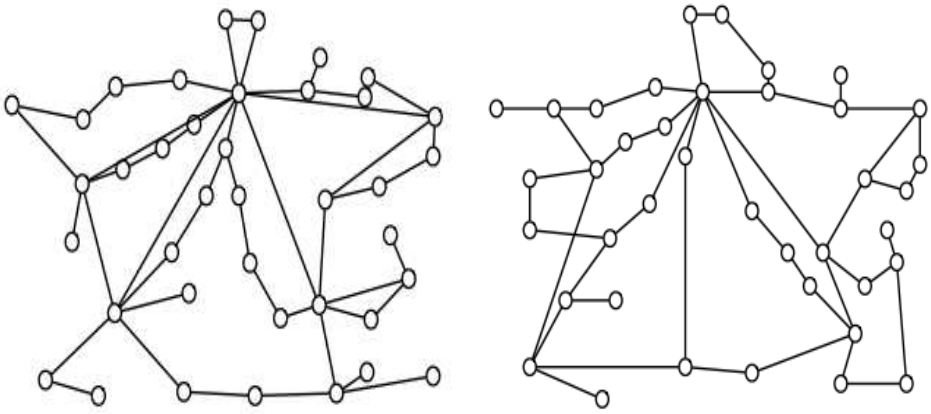


FIG. 4.5 – *Interconnexion des branches longues*

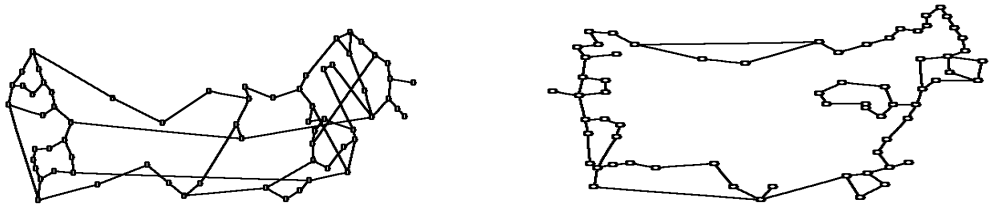


(a) Graphe du réseau Free réel (b) Graphe du réseau Free généré

FIG. 4.6 – *Comparaison des graphes*

Pour les réseaux très étendus dont les sites principaux sont distribués, l'algorithme fonctionne selon le principe décrit ci-dessus et fournit un résultat comme celui présenté sur les figures 4.7(a) et 4.7(b) représentant le réseau ARPANet.

Les graphes générés représentent des réseaux à l'échelle nationale, ce qui nous permet de simuler les interconnexions entre plusieurs réseaux de même pays, mais aussi des interconnexions entre des réseaux des pays différents offrant des informations précises sur les nœuds par lesquels ces interconnexions sont établies.



(a) Graphe du réseau Arpanet (b) Graphe du réseau Arpanet généré

FIG. 4.7 – *Comparaison des graphes*

4.4.3 Interconnexion des Systèmes Autonomes

Les graphes obtenus à l'issue des étapes précédentes représentent des réseaux de taille limitée qui permettent de simuler un seul AS. La deuxième et dernière phase consiste donc à interconnecter plusieurs graphes pour former un réseau constitué de plusieurs AS. L'interconnexion des AS se fait entre les nœuds des différents AS situés à proximité les uns des autres. Ce choix permet de simuler, non seulement l'interconnexion entre les AS de niveau 1, mais aussi entre les AS et leurs clients. En effet, dans la réalité les AS établissent leurs intercon-

nexions au niveau des point d'échange Internet (*Global Internet eXchange - GIX*) où ils ont très souvent des nœuds situés dans des même locaux ou dans des locaux très proches. Pour obtenir des résultats proches des topologies réelles des réseaux où un AS peut être sur plusieurs pays, les interconnexions se font uniquement entre les sites principaux et secondaires décrits plus haut dans ce document. A titre d'exemple, pour un graphe représentant un AS dont le réseau s'étend des États-Unis en France, notre algorithme aura forcément un site principal ou secondaire dans l'un ou l'autre de ces pays et son interconnexion avec d'autres AS (clients ou pairs) présents dans l'un de ses pays se fera à travers un de ses nœuds de ce pays. A partir d'un nombre d'AS connu ou choisi aléatoirement, l'algorithme effectuent une répartition des AS en différents niveaux et procède aux interconnexions entre les AS selon un critère défini au départ. La répartition permet de différencier les interconnexions entre les AS pairs et celles entre les AS clients et fournisseurs. Le critère évoqué ci-dessus permet d'indiquer si les interconnexions entre les AS se font avec un lien unique ou avec deux liens ayant un nœud en commun ou encore avec deux liens distincts et qui n'ont aucun nœud en commun (figure 4.8).

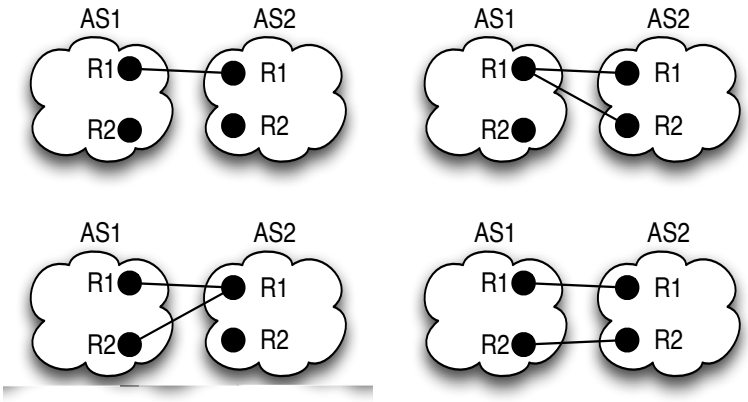


FIG. 4.8 – *Différentes interconnexions des AS*

La répartition des AS peut se faire de manière aléatoire (dans ce cas il est possible, suivant le nombre total d'AS d'avoir plusieurs niveaux) ou non (on précise le nombre de niveaux et le nombre d'AS de chaque niveau) ou encore fixer le nombre d'AS de niveau 1 sous forme de pourcentage du nombre total des AS. Pour les AS de niveau 1, l'algorithme établit un lien entre chacun des AS, pour les autres niveaux, l'algorithme détermine aléatoirement pour chaque AS, le nombre de ses pairs et le nombre de ses fournisseurs. Ce choix aléatoire n'est pas obligatoire, tous les paramètres choisis aléatoirement peuvent être fixés par l'utilisateur et fournis à l'algorithme comme données d'entrée. La liste des AS fournisseurs et celle des AS clients sont, quant à elles choisies par un système de préférence lié aux degrés de connectivité des AS fournisseurs potentiels. En effet, les auteurs de [36] ont démontré, avec des données du réseau Internet que les nouveaux AS se connectent, le plus souvent aux AS ayant les degrés de connectivité les plus élevés. La figure 4.9 montre un exemple de ce qu'il est possible d'obtenir, pour plus de lisibilité, nous avons choisi de représenter un seul lien entre chacun des AS.

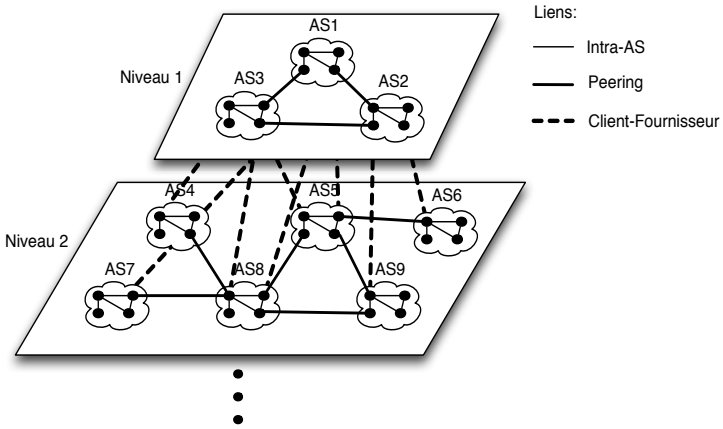


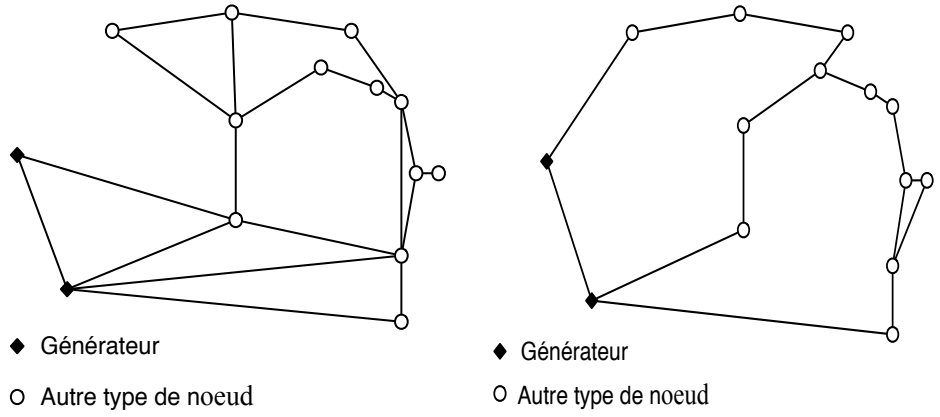
FIG. 4.9 – *Exemple d'interconnexion de systèmes autonomes*

4.4.4 Algorithme de génération des topologies des réseaux électriques

Pour démontrer la flexibilité de notre algorithme, nous l'utilisons pour générer quelques topologies des réseaux électriques et évaluons les résultats obtenus en comparant les topologies générées avec les topologies des réseaux électriques disponibles sur Internet.

Pour les graphes électriques, l'algorithme se base sur les éléments déterminants de la topologie, à savoir les sources de production et les charges (points de consommation). Mais, il fonctionne selon un principe de base identique à celui utilisé pour la génération des topologies des réseaux de communications. Les nœuds du graphe sont, tout d'abord subdivisés en deux catégories : les sources et les charges. Puis, l'algorithme procède à l'interconnexion des sources de productions entre elles. Cette interconnexion initiale permet d'avoir un graphe équilibré en terme de distribution des charges sur les différentes sources de production. L'ensemble des sources étant directement interconnectées entre elles, lorsqu'une source est défaillante, ses charges sont distribuées aux sources de production restantes qui, par conséquent se soutiennent comme dans les réseaux réels. Ensuite les autres sites représentant les postes de transformation et les charges sont connectés. Lors de la dernière étape, l'algorithme recherche les branches trop longues et les interconnecte si elles existent selon la même procedure que celle décrite dans l'algorithme de génération des topologies des réseaux de télécommunications. Cette dernière interconnexion permet de fournir un graphe plus maillé, donc plus robuste. Toutes ces interconnexions sont fondées sur la distance euclidienne et chacun des nœuds est interconnecté de manière à minimiser la longueur des liaisons directes. A l'issu de ces étapes, on obtient des graphes qui, comme ceux des réseaux de télécommunications respectent la règle de $N-1$. Les poids des nœuds ne sont pas utilisés dans le processus d'interconnecion pour la génération de topologie pour les réseaux électriques. Toutefois ces poids peuvent être utilisés, par exemple, dans une étude pour montrer que certains sites produisent ou consomment plus de l'énergie électrique ou encore pour évaluer l'impact d'une panne électrique en attribuant à ces nœuds un poids qui indiquent le nombre de clients représentés par chacun de ces nœuds. Un exemple de résultat est présenté sur les figures 4.10(a) et 4.10(b) qui représentent respectivement le graphe

IEEE[17] de 14 nœuds disponible sur Internet et le graphe correspondant généré par la technique proposée. On peut voir avec ces deux figures que l'algorithme proposé permet d'obtenir un graphe avec une robustesse identique à celle du graphe original, mais avec un nombre de liens inférieur à celui du graphe original.



(a) Graphe du réseau IEEE 14 nœuds original (b) Graphe du réseau IEEE 14 nœuds généré

FIG. 4.10 – *Comparaison des graphes*

4.4.5 Exemples de graphes générés

Comme évoqué dans la section précédente, la réalisation logicielle est effectuée à l'aide de Scilab[18]. Sur cet environnement, la durée d'exécution croît rapidement avec la taille du graphe à générer. En effet, l'augmentation du nombre de nœuds provoque, en plus de la charge liée au traitement des nœuds une charge supplémentaire non négligeable due à l'augmentation du nombre de liens à traiter. A titre d'exemple, la génération d'un graphe de 700 nœuds dure 40 heures (temps machine), alors que 5 heures suffisent pour générer un graphe de 505 nœuds. La dernière étape de l'algorithme, c'est à dire la recherche de l'existence ou non de longues branches est celle qui prend plus de temps. Mais cette variation de durée de génération en fonction du nombre de nœuds n'est valable que pour la technique de base de génération de topologie représentant un AS, pour l'interconnexion de plusieurs AS, l'algorithme est beaucoup plus rapide. Par exemple il ne nécessite que moins de 8 heures pour générer une topologie représentant 80 AS de 45 nœuds chacun, soit 3600 nœuds.

La plupart des modèles de la topologie Internet visent à fournir des graphes avec des paramètres les plus proches possible à ceux mesurés sur Internet, notamment la distribution des degrés, la longueur moyenne des chemins entre les nœuds, le cœfficient de clustering moyen, le diamètre et l'indice Alpha (α). L'indice α d'un graphe est le rapport du nombre de circuits fondamentaux que possède ce graphe sur le nombre maximum de circuits possibles : $\alpha = \frac{e-v+p}{2v-5}$

[17] http://www.ee.washington.edu/research/pstca/
[18] http://www.scilab.org

où e est le nombre d'arrêtes, v le nombre de nœuds et p le nombre de sous-graphes. Un sous-graphe est une composante connexe d'une graphe. Un graphe avec 1 seul sous-graphe est un graphe connexe alors qu'un graphe avec 2 sous-graphes est un graphe constitué de 2 composantes connexes qui ne sont pas connectés entre eux.

Pour valider les graphes obtenus avec l'algorithme proposé, nous évaluons, non seulement certaines métriques généralement utilisées pour caractériser les graphes (nombre de nœuds, nombre de liens, distribution des degrés des nœuds, le diamètre), mais aussi des métriques spécifiques convenables à l'estimation de la robustesse topologique des graphes étudiés. L'indice α, par exemple, nous permettra d'évaluer la connectivité des graphes car il détermine le nombre de circuits fondamentaux du graphe par rapport au nombre de circuits possibles. Nous utilisons la valeur de cette métrique et le partitionnement des graphes pour évaluer la connectivité, donc la robustesse des graphes. Nous comparons, sur la base de ces métriques, les graphes générés par notre algorithme à des graphes réels, des graphes standards (pour les réseaux électriques) et à des graphes issus d'autres travaux de recherche.

4.4.5.1 Comparaison des graphes par distribution des degrés

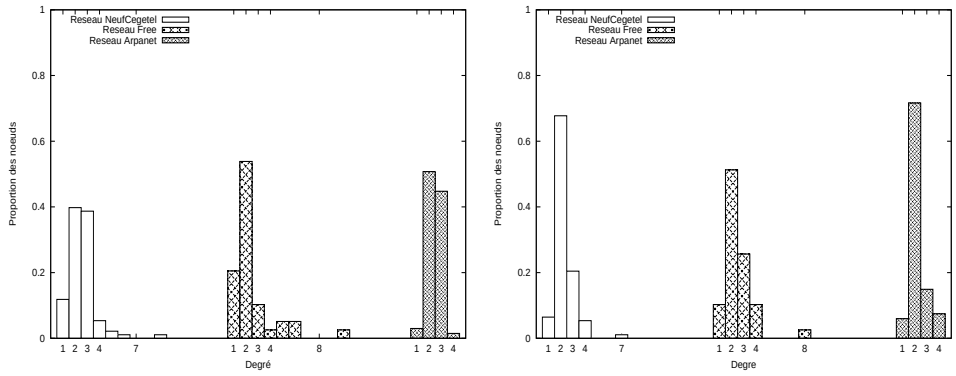
Graphes réseaux de télécommunications

Comme réseaux de référence utilisés, nous avons choisi 3 topologies très différentes, non seulement de par leurs tailles, mais aussi de par leurs structures. Il s'agit des réseaux Free, ARPANet dont les graphes sont présentés respectivement sur les figures 4.6(a) et 4.7(a) et le réseau Neufcegetel tels qu'il sont présentés sur les sites Web des opérateurs concernés. Le graphe représentant le réseau ARPANet utilisé est relativement ancien car celui qui est actuellement disponible sur Internet date des années 80. Malgré cet inconvénient, cette topologie a été utilisée car elle reste accessible sur Internet et parce que l'objectif est de valider les résultats en comparant les graphes générés par notre algorithme à des graphes représentant des réseaux réels. Le but n'est pas de générer un graphe proche du réseau actuel de celui de ARPANet, mais un graphe ayant une structure proche de celle de ce réseau. Par conséquent, pour cette comparaison, c'est la structure du graphe qui constitue un facteur déterminant.

Pour évaluer les résultats obtenus avec la technique proposée, nous avons, tout d'abord, procédé à la comparaison des distributions des degrés des nœuds des graphes réels des réseaux évoqués ci-dessus et les graphes générés par notre algorithme. Pour effectuer, cette comparaison, nous avons, d'une part reproduit les graphes des réseaux disponibles sur les sites Internet des opérateurs des réseaux concernés au format Scilab et, d'autre part créé des fichiers des données d'entrée pour l'algorithme. Pour rappel, ces fichiers contiennent les identifiants, les coordonnées et les poids des sites à interconnecter. Ces fichiers sont remplies manuellement, donc il est possible qu'il y ait des différences entre les coordonnées réelles des sites et celles contenues dans ces fichiers. Le format de ces fichiers est simple, ils sont composés d'un nombre de lignes correspondant au nombre de sites à interconnecter et 4 ou 5 colonnes selon que l'on veut ou non ajouter la superficie du site. Sur chaque ligne, il y a l'identifiant du site, l'abscisse, l'ordonnée, le poids et la superficie (optionnelle). La superficie permet de considérer le site, non pas comme un simple nœud, mais comme un réseau à part entière où on peut déployer un nombre de NRA (Nœud de Raccordement d'Abonnés), calculé en fonction de cette superficie

et de manière à respecter la distance maximale entre le NRA et les abonnés. Pour rappel, un NRA est un local technique d'un opérateur de télécommunications souvent proche du central téléphonique qui dessert les lignes d'abonnés d'un périmètre géographique défini. Les résultats présentés dans ce document concernent uniquement les réseaux de niveau national où ces sites sont présentés comme des simples nœuds.

Les résultats obtenus sont présentés sur les figures 4.11(a) et 4.11(b), l'axe des abscisses présente les degrés des différents nœuds et l'axe des ordonnées les proportions des nœuds correspondantes. Les différents types de barres correspondent aux différents réseaux répresentant, de gauche à droite, le réseau Neufcegtel, Free et ARPANet. Ces résultats montrent que même s'il y a une différence des proportions des nœuds du graphe réel et du graphe généré correspondant, les propriétés de base des distributions des degrés sont conservées. Les nœuds ayant 2 comme degré constituent la proportion la plus importante et, à l'exception des nœuds feuilles, la distribution des degrés suit une distribution différente d'une loi de puissance. Ce qui constitue un résultat intéressant car il démontre que les graphes représentant les topologies des réseaux intra-AS ne peuvent pas être générés avec les logiciels de génération des graphes sans-échelle.



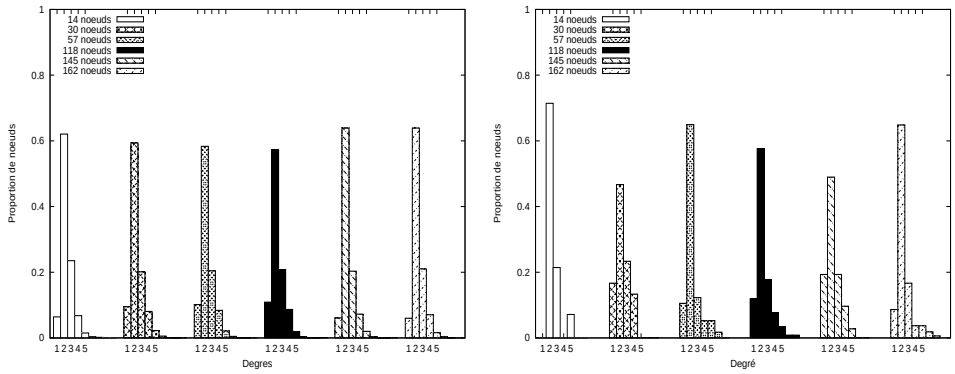
(a) Graphes télécom (b) Graphes télécom générés

FIG. 4.11 – *Distribution des degrés des graphes*

Graphes des réseaux électriques

Comme pour les réseaux de télécommunications, la comparaison des distributions des degrés des graphes électriques est réalisée sur la base des graphes représentant des réseaux réels ou standards et des graphes générés par l'algorithme. Cependant, pour les réseaux électriques, les données des graphes sont disponibles sur Internet, notamment sur le site Web du département de génie électrique de l'université de Washington, les fichiers utilisés correspondent exactement à ces données car ils n'ont pas été remplis à la main. Le but étant uniquement de démontrer qu'il est possible d'utiliser notre algorithme pour générer des graphes électriques, seules les informations d'interconnexion et celles relatives au nombre de générateurs ont été utilisées. Les figures 4.12(a) et 4.12(b) présentent les résultats obtenus concernant les graphes

standards de l'IEEE[19] et les graphes correspondants générés par notre algorithme. De gauche à droite sur la figure 4.12(a), nous présentons la distribution des degrés des graphes IEEE de 14, 30, 57, 118, 145 et 162 nœuds. La figure 4.12(b) présente les distributions des degrés des graphes générés avec des nombres de nœuds correspondant à ceux des graphes IEEE.



(a) Graphes électriques du standard IEEE (b) Graphes électriques générés

FIG. 4.12 – *Distribution des degrés des graphes*

On peut remarquer que, la différence des proportions des distributions des degrés entre les graphes générés et les graphes réels des graphes électriques est moins importante que celle des graphes télécom. Cette différence est principalement due au fait que les données utilisés pour les graphes des réseaux électriques soient plus proches des données réelles que pour celles utilisées pour générer les graphes des réseaux de télécommunications. En effet les données disponibles sur Internet sont directement utilisables avec Scilab pour générer les graphes pour les réseaux électriques alors que, pour les réseaux de télécommunications, il faut construire manuellement le graphe au format Scilab et constituer manuellement les fichiers de données utilisés par notre algorithme. Comme pour les graphes des réseaux de télécommunications, les résultats montrent que les graphes des réseaux électriques générés conservent les propriétés de base relatives aux distributions des degrés.

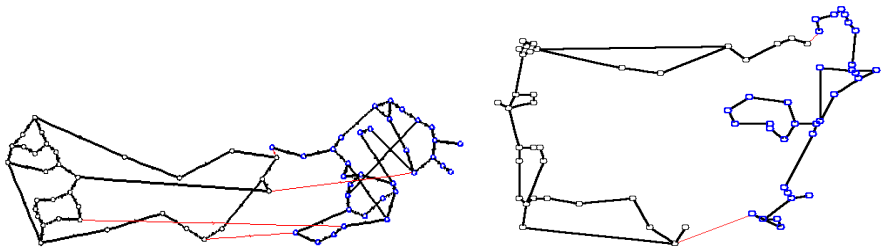
4.4.5.2 Comparaison des graphes par partitionnement

La réduction des propagations des défaillances passe nécessairement par la construction des topologies robustes et plus résistantes aux pannes. Pour valider les résultats de notre algorithme, il est donc indispensable de procéder à l'évaluation des graphes générés sous l'angle de la résistance aux pannes. Nous effectuons donc une comparaison des graphes réels et des graphes générés en utilisant la technique de partitionnement de graphe. Le partitionnement d'un graphe permet de déterminer ses points de faiblesse et d'évaluer les lignes de fracture possible d'un réseau lorsque ce graphe représente un réseau réel. La technique de partitionnement de graphe permet aussi, grâce à l'identification des points vulnérables de planifier la construction de nouvelles lignes ou de prévoir des mesures permettant aux composantes pouvant se former

[19] http ://www.ee.washington.edu/research/pstca/

après une défaillance de fonctionner de manière autonome. En particulier, pour les réseaux électriques, l'identification de ces lignes de coupure peut permettre de prévoir, en cas de fort déséquilibre de charge entre les différentes zones du réseau, les lignes où peuvent se produire une surcharge.

Pour réaliser ce partitionnement, nous avons choisi d'utiliser la méthode de Girvan et Newman décrite dans l'article [67]. Cette méthode est reconnue pour sa simplicité et la qualité des résultats qu'elle fournit. Sa complexité ($O(n^3)$) est son principal défaut par rapport à ses concurrents, mais reste polynomiale. Notre objectif étant de partitionner quelques graphes simples, nous avons choisi cette méthode pour la qualité de ses résultats et la simplicité de son implémentation sur Scilab. L'algorithme de Girvan et Newman est basée sur une méthode de division procédant par suppression itérative des liaisons ayant la plus forte valeur d'intermédiarité (*betweenness*) jusqu'à ce que le graphe se découpe en différents sous graphes. Donc le processus de suppression touche les liaisons inter-communautés. L'implémentation de cet algorithme sur Scilab consiste à calculer le cœfficient de centralité de chacune des arrêtes du graphe, de supprimer l'arrête ayant le cœfficient le plus élevé, de recalculer les cœfficients des arrêtes restantes et de continuer le processus juqu'à ce que le graphe ne soit plus connexe.



(a) Réseau Arpanet (b) Réseau Arpanet généré

FIG. 4.13 – *Résultats du partitionnement des graphes*

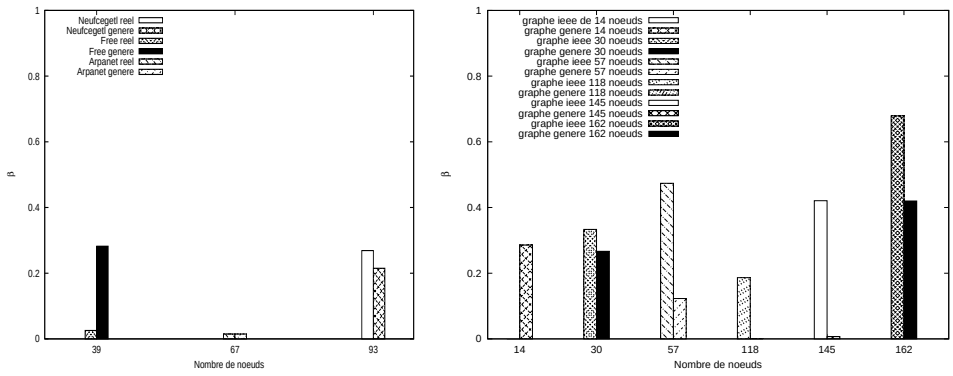
Les figures 4.13(a) et 4.13(b) montrent le résultat du partitionnement des graphes réels et générés représentant le réseau ARPANet. L'objectif étant de comparer simplement les graphes, nous nous limitons à un partitionnement d'un graphe en 2 composantes. Dans chacune de ces figures, le partitionnement divise le graphe en 2 composantes, quasiment de même taille (34 pour la première composante et 33 pour la deuxième). Pour faciliter la compréhension, nous présentons les résultats de façon à ce que les nœuds de chacune des 2 composantes aient la même épaisseur de bordure et la même couleur. Les liens faibles sont colorés en rouge et ont une épaisseur plus petite que celle des autres liens. Aussi, on peut remarquer qu'à l'exception des liens de redondance particuliers du graphe réel qui interconnectent directement des nœuds appartenant aux deux composantes, les 2 graphes ont, quasiment les mêmes liens faibles.

Pour comparer les différents graphes par partitionnement, nous avons défini une métrique qui permet de mesurer aussi la résistance aux pannes d'un graphe en se basant sur les tailles des composantes connexes formées à l'issu du partitionnement du graphe. Un graphe robuste est celui dont le partitionnement fournit une composante connexe avec un nombre maximum de nœuds. Lorsqu'un partitionnement d'un graphe fournit 2 composantes connexes, la métrique β

est égale à la valeur absolue de la différence du nombre de nœuds des 2 composantes divisée par le nombre de nœuds total du graphe.

$$\beta = \frac{|N_{c1} - N_{c2}|}{N_{tot}}$$

où N_{c1} est le nombre de nœuds de la première composante, N_{c2} est le nombre de nœuds de la deuxième composante et N_{tot} est le nombre de nœuds total du graphe. Ainsi, une valeur faible indique un graphe moins robuste. Par exemple, une valeur de β de 0% indique un graphe dont le partitionnement fournit deux composantes connexes de même taille, alors qu'une valeur de β égale à 100% indique un graphe connexe. Cette métrique nous permet, à la fois de situer les parties les plus vélnérables du réseau et de caractériser statistiquement la réaction du graphe face à des pannes. Ainsi, pour les réseaux électriques, cette métrique permet d'identifier les parties qui ont plus besoin d'être renforcées et de savoir sur quelle partie du réseau l'attention doit être portée en cas de risque de pannes. Pour les réseaux de type Internet où aucun abonné ne doit être isolé du reste du réseau, cette métrique permet, par exemple d'évaluer l'impact d'une panne en terme de nombre d'abonés isolés. Les figures 4.14(a) et 4.14(b) présentent la valeur de β pour quelques graphes télécoms et électriques générés par notre technique. On remarque que l'écart des valeurs de β entre le graphe généré et le graphe réel est plus important pour certains graphes que pour d'autres. Cet écart est dû essentiellement à la sensibilité de l'algorithme par rapport à la position des sites à interconnecter. Comme les coordonnées des sites sont saisies à la main, elles ne reflètenet pas exactement les coordonnées réelles. Puisque l'interconexion est fondée sur la distance euclidienne, les coordonnées font qu'un site sera connecté à un de ses voisins plutôt qu'à un autre. Une petite variation de ces coordonnées fait donc varier les liens les plus vulnérables comme on peut le voir sur la figure 4.13



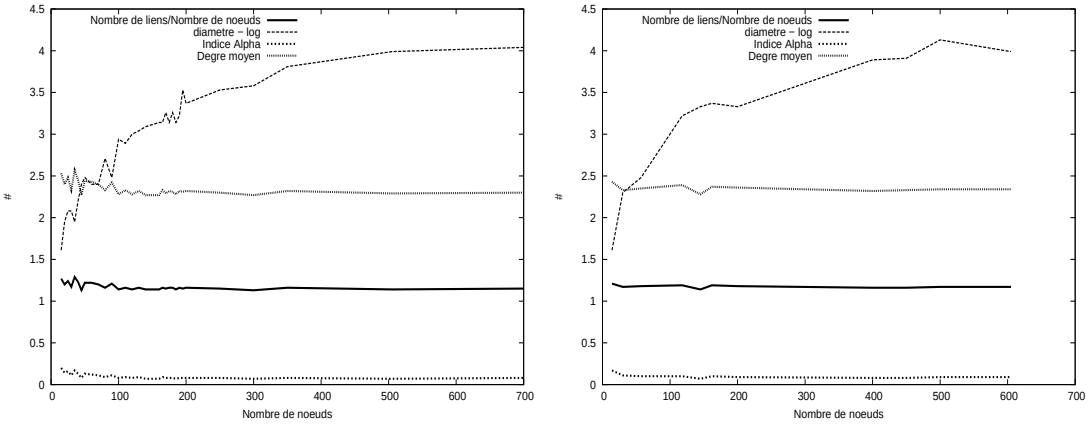
(a) Graphes des réseaux télécom (b) Graphes des réseaux électriques

FIG. 4.14 – *Résultats du partitionnement des graphes*

4.4.5.3 Évaluation d'autres paramètres des graphes

Nous avons démontré avec les résultats précédents que les graphes générés conservent les propriétés de base pour les distributions des degrés. Puisque ces résultats concernent des

graphes particuliers et ils portent uniquement sur la distribution des degrés, il est intéressant d'avoir une idée sur les résultats qu'on obtiendrait si on utilisait l'algorithme pour générer d'autres graphes et surtout si on évaluait des paramètres autre que la distribution des degrés. Pour répondre à ce besoin, nous présentons sur les figures 4.15(a) et 4.15(b) l'évolution du diamètre, du degré moyen, de l'indice Alpha (α), du nombre de liens de quelques graphes générés par l'algorithme et dont le nombre de nœuds varie entre 20 et 700.



(a) Graphes des réseaux télécom

(b) Graphes des réseaux électriques

FIG. 4.15 – *Evolution de quelques paramètres des graphes*

Comme on peut le voir avec les résultats présentés sur les figures 4.15(a) et 4.15(b), à l'exception du diamètre les propriétés de base des graphes ne varient quasiment pas avec le nombre de nœud des graphes générés. Pour plus de lisibilité, le nombre d'arêtes des graphes est divisé par le nombre de nœuds et le diamètre est représenté par la valeur de son logarithme. La variation du diamètre avec le nombre de nœuds est un comportement logique qui valide nos graphes, car cette variation montre que tous les paramètres des graphes ne restent pas figées autour de leurs valeurs initiales. La faible variation des autres paramètres, à savoir le rapport du nombre de liens sur le nombre de noeuds, la connectivité (ou l'indice Alpha) avec le nombre de nœuds montre que tous les graphes générés par l'algorithme conservent les mêmes propriétés de base, donc des résultats valides pour quelques graphes sont aussi valides pour les autres. Donc, On peut affirmer que, pour ce qui concerne les propriétés de base, les résultats sur la distribution des degrés présentés dans les sections précédentes sont valables pour l'ensemble des graphes générés par l'algorithme.

4.4.5.4 Graphes inter-AS de niveau AS et de niveau routeur

Les résultats présentés dans les sections précédentes concernent uniquement les graphes intra-AS, la présente section est consacrée à la présentation des résultats concernant les graphes inter-AS de niveau AS et de niveau routeur. Les graphes inter-AS de niveau AS sont les graphes où un AS est considéré comme un simple nœud et les liaisons représentées se limitent uniquement aux liaisons entre les AS, par conséquent les graphes intra-AS ne sont pas représentés.

Pour les graphes inter-AS de niveau routeur l'ensemble des routeurs BGP et des liaisons entre les routeurs BGP sont représentés. Ces liaisons peuvent être intra-domaines (liaisons *internal BGP ou iBGP*) ou inter-domaines (liaisons *external BGP ou eBGP*). La technique de génération procède à la distribution des AS en différents niveaux (AS de niveau 1 ou top level, AS de niveau 2, ...). Dans l'évaluation de la technique proposée, nous procédons à la génération des graphes avec 2 types de distribution des AS en différents niveaux. Une première distribution aléatoire où le nombre des AS de chaque niveau est choisi aléatoirement. Une deuxième distribution où le nombre d'AS de niveau 1 représente 50% du nombre d'AS total. En effet, les auteurs de [56] ont montré, à partir des données collectées par différents moniteurs que le réseau Internet est composé de 40 à 50% des AS qui appartiennent à des arbres dont 80% ont une profondeur de 1 (avec 3 comme profondeur maximale), les AS restant forment des graphes fortement connectés. Ce qui montre que 50 à 60% des AS du réseau Internet sont des AS de niveau 1. Les premiers résultats sur les graphes inter-AS de niveau AS sont présentés sur la figure 4.16.

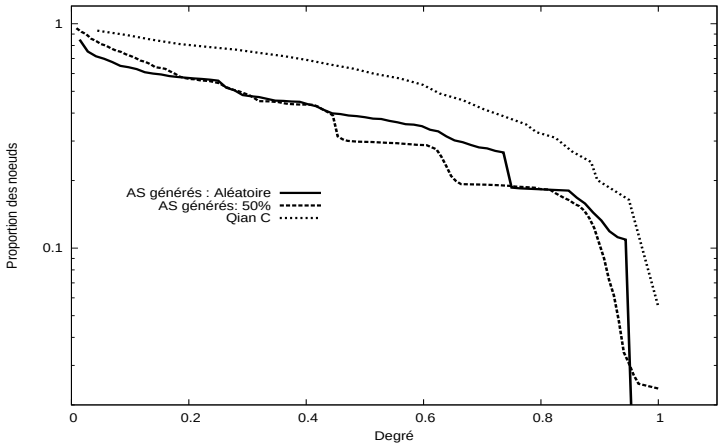
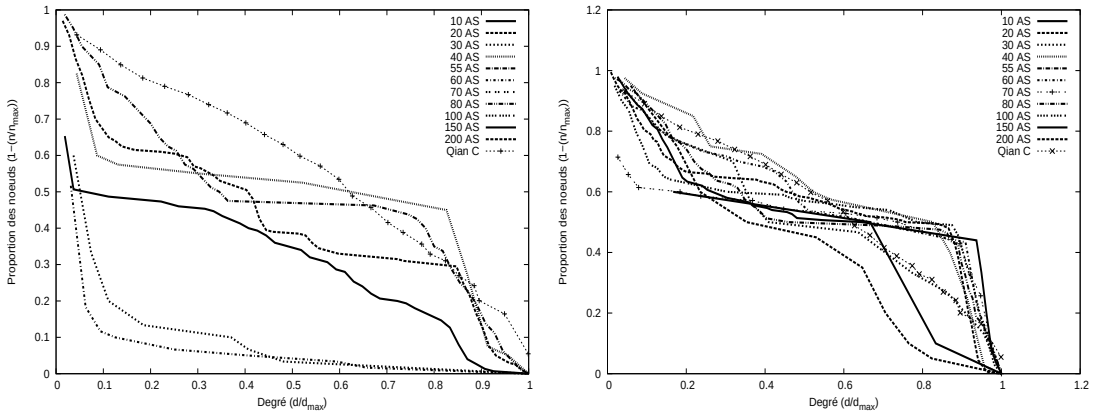


FIG. 4.16 – *Comparaison des distributions des degrés des graphes avec le graphe de référence (labélisé « Qian c »)*

La figure 4.16 présente la comparaison des fonctions cumulatives des distributions des degrés des graphes générés par notre algorithme et le graphe de référence. Le graphe de référence est celui obtenu par les travaux des auteurs de [36] présentés dans la section consacrée à l'état de l'art de ce chapitre. Pour rappel, ce graphe a été choisi comme référence compte tenu de la qualité des données utilisées par les auteurs qui couvrent de manière la plus complète les liaisons inter-domaines de niveau AS du réseau Internet. Les courbes représentent les résultats obtenus avec la technique proposée pour les graphes dont le nombre d'AS de niveau 1 est aléatoire et ceux dont le nombre d'AS de niveau 1 représentent 50% du nombre d'AS total. Ces courbes représentent les fonctions complémentaires des fonctions cumulatives $(1 - F_c(x))$ des distributions des degrés comme le graphe de référence dans [36] qui avait choisi cette fonction pour faciliter la comparaison avec la loi de puissance. La figure ci-dessus donne une idée sur la distribution moyenne des degrés des graphes, mais les différents graphes peuvent avoir des caractéristiques très différentes lorsqu'ils sont pris individuellement. Pour mieux appréhender

cette différence, nous présentons, sur les figures 4.17(a) et 4.17(b), les courbes des distributions des degrés de quelques graphes générés avec notre technique. Les tailles des graphes représentés sur ces figures varient entre 450 et 9000 nœuds. La figure 4.17(a) présente les distributions des degrés des graphes dont le nombre d'AS de niveau 1 est choisi de manière aléatoire alors que les graphes de la figure 4.17(b) sont générées avec un nombre d'AS de niveau 1 égal à 50% du nombre total d'AS.

Les résultats présentés sur ces 2 figures sont déterminants pour le choix du graphe utilisé pour les simulations des propagations des pannes car ils permettent d'éviter de faire sélectionner un graphe en se basant uniquement sur la moyenne des distributions des degrés de l'ensemble des graphes. Ainsi en comparant les résultats présentés sur les figures 4.16, 4.17(a) et 4.17(b) on constate que les graphes avec un nombre d'AS de niveau 1 fixé à la moitié du nombre total d'AS sont plus proches du graphe de référence à la différence des moyennes des distributions des degrés de ces graphes présentées sur la figure 4.16 qui montrent le contraire. Car, comme le montre la figure 4.17(b), l'écart entre les distributions des degrés des graphes avec un nombre d'AS de niveau 1 aléatoire et celle du graphe de référence est plus important que celui entre les distributions des degrés entre le graphe de référence et les graphes avec un nombre d'AS de niveau 1 égal à la moitié du nombre d'AS total.

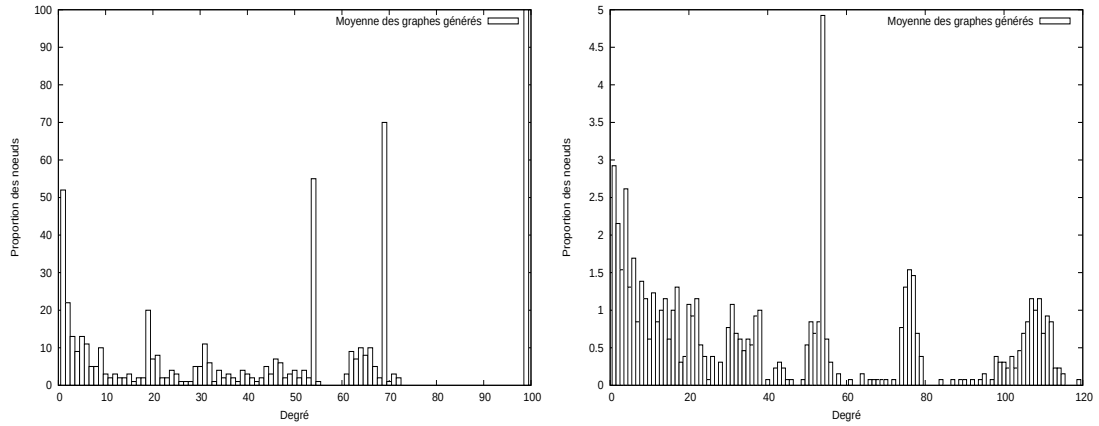


(a) Le nombre d'AS de niveau 1 est choisi aléatoirement (b) Le nombre d'AS de niveau 1 est égal à la moitié du nombre total des AS

FIG. 4.17 – *Fonction cumulative de la distribution des degrés des graphes inter AS de niveau AS*

Les courbes des figures 4.18(a) et 4.18(b) montrent l'évolution des distributions des degrés des graphes inter-AS de niveau AS. Ainsi, comme on peut le voir sur ces figures, les distributions des degrés de ces graphes sont très irrégulières et difficilement caractérisables. Ce qui est assez logique car, comme il a été évoqué précédemment, le nombre d'AS de niveau 1 est très élevé et ces AS ont aussi des degrés de connectivité très important. De ce fait, ils se différencient des graphes de niveau routeur dont un grand nombre de nœuds ont un degré de connectivité égal à 2.

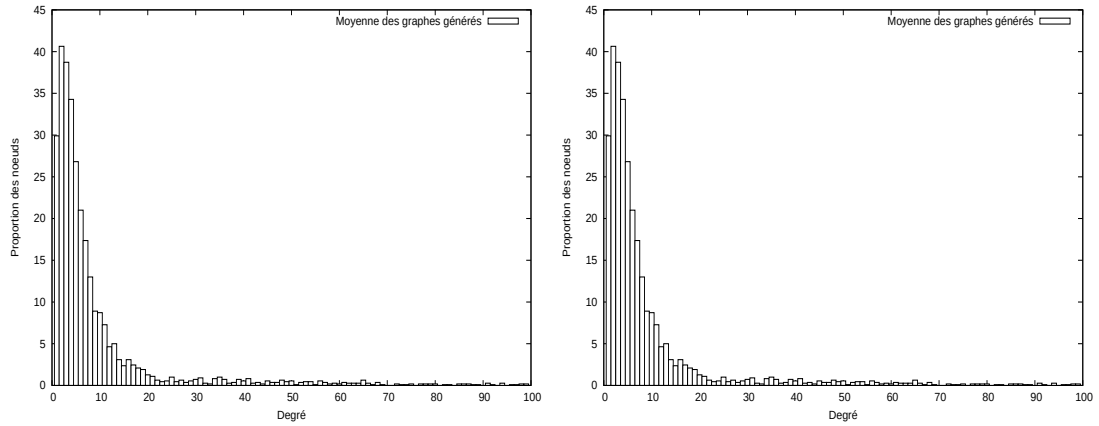
Les figures 4.19(a) et 4.19(b) présente les distributions de degrés des mêmes graphes, mais au niveau routeur. Elles montrent que les évolutions de ces distributions sont très différentes



(a) Le nombre d'AS de niveau 1 est choisi aléatoirement (b) Le nombre d'AS de niveau 1 est égal à la moitié du nombre total des AS

FIG. 4.18 – *Distribution des degrés des graphes inter AS de niveau AS*

pour les mêmes graphes selon que ces graphes soient de niveau routeur ou de niveau AS. Nous constatons que les distributions des degrés des graphes inter-AS de niveau routeur sont très proches de celles des graphes intra-AS.



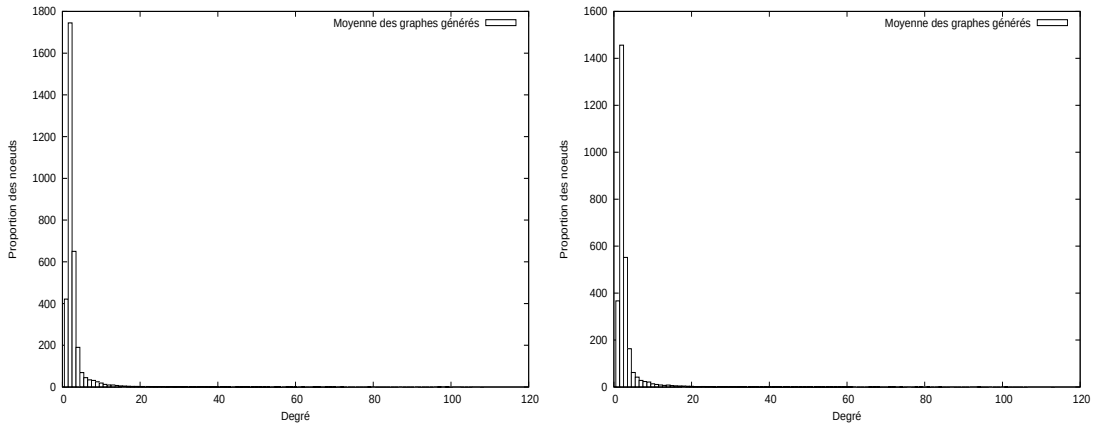
(a) Le nombre d'AS de niveau 1 est choisi aléatoirement (b) Le nombre d'AS de niveau 1 est égal à la moitié du nombre total des AS

FIG. 4.19 – *Distribution des degrés des graphes inter AS de niveau routeur*

4.4.5.5 Graphes intra-AS et inter-AS de niveau routeur

Pour terminer, nous présentons sur les figures 4.20(a) et 4.20(b) les distributions des degrés des graphes représentant aussi bien les graphes inter-AS que les graphes intra-AS. C'est à dire les graphes pouvant représenter les réseaux de type Internet, donc les réseaux inter-domaines

et intra-domaines. Le principal constat tiré des résultats présentés dans ce chapitre est que les distributions des degrés des graphes inter-AS de niveau AS sont très différentes de celles des autres graphes. Les graphes de niveau AS, largement utilisés dans la recherche ([16], [3]) ont des distributions des degrés qui évoluent de manière irrégulière.



(a) Le nombre d'AS de niveau 1 est choisi aléatoirement (b) Le nombre d'AS de niveau 1 est égal à la moitié du nombre total des AS

FIG. 4.20 – *Distribution des degrés des graphes intra et inter AS*

4.5 Conclusion partielle

La technique de génération des topologies présentée dans ce chapitre répond au besoin spécifique de disposer des topologies réalistes en nombre suffisant pour les simulations et autres expérimentations visant à faciliter la compréhension des interdépendances des infrastructures critiques. Deux contraintes ont été déterminantes pour la conception de la technique proposée. La première contrainte est la nécessité de disposer des topologies convenables à l'ensemble des infrastructures impliquées pour faciliter leur intégration dans un environnement de simulation unique malgré leur diversité. La seconde est celle relative à la flexibilité de la technique proposée pour s'adapter à la spécificité de chacune des infrastructures. La technique proposée répond à ces exigences en produisant des graphes qui conviennent aux topologies de tous les réseaux et en offrant une grande modularité pour faciliter l'adaptation de l'algorithme aux différentes étapes de déploiement de ces réseaux qui constituent la base fondamentale de l'algorithme proposé.

Bien que cette technique soit applicable à de nombreux réseaux, les résultats des évaluations présentés dans ce mémoire couvrent essentiellement les réseaux de télécommunications même si, pour démontrer la flexibilité de la technique, des graphes représentant les réseaux électriques ont été présentés. Les critères principaux utilisés pour évaluer les graphes sont la distribution des degrés, généralement utilisée pour évaluer la connectivité des topologies des réseaux et le partitionnement pour comparer les graphes obtenus avec les graphes de référence en terme de robustesse.

Les résultats des évaluations des graphes obtenus grâce à la technique proposée montrent que ces graphes ont des caractéristiques très proches de celles des graphes pris comme graphes de référence, notamment celui décrit dans [36] pour les réseaux de télécommunications et ceux du standard de l'IEEE[20] pour les graphes des réseaux électriques. Ces résultats montrent aussi qu'à l'exception des graphes de niveau AS, la distribution des degrés des nœuds de tous les graphes est assez régulière.

[20]http ://www.ee.washington.edu/research/pstca/

Chapitre 5

Modélisation et simulation des propagations des défaillances dues aux interdépendances des réseaux qui constituent l'Internet

5.1 Introduction

Dans les réseaux de télécommunications de type Internet, la plupart des travaux scientifiques consacrés à la modélisation et à la simulation des phénomènes de propagation des défaillances s'intéresse aux vers et virus informatiques. Ces travaux portent donc sur un aspect particulier de la propagation des défaillances et sont, par conséquent difficilement adaptables pour la modélisation d'autres phénomènes comme les attaques par déni de service, les corruptions des tables de routage et les pannes des routeurs. Le but du simulateur proposé dans ce chapitre est de couvrir l'ensemble des défaillances (pannes et attaques), mais limitées uniquement à celles qui se propagent et qui provoquent des dysfonctionnement de l'infrastructure matérielle et logiciel du réseau, par exemple des routeurs qui reçoivent et annoncent des fausses routes ou des routeurs qui arrêtent d'effectuer des calculs de routes à cause d'une table de routage complètement remplie par une large diffusion de virus ou encore des serveurs qui arrêtent de répondre aux requêtes à cause des attaques par déni de service diffusées sur le réseau. Puisque le modèle se veut suffisamment générique pour être facilement adaptable à d'autres infrastructures, il ne se focalise pas sur les causes de ces pannes qui peuvent varier d'une infrastructure à une autre. Par exemple une attaque d'un routeur pour le réseau de télécommunications ou court-circuit provoqué par un arbre pour le réseau électrique. Il caractérise l'évolution des pannes qui se propagent d'un composant à un autre quelle que soit la cause initiale de cette panne (attaque, défaut matériel ou logiciel, erreur humaine, etc.), ce simulateur ne prend donc pas en compte une panne qui touche un seul composant et qui ne se propage pas. Différents facteurs influent sur la vitesse et l'ampleur de ces propagations des défaillances. Ces facteurs comprennent, notamment les actions humaines, le taux de défaillances, le nombre de composants initialement défaillants, le taux de rétablissement des composants touchés, les systèmes

de défense, les différentes stratégies de confinement des pannes et la topologie. Pour le cas particulier des réseaux de télécommunications, on peut aussi citer la congestion du réseau, les délais, les bandes passantes, le trafic supplémentaire engendré par la défaillance (un virus par exemple), le taux d'occupation de la mémoire, la charge CPU des nœuds, les types de protocole (TCP avec son système de retransmission peut diffuser une défaillance moins rapidement que le protocole UDP), le trafic réseau, etc. Donc, dans la modélisation des propagations des pannes, la liste des facteurs à prendre en compte est très longue et compte tenu des contraintes liées aux ressources, notamment celles décrites par les auteurs de [146], il est souvent difficile de prendre en compte tous les paramètres qui influent la propagation des défaillances car même s'il existe des techniques comme PDNS[1] (une version distribuée de NS-2) et GTNetS[2] permettant de contourner certaines contraintes en matière de ressources informatiques, d'autres difficultés comme celles liées à l'accessibilité aux informations réelles sur le réseau Internet et à la quantité d'informations à traiter qu'engendrerait une telle approche persisteront toujours. Dès lors, il devient nécessaire de procéder à des simplifications en sélectionnant, par exemple, uniquement les paramètres essentiels au simulateur. Le véritable enjeu consiste donc à sélectionner efficacement ces paramètres pour réaliser un modèle pas trop complexe, mais qui permet de produire des résultats de bonne qualité. Dans ce chapitre, notre but est de mettre en œuvre un outil qui permet de simuler les propagations des pannes entre plusieurs réseaux de télécommunications interconnectés qui forment un réseau de type Internet et qui peut facilement être étendu pour intégrer d'autres infrastructures. Pour ce type de simulateur, les facteurs essentiels sont la topologie, le routage et l'état des réseaux impliqués. D'autres particularités et des facteurs additionnels peuvent exister pour chaque infrastructure et les simulateurs doivent être suffisamment génériques pour prendre en compte ces facteurs relatifs à chaque infrastructure simulée. Plusieurs travaux de recherche, notamment ceux des auteurs de [146] ont montré l'importance de la prise en compte de ces trois facteurs dans les modèles consacrés à la propagation des pannes dans le réseau Internet. Par conséquent, pour qu'un simulateur puisse fournir des résultats pertinents, il est nécessaire qu'il puisse caractériser ces facteurs de manière réaliste. Or, malgré l'importance de ces facteurs, certains travaux de recherche consacrés à la modélisation et à la simulation de la propagation des défaillances dans le réseau Internet utilisent des techniques très sensibles à la structure des topologies comme des chemins determinés par l'algorithme de Dijkstra et des modèles de propagations des défaillances fondés sur le modèle de propagation d'épidémie [45] sur des graphes approximatifs qui, parfois ne représentent que les liaisons inter-AS. Aussi certains de ces travaux utilisent des modèles mathématiques basés sur le modèle de propagation d'épidémie de base (fondée uniquement sur la loi d'action de masse) sans tenir compte des facteurs déterminants pour le fonctionnement du réseau Internet, comme le routage.

Dans les réseaux, les propagations des défaillances se font via la topologie, à partir d'un certain nombre de composants initialement touchés pour atteindre l'ensemble des composants vulnérables. De nombreux phénomènes qui se propagent dans les réseaux, notamment les virus informatiques ou les problèmes de routage peuvent être étudiés à l'aide du modèle d'épidémie [133, 152, 85, 131, 116]. Ce modèle, appelé aussi modèle homogène est utilisé depuis

[1] http://www.cc.gatech.edu/computing/pads/pdns.html
[2] http://www.ece.gatech.edu/research/labs/MANIACS/GTNetS/

de nombreuses années pour la modélisation des phénomènes comme la propagation des maladies [98, 35] à l'aide des concepts mathématiques.

Dans ce chapitre nous présentons un simulateur des propagations de défaillances dans les réseaux de télécommunications fondé sur un modèle de propagation d'épidémie amélioré et les résultats des simulations réalisées avec une topologie représentant des réseaux de type Internet. Le simulateur est fondé sur un principe générique et peut être facilement étendu pour étudier des propagations des défaillances sur d'autres infrastructures.

5.2 État de l'art de la modélisation et de la simulation des propagations des défaillances dans les réseaux de type Internet

Dans cette section nous présentons des travaux de recherche qui ont été réalisés pour la modélisation et la simulation des propagations des défaillances dans le réseau Internet. Plusieurs auteurs se sont intéressés à ce sujet et des nombreux résultats de recherche en ont été produits. Ainsi, dans l'article [61], les auteurs présentent une discussion sur les difficultés liées à la simulation de l'Internet à cause de l'hétérogénéité des composants matériels, des applications, des protocoles, de différents niveaux de congestion du réseau et des changements fréquents de l'infrastructure. En conclusion, les auteurs soulignent la nécessité de procéder à de multiples simulations pour obtenir des résultats pertinents et celle de compléter ces résultats par d'autres expérimentations, des analyses et des mesures. Le modèle proposé dans [86] décrit des techniques pour évaluer statistiquement les incidents liés à la propagations des virus dans un réseau de grande taille comme Internet. La première technique consiste à calculer l'impact d'une propagation de virus à partir du nombre de stations contaminées et d'une densité de probabilité de la durée de vie de la propagation et la deuxième technique, elle, utilise des équations différentielles établies à partir du nombre de stations initialement infectées et du taux rétablissement des stations infectées. Les résultats de leurs travaux montrent que la prévalence des virus informatiques était environ de 1 pour 1000 ordinateurs cibles en Amérique du nord en 1992.

Les auteurs de [35] s'intéressent à l'évaluation de l'efficacité des messages d'alerte sur les nouveaux virus informatiques, principalement pour les réseaux sociaux. Ils modélisent, avec le modèle d'épidémie un réseau représenté par un graphe avec différents mécanismes de propagation de virus (un-à-un, un-à-plusieurs, plusieurs-à-un, plusieurs-à-plusieurs). Dans le modèle proposé chaque nœud peut être infecté ou non ou encore dans un état spécifique suite à la réception d'un message d'alerte. Avec ce modèle, les auteurs montrent comment il est possible d'évaluer l'impact des propagations des virus dans un réseau à l'aide des graphes générés aléatoirement et comment limiter ses conséquences avec des techniques de propagation des messages d'alerte.

Le modèle proposé par les auteurs de [16] est basé sur un graphe représentant une topologie de niveau AS construite aléatoirement avec différentes lois (exponentielle et puissance) de distribution de degrés des nœuds. Dans leurs scénarios, les auteurs simulent les pannes en supprimant un nœud choisi aléatoirement et les attaques par la suppression du nœud de plus fort degré de connectivité, puis ils évaluent la tolérance aux pannes du graphe par le calcul de son diamètre. Pour un graphe, l'augmentation du diamètre signifie la réduction du nombre de

chemins entre les nœuds, donc la réduction de la connectivité du graphe. Avec leurs résultats, ils ont démontré que le diamètre varie considérablement pour les graphes avec une fonction de distribution exponentielle après une panne alors qu'il change très peu pour les graphes sans-échelle car c'est souvent les nœuds de plus faible degré qui sont sélectionnés par la fonction de choix aléatoire des nœuds à supprimer initialement. Pour le cas des attaques, c'est-à-dire le choix des nœuds de plus fort degré pour la défaillance initiale, les résultats obtenus sont semblables à ceux des pannes pour les graphes homogènes (graphes exponentiels), mais présentent une différence importante pour les graphes sans-échelle où la suppression de 5% des nœuds de plus fort degré provoque le doublement du diamètre du graphe.

Dans l'article [106], les auteurs réalisent des simulations avec le logiciel SSFNet [3] sur un graphe de niveau AS obtenu par abstraction sélective d'un graphe construit à partir des données collectées dans le cadre du projet Routeviews[3] de l'université de l'Oregon. L'abstraction sélective consiste à fusionner des AS lorsqu'ils sont directement connectés et n'ont pas un AS pair en commun pour réduire la taille du graphe en supprimant autant de liens que de nœuds. Le projet Routeviews a pour objectif la mise à disposition des informations temps-réels sur le routage Internet. Les informations fournies dans le cadre de ce projet ont servi de base pour de nombreux travaux comme ceux de NLANR (*National Laboratory for Applied Network Research*)[4] pour la visualisation de la liste des AS traversés par les paquets destinés à un préfixe et de CAIDA[5] pour déterminer la position géographique des hôtes à partir de leurs adresses IP. CAIDA est une association pour la collaboration entre les organismes de recherche visant à promouvoir une plus grande coopération dans l'ingénierie et la maintenance de l'infrastructure Internet. CAIDA est l'initiateur de nombreux projets sur la cartographie et la mesure de Internet et publie des rapports annuels qui décrivent, notamment les initiatives de recherche, l'état d'avance et les résultats de ses projets, ses publications et présentations et les statistiques du Web. Le modèle proposé est fondé sur une topologie simplifiée où chaque AS comporte un seul routeur et le reste de l'Internet est représenté par un AS. Ils se sont intéressés à la propagation des virus sur le réseau et ont défini un modèle basé sur la loi d'action de masse des modèles épidémiologiques SIR (*Susceptible-Infected-Removed*) et SIS (*Susceptible-Infected-Susceptible*) avec des probabilités d'infection et de rétablissement qui suivent une loi exponentielle. Les taux de contamination et de rétablissement sont calculés sur la base de l'espace d'adressage annoncé par les AS, obtenu à partir des informations collectées le 26 octobre 2001 par Routeviews et des données sur la propagation des virus CODE RED II[6] et NIMDA[7] disponibles sur le site Web de CAIDA[8]. Le modèle des défaillances est fondé sur la corrélation entre la propagation des virus, l'augmentation du trafic BGP et ses conséquences sur les charges CPU et de la mémoire.

Enfin, les auteurs évaluent, à chaque instant de la simulation, le nombre de nœuds défaillants en effectuant des calculs basés sur la charge CPU (calculée à partir du trafic réseau transitant par le routeur), les activités de routage (la charge mémoire calculée en fonction de

[3] http://www.routeviews.org
[4] http://moat.nlanr.net/ASx/
[5] http://www.caida.org
[6] http://www.cert.org/incident_notes/IN-2001-09.html
[7] http://www.cert.org/advisories/CA-2001-26.html
[8] http://www.caida.org

la taille de la table de routage) et le trafic de balayage des ports (*portscan*) d'un AS destiné aux autres AS. Leurs résultats montrent comment la propagation des virus informatiques peut provoquer des instabilités du protocole BGP, l'augmentation de l'utilisation mémoire et CPU des routeurs.

Les auteurs de [43] s'intéressent, quant à eux, à l'analyse des instabilités du routage BGP observées en juillet et septembre 2001 lors de l'apparition des virus informatiques CODE RED II[9] et NIMDA[10] à partir des données collectées par les moniteurs du projet RIPE RIS[11] (Réseaux IP Européens - *Routing Information Service*). Cette collecte est effectuée par les moniteurs situés principalement à Amsterdam. Les analyses ont été concentrées autour de certains événements observés lors de la propagation de ces virus, notamment l'augmentation du trafic échangé, la succession des événements anormaux pouvant conduire aux pannes des routeurs et l'augmentation considérable du trafic BGP dû aux messages de mise à jour des tables de routage échangés à la suite des instabilités. Avec leurs résultats, les auteurs identifient l'augmentation du trafic comme cause principale de défaillance et démontrent que le trafic constitué d'un nombre élevé de paquets IP en un temps relativement court entraîne la surcharge CPU, des insuffisances mémoires des routeurs et une augmentation du trafic ARP. Ce qui peut conduire à une augmentation de perte de messages BGP et à des erreurs d'allocation de mémoire qui provoquent des arrêts, des redémarrages et de reconfiguration des routeurs. L'article [34] présente une étude sur la réaction de trois types de routeurs face à une instabilité du protocole BGP. Les résultats de cette étude montrent que le routeur *Cisco*7000 arrête de répondre aux sollicitations après avoir reçu 140000 annonces de routes, *CiscoGSR* ne répond plus après la réception de 17000 annonces et *JuniperM*20 arrête de répondre après la réception de 500000 annonces. Avec cette étude, les auteurs montrent comment un nombre important d'annonces de routes BGP peut provoquer des pannes des routeurs, comment cette panne peut se propager à travers les routeurs et comment des mécanismes de contrôle de ressources comme la limitation du nombre de préfixe peut atténuer les propagations des défaillances à travers les routeurs.

Les travaux réalisés par les auteurs de [146] ont abouti à la mise en œuvre d'un environnement de simulation de propagation de virus appelé PAWS et constitué de 8 PC de la plateforme Emulab[12] communiquant via un réseau TCP/IP. Les simulations portent sur une topologie déduite à partir des données collectées par Routeviews[13]. La bande passante et la quantité de trafic sont calculées avec Pathneck[14]. Pour simplifier, les chemins entre les AS sont calculés avec l'algorithme de Djikstra. La simulation des congestions est fondée sur la valeur de la bande passante et la somme du trafic normal et le trafic engendré par le virus. La vulnérabilité d'un nœud est estimée sur la base de son CPU, son système d'exploitation, sa mémoire et le nombre de requête de balayage de ports reçu. Le modèle de propagation des virus utilise le taux de vulnérabilité, le taux de balayage de ports, la durée nécessaire pour la contamination d'un virus, l'espace d'adressage vulnérable au balayage de ports et la stratégie (aléatoire dans ce papier) utilisée. La propagation est simulée par des sélections successives d'une liste

[9] http://www.cert.org/incident_notes/IN-2001-09.html
[10] http://www.cert.org/advisories/CA-2001-26.html
[11] http://www.ripe.net/ris/
[12] http://www.emulab.net
[13] http://www.routeviews.org
[14] http://www.cs.cmu.edu/~hnn/pathneck/

d'adresses IP constituant la cible d'un nœud infecté et, pour chaque adresse IP, les calculs évoqués ci-dessus sont effectués pour savoir si le nœud cible est infecté ou non. Les simulations sont réalisées à partir des données collectées lors de la propagation des virus CODE RED II[15] et SLAMMER[16] et les résultats sont validés par une comparaison avec les informations sur la propagation de ces virus disponibles sur le site de CAIDA[17].

Les travaux des auteurs de [82] portent sur la modélisation de la propagation des défaillances dans un réseau composé de routeurs BGP. Ils développent un modèle fluide basé sur la théorie de propagation d'épidémie et analysent la durée de vie d'une défaillance dans un réseau en fonction des taux de contamination et de rétablissement des routeurs. Leur modèle utilise aussi le taux de service k_s qui indique le nombre de routeurs rétablis par unité de temps grâce à un routeur non touché, la charge k_a représentant la charge d'un routeur pour le fonctionnement normal de BGP et le taux de panne k_l qui indique le nombre de routeurs contaminés à cause de la charge imposée par la reinitialisation des sessions BGP. En appliquant ce modèle sur un graphe sous forme de clique (topologie entièrement maillée), les auteurs identifient un point de transition autour de $\frac{k_s}{k_l}$ et montrent que les pannes en cascade se produisent lorsque le nombre de routeurs initialement défaillants est supérieur à $\frac{k_s}{k_l}$ et elles s'estompent rapidement lorsque le nombre de routeurs initialement en panne est inférieur à cette valeur. Ils ont aussi montré que l'augmentation du nombre total de nœuds dans le réseau contribue à la réduction de la durée de vie de la défaillance.

Le cas spécifique de l'influence de la topologie des réseaux dans la propagation des défaillances a aussi fait l'objet de travaux de recherche même si les résultats obtenus ne traitent, pour le moment, que des topologies simples à cause des difficultés liées à la reproduction et au traitement de la topologie réelle de l'Internet. Les auteurs de [105], par exemple, se sont intéressés aux interconnexions de niveau routeur entre les AS. Avec un modèle portant uniquement sur les relations de peering entre les systèmes autonomes de niveau 1 (*Tier 1 AS peering*), les auteurs démontrent qu'il existe une différence entre les connectivités physique et logique pour un même réseau à cause du délai MRAI (*Minimum Route Advertisement Interval*) de propagation des informations de mise à jour des tables de routage entre les différents routeurs BGP. Ils ont aussi mis en évidence la nécessité pour ce type de modèle de disposer des données sur la position géographique des nœuds pour savoir exactement les sessions qui sont établies via un lien et les routeurs concernés. Les simulations des connexions physiques ont été réalisées avec un modèle mathématique basé sur la probabilité de défaillance, la durée inter-panne, la durée moyenne des pannes et le logiciel utilisé. Pour les connexions logiques, les simulations (avec SSFNet [3]) portent essentiellement sur les protocoles de connexions TCP (*Transmission Control Protocol*), de routage BGP et OSPF et de test ICMP (*Internet Control Message Protocol*), mais aussi avec une couche qui implémente la simulation des pannes sur une topologie où il y a une relation de *peering* unique entre chaque paire d'AS. La simulation d'une panne est réalisée par la simulation d'un simple redémarrage d'un routeur avec une probabilité fixée en début de la simulation et un temps de démarrage aléatoire compris entre 2 et 10 minutes. D'après leurs résultats, même si 90% des routeurs fonctionnent, certains routeurs ne commu-

[15] http://www.cert.org/incident_notes/IN-2001-09.html
[16] http://www.cert.org/advisories/CA-2003-04.html
[17] http://www.caida.org

niquent qu'avec moins de la moitié des routeurs pendant un certains temps à cause de délai nécessaire au rétablissement de la connectivité logique.

Les travaux présentés dans [150] décrivent une étude d'évaluation de l'impact de la topologie utilisée sur les résultats des simulations. Cette évaluation est fondée sur une comparaison sur la base du diamètre, du degré moyen des nœuds, du nombre de sauts moyen pour les paquets et du délai de quelques graphes (en anneau, étoile, graphe généré aléatoirement) fréquemment utilisés dans les simulations. Les résultats d'une comparaison de 100 graphes générés aléatoirement à 100 autres graphes avec un même degré moyen de nœud $(3,5)$ montrent que les graphes aléatoires ont $65,5\%$ de chance d'avoir des diamètres inférieurs à ceux des autres graphes. Pour comparer l'influence des topologies étudiées sur l'acheminement des paquets, les auteurs définissent un critère qui optimise à la fois le délai et le nombre de saut et leurs résultats montrent que les graphes aléatoires ont une valeur moyenne de ce critère 2% supérieure à celle des graphes dont la distribution des degrés suit une loi exponentielle.

Les travaux des auteurs de [143] proposent un modèle de propagation des virus à travers un graphe qui permet de calculer, à chaque instant t, le nombre de nœuds infectés. Ce nombre est calculé en fonction du taux d'infection, du taux de rétablissement et du nombre de nœuds infectés au temps $t-1$. Les simulations sont effectuées sur un graphe construit à partir de données collectées dans le cadre du projet Routeviews[18]. La génération du graphe est réalisé avec le logiciel BRITE[19] [99] qui permet de générer des graphes sans-échelle. Les auteurs ont établi une relation entre la valeur propre de la matrice d'adjacence du graphe et le seuil (calculé en fonction du degré de connectivité des nœuds) au delà duquel la contamination se transforme en épidémie et se propage rapidement. Ils ont aussi montré qu'en dessous de ce seuil le nombre de nœuds infectés décroît exponentiellement.

Dans [90] les auteurs se sont intéressés à l'influence de la topologie et des politiques de routage BGP dans la convergence et ont établi que le temps de convergence BGP après une panne dépend de la longueur du plus long chemin de secours entre les systèmes autonomes. Pour leurs simulations, les auteurs utilisent les logiciels MRT[20] et IPMA[21] pour générer des messages *UPDATE* (messages de mise à jour des tables de routage) du protocole BGP et leurs résultats démontrent que le temps de convergence dépend fortement de la valeur du temporisateur (*timer*) MRAI et très peu des délais de traitement et de propagation.

Pour améliorer les modèles basés sur la propagation d'épidémie, les auteurs de [116] utilisent les logiciels de simulation PDNS [23] et GTNetS [123] pour développer un modèle de propagation des virus de niveau paquet (couche IP, utilisation des adresses pour choisir une liste de victimes potentielles). Les résultats des différentes simulations effectuées montrent que la courbe de l'évolution de l'épidémie suit la même trajectoire que que celle du modèle d'épidémie simple, mais l'introduction du modèle de niveau paquet permet de modéliser plus convenablement le comportement des virus, notamment le choix de liste des adresses à scanner et l'intensité du trafic.

Les auteurs de l'article [94] propose un modèle de simulation de la propagation des virus informatiques fondé sur le simulateur réseau SSFNet [3] et le modèle de propagation d'épidémie.

[18] http://www.routeviews.org
[19] http://www.cs.bu.edu/faculty/matta/Research/BRITE/
[20] http://mrt.sourceforge.net/
[21] http://www.merit.edu/networkresearch/projecthistory/ipma/index.php

Le modèle proposé consiste à utiliser SSFNet [3] pour générer du trafic qui se propage selon le modèle de propagation d'épidémie afin d'évaluer la performance du système de détection des virus DIBS/TRAFEN [24]. Les résultats de simulation de la propagation des virus CODE RED II[22] et SLAMMER[23] montrent que l'utilisation de DIBS/TRAFEN [24] aurait permis de détecter le virus CODE RED avant la contamination de $0,2\%$ des ordinateurs vulnérables et la supervision de seulement deux réseaux de classe B avec DIBS/TRAFEN [24] aurait permis de détecter le virus SLAMMER[24] après une contamination de seulement $0,01\%$ des ordinateurs vulnérables.

5.3 Limites des outils existants pour la modélisation et la simulation des propagations des défaillances dans les réseaux de type Internet

Les travaux présentés dans cette section permettent de constater que la plupart des modèles et simulateurs est basée uniquement sur des topologies de niveau AS à cause, notamment de la nécessité de simplification qui conduit, parfois à la fusion des AS, la suppression des liens, la prise en compte uniquement des AS de niveau 1 ou sur des graphes générés aléatoirement, des graphes simples et réguliers (clique, graphe complet, hypercube) ou encore des graphes générés à partir des données collectées par quelques moniteurs qui n'ont pas forcément une vision globale du réseau concerné. Dans ce contexte, il est impossible de faire la différence entre un AS de petite échelle comme un ISP (*Internet Service Provider*) et un AS de grande échelle avec des interconnexions dans plusieurs endroits du monde et qui reste donc plus difficile à déconnecter du réseau par des pannes en cascade qu'un petit AS d'un campus universitaire par exemple. Or des travaux comme ceux de [146] ont montré que la propagation des virus est étroitement liée à la topologie du réseau. Aussi les topologies de niveau AS sont inadaptées pour l'ensemble des modélisations et des simulations basées sur la théorie des graphes car elles représentent un AS par un seul nœud alors qu'en pratique un AS est constitué par plusieurs nœuds, ce qui conduit à un graphe où plusieurs liens du graphe réel sont ignorés. La simulation des propagations d'épidémie utilise plusieurs algorithmes sensibles au nombre de liens du graphe, par exemple, la simulation du routage intra-AS avec des chemins calculés par l'algorithme de Dikstra.

Par ailleurs, à l'exception de ceux qui portent sur des cas particuliers (propagation du virus CODE RED II[25] par exemple), ces travaux se fondent uniquement sur les modèles de propagation d'épidémie de base, à savoir sur la loi d'action de masse. Ces modèles sont, par conséquent difficilement adaptables à d'autres infrastructures ou n'offrent aucun moyen de prendre en compte l'influence de l'ensemble des protocoles de routage des réseaux de cœur qui, pourtant jouent un rôle déterminant dans la propagation des défaillances dans les réseaux de télécommunications. C'est pourquoi la technique de modélisation et de simulation des propagations des défaillances proposée dans ce chapitre est fondée sur un modèle de propagation d'épidémie modifié pour être facilement adapté à d'autres infrastructures tout en offrant la pos-

[22] http://www.cert.org/incident_notes/IN-2001-09.html
[23] http://www.cert.org/advisories/CA-2003-04.html
[24] http://www.cert.org/advisories/CA-2003-04.html
[25] http://www.cert.org/incident_notes/IN-2001-09.html

sibilité de mettre en œuvre les principaux facteurs qui influent la propagation des défaillances dans chacune des infrastructures impliquées.

5.4 Description du simulateur des propagations des défaillances proposé

5.4.1 Introduction

Dans les réseaux de type Internet les pannes généralisées apparaissent généralement suite à une défaillance de l'infrastructure de routage. Dans ce cas, des défauts logiciels peuvent, non seulement avoir des impacts négatifs sur le fonctionnement du réseau, mais aussi conduire à des défaillances matérielles de certains composants du réseau. Par exemple, une erreur dans une table de routage conduit à une défaillance logique car tous les paquets envoyés à un routeur dont la table de routage ne contient pas un chemin vers les destinations de ces paquets seront perdus. Aussi il a été démontré par les auteurs de [43] que lors de la propagation d'un virus la plupart des adresses scannées ne sont pas dans les tables de routage, ce qui génère des messages BGP et des messages ICMP lorsque les adresses sont invalides. Tout ce trafic supplémentaire s'ajoute au trafic BGP, cette situation peut provoquer une surcharge CPU et conduire aux pannes de certains routeurs. Ces pannes entraînent de nouveaux messages BGP auxquels s'ajoutent les messages BGP émis par les routeurs qui redémarrent après les pannes et le cycle recommence. Par conséquent, pour fournir des résultats pertinents, le simulateur que nous proposons dans ce chapitre inclut tous les paramètres relatifs à la topologie, à la charge des nœuds, à la vitesse de propagation, c'est à dire de l'influence des protocoles de routage pour permettre de mieux comprendre comment des événements parfois purement logiques peuvent conduire à des défaillances logicielles, mais aussi matérielles. Pour la conception du simulateur, nous considérons tous les événements qui se succèdent après ces défauts matériels et logiciels aboutissant au ralentissement, à la saturation, à l'interruption des services du réseau et aux pertes de paquets causées par des routages erronés. Donc, dans notre simulateur, la défaillance d'un routeur ne se limite pas seulement à une panne matérielle, mais elle comprend aussi l'incapacité du routeur d'acheminer un paquet reçu à cause d'un dysfonctionnement matériel ou logiciel, d'une surcharge ou de l'existence de fausse route dans sa table de routage. Pour ce simulateur, le problème de fausse route dans la table de routage d'un routeur se manifeste lorsqu'un ou plusieurs de ses voisins deviennent incapables d'acheminer des paquets. En effet, pour éviter d'inonder le réseau par des messages de mise à jour ou de suppression des routes envoyés par les protocoles de routage, tous ces protocoles possèdent un paramètre qui permet de limiter l'intervalle de temps entre deux annonces de mise à jour successives. Ces valeurs sont définies avec les paramètres du *routing-update-timer* pour le protocole RIP, du *InfTransDelay* pour le protocole OSPF et du *MinRouteAdvertisementIntervalTime* pour le protocole BGP lors de la configuration. Lorsqu'un routeur tombe en panne, les autres routeurs qui ont, dans leurs tables de routage, des chemins qui passent par le routeur défaillant auront des fausses routes tant que ces derniers n'ont pas reçu l'annonce relative à cette défaillance. Donc, les valeurs de ces paramètres constituent aussi des facteurs importants qui influent fortement la durée de vie de ces fausses routes et sur la vitesse des propagations des pannes. Ces valeurs étant différentes selon

les protocoles, il est alors indispensable que le simulateur soit capable d'identifier le protocole impliqué à chaque fois que des nœuds du graphe doivent communiquer entre eux.

Dans ce chapitre, notre but est de concevoir un simulateur de propagation des pannes basé sur la théorie de propagation d'épidémies, suffisamment générique, mais qui ne se limite pas aux interdépendances fonctionnelles, c'est-à-dire à un simulateur basé uniquement sur des approches où la défaillance d'un composant d'une infrastructure provoque systématiquement la panne des composants des autres infrastructures qui sont dépendants du composant défaillant.

L'objectif de notre simulateur est de combler la limite des simulateurs existants en terme de compromis entre généricité et pertinence en offrant des moyens d'étudier la succession des événements qui conduisent aux pannes en cascade tout en offrant des possibilités d'extension pour couvrir plusieurs infrastructures. Le développement d'un tel simulateur pour l'ensemble des infrastructures interdépendantes est un travail complexe, c'est pourquoi notre simulateur est consacré, dans un premier temps, aux réseaux de télécommunications, principalement de l'Internet. Cependant, à la différence des outils de simulation spécifiques, notre simulateur est fondé sur les graphes et le modèle de propagation d'épidémie largement utilisés pour la modélisation et la simulation des infrastructures de nombreux domaines, il peut donc être facilement étendu à toutes les infrastructures qui peuvent être modélisées et simulées par les graphes et le modèle de propagation d'épidémie.

Le modèle d'épidémie de base considère une population de taille N dont chaque individu peut être dans l'un des 3 états suivants : vulnérable S (*Susceptible*), infecté I (*Infected*) ou guéri R (*Removed*). On parle ainsi de modèle SIR et, pour une population homogène, on peut écrire $N = S + I + R$. Il y a certains cas où les individus guéris ne sont pas immunisés et deviennent donc vulnérables après une guérison, ce modèle est appelé le modèle SIS (*Susceptible - Infected - Susceptible*). Le modèle d'épidémie est principalement fondé sur des systèmes d'équations différentielles ou aux dérivées partielles. A l'instant *t*, les équations différentielles de base d'un modèle SIR appelées aussi équations de transition des individus d'un état (S, I ou R) à un autre s'écrivent de la manière suivante :

$$\begin{aligned} \frac{dS(t)}{dt} &= -\alpha \frac{S(t)}{I(t)} \\ \frac{dI(t)}{dt} &= \alpha S(t) I(t) - \beta I(t) \\ \frac{dR(t)}{dt} &= \beta I(t) \end{aligned}$$

où α est le taux d'infection et β le taux de guérison.

Ces équations sont fondées sur la loi d'action de masse pour une population homogène, c'est à dire un contexte dans lequel le taux d'interaction entre les individus de chaque sous-ensemble est proportionnel au produit du nombre d'individus dans chacun des sous-ensembles. Pour un graphe, les équations ci-dessus permettent de calculer le nombre de nœuds infectés $I(t)$ à l'instant *t* en fonction du taux d'infection α, du taux de guérison β, du nombre de nœuds infectés à l'instant $I(t-1)$ et le nombre de nœuds vulnérables $R(t)$. Donc ce modèle se limite à une évaluation quantitative de l'ampleur d'une panne à un instant t. On constate donc que ce modèle tel qu'il est décrit ci-dessus ne convient pas au réseau de télécommunications où un nœud ne peut être touché que si, au moins un de ses voisins est défaillant et que ce voisin peut transmettre cette défaillance. Pour adapter ce modèle aux propagations des défaillances dans les réseaux de télécommunications, nous proposons un simulateur qui peut être décrit comme suit : Un nœud

est défaillant à un instant t si, au moins l'un de ses voisins est défaillant à l'instant $t-1$ et compte tenu des contraintes liées aux protocoles de routage et à la durée nécessaire au processus d'acheminement, le nœud défaillant est capable de transmettre cette défaillance à ses voisins à l'instant t. L'algorithme 3 présente un échantillon du simulateur proposé. Pour faciliter la lisibilité, nous y présentons uniquement l'échantillon de la simulation des défaillances sans la partie consacrée à la propagation du rétablissement des nœuds et la répartition des charges entre les routeurs.

```
input : G : Graph du réseau, BGP_N : Nœuds BGP, BGP_Interval :
        MinRouteAdvertisementIntervalTime, OSPF_Interval : InfTransDelay,
        Sim_Time_Step : Intervalle de temps de Simulation, Sim_Duration : Durée de
        la simulation
while Sim_Time < Sim_Duration do
    for i ← 1 to Nodes_Number do
        for k ← 1 to Infected_Nodes_Number do
            if voisin(j,k) == true then
                T_Route_Update ←
                10 * Sim_Time_Step * (path_d(k)/Reference_Value);
                if k ∈ BGP_Nodes_List then
                    Next_Time ⟵ Previous_Time(Infected_Nodes(k)) +
                    T_Route_Update + BGP_Interval;
                else
                    Next_Time ⟵ Previous_Time(Infected_Nodes(k)) +
                    T_Route_Update + OSPF_Interval;
                if Next_Time >= Current_Time then
                    if i is not infected and i is not inoculated then
                    Infected_Nodes ⟵ Infected_Nodes + i;
                    else if i is inoculated then
                    Inoculation_Nodes ⟵ Inoculation_Nodes + i ;
                else
                    if i is not infected and i is not inoculated then
                    Routes_Number ⟵ compute_failed_routes(j,k,G) ;
                    Failed_Routes(j) ⟵ Routes_Number ;
                    Failure_Duration(j) ⟵ Next_Time − Current_Time ;
```

Algorithm 3: Échantillon de l'algorithme de simulation des propagations des défaillances

5.4.2 Modélisation et Simulation du fonctionnement des routeurs

Le premier axe de l'adaptation du modèle d'épidémie pour simuler le fonctionnement des réseaux consiste à caractériser l'influence des protocoles de routage à la vitesse de propagation des pannes. Pour simuler cette fonctionnalité, notre modèle utilise un intervalle de temps nécessaire pour la transmission d'une information entre deux routeurs voisins. La valeur de cet intervalle est calculée avec les valeurs de l'intervalle de temps minimum (*MinRouteAdvertise-*

mentIntervalTime) entre deux annonces successives, du temps de calcul des nouvelles routes et de celui de la mise à jour de la table de routage après une défaillance. En effet, lorsqu'un routeur envoie une annonce de modification ou de suppression de route à ses voisins, il arme un temporisateur dont la valeur est celle de l'intervalle de temps minimum entre deux envois successifs d'annonce de mise à jour. Même si ce routeur reçoit un nouveau message de modification de route d'un de ses voisins, il ne transmettra cette information qu'à l'expiration du temporisateur armé lors de l'envoi de la précédente annonce. Aussi cette annonce ne sera envoyée qu'après que le routeur ait effectué les calculs des nouvelles routes qu'il doit transmettre à ses voisins et qu'il ait mis à jour sa table de routage. Dans notre simulateur, nous utilisons donc les temporisateurs relatifs à ces différents paramètres, le premier est le temps nécessaire pour que le routeur effectue le calcul des nouvelles routes et la mise à jour de sa table de routage (*T_Route_Update*) et le second est celui de la valeur de *T_Advertisement_Interval* qui correspond à *MinRouteAdvertisementIntervalTime* dans ce simulateur. Un nœud infecté ne peut donc contaminer un de ses voisins qu'après un temps $T\_Infection(0) = T\_Route\_Update + T\_Advertisement\_Interval$. Pour rappel, $T\_Infection(N)$ est le temps nécessaire pour qu'un routeur infecté contamine un routeur situé à une distance de N sauts. Notre simulateur étant basé sur le processus de contact, les contaminations ne se font qu'entre voisins, donc $N = 0$. Lorsqu'un routeur reçoit une annonce, il calcule les nouvelles routes et met à jour sa table de routage, puis il vérifie le temps écoulé depuis la dernière annonce qu'il ait faite à ses voisins. Si ce temps est supérieur ou égal à *T_Advertisement_Interval* alors il annonce immédiatement la mise à jour à ses voisins, si non il attend l'expiration du temporisateur avant d'envoyer l'annonce. Donc le délai entre l'infection de deux routeurs voisins peut être égale *T_Route_Update* ou *T_Route_Update*+ fraction de *T_Advertisement_Interval* ou encore $T\_Route\_Update + T\_Advertisement\_Interval$. Dans notre simulateur, la valeur de *T_Advertisement_Interval* est fixée à 60 secondes pour eBGP et à 30 secondes pour iBGP (*internal BGP*) et OSPF. En effet, pour une question de convergence, la valeur du *MinRouteAdvertisementIntervalTime* pour les communications intra-AS doit être inférieure à celle des communications inter-AS. Pour chaque routeur, la valeur de *T_Route_Update* est fixée à 5 secondes auxquelles on ajoute une valeur calculée en fonction de la taille de la table de routage du routeur concerné. La taille de la table de routage d'un routeur est exprimée en fonction du nombre de plus courts chemins qui passent par ce routeur. Le calcul de cette valeur ajoutée à *T_Route_Update*, se fait en fonction du nombre de chemins qui passent par le nœud en question. Par exemple, un nœud avec un nombre de chemins maximum aura un temps de calcul égal à 1 unité de temps choisie pour la simulation alors qu'un routeur avec un nombre de chemins égal à 20% de la valeur maximale du nombre de chemins aura une valeur de $0,2$ unité de temps. Avec ces valeurs, nous avons choisi de fixer l'unité de temps de la simulation à 1 minute, car l'évaluation de l'état du réseau simulé à chaque minute permet de caractériser l'influence des valeurs des paramètres décrits ci-dessus, notamment la durée minimale entre deux annonces successives de mise à jour des routes. Ce simulateur permet, notamment d'évaluer l'évolution du nombre de nœuds touchés, celui des nœuds rétablis, la durée nécessaire pour l'absorption de la défaillance lorsqu'il existe des nœuds immunisés, si non la durée nécessaire à l'effondrement du réseau en fonction des nœuds contaminés en début de simulation.

5.4.3 Modélisation et Simulation du transfert de charge entre les routeurs

Le deuxième axe de notre simulateur concerne la répartition de la charge entre les routeurs lorsque le réseau est victime d'une défaillance et le délai nécessaire à la restauration des tables de routage des nœuds impactés par la défaillance d'un ou plusieurs routeurs. En effet, lorsqu'un routeur du réseau tombe en panne, ses voisins détectent cette panne et envoient des annonces aux autres routeurs du réseau qui recalculent les routes et remplacent les routes qui passaient par le routeur défaillant. Ce changement provoque très souvent l'augmentation du nombre de routes qui passent par certains routeurs. Aussi le trafic supplémentaire induit par une instabilité de l'infrastructure de routage peut conduire, parfois à une indisponibilité des routeurs. Des travaux de recherche comme ceux des auteurs de [43] ont démontré que l'accroissement du trafic BGP peut amplifier la charge CPU des routeurs et cette amplification provoque des effets indésirables allant jusqu'aux pannes des routeurs. En effet, une charge CPU importante pendant une durée relativement longue ralentit le calcul des routes exécuté lors des mises à jour des tables de routage BGP, ce qui conduit à un temps de convergence plus long. L'utilisation maximale du CPU des routeurs empêche l'exécution des autres tâches comme le traitement approprié des messages *KEEP ALIVE* et peut conduire au *crash* des routeurs dans les cas extrêmes. Un enjeu important consiste donc à savoir si les propagations des défaillances dans les réseaux provoquent une augmentation des charges CPU des routeurs BGP. Des travaux intéressants ont été réalisés sur ce sujet et les résultats obtenus par les auteurs de [14], par exemple, montrent que les processus BGP peuvent provoquer une augmentation de la charge CPU avoisinant 20% lors des instabilités pour des durées relativement longues (environ 10 heures). Ces résultats sont issus des études menées sur le réseau Sprint (AS 1239), notamment lors de la propagation du virus informatique *SLAMMER*[26] en janvier 2003. Ces études ont aussi montré que durant les fonctionnements corrects des réseaux, les processus BGP consomment en moyenne 60% des ressources CPU disponibles des routeurs, mais les charges CPU moyennes restent inférieures à 50% des capacités de ces routeurs. Toutefois, les auteurs notent l'existence des périodes relativement courtes (environ 5 secondes) durant lesquelles les processus BGP peuvent consommer des quantités importantes de ressources (plus de 95%) sans engendrer de dysfonctionnements majeurs du réseau. Pour modéliser les pannes des routeurs provoquées par des instabilités causées par la propagation des défaillances, il est nécessaire d'analyser les conditions dans lesquelles les processus BGP provoquent des augmentations des charges CPU pendant des durées relativement longues notamment l'apport de chaque type de processus BGP à des situations qui conduisent aux surcharges. Les études des auteurs de [142] menées à partir des données collectées par certains moniteurs du projet RIPE NCC[27] sur la période du 10 au 30 septembre 2001 (période couvrant celle de la propagation du virus informatique *NIMDA*[28] le 18 septembre) montrent que les échanges de messages BGP dus à la réinitialisation des sessions constituent le processus qui engendrent le plus de trafic (environ 40% des messages échangés). Les messages de type *Implicit withdraw* viennent en deuxième position avec près de 38% du trafic BGP généré.

On s'aperçoit, avec ces résultats que les congestions et les défaillances des liens et des

[26] http://www.cert.org/advisories/CA-2003-04.html
[27] http://www.ripe.net/info/ncc/index.html
[28] http://www.cert.org/advisories/CA-2001-26.html

nœuds qui engendrent les phénomènes de réinitialisation de sessions constituent avec les processus des mises à jour des informations de routage les phénomènes qui engendrent un important trafic BGP. Or les propagations des défaillances conduisent souvent à des situations de modification fréquente des informations de routage, de congestion (attaques de type *DOS* par exemple) ou, dans les cas extrêmes à des *crashs* des nœuds du réseau. La modélisation de l'augmentation de charge CPU nécessite des informations de niveau paquet. Le développement d'un simulateur de propagation des pannes entre plusieurs infrastructures et capable de prendre en compte des informations de niveau paquet se révélerait trop complexe et nécessiterait beaucoup de ressources pour fonctionner. Pour faire face à cette difficulté nous nous référons, comme expliqué plus haut dans ce document, au nombre de plus courts chemins qui passent par un nœud et nous utilisons cette valeur pour modéliser le nombre de messages susceptibles de transiter par un routeur.

Étant donné que les augmentations du trafic des protocoles de routage n'entraîne que des augmentations sensibles de la charge CPU des routeurs, nous fixons le seuil acceptable pour l'augmentation du nombre de routes qui passent par un nœud à une valeur relativement élevée (70%) pour la simulation des pannes des routeurs. La valeur de ce seuil, en elle-même n'est pas très déterminante car elle permet juste de voir l'impact de la panne d'un nœud en matière de transfert des charges vers d'autres nœuds. Une valeur trop élevée empêcherait d'identifier des nœuds dont la charge a fortement augmenté à cause de la défaillance d'un autre nœud. Aussi ce système de calcul de la répartition des routes permet d'évaluer le nombre de fausses routes et leur durée de vie, c'est à dire le temps durant lequel les routes d'un nœud qui passent par un voisin déjà en panne n'ont pas été mises à jour. Les scénarios décrits ci-dessus sont valables, à la fois pour les protocoles intra-AS et inter-AS.

5.4.4 Choix de la topologie utilisée pour les simulations

Le dernier défi pour le simulateur proposé est celui du choix de la topologie utilisée. En effet, le réseau Internet compte environ 26000 AS [109] dont 20 à 30% sont des AS de transit. Développer un simulateur pour un réseau de cette taille en tenant compte de l'ensemble des informations relatives aux caractéristiques des réseaux évoquées ci-dessus se révélerait une tâche complexe. Toutes les topologies (générées ou déduites à partir des données réelles) du réseau Internet utilisées actuellement par les chercheurs représentent uniquement les liaisons inter-AS. Puisque notre simulateur doit offrir des possibilités pour évaluer les vulnérabilités liées à l'interconnexion de plus en plus croissante des réseaux dédiés au réseau Internet, une topologie représentant uniquement les liaisons inter-AS est inadaptée. Il faut donc, trouver une topologie représentant aussi bien les réseaux intra-AS que les liaisons inter-AS. Par ailleurs, les graphes utilisés par le simulateur doivent offrir des moyens qui permettent de distinguer les défaillances intra-AS et inter-AS et d'identifier chacun des nœuds, des liens et des AS de la topologie considérée pour savoir exactement les communications qui sont établies via un lien, les nœuds touchés par une défaillance et leurs positions. Pour satisfaire ces contraintes, nous appliquons notre simulateur sur un des graphes générés selon la technique de génération de topologie décrite dans le chapitre précédent de ce manuscrit. Le choix du graphe est basé sur la taille et la représentativité de ce graphe par rapport au réseau Internet. Compte tenu de la nécessité de modéliser des réseaux intra-AS et inter-AS de niveau routeur, il faut que le

graphe présente des caractéristiques d'interconnexions qui soient proches de celles du réseau Internet tout en ayant une taille convenable aux simulations. Le choix du graphe utilisé pour la simulation est fait à partir des résultats obtenus sur l'évaluation des différents scénarios de validation de la technique de génération présentés dans le chapitre 4. Nous utilisons donc les résultats présentés sur les figures 4.17(a) et 4.17(b) représentant des comparaisons des distributions des degrés de quelques graphes générés et du graphe de référence pour sélectionner le graphe le plus proche du graphe de référence, mais ayant une taille convenable aux différents scénarios de simulation. Sur la base de ce critère, nous sélectionnons, à partir des résultats présentés 4.17(b), le graphe de 30 AS. Les résultats présentés dans la section suivante sont obtenus à partir des simulations appliquées à ce graphe composé de 1350 nœuds (30 AS de 45 nœuds). Les scénarios de simulation consistent à sélectionner un nœud initialement défaillant, quelques nœuds immunisés (sélectionnés aléatoirement) et à simuler l'évolution de la défaillance dans le réseau.

5.4.5 Simulations et Résultats

Les résultats présentés dans cette section sont obtenus à partir des simulations basées sur des métriques destinées à évaluer, non seulement la vitesse de propagation et l'ampleur des défaillances, mais aussi la durée nécessaire à l'absorption de ces défaillances lorsqu'il existe des nœuds immunisés dans le réseau considéré. La figure 5.1 présente l'évolution du nombre de nœuds touchés par la défaillance et celui des nœuds immunisés en fonction du temps de la simulation. Ces courbes montrent que peu de temps après la défaillance initiale le nombre de nœuds touchés évolue de manière exponentielle lorsqu'il n'existe pas de nœud immunisé. Dans le cas où le réseau compte des nœuds immunisés, cette évolution se poursuit jusqu'au début de réaction des nœuds immunisés, puis le nombre de nœuds défaillants chute après une durée qui dépend, notamment, du nombre de sauts entre le nœud touché initialement et les nœuds immunisés.

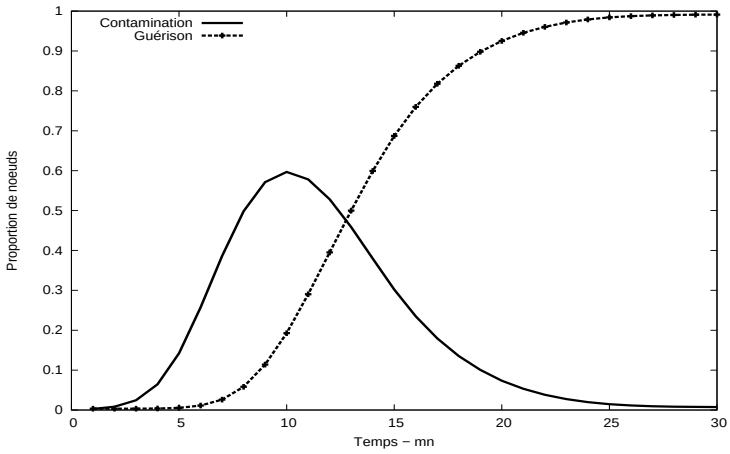


FIG. 5.1 – *Évolution du nombre de nœuds contaminés et rétablis en fonction du temps*

La figure 5.2 montre la durée de vie de la défaillance en fonction de ce nombre de sauts.

Cette figure montre que la durée d'absorption de la défaillance dépend de plusieurs facteurs car elle permet de constater que des défaillances touchant un nœud situé à une distance plus importante par rapport aux nœuds immunisés peuvent être absorbées plus rapidement que d'autres défaillances dont les nœuds initialement touchés sont plus proches des nœuds immunisés. Les autres facteurs déterminants pour la durée d'absorption sont la connectivité du nœud initialement défaillant, les valeurs des temporisateurs des protocoles de routage décrits dans les sections précédentes, les charges des routeurs, etc.

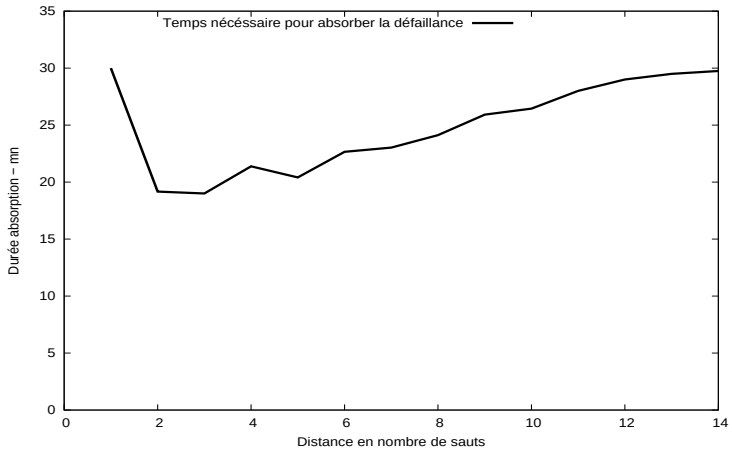


FIG. 5.2 – *Évolution de la durée d'absorption de la défaillance en fonction de la distance entre le nœud initialement défaillant et les nœuds immunisés*

Pratiquement, ce scénario correspond aux phénomènes observés lors d'une corruption des tables de routage par l'annonce de fausses routes (*IP hijacking* par exemple). Les fausses routes enregistrées par les routeurs survivent tant qu'il n'y a pas d'autres routeurs qui disposent de meilleures routes vers les mêmes destinations. Dès que la propagation des mises à jour des tables de routage atteint des routeurs qui possèdent des meilleures chemins vers ces préfixes, ces derniers ne mettent pas à jour leurs tables de routage et propagent, à leur tour ces meilleurs chemins qui remplacent au fur et à mesure les fausses routes déjà enregistrées par d'autres routeurs.

Les résultats décrits ci-dessus sont ceux issus des simulations axées sur l'évolution de la défaillance et le temps nécessaire pour l'effondrement du réseau ou pour l'absorption de la défaillance lorsque des nœuds immunisés permettent de stopper la propagation. Pour évoluer la robustesse topologique du réseau simulé face aux propagations des défaillances, nous effectuons des simulations des pannes des nœuds lorsqu'ils enregistrent de très fortes charges. Comme évoqué dans la section consacrée à la description du simulateur, ces simulations sont fondées sur le transfert des charges entre les nœuds en terme de nombre de chemins. Lorsque l'augmentation de ce nombre de chemins pour un nœud à cause des pannes d'autres nœuds atteint la valeur de 70% de son nombre de chemins à l'état stable ce nœud est supprimé du graphe. Les résultats de ces simulations sont présentés dans les figures 5.3 et 5.4.

La figure 5.3 présente la durée entre le début de simulation et la déconnexion du graphe. Les résultats présentés dans cette figure concernent uniquement les scénarios avec des nœuds

dont la suppression initiale provoque une augmentation du nombre de chemins qui passent par un autre nœud, c'est à dire environ la moitié du nombre total des nœuds qui ont été supprimés lors des simulations. Avec cette figure, on peut voir que la panne de plus de 70% des nœuds de cette moitié provoque la déconnexion du graphe seulement 3 minutes après la panne initiale. Dans cette figure, la proportion des nœuds dont la suppression provoquent la déconnexion du graphe, 1 minute après le début de simulation ne présente que peu d'intérêt car elle concerne généralement les nœuds qui connectent les nœuds feuilles au graphe et une fois ces nœuds sont supprimés le nœud feuille devient isolé et le graphe est considéré comme non connexe même si le nombre de nœuds isolés est très faible.

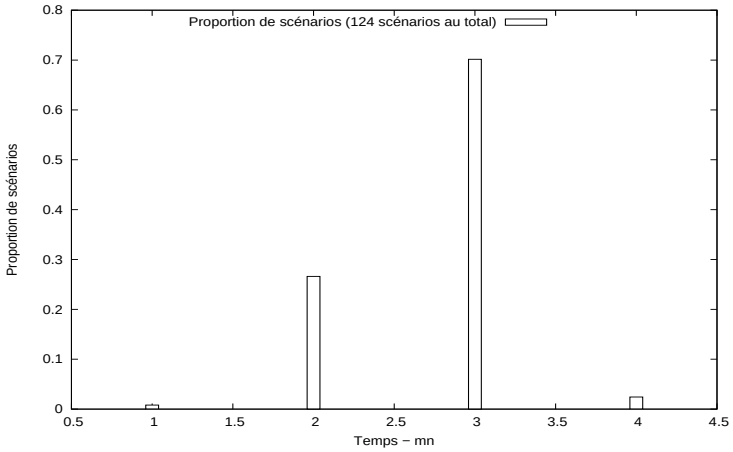


FIG. 5.3 – *Proportion du nombre de scénarios avec des graphes non connexes*

La figure 5.4 montre l'évolution de la durée de vie des fausses routes suite à une défaillance d'un nœud. Pour rappel, les fausses routes apparaissent lorsqu'un routeur est défaillant, mais les autres routeurs ayant dans leurs tables de routage des chemins qui passent par le routeur défaillant n'ont pas reçu un message relatif à cette défaillance pour supprimer les routes impactées. Dans cette figure, on peut voir que la durée maximale se situe toujours en début de simulation et vaut environ $3,5$ minutes. Cette valeur qui correspond aux caractéristiques du réseau simulé, montre qu'il est possible d'avoir une perte de paquets pendant une durée relativement longue lorsqu'il y a une panne de routeur. Après un temps de simulation de $3,5$ minutes, la valeur moyenne de cette durée reste constante pour l'ensemble des simulations. Ceci est dû au fait que le nombre de fausses routes est calculé uniquement si le graphe est connexe et puisque le graphe devient non connexe quelques minutes après le début de la simulation, cette durée n'est plus modifiée jusqu'à la fin de la simulation.

5.5 Conclusion partielle

Le simulateur des propagations des défaillances présenté dans ce chapitre décrit une approche simple pour étudier les propagations des défaillances dans les réseaux de télécommunications. Il se limite à la modélisation des principaux facteurs qui influent ces propagations,

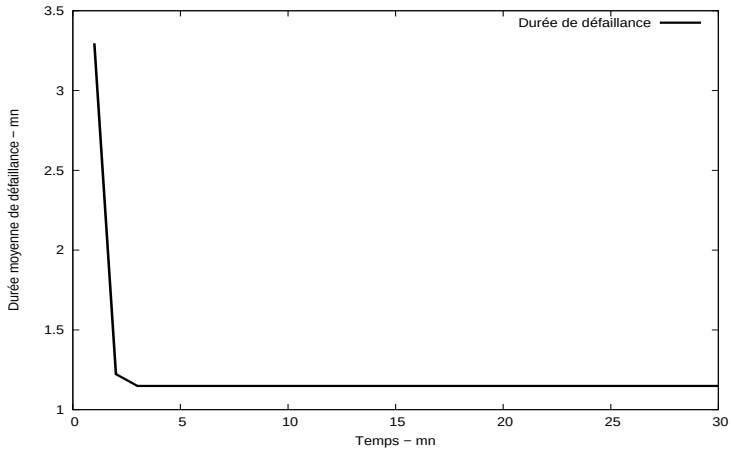


FIG. 5.4 – *Évolution de la durée de vie des fausses routes*

mais il offre un niveau d'abstraction et une flexibilité qui permettent de l'adapter à la plupart des infrastructures susceptibles d'être victimes des propagations des défaillances. Toutefois, il est difficile de trouver un rapport optimal entre le niveau d'abstraction pour réduire la complexité et le nombre de paramètres à prendre en compte dans le simulateur pour être le plus proche possible du fonctionnement réel des infrastructures impliquées dans un simulateur multi-infrastructures. C'est pourquoi le simulateur proposé est fondé sur les graphes pour avoir une base topologique commune adaptée à un nombre important d'infrastructures et offrir la possibilité d'implémenter des caractéristiques fonctionnelles très variées pour couvrir l'ensemble des infrastructures concernées.

Les résultats des simulations présentés dans ce chapitre ont permis, non seulement de valider le simulateur, mais aussi de caractériser les propagations des défaillances dans les réseaux des télécommunications. Ils démontrent que pour les défaillances logicielles, l'existence des nœuds immunisés permet de réduire considérablement la durée de vie d'une défaillance dans un réseau. Ils montrent aussi que la durée d'absorption est étroitement liée à la distance entre le nœud initialement infecté et les nœuds immunisés, du degré de connectivité des nœuds infectés, des paramètres des protocoles de routage. Les simulations décrites dans ce chapitre ont aussi montré que pour les propagations des défaillances matérielles touchant les nœuds du réseau, le temps nécessaire pour l'apparition des zones isolées dans un réseau est relativement court. Cependant, le simulateur se limite à examiner la connexité du graphe sans évaluer le nombre de nœuds déconnectés. Cette faiblesse empêche de faire une distinction entre les déconnexions du graphe qui provoquent l'isolement d'une grande partie du réseau et celles qui provoquent la déconnexion de quelques nœuds qui, dans le cas pratique reste moins grave. La valeur de la durée entre la défaillance initiale et la déconnexion de certains nœuds présentée par la figure 5.3 est une valeur moyenne concernant les déconnexions graves et moins graves, mais cette limite peut facilement être corrigée en calculant, par exemple la taille de chacune des composantes d'un réseau non connexe.

Ces résultats démontrent aussi que la vitesse des propagations des défaillances logicielles croit exponentiellement quelques minutes après le début de la défaillance comme il a été très

souvent le cas lors des propagations des virus informatiques dans les réseaux, notamment celle du virus CODE RED II[29] décrit dans [106]. Ces propagations rapides des défaillances empêchent les opérateurs de prendre les dispositions nécessaires pour réduire leur impact.

Le simulateur des propagations des défaillances proposé étant fondé sur la théorie des graphes, son adaptation pour la simulation des réseaux électriques peut se faire par le développement et l'intégration des fonctionnalités permettant de simuler les caractéristiques dynamiques des réseaux électriques. Pour pouvoir évaluer de manière plus précise l'état de ces réseaux du point de vue des interactions avec les autres infrastructures comme le réseau de télécommunications, le simulateur des réseaux électriques ne doit pas se limiter à la méthode de *DC Load Flow* présentée dans le chapitre 2. Il doit permettre de simuler, par exemple, les calculs de répartition de charge optimaux (*optimal power flow*), des analyses de la stabilité transitoire, la simulation du fonctionnement des générateurs, des lignes électriques et les charges. La mise en œuvre de ces fonctionnalité nécessitent une expertise du niveau des spécialistes, c'est pourquoi nous ne nous étendons pas sur le cas spécifique de l'intégration du réseau électrique dans le simulateur proposé.

Le chapitre suivant présentera une proposition d'approche inspirée des techniques de supervision des réseaux pour permettre une détection rapide des défaillances et, donc de lutter plus efficacement contre leurs propagations dans les réseaux.

[29] http://www.cert.org/incident_notes/IN-2001-09.html

Chapitre 6

Détection des propagations des défaillances à l'aide de l'échange d'informations entre différents réseaux

6.1 Introduction

La dépendance de plus en plus forte des infrastructures critiques aux réseaux de télécommunications et les difficultés liées à la détection des défaillances matérielles et logicielles des réseaux de grande taille et à l'évaluation des conséquences des défaillances de grande envergure impliquant plusieurs réseaux de télécommunications (Internet principalement), obligent à réfléchir sur la mise en place de nouvelles techniques permettant de limiter les conséquences des pannes des réseaux de télécommunications comme Internet sur les autres infrastructures critiques. L'Internet est, par définition le réseau des réseaux et la qualité des services qu'il offre dépend fortement de l'interconnexion des nombreux réseaux qui le constituent. Tout phénomène isolant une partie de ce réseau empêcherait cette dernière d'accéder à la plupart des services Internet et, par conséquent conduirait à une dégradation significative des services. L'échange de trafic et l'inexistence des systèmes de filtrage du trafic entre les différents réseaux de l'Internet favorisent le transfert des flux souillés d'un réseau vers plusieurs autres réseaux. Or traditionnellement les opérateurs des réseaux s'occupent chacun de la protection de sa propre infrastructure. Ils ont des techniques de supervision permettent de détecter, d'isoler, voire d'arrêter la progression d'une défaillance dans les réseaux dont ils assurent la gestion et l'exploitation. Ces techniques de supervision permettent aussi d'avoir des informations très complètes et de pouvoir détecter en temps réel les pannes, mais elles couvrent uniquement des réseaux singuliers alors que les menaces pour chacun de ces réseaux peuvent venir de n'importe quel autre réseau. Pour détecter les défaillances dans l'ensemble des réseaux qui constituent l'Internet, il est nécessaire de concevoir des techniques capables de couvrir plusieurs réseaux tout en tenant compte des nombreuses contraintes liées à la différence des politiques de gestion de ces réseaux et des contraintes temporelles pour le délai la détection de ces défaillances.

Donc, ces techniques, à la différence des systèmes de supervision actuels, doivent tenir compte de toutes ces contraintes et être fondées sur un système permettant aux différents opérateurs d'échanger des informations sur l'état de leurs réseaux. Car, comme le recommandent de nombreux rapports [107, 65, 108] sur la protection des infrastructures critiques, la détection des propagations des pannes dans les infrastructures critiques nécessitent l'échange d'informations entre les différents opérateurs privés et publics en charge de la gestion de ces infrastructures.

D'après les travaux des auteurs de [74], il existe 2 méthodes de détection des pannes dans les réseaux de télécommunications : la méthode utilisant des messages de notification (*heartbeats*) appelée aussi méthode *push* et la méthode de sondes (*polling*) appelée aussi méthode *pull*. Avec la première méthode, la station supervisée envoie périodiquement des messages à une station centrale pour indiquer sa disponibilité. Lorsque la station centrale ou la station de supervision ne reçoit pas de message pendant un intervalle de temps fixé au départ, elle considère que la station supervisée est en panne. Avec la deuxième méthode, c'est la station de supervision qui envoie des requêtes à la station supervisée. A la réception de la requête, la station supervisée doit renvoyer une réponse. A défaut de réponse pendant un intervalle de temps connu, la station supervisée est considérée comme défaillante.

Ces deux techniques conviennent pour des réseaux de petite taille ou encore des réseaux administrativement gérés par un même opérateur, mais leur mise en œuvre dans un réseau de type Internet s'avère difficile, voire impossible à cause, notamment de la manière dont les réseaux qui constituent Internet sont gérés, de la taille du réseau Internet et des contraintes politiques entre les différents réseaux. C'est pourquoi, nous proposons dans ce chapitre, une nouvelle architecture de détection consacrée principalement aux pannes susceptibles de se propager dans les réseaux de télécommunications afin de pouvoir limiter l'impact des propagations des pannes sur les autres infrastructures critiques dépendantes des réseaux de télécommunications.

6.2 État de l'art de la détection des pannes dans les réseaux de télécommunications de type Internet

La lutte contre les propagations des pannes dans les réseaux de télécommunications modernes comme Internet nécessite la mise en place des techniques de détection des pannes efficaces pour détecter ces pannes avec des délais les plus courts possibles afin de pouvoir prendre les mesures nécessaires à leur élimination avant qu'elles n'aient pris des proportions incontrôlables. Puisque ces infrastructures de télécommunications, notamment l'Internet sont des interconnexions de plusieurs réseaux gérés par des opérateurs différents, ces techniques de détection et de lutte contre les propagations des pannes doivent être conçues en tenant compte des contraintes liées, notamment aux politiques de gestion des différents réseaux qui constituent Internet. C'est pourquoi, à l'image de l'échange d'informations de routage entre les différents réseaux, des dispositifs techniques d'échanges d'informations sur les pannes permettraient de détecter et de lutter de manière plus efficace contre les propagations des pannes. Malgré cette nécessité, les actions pour le développement de ces outils sont encore embryonnaires. En effet, de nombreux outils de détection des pannes sont disponibles, mais la détection des pannes simultanées touchant plusieurs réseaux de l'Internet n'est possible qu'avec un accès instantané aux informations concernant l'ensemble des composants défaillants qui, parfois se situent

dans des réseaux différents et géographiquement éloignés les uns des autres, mais qui sont interdépendants. De ce fait il est indispensable de mettre en place des techniques permettant d'alerter les opérateurs des dangers imminents que sont notamment les propagations des virus, les attaques par déni de service de grande ampleur et les autres types de pannes susceptibles de se propager. Actuellement les dispositifs conçus pour limiter les propagations des défaillances dans les réseaux de télécommunications sont constitués, pour la plupart des techniques limitées à des réseaux singuliers ou des organismes administratifs qui ne sont pas assez efficaces pour empêcher la propagation des pannes comme les virus, les attaques des serveurs DNS.

Parmi ces organismes administratifs on peut citer le COSSI (Centre Opérationnel de la Sécurité des Systèmes d'Information) et le CERTA (Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques Informatiques) en France, la commission fédérale des communications (*Federal Communications Commission - FCC*[1]) aux États-Unis et des structures analogues appelées CERT (*Computer Emergency Response Team*) dans de nombreux autres pays. Ces organismes publient des rapports précis sur les défaillances de grande ampleur des infrastructures de télécommunications. Mais ces rapports ne sont accessibles qu'aux membres de ces organismes et aux administrations publiques [1]. Des forums spécialisés sont aussi mis en place dans certains pays, comme TISN (*Trusted Information Sharing Network*)[2] en Australie qui regroupe les propriétaires et les exploitants des infrastructures critiques. Les membres de ce forum partagent les informations relatives à la sécurité de leurs infrastructures, les menaces, les vulnérabilités et les actions à entreprendre pour faire face aux différents défis liés à la sécurité des infrastructures critiques. Compte tenu du moyen d'action utilisé, ces mesures ont des capacités limitées à cause, notamment de la nécessité des accords politiques, administratifs et économiques des membres pour adopter des actions après une panne. Ces accords engendrent des délais très longs et ces types de dispositifs n'offrent aucune garantie sur la mise à disposition des informations sur les incidents en un temps relativement court pour pouvoir entreprendre les actions appropriées pour empêcher les propagations des pannes.

Le développement des services et des technologies Web ont permis l'émergence de nouveaux types de dispositifs comme IT-ISAC (*Information Technology - Information Sharing and Analysis Center*)[3]utilisant les services Web pour publier les informations sur les vulnérabilités des systèmes informatiques et de télécommunications, sur les menaces et les incidents survenues à des infrastructures. Si ces portails Web permettent de se passer des accords évoqués ci-dessus, les informations ne sont publiées que lorsque les membres des portails sont au courant de ces pannes, donc parfois après un délai relativement important. Ces informations publiées après les incidents permettent de prendre des mesures pour empêcher des défaillances de même nature dans le future, mais ne contribuent pas à freiner ou à stopper la propagation de la défaillance en question.

Une autre catégorie d'outils disponibles utilise aussi les services Web, mais ces portails sont plus spécialisés et l'accès aux informations est réservé aux opérateurs préalablement enregistrés. Par exemple, MIT (*Middleware Improved Technology*) [60] développé, en 2009, dans le cadre du projet IRRIIS est l'une des techniques de cette catégorie. Il s'agit d'un portail utilisant les services Web et qui permet de gérer des groupes qui s'enregistrent pour accéder à

[1] http://www.fcc.gov
[2] http://www.tisn.gov.au/
[3] https://www.it-isac.org/

des services précis. Une fois enregistré, un opérateur peut visualiser les incidents publiés, créer des nouveaux incidents et obtenir un aperçu général d'un réseau. Les informations publiées se limitent aux réseaux électriques et de télécommunications. SDX (*System Data Exchange*)[4], le système d'échange d'informations entre opérateurs des réseaux électriques nord américains mis en place par le NERC[5] fonctionne aussi sur la base d'un portail Web où les opérateurs des centres de contrôle enregistrés publient des informations très précises sur les composants de leurs réseaux affectés par des défaillances. Les informations comprennent, entre autres : l'infrastructure, les composants touchés, la date, l'heure, la sévérité, l'ampleur et la description de l'incident.

Ces deux derniers outils offrent des possibilités intéressantes, les informations sont précises et convenables pour la plupart des actions que doivent entreprendre les opérateurs des infrastructures concernées. Leurs limites concernent la synchronisation entre les défaillances, la publication des informations sur ces défaillances et l'accès à ces informations par les opérateurs tiers. En effet, les informations sur les défaillances ne sont publiées que lorsqu'il existe des informations précises sur les défaillances, généralement après que ces défaillances soient déjà éliminées et l'accès à ces informations par les autres opérateurs peut se faire avec un retard très important par rapport au début de ces défaillances. Donc ce type d'outils n'est adapté que pour des infrastructures où la propagation des défaillances est lente, comme les réseaux électriques, mais ne convient pas à des infrastructures comme les réseaux de télécommunications où le délai de propagation des pannes est de l'ordre de quelques secondes à quelques minutes.

Pour faire face aux difficultés liées à l'obtention des informations sur les défaillances des infrastructures, certains chercheurs utilisent les rapports publics pour étudier les propagations des pannes dans ces infrastructures. Mais les informations contenues dans ces rapports sont, en général insuffisantes et non précises, les auteurs de [71], par exemple utilisent 347 rapports publiés entre 1994 et 2005 par le forum pour l'analyse des risques de l'ACM (*Association for Computing Machiner's RISKS*[6]) pour caractériser les pannes des réseaux de télécommunications en terme d'origine, d'impact et d'évolution temporelle et spatiale. Leurs résultats montrent que 65% des pannes sont des pannes logicielles, 68% d'entre elles ont un impact majeur sur les autres infrastructures et 21% impactent la sûreté publique. Dans le cadre de sa thèse, l'auteur de [79] analyse l'ensemble des incidents survenus sur le réseau Internet entre 1989 et 1995 et reportés au centre des services de prévention des risques et d'assistance aux traitements d'incidents (*Computer Emergency Response Team - CERT*) des États-Unis pour développer une taxonomie pour la classification des attaques et autres incidents du réseau Internet et l'élaboration d'un ensemble de recommandations pour améliorer la sécurité de l'Internet. L'article [32] définit une classification des défaillances Internet, mais limitée uniquement aux attaques. Les auteurs de cet article montrent que ces attaques peuvent être classées en 4 catégories : les attaques des serveurs DNS, les corruptions des tables de routage, les attaques par déni de service et la prise de contrôle de certains routeurs pour provoquer des traitements incorrects des paquets pouvant conduire à des boucles et à des congestions par exemple.

Dans [30], les auteurs proposent d'étendre le logiciel de simulation des grilles de calcul

[4] http://www.nerc.com/docs/oc/sdx/SDX_CoS_010.pdf
[5] http://www.nerc.com/
[6] The RISKS Forum : http://catless.ncl.ac.uk/Risks

informatique GridSim[7] pour la détection des défaillances des ressources matérielles et logicielles constituant la grille de calcul tout en tenant compte des caractéristiques distribuées et la différence des politiques de gestion de ces ressources qui appartiennent à différents réseaux. Leur technique de détection de défaillance est fondée sur la maintenance d'une liste des ressources utilisées par chaque utilisateur et l'envoi périodique des messages sondes à l'ensemble des ressources utilisées pour pouvoir détecter les ressources défaillantes, c'est à dire celles qui ne répondent pas aux messages.

Les auteurs de [132] recensent l'ensemble des publications scientifiques consacrées aux techniques de détection des virus et vers informatiques dans le réseau Internet avant 2002. Bien que cet article présente une bibliographie très riche, il se limite uniquement aux travaux consacrés aux propagations des virus et vers informatiques.

L'article [74] présente des travaux plus adaptés à la détection des propagations des défaillances dans le réseau Internet. Les auteurs de cet article exposent aussi les différentes contraintes pour la conception d'une technique de détection de défaillances dans un réseau distribué, notamment la nécessité d'éviter d'inonder le réseau par des messages destinés uniquement à la détection des défaillances, le passage à l'échelle, la perte des paquets et la généricité pour pouvoir prendre en charge différents protocoles et applications, les fréquents changements de topologie du réseau et la sécurité des communications. Ensuite ils identifient les différentes techniques actuellement utilisées, notamment la technique *Globus Toolkit* [134] qui consiste à déployer des moniteurs et des collecteurs de données. Les moniteurs surveillent la machine sur laquelle ils sont installées ainsi que les processus qui tournent sur cette machine. Ces moniteurs transmettent périodiquement les informations sur l'état des composants aux collecteurs qui identifient les ressources défaillantes et les notifient à l'application *Globus Toolkit*. La deuxième technique exposée dans cet article est une approche hiérarchique basée sur une structure en arbre et proposée par les auteurs de [58]. Cette technique est constituée de détecteurs des défaillances qui supervisent un ensemble d'objets d'un sous-réseau. Ces détecteurs de défaillances des différents sous-réseaux échangent des messages entre eux et fournissent des informations sur les défaillances aux postes clients qui collectent l'ensemble des informations. La troisième technique est celle fondée sur le protocole appelé *Gossip-style protocol* [70, 141] et qui comprend deux variétés : le *Gossip* de base (*basic gossiping*) et le *Gossip* hiérarchique (*multi-level gossiping*). Pour rappel, le terme *Gossip* désigne une rumeur, en particulier sur les affaires personnelles ou privées des autres. Il constitue l'un des moyens les plus anciens et le plus courant de partage (non prouvé) des faits et des opinions, mais il a également une réputation pour l'introduction d'erreurs et d'autres variations dans les informations transmises[8]. Donc, c'est moyen non sûr d'échanger des informations. Dans le *Gossip* de base, il existe un détecteur de défaillance pour chaque station du réseau. Chaque détecteur maintient une liste de l'ensemble des détecteurs avec lesquels il communique avec une entrée pour un compteur des messages *heartbeats* utilisé pour la détection des défaillances. Un détecteur sonde aléatoirement d'autres détecteurs, incrémente le compteur de *heartbeats* et transmet sa liste aux autres détecteurs. Chaque détecteur qui reçoit une liste compare celle-ci avec sa liste et stocke une nouvelle liste avec le maximum de compteur de *heartbeats* pour chaque membre. Si la

[7] http://www.buyya.com/gridsim/
[8] http://en.wikipedia.org/wiki/Gossip

valeur du compteur de *heartbeats* d'un membre A maintenu par un détecteur B n'augmente pas jusqu'à l'expiration d'un temporisateur, la station qui héberge le module de détection B est considérée défaillante. Pour assurer le passage à l'échelle, le *Gossip* hiérarchique utilise la structure hiérarchique de l'Internet. Les messages à l'intérieur d'un sous-réseau sont échangés avec le *Gossip* de base et seulement un nombre limité de messages est échangé entre les différents sous-réseaux, puis un nombre encore moins important de messages est échangé entre les différents domaines du réseau Internet. La technique proposée dans [37] s'intéresse à la qualité des détecteurs des défaillances, particulièrement au délai de détection des défaillances et à leurs capacités d'éviter des fausses-détections dans un système avec certaines distributions de probabilités de perte pour les messages. Les auteurs de cet article proposent un algorithme qui s'adapte aux changements de la topologie et de l'état du réseau pour améliorer la performance et la fiabilité des détecteurs des défaillances. Dans le protocole de détection des défaillances proposé dans [59], les processus se supervisent entre eux par échange de messages avec acquittement. Avec ces protocoles, les processus utilisent trois primitives (*SEND*, *RECEIVE*, *QUERY*) pour envoyer des messages, recevoir des messages et envoyer des requêtes à des moniteurs suspects. Lorsqu'un moniteur qui envoie un *QUERY* ne reçoit pas de réponse jusqu'à l'expiration d'un temporisateur, il considère que le moniteur destinataire de la requête est défaillant. Ce protocole vise essentiellement à réduire le nombre de messages échangés entre les moniteurs. Enfin, la technique proposée dans [130] utilise un algorithme fondé sur le consensus pour réduire le nombre de messages échangés par les moniteurs et améliorer la performance du protocole de détection des défaillances.

Dans l'article [113], les auteurs définissent un ensemble de critères pour comparer les différentes techniques de détection des défaillances et utilisent ces critères pour évaluer les principales techniques de supervision dans un réseau distribué de grande taille. Ces critères sont basés sur l'exactitude de la technique, c'est-à-dire la capacité de la technique à éviter des fausses-détection, l'exhaustivité ou sa capacité à détecter toutes les défaillances, la performance ou sa capacité à réduire le nombre de ressources utilisées, sa flexibilité par rapport aux topologies et aux conditions du réseau et le passage à l'échelle de la technique de détection. Leurs résultats montrent qu'avec toutes les techniques comme [151] où n'importe quel moniteur qui détecte une défaillance est capable d'envoyer une notification, il est possible de maintenir le temps de détection constant même si la taille du réseau augmente. Ils ont aussi montré que dans les réseaux de grande taille, les algorithmes flexibles sont plus fiables que ceux dont les temporisateurs sont fixes et ceux qui nécessitent une topologie stable.

6.3 Limites des outils existants pour la détection des propagations des pannes

Les techniques présentées ci-dessus conviennent à des infrastructures dans lesquelles la propagation des défaillances est relativement lente, à des réseaux de petite taille et où les différences de politiques de gestion entre les réseaux ne sont pas prises en compte. En effet, l'utilisation des informations mises à dispositions par les organismes comme les CERT impliquent des délais importants et des détections des défaillances non automatisées. Par conséquent, elles ne permettent pas de lutter efficacement contre les propagations des défaillances

dans les infrastructures de type Internet où les défaillances se propagent très rapidement et où il est impossible de rendre disponibles des informations détaillées sur l'ensemble des ressources matérielles et logicielles du réseau. A titre d'exemple, lors de la diffusion du virus informatique NIMDA[9] en 2001, une augmentation exponentielle des avertissements BGP avaient été constatée. En deux heures environ, le moniteur *rrc*00 (moniteur déployé par RIPE NCC[10], situé à Amsterdam) enregistre un nombre d'avertissements qui passe de 400 par minute à 200000 par minute. Lors de la panne électrique d'août 2003 aux États-Unis et au Canada, le rapport de l'enquête [63] conduite conjointement par des experts Américains et Canadiens indiquent, parmi les causes du blackout, l'utilisation des données erronées par le centre de coordination MISO (*Midwest Independent System Operator*) chargé de coordonner 37 centres de contrôle de la région centre-ouest des États-Unis. En effet, le rapport indique que l'utilisation des données non temps réels par ce centre de coordination avait empêché de se rendre compte de la défaillance de la ligne $345kV$ reliant Stuart et Atlanta de la société *Dayton Power and Light*. Ceci a conduit à une estimation fausse de l'état du système et à l'absence d'avertissement à l'opérateur *FirstEnergy* du risque lié à cette défaillance. Ce manque de communications entre les centres de coordination et les opérateurs a considérablement contribué à la propagation des pannes et à l'écroulement du réseau. Ces exemples de pannes montrent que des outils comme SDX[11] ou MIT ne sont pas efficaces lorsque la propagation des défaillances est rapide et ne permet pas la mise en place d'une véritable coordination entre les organismes comme les CERT. Leurs limites sont, entre autres, le manque de synchronisation pour la mise à disposition des informations immédiatement après le début des pannes à cause de l'absence de contrainte temporelle sur l'accès aux informations et la mise à jour des bases de données. Ce qui fait que les informations disponibles ne sont pas temps réel ou lorsque ces informations sont disponibles à temps, les opérateurs qui en ont besoin ne sont pas alertés pour qu'ils puissent entreprendre des actions appropriées.

Les techniques basées sur le déploiement des moniteurs ne comportent pas les carences décrites ci-dessus, elles fonctionnent très bien pour un réseau géré par un même opérateur. Mais elles présentent de nombreuses limites dans le contexte des interdépendances à cause du fait qu'elles soient incapables de prendre en compte les différences politiques des différents systèmes autonomes et qu'elles nécessitent de déployer des moniteurs pour chaque entité à superviser de toutes les infrastructures impliquées, ce qui peut être difficile à mettre en œuvre pour des infrastructures qui ont déjà leur propre système de supervision. Pour un réseau de grande taille, les systèmes avec moniteurs comme la technique proposée dans [134] peuvent se révéler trop coûteux car la diffusion des informations par chacun des moniteurs peut engendrer un trafic important. Quant à celle exposée dans [58], elle est fondée sur une structure en arbre fixe et permet, donc de réduire le trafic engendré par les moniteurs, mais ne s'adapte pas à la topologie de l'internet et ses changements fréquents. *Gossip* [141] ne fonctionne pas lorsqu'un grand nombre de composants est défaillant. Durant certaines périodes de congestion, les messages *heartbeats* peuvent être perdus et il est possible d'avoir des délais importants qui peuvent conduire à une erreur d'interprétation. Enfin, les techniques [37] et [59] sont fondées sur les applications et, par conséquent dépendent fortement de celles-ci. Cette dépendance rend

[9] http://www.cert.org/advisories/CA-2001-26.html
[10] http://www.ripe.net/info/ncc/index.html
[11] http://www.nerc.com/docs/oc/sdx/SDX_CoS_010.pdf

ces techniques non flexibles et, donc difficilement adaptables à d'autres infrastructures, voire à d'autres réseaux de télécommunications avec de nouvelles applications.

Or, chaque opérateur d'un réseau particulier connecté à l'Internet dispose des moyens techniques lui permettant d'assurer la supervision de l'ensemble de son réseau. Ces différents opérateurs échangent aussi certaines informations concernant leurs réseaux pour l'acheminement du trafic. C'est le cas des informations sur le routage que certains opérateurs publient sur des sites à accès public fournissant des base de données contenant des informations sur le routage Internet de nombreux réseaux et appelés IRR (*Internet Routing Registry*) comme RIPE (Réseau IP Européen)[12], RADb[13] et EASYNET[14]. Ainsi, selon les auteurs de [36], en mai 2001 76,3% des 2673 AS enregistrés sur RADb[15] et 93,6% des 4492 AS enregistrés sur RIPE publient des informations relatives aux politiques de routage. Pour la plupart de ces IRR, l'enregistrement pour la publication de ces informations de routage par les opérateurs n'est pas gratuit, chez RADb par exemple le prix varie entre 395 et 495 dollars américain selon que l'opérateur soit à but lucratif ou non.

Par conséquent, il est tout à fait possible qu'un opérateur qui détecte une anomalie dans son réseau puisse avertir ses voisins (réseaux auxquels il est connecté) pour que ces derniers puissent filtrer ce flux par exemple. Le principal défi consiste à définir les règles de cet échange, notamment celles qui concernent le type d'informations échangées, la périodicité et les acteurs car il serait difficile, voire impossible que les opérateurs de tous les réseaux de l'Internet échangent des informations entre eux. Toutefois la structure hiérarchique du réseau Internet offre la possibilité de réduire significativement le nombre d'échanges, comme cela se fait avec les échanges BGP. Dans ce contexte, la détection des pannes consiste à concevoir une technique qui permet à chaque opérateur de communiquer l'état de son réseau obtenu à partir de son propre système de supervision à un ou plusieurs collecteurs d'informations issues des différents réseaux impliqués et qui auront une vision générale sur l'ensemble de ces réseaux.

La réutilisation des informations de supervision permet de surmonter l'ensemble des difficultés évoquées ci-dessus, car cette technique ne nécessite pas le déploiement de moniteur pour l'ensemble des entités supervisées des infrastructures impliquées. Ce choix permet, à la fois de réduire le nombre de messages échangés et d'offrir à l'opérateur de chaque réseau de choisir là où sera installé le module qui transmettra les informations au collecteur et de contrôler les informations que ce module doit communiquer au collecteur.

6.4 Description de l'architecture de détection des propagations des défaillances multi-réseaux proposée

6.4.1 Introduction

Pour protéger les réseaux contre les propagations des pannes, il est nécessaire de disposer de techniques efficaces de détection de ces défaillances quelque soit le nombre de réseaux

[12] http://www.ripe.net/
[13] Routing Assets DataBase
[14] http://http://lg.easynet.net/lg.php
[15] http://www.ra.net

impliqués et la vitesse de propagation de ces défaillances. Or les débits des réseaux sont de plus en plus importants, l'avènement des commutateurs haut débit et les fibres optiques ont permis d'atteindre des débits au delà du Gigabit par seconde (10 Terabits par seconde pour les records en laboratoire de recherche [69]). La vitesse de propagation de certains types de défaillances, est étroitement liée à l'état du réseau comme les débits réels et l'existence ou non des congestion. Par conséquent, la propagation des défaillances dans les réseaux avec des débits de l'ordre de Terabit peut être très rapide et il est possible que cette rapidité empêche toute coordination entre opérateurs pour stopper rapidement cette propagation. A titre d'exemple, lors de la propagation du virus CODE RED II[16], les calculs effectués par les auteurs de [106] ont démontré, à partir des informations disponibles sur le site Web de CAIDA[17], que la vitesse de la progression du virus était environ de 300 hôtes contaminés par minute. Les attaques de type *DOS*, par exemple, peuvent viser simultanément plusieurs cibles et utiliser un nombre important d'ordinateurs (*botnet*) appartenant à des réseaux différents, ce qui montre que les menaces peuvent venir de partout et chaque ordinateur vulnérable du réseau constitue une menace pour la sécurité de tous les autres systèmes connectés. Aussi, la nécessité de disposer des informations temps réels sur les défaillances rend indispensable la mise en place d'une technique de détection qui couvre l'ensemble des réseaux impliqués, ce qui nécessite donc un échange d'informations entre les différents opérateurs de ces réseaux. Ce besoin d'échange d'informations entre opérateurs a été identifié depuis plusieurs années, notamment dans le cadre du rapport de la PCCIP publié en 1997 qui prône un partenariat entre les opérateurs (*Public Private Partnership - PPP*). Le principal frein à la conception d'une technique de ce type est la complexité nécessaire à la prise en compte des différentes politiques entre les opérateurs des réseaux, le trafic qu'un système de supervision qui couvre tout le réseau Internet peut engendrer, la réticence des opérateurs à communiquer les défaillances de leurs réseaux et à déployer un système de détection unique qui remplacerait tous les systèmes de supervision actuels.

La solution technique qui permet de satisfaire toutes ces contraintes est la mise en place d'un système permettant, sous réserve d'un accord préalable entre les opérateurs des différents réseaux concernés, d'échanger automatiquement et périodiquement des informations sur l'accessibilité de certains équipements critiques et leurs états, c'est à dire de communiquer les informations sur la détection d'une menace susceptible de provoquer des pannes en cascade. Par exemple, une simple commande « ping » d'un équipement permet de connaître si un équipement est accessible ou non et l'envoi de la valeur du RTA (*Roundtrip Time Average*) à d'autres opérateurs leur permettrait d'évaluer l'état d'un réseau tiers, comme la congestion. Un échange d'informations limité uniquement à l'accessibilité d'un équipement et à la détection d'un équipement victime d'une défaillance permet de réduire le trafic échangé, de ne pas divulguer des informations confidentielles et d'éviter la dégradation de performance et l'utilisation importante des ressources que provoquent les systèmes de supervision applicative comme NetFlow[18] et IPFIX (*IP Flow Information Export*)[19]. En effet, l'expérience montre que ce type de logiciels de supervision applicative provoque des surcharges de la mémoire et une dégradation de la performance du routage et du traitement à cause de la nécessité de traiter les paquets.

[16] http://www.cert.org/incident_notes/IN-2001-09.html
[17] http://www.caida.org
[18] http://www.cisco.com/web/go/netflow
[19] http://www.ietf.org/dyn/wg/charter/ipfix-charter.html

Ces logiciels peuvent aussi faciliter les attaques visant les équipements supervisés à cause de la visibilité des informations sur la couche IP. Une autre contrainte majeure est la nécessité que le système soit suffisamment générique pour être capable de fonctionner dans un environnement fortement hétérogène pour couvrir différents réseaux et permettre l'intégration d'autres infrastructures comme les réseaux électriques. Par exemple l'échange des informations sur les défaillances doit pouvoir se faire entre des infrastructures qui utilisent différents logiciels de supervision comme Nagios[20] pour les réseaux de télécommunications et DNP[21] pour les réseaux électriques.

Pour satisfaire les contraintes évoquées ci-dessus, nous proposons dans ce chapitre une architecture de détection de pannes fondée sur la collecte des informations temps réels sur les infrastructures fournies par différents logiciels de supervision. La technique proposée est définie suivant une architecture client-serveur constituée de deux programmes distincts capables de communiquer à distance pour échanger des données préalablement spécifiées avec pour principal objectif de :

- Permettre une détection rapide des menaces de pannes en cascade et la réduction significative de leurs conséquences
- Couvrir plusieurs infrastructures gérées par différents opérateurs
- Offrir la possibilité de contrôler l'accès aux différentes informations et de sécuriser les données échangées
- Réduire le trafic échangé pour la détection des pannes
- Être suffisamment générique pour être capable de couvrir des infrastructures hétérogènes

6.4.2 Contraintes techniques

Avant la description de l'architecture proposée, nous présentons une synthèse des contraintes techniques qui influent sur la conception du système proposé. Lors de la conception de tout système de communication entre des réseaux administrés par des opérateurs différents, la première contrainte qui apparaît est la nécessité, pour chacun des opérateurs impliqués d'appliquer ses propres règles pour lui permettre de garder un contrôle de ses systèmes matériels et logiciels et pour sélectionner les données qu'il communique aux autres opérateurs. Cette contrainte est purement fonctionnelle et permet aux opérateurs d'avoir un contrôle total et un libre choix sur les données qu'ils communiquent.

La deuxième contrainte est celle relative aux ressources matérielles. En effet, la plupart des composants matériels et logiciels des infrastructures opèrent généralement à la limite de leurs capacités pour des raisons économiques, un système destiné uniquement à la réduction des pannes en cascade (sans retour direct sur investissement) doit nécessiter le moins de ressources possibles. Par exemple, pour le cas particulier des réseaux de télécommunications, l'utilisation de la fibre optique dans les réseaux de cœur a permis d'atteindre des débits très élevés, aujourd'hui le principal facteur de limitation des débits est la capacité des routeurs et commutateurs. Par conséquent, même si l'état de ces routeurs constituent un facteur important dans la lutte contre les pannes en cascade, il serait trop pénalisant de déployer sur ces routeurs un système trop consommateur de ressources qui réduirait leur performance.

[20] http://www.nagios.org
[21] http://www.dnp.org/

La troisième contrainte est celle qui concerne la fréquence des communications pour transmettre des informations sur l'état de l'infrastructure. Une fréquence élevée permet de détecter plus rapidement les pannes, mais engendre plus de trafic alors qu'une fréquence trop basse conduirait à une estimation erronée de l'état de l'infrastructure concernée. Une telle erreur sur l'estimation de l'état d'une infrastructure peut avoir un impact négatif lorsqu'elle est victime d'une défaillance. À tire d'exemple, dans le rapport [63] sur la panne électrique du 14 août 2003 aux États-Unis, les auteurs soulignent que l'estimation erronée de l'état du réseau par le centre de contrôle de l'organisation régionale du réseau de transport du Midwest (*MISO*) a contribué fortement à l'aggravation de la panne. Cette fausse estimation a été causée par un dysfonctionnement de l'estimateur de l'état du réseau qui, à partir des données temps réel du réseau électrique fournit un modèle informatique qui indique le fonctionnement normal ou la défaillance du réseau. Dans le fonctionnement normal, les données sur le réseau sont mises à jour toutes les 5 minutes, mais suite à l'interruption du fonctionnement automatique de l'estimateur de l'état, les informations sur l'état du réseau n'ont pas été mises à jour et le modèle présenté était fondé sur des données obsolètes. Ce qui démontre que même s'il faut limiter le trafic des données échangées, il est nécessaire de réduire l'intervalle de temps des échanges d'informations pour que les données collectées reflètent, à chaque instant l'état réel des infrastructures.

La dernière contrainte que nous abordons dans cette section est la nécessité pour le système de fonctionner sur des environnements hétérogènes et de traiter des informations de différents types. En effet, même si le système développé ne concerne, pour le moment que les réseaux de télécommunications, il est possible qu'il soit étendu pour permettre l'échange d'informations entre infrastructures hétérogènes, par exemple entre les opérateurs des réseaux électriques et les réseaux télécommunications. Par conséquent le système ne doit pas être conçu uniquement pour le trafic IP et doit permettre de transmettre et recevoir des informations concernant aussi bien les routeurs IP que des générateurs et transformateurs des réseaux électriques par exemple.

6.4.3 Réalisation logicielle

Dans cette section, nous exposons les choix qui ont été faits pour la conception et la réalisation de l'architecture proposée sur la base des contraintes évoquées dans la section précédente. L'architecture retenue est l'approche client-serveur, ce choix offre de nombreux avantages. Avec l'approche client-serveur, on peut facilement choisir les entités impliquées dans un échange, de contrôler les informations échangées et de gérer les acteurs impliqués pour chaque accord d'échange d'informations établi. Ainsi chaque opérateur peut choisir d'échanger des informations avec un ou plusieurs autres opérateurs et, donc peut sélectionner les informations qu'il est disposé à communiquer alors qu'une approche pair à pair aurait permis, par exemple à un opérateur tiers de récevoir des informations destinées à un autre opérateur. Pour le système actuellement implémenté, le contrôle d'accès est réalisé à l'aide de l'adresse IP de l'hôte client et le stockage des informations qu'un opérateur souhaite communiquer dans un fichier placé dans un répertoire spécifique. Cependant, il est possible que ces informations soient stockées sous une autre forme, par exemple dans une base de données et de renforcer le contrôler d'accès en utilisant des techniques d'authentification forte et de procédés spécifiques pour accéder aux informations, par exemple la technique PolyOrBAC décrite dans l'article [13]. Ce fichier est ré-

gulièrement mis à jour par le logiciel de supervision du réseau concerné. Avec cette technique, le programme qui transmet les informations à d'autres opérateurs ne nécessite pas une installation obligatoire sur le composant supervisé. Cette démarche offre un large choix sur l'hôte qui héberge ce programme. On peut ainsi l'installer directement sur l'hôte à partir duquel le réseau est supervisé ou sur un hôte dédié à cette tâche pour séparer la supervision interne du réseau et le système d'échange d'information dédié à la détection des pannes inter-réseaux. Lorsque ce programme est hébergé par l'hôte à partir duquel le réseau est supervisé, l'architecture proposée ne génère aucun trafic supplémentaire entre la station de supervision du réseau et les équipements supervisés. Dans ces conditions, le système proposé se greffe simplement au système de supervision existant du réseau pour transmettre les données sélectionnées à partir des informations fournies par le système de supervision local.

La réutilisation des informations fournies par les logiciels de supervision comporte certains inconvénients, notamment l'impossibilité de pouvoir contrôler la pertinence des informations sur l'état des composants fournies par ces logiciels, donc l'incapacité de détecter les faux-positifs et les faux-négatifs. Le fait de réutiliser les informations collectées par les logiciels de supervision des infrastructures impliquées empêche le centre de supervision de déployer son propre système de supervision sur les composants des infrastructures. Par conséquent, la pertinence des informations sur l'état des infrastructures dépend des logiciels de supervision interne des infrastructures. Mais malgré ces inconvénients, la réutilisation des logiciels de supervision offre des avantages qui dépassent largement ses défauts. Elle permet, par exemple de contourner le problème lié à la réticence des opérateurs de déployer de nouveaux systèmes de supervision qui transmet des informations à des entités externes. Cette option permet aussi de limiter le trafic supplémentaire au seul trafic engendré par l'échange d'informations entre les opérateurs impliqués. Avec une simple variable, il est possible de paramétrer l'intervalle de temps entre deux connexions successives qui permet au programme client de récupérer les informations transmises par le serveur et de limiter le trafic entre les deux réseaux impliqués au strict nécessaire. Notre système assure uniquement l'échange des données et ne procède à aucun traitement spécifique des informations, ce qui limite l'utilisation des ressources mémoire et de CPU à une proportion très faible. Le chiffrement des données peut être fait avec le protocole SSL (*Secure Sockets Layer*). L'implémentation est faite avec le langage C dont le choix est le résultat d'un compromis entre portabilité et rapidité d'exécution.

Le déploiement de l'architecture proposée peut être distribué ou centralisé. Dans le premier cas, les modules client et serveur sont installés sur chaque infrastructure participant qui peut à la fois recevoir et transmettre des informations dédiées à la détection des défaillances. Ce type de déploiement présente de nombreux avantages comme la tolérance aux pannes et la répartition du trafic engendré sur différentes liaisons. Les inconvénients de cette approche sont, principalement liés à la complexité liée au contrôle de la qualité des informations échangées puisque chaque entité envoie et reçoit des informations de sa propre initiative et la mise en place d'une structure de contrôle qui couvre l'ensemble des infrastructures peut être délicat lorsque le nombre d'infrastructures est important.

Le deuxième type de déploiement consiste à déployer sur les infrastructures impliquées seulement le module serveur qui transmet les données de chacune des infrastructures à un seul poste sur lequel est installé le module client qui collecte ces données. Cette deuxième approche est plus facile à mettre en œuvre et offre l'avantage lié à la simplicité de gestion et de

contrôle des informations collectées car elles sont toutes stockées sur un même hôte qui peut être géré par une structure indépendante qui assure le contrôle des informations fournies par l'ensemble des infrastructures impliquées. Le principal inconvénient de l'approche centralisée est la vulnérabilité du centre de supervision face aux pannes et attaques et les risques liés au fait qu'une seule organisation ait accès à l'ensemble des informations concernant plusieurs infrastructures.

6.4.4 Environnement de test

A l'issue de l'implémentation de l'architecture proposée, il était nécessaire de choisir une plateforme de test convenable en terme de topologie, de protocoles de communication et de système de supervision. L'environnement de test utilisé est un réseau virtuel composé de 5 AS avec 6 nœuds pour chacun des AS. La topologie utilisée est obtenue avec la technique décrite dans le chapitre 5 et est présentée sur la figure 6.1.

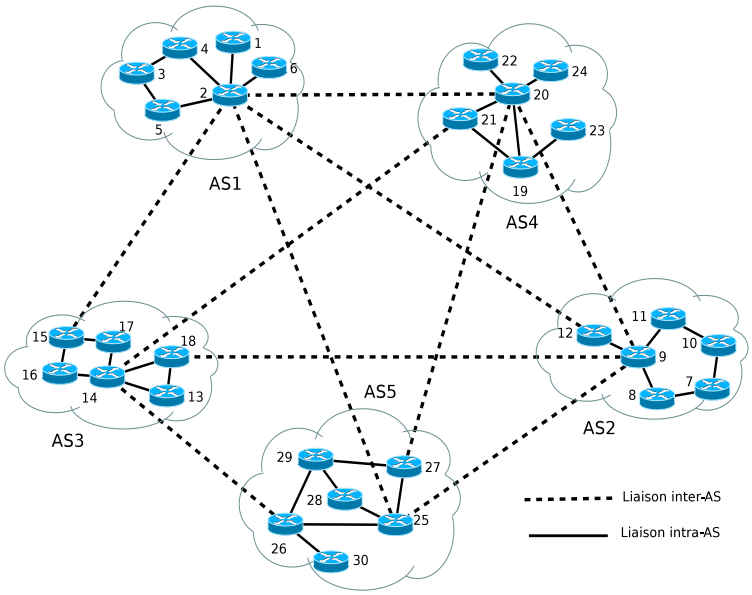


FIG. 6.1 – *Topologie du réseau de test*

Le réseau est construit avec le logiciel de virtualisation NetKit[22]. NetKit[23] est basé sur UML (*User Mode Linux*)[24] et permet d'émuler facilement un réseau sur une seule machine physique. Il offre l'avantage de permettre de configurer avec une grande simplicité un réseau composé aussi bien de routeurs BGP que de routeurs RIP. Cette configuration se fait avec un fichier qui décrit la topologie de niveau liaison du réseau et plusieurs autres fichiers de configuration identiques à ceux que l'on rencontre dans les réseaux réels. Nous avons développé des scripts Perl qui permettent de générer ces fichiers, à partir du graphe fourni par la technique de

[22] http://wiki.netkit.org/index.php/Main_Page
[23] http://wiki.netkit.org/index.php/Main_Page
[24] http://user-mode-linux.sourceforge.net/

génération de topologie, pour obtenir un réseau constitué de machines virtuelles correspondant à ce graphe et composé des routeurs (RIP et BGP) et des liens intra-domaines et inter-domaines. La lenteur est le principal défaut que l'on reproche à tous les logiciels de virtualisation basés sur UML comme NetKit[25]. Cette faible performance constitue un handicap important pour les systèmes visant à tester les performances d'un protocole ou d'un système, mais elle a un impact très limité sur notre système dont le but se limite au test de bon fonctionnement du système de détection des défaillances. A cause des contraintes de ressources matérielles et de temps, notre système a été testé sur une topologie de taille relativement limitée. Néanmoins, nous avons choisi cette topologie de manière à couvrir les facteurs qui sont déterminants pour notre système, c'est à dire de manière à ce qu'on ait des réseaux assez représentatifs des réseaux de type Internet en terme de fonctionnement, notamment les protocoles de routage. Pour effectuer nos tests, nous avons utilisé le logiciel de supervision nagios[26]. Un serveur nagios est installé pour chaque AS et assure la supervision de tous les routeurs de l'AS où il est installé. Les services supervisés se limitent à l'accessibilité de l'hôte supervisé, c'est à dire la durée moyenne d'une requête ICMP *ECHO* entre la station de supervision et le routeur supervisé et, pour certains routeurs le trafic de certaines interfaces ethernet. Ce choix s'explique par le besoin de limiter le trafic échangé entre différents AS et celui de démontrer qu'il est possible de sélectionner une grande variété de services à superviser pour faciliter la détection des pannes. L'environnement de test est présenté sur la figure 6.2, le logiciel nagios est installé sur les nœuds 2, 8, 14, 19 et 26.

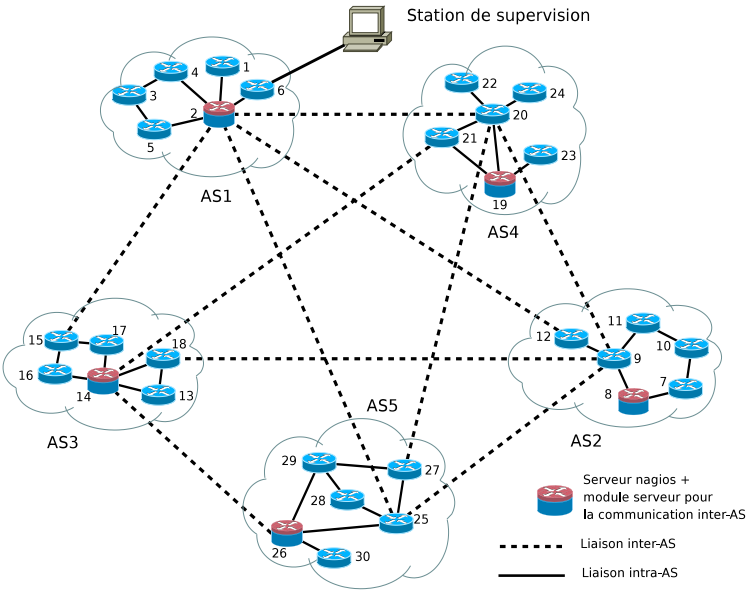


FIG. 6.2 – *Environnement de test*

[25] http://wiki.netkit.org/index.php/Main_Page
[26] http://www.nagios.org

6.4.5 Tests et résulats

La validation et l'évaluation du système de détection des défaillances ont été faites sur le réseau virtuel présenté ci-dessus. Le système de détection des défaillances se base sur la mise à disposition de l'état des hôtes concernés périodiquement de manière à pouvoir détecter des éventuelles défaillances avec un délai relativement court. Ce système peut être centralisé ou distribué. Dans le premier cas, l'ensemble des données sont transmises à un seul centre de traitement, alors que pour un système distribué les données sont échangées entre les réseaux impliqués. Chacune de ces deux approches a ses avantages et ses inconvénients. La première approche présente l'avantage de faciliter le traitement et le contrôle d'accès aux informations, mais présente l'inconvénient d'être plus vulnérable aux attaques.

L'un des avantages de la deuxième approche est d'être moins vulnérable car les données sensibles sont distribuées sur plusieurs sites et ne sont accessibles qu'aux opérateurs, mais reste plus difficile à contrôler en terme de respect des règles d'échanges des données par exemple.

Pour les résultats présentés dans ce manuscrit, les données de l'ensemble des 5 AS sont transmises à un seul hôte qui assurent le traitement de ces données et la mise à disposition des résultats comme le montre la figure 6.2. Cette approche centralisée a été choisie pour sa simplicité et compte tenu de la nature du réseau utilisé pour les tests. En effet, étant donné que nous utilisons un réseau virtuel, l'augmentation de la quantité d'informations à traiter par un des routeurs virtuels présentait un risque de dépassement mémoire, c'est pourquoi nous avons réduit la charge de ces nœuds au strict nécessaire pour permettre de virtualiser un réseau constitué de 30 routeurs sur un seul hôte physique.

Afin de valider notre système, le logiciel Nagios installé sur les hôtes 2, 8, 14, 19 et 26 supervise respectivement les routeurs de l'AS1, l'AS2, l'AS3, l'AS4 et l'AS5 et met à jour l'état de ces routeurs périodiquement (toutes les 10 secondes pour notre configuration), ces hôtes hébergent aussi le module serveur de notre système qui transmet les données au programme client installé sur l'hôte qui collecte l'ensemble des données provenant des AS.

Bien que de nombreux services (espace disque, charge CPU, nombre de processus, etc.) soient supervisés dans chaque AS, seules les valeurs du RTA et du trafic des interfaces sont transmises dans le cadre des échanges d'informations entre les différents AS.

La figure 6.3 présente les valeurs du RTA des routeurs 2 à 5 de l'AS1, les valeurs pour les autres AS présentent des comportements similaires, nous présentons seulement les valeurs de quelques routeurs pour faciliter la lisibilité. Les valeurs du RTA présentées sur cette figure sont en milliseconde et la période des échanges des données est fixée à 1 minute. Ces valeurs désignent les RTA entre les routeurs concernés et le routeur sur lequel est installé le serveur Nagios, c'est à dire le routeur r2.

Pour montrer qu'il est possible d'échanger des données autres que celles du RTA, nous présentons sur la figure 6.4, les valeurs du trafic entrant et sortant de l'interface *eth*3 du routeur *r*7. Comme on pouvait s'y attendre, les résultats présentés sur ces deux figures montrent qu'il est possible d'avoir une vision sur l'état des réseaux et de détecter des fortes augmentations de trafic des interfaces réseaux des routeurs que peuvent provoquer certains types de défaillances, comme celles des propagations des virus dans le réseau Internet.

Après la validation de l'architecture de détection des défaillances avec les résultats présentés sur les figures 6.3 et 6.4, les résultats présentés sur les figures suivantes sont consacrés à

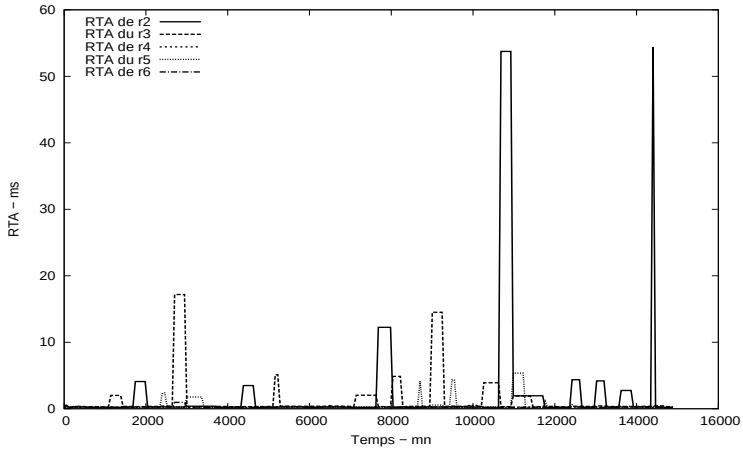


FIG. 6.3 – *Variation du RTA pour 5 routeurs de l'AS1*

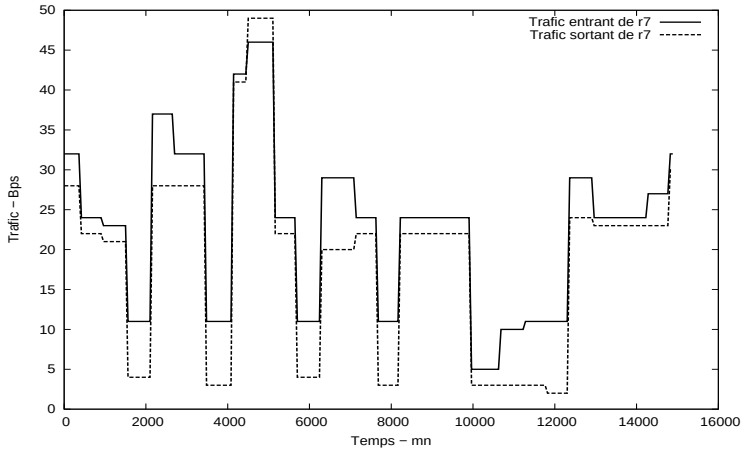


FIG. 6.4 – *Variation du trafic de l'interface eth3 du routeur r7*

l'évaluation de la performance du système en terme de détection des défaillances. La figure 6.5 représente quelques valeurs du délai nécessaire pour détecter les défaillances aléatoires pour une période d'échange d'informations entre opérateurs fixée à 1 minute. Cette figure montre que pour 451 pannes, 28% sont détectées avec un délai inférieur ou égal à 15 secondes, 26% avec délai compris entre 15 et 30 secondes, 46% avec un délai compris entre 30 et 45 secondes et 54% avec un délai de 45 à 59 secondes.

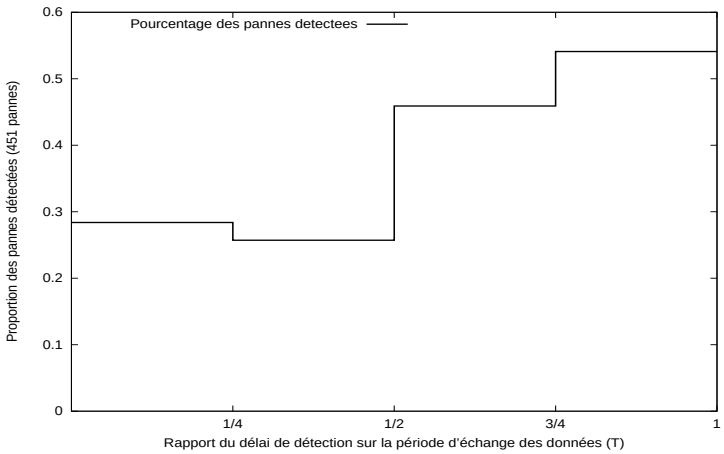


FIG. 6.5 – *Proportion des pannes détectées pour différents intervalles de temps*

La figure 6.6 montre la proportion des pannes détectées pour quelques fractions de la durée entre deux échanges successifs de données. Les résultats représentés sur cette figure montrent que, pour un test durant lequel 451 pannes se sont produites, environ 80% de ces pannes sont détectées avec un délai inférieur ou égal à $\frac{3}{4}$ de la période entre les échanges des données et une grande proportion de ces pannes (environ 30%) sont détectées dans un délai inférieur à $\frac{1}{4}$ de cet intervalle, c'est à dire de 25 secondes pour une période d'une minute.

Dans la figure 6.7 nous représentons les délais de détection des pannes pour différentes valeurs de la période des échanges des données entre les différents AS. Les résultats représentés sur cette figure montrent qu'en général la proportion des pannes détectées augmente linéairement avec le délai de détection qui, à son tour augmente avec la période des échanges de données. Comme on peut le voir sur la figure le nombre de pannes détectées à chacune des fractions de la période des échanges de données est très proche pour les différentes valeurs de cette période. Ce qui veut dire que pour la valeur de cette période égale à 2 minutes, le nombre de pannes détectés avec un délai d'une minute est sensiblement le même que celui des pannes qui pourraient être détectés avec un délai de 2 minutes lorsque la valeur de la période est égale à 4 minutes.

Les résultats représentés sur les figures précédentes, notamment ceux représentés sur la figure 6.7 montrent que le délai de détection des pannes varie avec la période d'échanges des données. Étant donné qu'une période d'échanges de données plus courte engendre plus de trafic échangé, nous représentons sur les figures 6.8(a) et 6.8(b) les résultats comparatifs de ces deux paramètres qui peuvent s'avérer utiles pour trouver des valeurs optimales pour ces deux paramètres. C'est à dire une valeur de la période d'échanges de données qui permet de

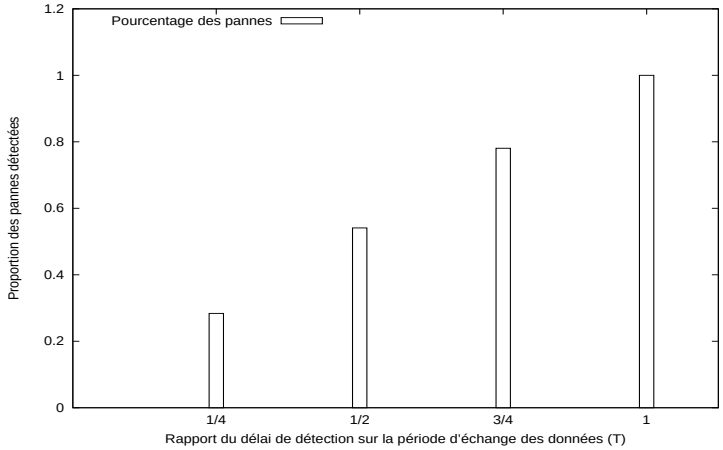


FIG. 6.6 – *Proportion des pannes détectées pour différentes fractions de la période d'échange des données*

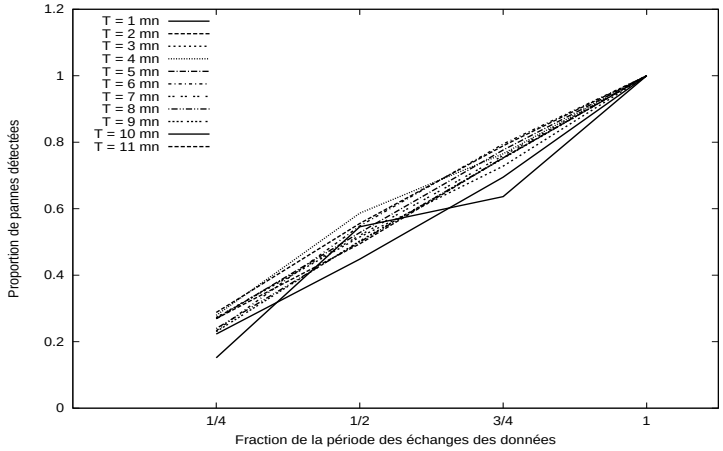
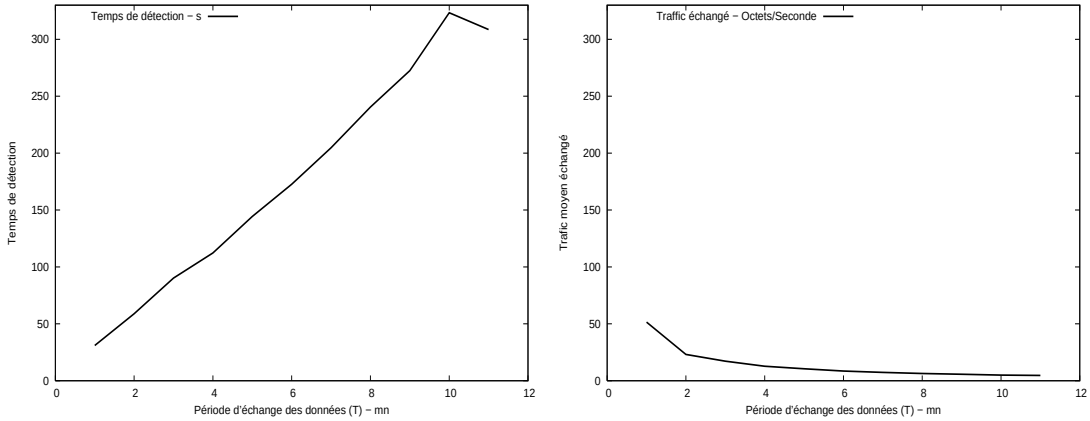


FIG. 6.7 – *Délais de détection des pannes en fonction de la période d'échange des données*

détecter les pannes avec un délai de détection relativement court sans engendrer de trafic trop important. Sur ces figures nous représentons l'évolution du délai de détection des pannes et celle du trafic échangé en fonction de la période d'échange des données. L'évolution de ces graphiques montre que, pour ce réseau de test, une valeur de la période d'échange de données fixée à 2 minutes constitue un bon compromis pour avoir un délai de détection relativement court sans engendrer de trafic trop important.



(a) Variation du délai de détection (b) Variation du trafic engendré

FIG. 6.8 – *Variation du temps de détection et du trafic échangé en fonction de la période d'échange des données*

6.5 Conclusion partielle

Dans ce chapitre, nous avons présenté une nouvelle approche basée sur la supervision des réseaux pour détecter automatiquement les pannes avec des délais de détection relativement courts afin de pouvoir lutter contre les propagations des défaillances de manière plus efficace. Les résultats des tests effectués sur un réseau virtuel montrent qu'elle permet d'évaluer simultanément l'état de plusieurs réseaux avec une grande efficacité. Dans le cadre de ces tests, nos modules d'échanges de données entre opérateurs ont été intégrés avec succès avec un logiciel de supervision libre et largement utilisé, ce qui constitue un avantage non négligeable compte tenu de la diversité des logiciels de supervision des réseaux utilisés par les opérateurs.

Puisque chaque réseau a ses caractéristiques particulières, notamment en terme de topologie, l'évaluation de l'architecture proposée sur différentes topologies de test ne présente que peu d'intérêt. Par conséquent, les résultats présentés dans ce chapitre ont été obtenus à partir des expérimentations portant essentiellement sur une variation de la période d'échange des données entre les différents AS impliqués. La valeur de ce paramètre constitue un facteur important pour limiter le trafic supplémentaire échangé et pour la réduction du délai de détection des pannes.

Les résultats des tests réalisés pour des valeurs de la période d'échanges de données variant entre 1 et 10 minutes ont permis d'évaluer l'influence de cette valeur sur l'efficacité, en terme

de délai de détection des pannes de l'architecture proposée. Ces résultats montrent que les proportions des pannes détectées pour la même fraction de cette valeur sont très proches pour différentes valeurs (1 à 11 minutes) de la période d'échange. Ce qui signifie que l'architecture proposée permet de détecter les pannes avec un délai plus ou moins court selon que la période d'échange de données soit courte ou longue.

Étant donné qu'une courte période d'échanges de données engendre plus de trafic, nous avons aussi effectué une évaluation comparative des délais de détection des pannes et du trafic échangé en fonction de la valeur de la période d'échange de données. Les résultats obtenus ont montré qu'il est possible de trouver une valeur de cette période qui constitue un bon compromis entre le délai de détection des pannes et le trafic engendré par l'échange d'informations.

Conclusion générale et perspectives

La société moderne repose de plus en plus sur des services comme l'électricité, les télécommunications, les transports et d'autres encore à tel point que tout dysfonctionnement des infrastructures qui fournissent ces services peut avoir des conséquences graves sur le bien être des citoyens. Ces infrastructures sont fortement interdépendantes et une défaillance d'une de ces infrastructures peut se propager, par effet de cascade ou d'escalade pour provoquer des pannes d'autres infrastructures. Les récents progrès des technologies de l'information et de la communication ont contribué à la modernisation de ces infrastructures et à leur efficacité en automatisant de nombreux processus et en facilitant, notamment le pilotage à distance des équipements clefs de ces infrastructures. Mais cette modernisation a aussi conduit à une interconnexion de plus en plus grandissante de l'Internet avec les réseaux dédiés de ces infrastructures. Cette interconnexion massive fait apparaître de nouvelles vulnérabilités pour ces infrastructures en les exposant à la plupart des nombreuses menaces émanant de l'Internet. Conscients de cette situation, les États ont pris, ces dernières années, d'importantes mesures pour la protection de ces infrastructures face aux cyber-menaces et plusieurs projets de recherche portant sur ces sujet ont été initiés. Mais, les nombreux travaux de recherche issus de ces projets s'intéressent, d'un côté à l'amélioration de la sécurité de l'Internet et de l'autre, à la protection des infrastructures critiques. Dans le cadre de cette thèse, nous nous sommes intéressés à l'étude de la propagation des cyber-défaillances susceptibles de toucher les réseaux dédiés aux infrastructures critiques. Les travaux réalisés montrent que les interdépendances entre les infrastructures deviennent de plus en plus croissantes et renforcent les difficultés liées à la protection de nombreuses infrastructures modernes. La complexité croissante de ces interdépendances rend difficile la maîtrise de l'ensemble des phénomènes qui peuvent résulter de celles-ci. Ceci conduit, parfois, à la propagation inattendue des défaillances entre différentes infrastructures causant des conséquences de grande ampleur comme les pannes généralisées. Ils montrent aussi que les études scientifiques concernant ces phénomènes nécessitent des données et des topologies détaillées et réalistes pour caractériser et représenter les infrastructures concernées. Mais, malgré ces difficultés, les différentes propositions présentées dans ce manuscrit montrent qu'il est possible de concevoir des architectures et techniques génériques qui offrent des moyens de sélectionner les principaux facteurs qui influent les phénomènes étudiés et, ainsi de limiter la complexité et le temps de calcul tout en produisant des résultats pertinents. Les différents chapitres de ce manuscrit traitent essentiellement la modélisation et la simulation des propagations des défaillances dans les réseaux de télécommunications de type Internet qui sont susceptibles de provoquer des pannes dans les autres infrastructures. Les contributions présentées dans les différents chapitres de ce manuscrit se focalisent sur la compréhension des

phénomènes de propagation des défaillances qui peuvent résulter des interdépendances, elles constituent donc une étape importante pour la protection des infrastructures modernes.

Le chapitre 3 de ce mémoire présente une technique de modélisation et de simulation des propagations des pannes entre les réseaux électriques et de télécommunications fondée sur les graphes pour représenter les topologies des deux réseaux, la méthode *DC load Flow* pour caractériser le transfert des charges dans le réseau électrique et un modèle spécifique pour définir le rôle des protocoles de routage dans les propagations des pannes. Après avoir présenté les différentes techniques existant pour la simulation des interdépendances et des propagations des défaillances et identifié leurs limites, ce chapitre a été essentiellement consacré à la conception d'un modèle et d'un simulateur adaptés à l'étude des interdépendances et aux propagations des pannes. Le scénario illustrant ce modèle met en œuvre des topologies représentant le principal opérateur de réseau de transport électrique (RTE) et un important opérateur de réseau de télécommunications (Free) en France. Il décrit une réduction de l'ampleur d'une panne électrique par les opérations de délestage rapide favorisées par une bonne réactivité des protocoles de routage. En effet, lors d'une panne électrique l'accès à distance, via les réseaux de télécommunications, à certains postes électriques permet de procéder à des délestages pour réduire la charge de manière appropriée afin d'équilibrer la production et la consommation. Et, dans les réseaux de télécommunications, lors d'une panne d'un routeur, à cause d'une coupure électrique par exemple, les protocoles de routage mettent un certain temps avant de rétablir les routes par un calcul des chemins alternatifs permettant de contourner le routeur défaillant. Les simulations réalisées sont fondées sur l'algorithme du flux maximum et les résultats obtenus montrent que, pour les deux réseaux simulés, la réduction du temps nécessaire à la détection de la panne d'un routeur de 600 à 6 secondes réduit le nombre de lignes électriques touchées de 20 à 2 lignes pour la même valeur de temps de simulation, c'est à dire 100 secondes après la panne initiale. Ils montrent aussi que cette dépendance de l'ampleur des pannes électriques à la réactivité du réseau de télécommunication se limite à une faible proportion ($1,4\%$) de l'ensemble des simulations réalisées. Ce faible pourcentage est dû, notamment à la structure du graphe représentant le réseau électrique dont la coupure initiale de la plupart des liens ne provoque pas de surcharge d'autres liens. Cette étude nous a permis de mettre en lumière le rapport étroit entre les réseaux électriques et de télécommunications et a permis de montrer qu'un réseau de télécommunications fiable permet de limiter les conséquences d'une panne électrique, mais aussi l'attaque de ce réseau de télécommunications peut constituer un moyen efficace pour altérer des grandes infrastructures comme le réseau électrique. À travers cette étude nous nous sommes aussi rendu compte de la nécessité de disposer des topologies réalistes en nombre suffisant pour les travaux de modélisation et de simulation de tous les phénomènes relatifs aux interdépendances entre les infrastructures.

Dans le troisième chapitre, nous décrivons un nouveau générateur de topologies fondé sur la distance euclidienne. Ce générateur permet de produire des graphes représentant tous les niveaux du réseau Internet : des petits réseaux locaux aux grands réseaux de transit ayant des points de présence dans la plupart des pays du monde. L'algorithme utilisé adopte une approche qui permet, tout d'abord d'interconnecter l'ensemble des nœuds sélectionnés pour représenter les points de présence, puis les nœuds restant sont interconnectés aux différents points de présence sur la base de la distance euclidienne. Cette technique permet de générer des graphes adaptés aux études des interdépendances, notamment entre les réseaux dédiés et

le réseau Internet, mais aussi entre différentes infrastructures comme les réseaux électrique et de télécommunications. Pour permettre de générer plusieurs topologies, la technique proposée peut utiliser des nœuds avec des coordonnées et des poids obtenus aléatoirement. Cependant, ce choix aléatoire se limite à la caractérisation des nœuds et au choix du nombre d'AS fournisseurs et celui des AS pairs, pour l'interconnexion proprement dite la technique utilise la distance euclidienne, des contraintes techniques pour la conception des réseaux et la préférence basée sur le degré de connectivité. L'absence de choix aléatoire dans le processus d'interconnexion permet de générer plusieurs topologies cohérentes avec différentes caractéristiques (différentes positions des nœuds par exemple) des sites à interconnecter. À la différence d'autres techniques qui proposent l'interconnexion des points de présence avec une structure en arbre, la technique proposée tient compte des contraintes techniques et économiques pour interconnecter ces points de présence. La raison de ce choix est qu'au fur et à mesure que les opérateurs font évoluer leurs réseaux, ils connectent de nouveaux sites tout en renforçant la connecticité de leurs réseaux afin de renforcer la robustesse de ceux-ci. La technique proposée adopte cette approche en interconnectant les points de présence entre eux, c'est ce qui permet d'améliorer la connectivité du graphe lorsque le nombre de sites à interconnecter augmente tout en minimisant le nombre de liens d'interconnexion. L'interconnexion des systèmes autonomes est fondée sur des résultats des travaux, notamment ceux des auteurs de [56] qui ont montré qu'environ 50% des systèmes autonomes formant Internet sont de niveau 1, ceci nous a permis d'éviter la distribution des systèmes autonomes de manière purement aléatoire. Le but de la technique présentée dans ce chapitre est d'offrir la possibilité de générer des graphes représentant plusieurs infrastructures tout en restant les plus réalistes possibles afin de pouvoir les utiliser lors des simulations destinées à étudier les interdépendances. Les graphes obtenus ont été comparés à plusieurs graphes représentant des réseaux réels sur la base de la connectivité (distribution des degrés) et de la robustesse (partitionnement des graphes). Les résultats montrent que les distributions des degrés des graphes de niveau AS et les graphes intra-AS sont très différentes. Etudier donc le réseau avec des graphes ne représentant que les interconnexions de niveau AS peut conduire à des résulats approximatifs. Pour faciliter le prise en compte de ces spécificités des interconnexions intra et inter-AS, la technique proposée est très modulaire et offre différents niveaux d'interconnexion : l'interconnexion des POP, des AS et celle entre les différents nœuds qui constituent un point de présence.

Le quatrième chapitre de ce manuscrit décrit un simulateur des propagations des défaillances dans les réseaux de type de Internet. La technique proposée est fondée sur le modèle d'épidémie adapté au contexte des réseaux de télécommunications. L'adaptation concerne le taux d'infection, celui du rétablissement des nœuds touchés et la vitesse de la propagation des défaillances. Si, dans le modèle d'épidémie de base les taux d'infection et de rétablissement sont compris entre 0 et 1, dans le modèle proposé les valeurs de ces deux paramètres sont fixées à 1, mais la propagation de la défaillance et du rétablissement ne se font qu'entre des nœuds voisins et lorsque les conditions modélisant les caractéristiques des protocoles du routage sont satisfaites. Le but de ce simulateur est de fournir un moyen permettant d'intégrer dans un seul environnement des modèles et de simulateurs des propagations des défaillances pour des infrastructures hétérogènes. A la différence des simulateurs spécifiquement conçus pour ces infrastructures capables de modéliser celles-ci en détail, la technique proposée se limite à la modélisation des facteurs qui influent la propagation des défaillances afin de faciliter l'intégration des modèles

et simulateurs de plusieurs infrastructures avec une complexité moindre. La prise en compte des facteurs concernant uniquement le routage limite les détails à un niveau relativement faible car les couches transport et applicative peuvent aussi influer la vitesse de propagation des défaillances, mais cette simplification permet de réduire la complexité des modèles pour pouvoir intégrer plus d'infrastructures tout en conservant les facteurs clefs qui influent ces propagations des défaillances. Les simulations et les résultats présentés dans ce chapitre ne concernent que les réseaux de télécommunications, mais portent sur une topologie qui couvre tous les niveaux d'un réseau de type Internet. Les résultats présentés montrent que lorsque la topologie contient des nœuds immunisés face à certains types de défaillances comme la propagation des fausses routes, la durée de vie de la défaillance dépend du nombre de sauts entre le nœud initialement touché et le nœud immunisé le plus proche, mais aussi au degré de connectivité des nœuds touchés et l'état du réseau qui influent la vitesse de propagation. Ils montrent aussi que pour le graphe utilisé pour les simulations, les nœuds dont une panne provoque de surcharges des nœuds voisins ne concernent que la moitié du nombre total des nœuds du graphe. Et parmi cette moitié, les pannes provoquent l'isolement de certains nœuds du graphe étudié seulement 3 minutes après la panne initiale pour environ 70% des nœuds. Aussi nous avons identifié une durée des fausses routes causées par des pannes des routeurs relativement élevée (environ $3,5$ minutes) qui peut engendrer des pertes de paquets importantes surtout pour les réseaux haut débit. La réduction des valeurs de la durée minimum entre 2 annonces de route pour les protocoles de routage permet de réduire la durée de vie des fausses routes, mais augmente aussi le trafic lié aux annonces des protocoles de routage.

Enfin, le dernier chapitre étudie différentes techniques de détection des pannes et décrit une architecture basée sur des logiciels de supervision existant pour la détection des propagations des défaillances dans les réseaux. L'infrastructure proposée est constituée des programmes client et serveur qui permettent la communication périodique des informations sur l'état des infrastructures fournies par ces logiciels de supervision. La conception de l'architecture présentée dans ce chapitre est basée sur les contraintes liées à la nécessité de réduire le trafic et du délais de détection des défaillances, de la réutilisation des outils de supervision existants et du contrôle d'accès aux informations qui constitue un facteur essentiel pour une technique de détection des propagations des défaillances liées aux interdépendances qui impliquent plusieurs réseaux. Pour valider la technique, nous avons présenté dans ce chapitre des tests réalisés sur un réseau virtuel composé de 5 AS constitués de 6 routeurs chacun, soit un total de 30 routeurs dont 10 routeurs BGP. La création du réseau est réalisée avec le logiciel Netkit[27]. Ensuite nous avons déployé le logiciel de supervision Nagios[28] sur chaque AS et réalisé différents scénarios de tests. Les résultats des tests consacrés à la validation de la technique montrent qu'elle permet de détecter toutes les défaillances avec un délai inférieur à la période d'échange d'informations entre le client qui collecte et le serveur qui fournit ces informations. Puis, nous avons réalisé des tests et évalué le délai nécessaire à la détection des défaillances et les résultats montrent qu'environ 80% des défaillances sont détectées avec un délai inférieur ou égale à $\frac{3}{4}$ de la valeur de cette période d'échange d'informations. Par conséquent la réduction de la période d'échange d'informations est le principal moyen de réduire le délai de détection des pannes, mais cette so-

[27] http://www.netkit.org
[28] http://www.nagios.org

lution présente l'inconvénient d'accroître le trafic lié à l'échange des informations. Toutefois, nous avons aussi montré qu'il est possible de trouver une valeur pour la période d'échange d'informations qui constitue un bon compromis entre la nécessité d'augmenter la fréquence d'échange d'informations et celle de réduire le trafic échangé.

Les principales difficultés rencontrées dans le cadre de cette thèse consacrée aux interdépendances ont pour origine l'hétérogénieté et la taille des infrastructures impliquées, mais aussi la complexité des interdépendances et les phénomènes qui en résultent. Les différents outils, modèles et techniques présentés dans ce manuscrit constituent une première étape pour améliorer la compréhension des phénomènes complexes relatifs à ces interdépendances qui impliquent des infrastructures très hétérogènes. Elles permettent de pallier aux nombreuses limites des outils existants en matière de modélisation et de simulation des interdépendances ainsi que la détection des propagations des pannes multi-réseaux. Cependant, plusieurs améliorations peuvent être apportées aux contributions proposées dans le cadre de cette thèse. Dans un premier temps, il serait intéressant de tester la technique de génération de topologie présentée dans le chapitre 4 pour des infrastructures autres que les réseaux de télécommunications. Il s'agirait, par exemple de générer des topologies des réseaux électriques avec des facteurs déterminants pour le fonctionnement de ces infrastructures afin d'évaluer sa flexibilité de manière plus réaliste. L'extension du simulateur des propagations des défaillances présenté dans le chapitre 5 à d'autres infrastructures permettra de caractériser les propagations des pannes impliquant plusieurs infrastructures hétérogènes. Les différentes techniques conçues dans le cadre de cette thèse ont été validées par des simulations avec quelques simplifications pour réduire la complexité et le temps de calcul. Une piste d'amélioration consiste donc à déployer les différentes techniques présentées dans ce manuscrit sur des réseaux réels et de réaliser des tests avec des paramètres moins approximatifs. La mise en œuvre dans des infrastructures hétérogènes et réelles de la technique de détection des pannes décrit dans le chapitre 6 est une autre piste pour le prolongement de ce travail.

Glossaire

capacité *La capacité représente la quantité de charge électrique stockée pour un potentiel électrique donné*

modèle d'épidémie *L'épidémie est un mal qui touche rapidement et dans un même lieu un grand nombre de cibles en se propageant de proche en proche (contagion). Dans ce rapport le modèle d'épidémie ou la théorie des épidémies désignent la technique utilisée pour caractériser l'évolution d'une défaillance qui se propage au sein d'une ou plusieurs infrastructures*

infrastructures critiques *L'ensemble des installations, réseaux, services, systèmes, actifs et documents nationaux d'une importance vitale, dont la destruction, l'endommagement, l'interruption de fonction ou la divulgation menacerait la sécurité nationale, l'économie nationale, la santé, la sûreté de la population ou le bon fonctionnement des pouvoirs publics*

NRA *Nœud de Raccordement d'Abonnés*

pannes en cascade *Dans ce manuscrit, les pannes en cascade désignent les défaillances au cours desquelles la défaillance d'une infrastructure provoque le dysfonctionnement d'un composant d'une autre infrastructures qui, à son tour provoque la panne de cette infrastructure. Par exemple une panne électrique locale (à cause d'une coupure de câble haute tension par exemple) peut entraîner l'arrêt des services de télécommunications à cet endroit qui provoque l'accroissement du trafic, puis la panne du reste du réseau de télécommunication. Enfin cette panne du réseau de télécommunications peut, à son tour provoquer des défaillances pour d'autres infrastructures à la suite de la perte de leurs systèmes de supervion*

réactance électrique *La réactance d'un circuit électrique est la partie imaginaire de son impédance induite par la présence d'une inductance ou d'un condensateur dans le circuit*

résistance électrique *l'aptitude d'un conducteur à s'opposer au passage du courant électrique*

vers informatiques *Un ver informatique est un logiciel malveillant capable de se reproduire sur plusieurs ordinateurs en utilisant le réseau*

virus informatiques *C'est un programme informatique capable de se propager en s'insérant dans d'autres programmes informatiques. Contrairement au ver qui est autonome et qui s'installe dans le disque dur, le virus a besoin de programmes "hôtes" pour remplir sa*

mission. Au sens large, on utilise souvent le mot virus pour désigner tout programme malveillant. C'est cette forme qui est utilisée dans ce mémoire car, dans le cadre des propagations des défaillances, ver et virus informatiques visent le même objectif en rapport, celui de rendre le réseau incapable de fournir les services attendus en surchargeant et en faisant tomber des composants clés de l'infrastructure comme les routeurs et les serveurs

Liste des Acronymes

AIMS ..... *Agent-Based Infrastructure Modeling and Simulation*

AML ..... *Agent Modeling Language*

AS ..... *Autonomous System*

ATETES ..... *Adapting Traffic Evolution Topology gEnerators*

BGL ..... *Boost Graph Library*

BGP ..... *Border Gateway Protocol*

BPEL ..... *Business Process Execution Language*

CAIDA ..... *Cooperative Association for Internet Data Analysis*

CERT ..... *Computer Emergency Response Team*

CERTA ..... Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques Informatiques

CI2RCO ..... *Critical Information Infrastructure Research Co-ordination*

CIAO ..... *Columbia International Affairs Online*

CIMS ..... *Critical Infrastructure Modeling System*

CISIA ..... *An Agent Based Simulator for Critical Interdependent Infrastructures*

COSSI ..... Centre Opérationnel de la Sécurité des Systèmes d'Information

CPU ..... *Central Processing Unit*

DARPA ..... *Defense Advanced Research Projects Agency*

DDS ..... *Data Distribution Service for Real-time Systems*

DIESIS ..... *Design of an Interoperable European federated Simulation network for critical InfrStracture*

DIS ..... *Distributed Interactive Simulation*

DMSO ..... *Defense Modeling and Simulation Office*

DNS ..... *Domain Name System*

DOS ..... *Denial-Of-Service*

EMTP ..... *ElectroMagnetic Transients Program*

ENPC ..... École Nationale des Ponts et Chaussées

EPCIP ..... *European Programme for Critical Infrastructure Protection*
GPRS ..... *General Packet Radio Service*
GSM ..... *Global System for Mobile Communications*
HLA ..... *High Level Architecture* (IEEE-1516)
IAIP ..... *Information Analysis and Infrastructure Protection Directorate*
IBGP ..... *internal BGP*
ICMP ..... *Internet Control Message Protocol*
IED ..... *Intelligent Electronic Device*
IEEE ..... *Institute of Electrical and Electronics Engineers*
IIM ..... *Inoperability Input-output Model*
IIS ..... *Internet Information Services*
INL ..... *Idaho National Laboratory*
INRIA ..... Institut National de Recherche en Informatique et en Automatique
INSEE ..... Institut National de la Statistique et des Études Économiques
IP ..... *Internet Protocol*
IPFIX ..... *IP Flow Information Export*
IRR ..... *Internet Routing Registry*
IRRIIS ..... *Integrated Risk Reduction of Information-based Infrastructure Systems*
ISP ..... *Internet Service Provider*
IT-ISAC ..... *Information Technology - Information Sharing and Analysis Center*
UML ..... *Unified Modeling Language*
MDT ..... *Mean Down Time*
MISO ..... *Midwest Independent System Operator*
MIT ..... *Middleware Improved Technology*
MRAI ..... *Minimum Route Advertisement Interval*
NERC ..... *North American Electric Reliability Council*
NLANR ..... *National Laboratory for Applied Network Research*
NRA ..... Nœud de Raccordement d'Abonnés
ONERA ..... Office National d'Etudes et de Recherches Aérospatiales
OSPF ..... *Open Shortest Path First*
PCCIP ..... *President's Commission on Critical Infrastructure Protection*
PSAT ..... *Power System Analysis Toolbox*
PSLF ..... *Positive Sequence Load Flow Software*
RESIST ..... *Resilience for Survivability in Information Society Technologies*
RIP ..... *Routing Information Protocol*

RIPE . . . . . Réseau IP Européen
RTA . . . . . *Roundtrip Time Average*
RTE . . . . . Réseau de Transport d'Électricité
RTI . . . . . *RunTime Infrastructure*
SCADA . . . . . *Supervisory Control And Data Acquisition*
SDX . . . . . *System Data Exchange*
SSL . . . . . *Secure Sockets Layer*
TCP . . . . . *Transmission Control Protocol*
TEFTS . . . . . *Transient Stability Program to Study Energy Functions*
TISN . . . . . *Trusted Information Sharing Network*
UCTE . . . . . *Union for the Co-ordination of Transmission of Electricity*
UML . . . . . *User Mode Linux*
WSCC . . . . . *Western Systems Coordinating Council*
WSRF . . . . . *Web Services Resource Frame-work*

Bibliographie

[1] Fcc network outage reporting system.

[2] Ieee 1278.1a-1998 - standard for distributed interactive simulation - application protocols.

[3] Ssfnet : Scalable simulation framework network models.

[4] Common format for exchange of solved load flow data. 92(6) :1916–1925, 1973.

[5] Extended transient-midterm stability package : User's manual for the power flow program, jan 1987.

[6] Methodology for the integration of hvdc links in large ac systems-phase 2 : Advanced concepts. 1, apr 1987.

[7] Computer attacks at department of defense pose increasing risks. Technical report, may 1996.

[8] Executive order 13010. critical infrastructure protection, jul 1996.

[9] Request for comments : 1035, April 1998.

[10] Request for comments : 2328, apr 1998.

[11] Request for comments : 2453, nov 1998.

[12] Ieee std. 1516-2000. ieee standard for modeling and simulation high level architecture (hla) - framework and rules, 2000.

[13] A. B. e. M. K. A. E. Kalam, Y. Deswarte. Access control for collaborative systems : A web services based approach. In *IEEE International Conference on Web Services*, number 9869128, pages 1064–1071, July 2007.

[14] S. Agarwal, C.-N. Chuah, S. Bhattacharyya, and C. Diot. Impact of BGP Dynamics on Router CPU Utilization. In *Lecture Notes in Computer Science*, volume 3015, pages 278–288, May 2004.

[15] W. Aiello, F. Chung, and L. Lu. A random graph model for massive graphs. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 171–180, 2000.

[16] R. Albert, H. Jeong, and A. Barabasi. Error and attack tolerance of complex networks. In *Nature*, number 406, pages 378–382, July 2000.

[17] k. c. Andre Broido. Complexity of global routing policies, 2001.

[18] H. Astok, K. Edasi, M. Heidelberg, I. Odrats, M. Saarmann, U. Vallner, H. Hinsberg, K. Riismaa, E. Maaten, L. Leht, T. Türna, R. Oorn, R. Semjonova, T. Viira, G. Hämmal, I. Vali, A. Kalja, and J. Tepandi. Information technology in public administration of estonia. Technical report, 2008.

[19] S. B. and A. O. Fast decoupled load flow. In *IEEE transaction on Power Apparatus and Systems*, volume PAS-93, pages 859–869, jan 2007.

[20] L. BAGHLI. *Réalisation d'un Environnement Graphique avec Base de Données pour l'Analyse et la Simulation de Réseaux électriques*. PhD thesis, 1994.

[21] N. Bailey. The mathematical theory of infectious diseases and its applications, 1975.

[22] C. Balducelli, S. Bologna, A. D. Pietro, and G. Vicoli. Analysing interdependencies of critical infrastructures using agent discrete event simulation. 2(4) :306 – 318, 2005.

[23] V. H. Berk, R. S. Gray, and G. Bakos. Using sensor networks and data fusion for early detection of active worms. In *Proceedings of AeroSense 2003 : SPIE's 17th Annual International Symposium on Aerospace/Defense Sensing, Simulation, and Controls*, apr 2003.

[24] V. H. Berk, R. S. Gray, and G. Bakos. Using sensor networks and data fusion for early detection of active worms. In *Proceedings of AeroSense 2003 : SPIE's 17th Annual International Symposium on Aerospace/Defense Sensing, Simulation, and Controls*, apr 2003.

[25] C. Beyel, A. U. RüdigerKlein, and A. von Boguszewski. SimCIP IRRIIS DemoMeeting, May 2009.

[26] B. Bréholée and P. Siron. Design and implementation of a hla inter-federation bridge. In *European Simulation Interoperability Workshop, Stockholm (Sweden)*, jun 2003.

[27] R. S. Cahn. 1998.

[28] S. Cai, L. Gao, W. Gong, and W.-Q. Xu. On generating internet hierarchical topology. In *43rd IEEE Conference on Decision and COntrol (CDC)*, volume 5, pages 4655–4660, 2004.

[29] K. Calvert, M. Doar, and E. Zegura. Modeling internet topology. jun 1997.

[30] A. Caminero, A. Sulistio, B. Caminero, C. Carrion, and R. Buyya. Extending gridsim with an architecture for failure detection. In *Proceedings of the 13th International Conference on Parallel and Distributed Systems*, volume 1, pages 1–8, 2007.

[31] C. A. Canizares. Computer Simulation of Power Systems & Power Computer Systems Aplications, Jan. 2003.

[32] A. Chakrabarti and G. Manimaran. Internet infrastructure security : A taxonomy. In *IEEE Network*, volume 16, pages 13–21, dec 2002.

[33] A. Champion, D. Chan, and M. Brand. 2007 : Year of the botnet ?, 2009.

[34] D. F. Chang, R. Govindan, and J. Heidemann. An empirical study of router response to large bgp routing table load. Technical report, 2001.

[35] L.-C. Chen and K. M. Carley. A computational model of computer virus propagation. In *Center for Computational Analysis of Social and Organizational Systems (CASOS). Carnegie Mellon University*, 2001.

[36] Q. Chen, H. Chang, R. Govindan, S. Jamin, S. J. Shenker, and W. Willinger. The Origin of Power Laws in Internet Topologies Revisited. In *INFOCOM*, 2002.

[37] W. Chen, S. Toueg, and M. K. Aguilera. A gossip-style failure detection service. In *On the quality of service of failure detectors. IEEE Transactions on Computers*, volume 51, pages 13–32, 2002.

[38] L. P. Chew. Constrained delaunay triangulations. In *Proceedings of the third annual symposium on Computational geometry*, pages 215–222, 1987.

[39] D. Clark, W. Lehr, P. Faratin, S. Bauer, and J. Wroclawski. The growth of internet overlay networks : Implications for architecture, industry structure and policy. In *Telecommunications Policy Research Conference (TPRC-05), Washington, DC.*, 2005.

[40] G. Clark, T. Courtney, D. Daly, D. Deavours, S. Derisavi, J. M. Doyle, W. H. Sanders, and P. Webster. The möbius modeling tool. In *Proceedings of the 9th International Workshop on Petri Nets and Performance Models*, pages 241–250, sep 2001.

[41] I. Committee. Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy. Technical report, Apr. 2004.

[42] N. A. E. R. Council. SQL Slammer worm lessons learned for consideration by the electricity sector, June 2003.

[43] J. Cowie, A. T. Ogielski, Y. Yuan, and B. Premore. Internet worms and Global routing instabilities. In *Scalability and traffic control in IP networks. Conference NÂř2*, volume 4868, pages 195–199, Aug. 2002.

[44] D. D. D., P. M. R., and M. Milo. Cims : A framework for infrastructure interdependency modeling and analysis. In *Proceedings of the 2006 Winter Simulation Conference, IEEE*, volume 39, page 478 ? 485, dec 2006.

[45] D. Daley and J. Gani. Epidemic modeling, 1991.

[46] S. Delamare, A.-A. Diallo, and C. Chaudet. High-level modelling of critical infrastructures' interdependencies. In *Critical Infrastructures as Complex Systems conference, co-located with European Conference on Complex Systems (ECCS 2007)*, oct 2007.

[47] S. Delamare, A.-A. Diallo, and C. Chaudet. High-level modelling of critical infrastructures' interdependencies. 5(1/2) :100–119, 2009.

[48] P. J. Denning. The arpanet after twenty years. In *American Scientist 77*, pages 530–535, dec 1989.

[49] J. A. Derosier. Internet topology generation based on reverse-engineered design principles : Performance tradeoffs between heuristic and optimization-based approaches. Technical Report A456384, jun 2008.

[50] A.-A. Diallo and C. Chaudet. An alternate topology generator for joint study of power grids and communication networks. In *4th International Workshop on Critical Information Infrastructures Security (CRITIS'09)*, oct 2009.

[51] P. D.J.Âă, S. N. W. S.Âă, and C. D. Linking discrete event simulation models using hla. In *Systems, Man and Cybernetics, 2005 IEEE International Conference*, volume 1, pages 696–701, jan 2006.

[52] M. B. Doa. A better model for generating test networks. In *Global Telecommunications Conference, 1996. GLOBECOM '96*, pages 86–93, aug 2002.

[53] D. D. Dudenhoeffer, M. R. Permann, S. Woosley, R. Timpany, C. Miller, A. McDermott, and D. M. Manic. Interdependency Modeling and Emergency Response. In *ACM Summer Computer Simulation Conference*, pages 1230–1237, 2007.

[54] S. Duflos, A. Diallo, and G. L. Grand. An Overlay Simulator for Interdependent Critical Information Infrastructures. jun 2007.

[55] K. EJ, Godschalk, D. Chapin, FS, and Jr, 1995.

[56] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the Internet topology. In *SIGCOMM*, pages 251–262, 1999.

[57] P. Faratin, D. Clark, P. Gilmore, S. Bauer, A. Berger, and W. Lehr. Complexity of internet interconnections : Technology, incentives and implications for policy. In *The 35th Research Conference on Communication, Information and Internet Policy (TPRC)*, 2007.

[58] P. Felber, X. Défago, R. Guerraoui, and P. Oser. Failure detectors as first class objects. In *Proc. of the 9th IEEE International Symp. on Distributed Objects and Applications(DOA'99)*, pages 132–141, sep 1999.

[59] C. Fetzer, M. Raynal, and F. Tronel. An adaptive failure detection protocol. In *Proc. of the 8th IEEE Pacific Rim Symp. on Dependable Computing(PRDC-8)*, 2001.

[60] F. Flentge. Irriis - intergated risk reduction of information-based inffrastructure systems.

[61] S. Floyd and V. Paxson. Difficulties in simulating the internet. In *IEEE/ACM Transactions on Networking*, volume 9, pages 392–403, aug 2001.

[62] U. for the Co-ordination of Transmission of Electricity. Final Report on the European System Disturbance on 4 November 2006. Technical report, Nov. 2006.

[63] U. C. P. S. O. T. Force. Final Report on the August 14, 2003 Blackout in the United States and Canada : Causes and Recommendations. Technical report, Apr. 2004.

[64] A. Ganesh, L. Massoulié, and D. Towsley. The Effect of Network Topology on the Spread of Epidemics. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 2, pages 1455–1466, Aug. 2005.

[65] U. G. A. O. (GAO). Critical infrastructure protection. improving information sharing with infrastructure sectors. Technical report, jun 2004.

[66] A. Ghorbani and S. Marsh. Agent-based infrastructure modeling and simulation (aims), jul 2006.

[67] M. Girvan and N. M. E. J. Community structure in social and biological networks. In *The National Academy of Sciences*, Dec. 2002.

[68] W. D. Grover. Mesh-based survivable networks. In *Prentice Hall PTR*, 2004.

[69] D. Guetta. La commutation tout optique pour les réseaux àă fibre optique.

[70] I. Gupta, T. D. Chandra, and G. S. Goldszmidt. On scalable and efficient distributed failure detectors. In *Proc. of the 20th Annual ACM Symp. on Principles of distributed computing*, pages 170–179, 2001.

[71] R. H.A, B. K., and M. J.R. Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. 5(3) :220–244, 2009.

[72] H. Haddadi, A. Moore, R. Mortier, M. Rio, and G. Iannaccone. End-to-end network topology generation. In *ACM SIGCOMM poster Session*, aug 2007.

[73] B. Hans-Georg, S. Hans-Paul, and W. Ingo. How to analyse evolutionary algorithms. In *Theoretical Computer Science*, pages 101–130, 2002.

[74] N. Hayashibara, A. Cherif, and T. Katayama. Failure detectors for large-scale distributed systems. In *The 21th Symp. on Reliable Distributed Systems, (SRDS)*, 2002.

[75] O. Headquarters. Data distribution service for real-time systems version 1.2, jan 2007.

[76] P. Hirsch. Transmission fast simulation and modeling (t-fsm)-functional requirements.

[77] K. Hopkinson, X. Wang, R. Giovanini, J. Thorp, K. Birman, and D. Coury. EPOCHS : A Platform for Agent-Based Electric Power and Communication Simulation Built From Commercial Off-the-Shelf Components. In *Simulation Conference, 2003. Proceedings of the 2003 Winter*, volume 2, pages 1158–1116, Jan. 2004.

[78] G. Houston. Analyzing the internet's bgp routing table. In *The Internet Protocol Journal*, volume 4, mar 2001.

[79] J. D. Howard. *An analysis of security incidents on the Internet 1989-1995*. PhD thesis, apr 19997.

[80] M. Imbrogno, W. Robbins, and G. Pieris. Selecting a hla run-time infrastructure : Overview of critical issues affecting the decision process for war-in-a-box. Technical report, jul 2004.

[81] Jian-qiangăLiu, Jiang-xingăWu, XiaoăHuang, and DanăLi. A generating method for internet topology with multi-ases and multi-tiers. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 1363–1373, feb 2009.

[82] E. G. C. Jr, Z. Ge, V. Misra, and D. Towsley. Network Resilience : Exploring Cascading Failures within BGP. 2002.

[83] S. N. K. and W. S. Graph models of critical infrastructure interdependencies. In *Inter-Domain Management, Proceedings of the First International Conference on Autonomous Infrastructure, Management, and Security (AIMS 2007)*, volume 4543, pages 208–211, jun 2007.

[84] X. C. M. K. and K. Y. P. N. A new network topology evolution generator based on traffic increase and distribution model. In *Sixth International Conference on Networking, 2007. ICN'07*, pages 56–56, apr 2007.

[85] J. Kephart and S. White. Measuring and modeling computer virus prevalence. In *Proc. of the 1993 IEEE Symposium on Research in Security and Privacy*, may 1993.

[86] J. Kephart and S. White. Measuring and modeling computer virus prevalence. In *Proc. of the 1993 IEEE Symposium on Research in Security and Privacy*, may 1993.

[87] A. Krause. Generating networks with realistic properties : The topology of locally evolving random graphs. In *WEHIA*, June 2006.

[88] A. Krings and P. Oman. Toward developing genetic algorithms to aid in critical infrastructure modeling. In *2007 IEEE Conference on Technologies for Homeland Security*, may 2007.

[89] A. Krings and P. Oman. Toward developing genetic algorithms to aid in critical infrastructure modeling. In *2007 IEEE Conference on Technologies for Homeland Security*, may 2007.

[90] C. Labovitz, A. Ahuja, R. Wattenhofer, and S. Venkatachary. The impact of Internet Policy and Topology on Delayed Routing Convergence. In *INFOCOM : Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 1, pages 537–546, Aug. 2002.

[91] M.-A. Laverdière. Slammer : Before, During and After, Feb. 2004.

[92] E. E. Lee, J. E. Mitchell, and W. Wallace. Assessing vulnerability of proposed designs for interdependent infrastructure systems. In *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

[93] L. Li, D. Alderson, W. Willinger, and J. Doyle. A first principles approach to understanding the internet's router-level topology. In *ACM SIGCOMM*, 2004.

[94] M. Liljenstam, D. Nicol, V. Berk, and R. Grayo. Simulating realistic network worm traffic for worm warning system design and testing. In *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, 2003.

[95] G. Lin and J. YueFeng. A novel hybrid topology generator for network simulation. In *Network Architectures, Management, and Applications. Proceedings of the SPIE*, volume 6784, 2007.

[96] P. Mahadevan, C. Hubble, D. Krioukov, B. Huffaker, and A. Vahdat. Orbis : Rescaling Degree Correlations to Generate Annotated Internet Topologies. In *SIGCOMM : the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 325–336, 2007.

[97] P. Mahadevan, D. Krioukov, K. Fall, and A. Vahdat. Systematic topology analysis and generation using degree correlations. In *SIGCOMM : the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 135–146, 2006.

[98] A. G. McKendrick. Applications of mathematics to medical problems. In *Proceedings of Edin. Math. Society*, volume 14, pages 98–130, 1926.

[99] A. Medina, A. Lakhina, I. Matta, and J. Byers. Brite : An approach to universal topology generation. In *Proceedings of MASCOTS '01*, aug 2001.

[100] F. Milano. An open source power system analysis toolbox. In *The first IEEE panel session on Open Source Software at the PES Meeting of Montreal*, jun 2006.

[101] D. Miller and J. Thorpe. Simnet : the advent of simulator networking. In *Proceedings of the IEEE*, volume 83, pages 1114–1123, aug 1995.

[102] H.-S. J. Min, W. Beyeler, T. Brown, Y. J. Son, and A. T. Jones. Toward modeling and simulation of critical national infrastructure interdependencies. In *IIE Transaction*, pages 57–71, jan 2007.

[103] J. Moteff, C. Copeland, and J. Fischer. Critical Infrastructures : What Makes an Infrastructure Critical ? Technical report, jan 2003.

[104] J. Moteff and P. Parfomak. Critical Infrastructure and Key Assets : Definition and Identification. In *Resources, Science, and Industry Division of the Congressional Research Service*, Oct. 2004.

[105] D. Nicol, B. Premore, A. Ogielski, and M. Liljenstam. Using simulation to understand dynamic connectivity at the core of the internet. In *UKSim 2003 Cambridge University, England*, Apr. 2003.

[106] D. Nicol, B. Premore, Y. Yuan, and M. Liljenstam. A mixed Abstraction Level Simulation Model of Large-Scale Internet Worm Infestations. In *Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002. Proceedings. 10th IEEE International Symposium on*, number 7597209, pages 109–116, Jan. 2003.

[107] D. of Homeland Security. Protection of voluntarily shared critical infrastructure information. Technical report.

[108] T. N. A. of Regulatory Utility Commissioners (NARUC). Information sharing practices in regulated critical infrastructure states analysis and recommendations. Technical report, 2007.

[109] R. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang. In Search of the Elusive Ground Truth : The Internet's AS-level Connectivity Structure. In *ACM SIGMETRICS Performance Evaluation Review*, pages 217–228, 2008.

[110] G. O'Reilly, S. Richman, and A. Kelic. Power, telecommunications, and emergency services in a converged network world. In *Design and Reliable Communication Networks, 2007. DRCN 2007. 6th International Workshop on*, number 10428641, pages 1–6, Oct. 2007.

[111] T. D. O'Rourke. Critical infrastructure, interdependencies, and resilience, 2007.

[112] S. Panzieri, R. Setola, and G. Ulivi. An agent based simulator for critical interdependent infrastructures (cisia). In *2ème Conférence Internationale sur les Infrastructures Critiques*, oct 2004.

[113] M. Pasin, S. Fontaine, and S. Bouchenak. Failure detection in large scale systems : a survey, 2005.

[114] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann. Critical Infrastructure Interdependency Modeling : A Survey of U.S. and International Research. Technical report, Aug. 2006.

[115] J. Peerenboom. Critical infrastructures interdependencies integrator (ci^3).

[116] K. Perumalla and S. Sundaragopalan. High-fidelity modeling of computer network worms. In *Annual Computer Security Applications Conference (ACSAC)*, dec 2004.

[117] T. PETERMANN. *A statistical physics perspective of complex networks : from the architecture of the internet and the brain to the spreading of an epidemic*. PhD thesis, 2005.

[118] B. Quoitin. Topology generation based on network design heuristics. In *International Conference On Emerging Networking Experiments And Technologies. Proceedings of the 2005 ACM conference on Emerging network experiment and technology*, pages 278–279, 2005.

[119] G. R. and T. H. Heuristics for internet map discovery. In *Proceedings of the IEEE Infocom*, mar 2000.

[120] H. A. Rahman, K. Beznosov, and J. R. Marti. Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. *International Journal of Critical Infrastructures*, 5(3) :220–244, 2009.

[121] M. Rahman, A. PakÅątas, and F. ZhigangWang. Network topology generation and discovery tools. In *Proc. of the 7th EPSRC Annual Postgraduate Sym-posium on the Convergence of Telecommunications, Net-working and Broadcasting (EPSRC PGNet 2006)*, pages 26–27, jun 2006.

[122] Y. Rekhter, T. Li, and S. Hares. Request for comments : 4271, jan 2006.

[123] G. Riley, R. Fujimoto, and M. Ammar. A generic framework for parallelization of network simulations. In *Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication*, mar 1999.

[124] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, Understanding, and Analyzing Critical Infrastructures interdependencies. In *In IEEE Control Systems Magazine*, Dec. 2001.

[125] E. Rome, S. Bologna, E. Gelenbe, E. Luiijf, and V. Masucci. Diesis - design of an interoperable european federated simulation network for critical infrastructures. In *Proceedings of the 2009 SISO European Simulation Interoperability Workshop (ESIW '09)*, pages 139–146, jul 2009.

[126] B. Rozel. *La sécurisation des infrastructures critiques : recherche d'une mÃl'thodologie d'identification des vulnÃl'rabilitÃl's et modÃl'lisation des interdÃl'pendances*. PhD thesis, July 2009.

[127] B. Rozel, M. Viziteu, R. Caire, N. Hadjsaid, and J.-P. Rognon. Towards a Common Model for Studying Critical Infrastructure Interdependencies. In *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, number 10141967, pages 1–6, Aug. 2008.

[128] J. M. Sarriegi, F. O. Sveen, J. Torres, and J. J. Gonzalez. Towards a research framework for critical infrastructure interdependencies. In *International Journal of Emergency Management*, volume 5, pages 235 – 249, 2008.

[129] J. Schonwdder and H. Langendorfer. Tcl extensions for network management applications. In *Pruc. TcLTk Workrhup*, pages 279–288, 1995.

[130] N. Sergent, X. Défago, and A. Schiper. Impact of a failure detection mechanism on the performance of consensus. In *Proc. of the 8th IEEE Pacific Rim Symp. on Dependable Computing(PRDC-8)*, pages 137–145, 2001.

[131] Z. Shen, L. Gao, and K. Kwiat. Modeling the spread of active worms. In *Proceedings of INFOCOM*, 2003.

[132] P. K. Singh and A. Lakhotia. Analysis and detection of computer viruses and worms :an annotated bibliography. In *ACM SIGPLAN Notices*, volume 37, pages 29–35, feb 2002.

[133] S. Staniford, V. Paxson, and N. Weaver. How to 0wn the internet in your spare time. In *Proceedings of the* 11^th *USENIX Security Symposium*, 2002.

[134] P. Stelling, I. Foster, C. Kesselman, C. Lee, and G. von Laszewski. A fault detection service for wide area distributed computations. In *Proc. of the 7th IEEE Symp On High Performance Distributed Computing*, pages 268–278, jul 1998.

[135] S. Strassburger. On the HLA-based coupling of simulation tools. In *European Simulation Multiconf*, 1999.

[136] N. K. Svendsen and S. D. Wolthusen. An analysis of cyclical interdÃl'pendencies in critical infrastructures. In *2nd International Workshop on Critical Information Infrastructures Security*, oct 2007.

[137] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger. Network topology generators : degree-based vs. structural. In *Proceedings of the 2002 SIGCOMM conference. ACM SIGCOMM Computer Communication Review*, volume 32, pages 147–159, oct 2002.

[138] A. N. A. Team. July, 2009 south korea and us ddos attacks, jul 2009.

[139] W. J. Tolone, D. Wilson, A. Raja, W. ning Xiang, H. Hao, S. Phelps, and E. W. Johnson. Critical infrastructure integration modeling and simulation. 3073, 2004.

[140] I. Trencansky and R. Cervenka. Agent Modeling Language (AML) : A Comprehensive Approach to Modeling MAS. *Informatica*, 29 :391–400, 2005.

[141] R. van Renesse, Y. Minsky, and M. Hayden. A gossip-style failure detection service. In *In Middleware '98*, 1998.

[142] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, and L. Zhang. Observation and Analysis of BGP Behavior under Stress. In *The 2nd ACM SIGCOMM Workshop on Internet Measurement Conference*, pages 183–195, 2002.

[143] Y. Wang, D. Chakrabarti, C. Wang, and C. Faloutsos. Epidemic Spreading in Real Networks : An Eigenvalue Wiewpoint. In *22nd International Symposium on Reliable Distributed Systems*, number 7847000, pages 25–34, Oct. 2003.

[144] Z. Wang, R. J. Thomas, and A. Scaglione. Generating Random Topology Power Grids. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, number 9912432, pages 183–183, Jan. 2008.

[145] B. M. Waxman. Routing of multipoint connections. *Selected Areas in Communications, IEEE Journal on*, (3330780) :1617–1622, Aug. 1998.

[146] S. Wei, J. Mircovic, and M. Swany. Distributed Worm Simulation with a Realistic Internet Model. In *Principles of Advanced and Distributed Simulation, 2005. PADS 2005. Workshop on*, number 8588067, pages 71–79, June 2005.

[147] H. Y. Y., H. B. M., L. J. H., S. Joost, C. Kenneth, and C. LIAN. Inoperability input-output model for interdependent infrastructure sectors. ii : Case studies. 11(2) :80–92, jun 2005.

[148] E. Zegura, K. Calvert, and S. Bhattacharjee. How to Model an Internetwork. In *INFOCOM '96. Fifteenth Annual Joint Conference of the IEEE Computer Societies. Networking the Next Generation. Proceedings IEEE*, volume 2, pages 594–602, Aug. 2002.

[149] E. Zegura, K. Calvert, and M. Donahoo. A quantitative comparison of graph-based models for internet topology. In *IEEE/ACM Transactions on Networking*, volume 5, 1997.

[150] E. Zegura, K. Calvert, and M. Donahoo. A quantitative comparison of graph-based models for internet topology. In *IEEE/ACM Transactions on Networking*, volume 6, dec 1997.

[151] S. Q. Zhuang, D. Geels, I. Stoica, and R. H. Katz. On failure detection algorithms in overlay networks. In *Proceedings IEEE INFOCOM Conference*, 2005.

[152] C. C. Zou, W. Gong, and D. Towsley. Code red worm propagation modeling and analysis. In *Proceedings of the 9th ACM conference on Computer and communications security*, 2002.

Table des figures