14e Congrès des Doctorants 2013
EDSYS (École Doctorale Systèmes)
16 Avril, Tarbes

Vulnérabilité des réseaux face aux catastrophes naturelles
Congrès des Doctorants EDSYS 2013

Daouda KAMISSOKO (daouda.kamissoko@enit.fr)
EDSYS, Toulouse
IRIT-LGP/INPT, Toulouse
Thèse encadrée par: Pascale Zaraté (IRIT/UT1--SMAC) et François Pérès (LGP-SDC)

Résumé *Dans ce papier, nous présentons l'état d'avancement du projet VESTA (Vulnérabilité des réseaux face aux catastrophes naturelles). Après la définition des concepts clés, nous faisons un état de l'art de la modélisation des réseaux et de l'analyse de la vulnérabilité. Nous identifions ainsi les limites de l'un et les carences de l'autre. Par la suite, nous présentons notre proposition de modèle en deux axes. La modélisation des réseaux en tenant compte des interdépendances d'une part et celle de la vulnérabilité d'autre part.*

A. INTRODUCTION

Dans un contexte de forte industrialisation, nos sociétés dépendent de plus en plus des réseaux tels que l'eau, l'électricité, le gaz et les télécommunications. Le nombre et la diversité des évènements comme l'épisode neigeux en île de France l'hiver dernier, ont démontré la vulnérabilité de ces infrastructures vis-à-vis des catastrophes naturelles. À cause des interdépendances, le dysfonctionnement d'un composant est susceptible de se propager aux autres, à une échelle pouvant dépasser celle d'un pays, rendant ardue toute analyse de vulnérabilité.

L'objectif de ce papier est de présenter l'état du projet VESTA sur l'analyse de la vulnérabilité des réseaux.

Pour y parvenir, nous commençons par définir les concepts clés, avant de détailler la méthodologie d'analyse. Celle-ci commence par une circonscription du contexte. Étape cruciale pour poser les limites des systèmes à analyser. Après un état de l'art de la modélisation des réseaux et de la vulnérabilité, nous proposons une méthode de modélisation de celles-ci intégrable à la théorie des graphes. Les derniers paragraphes présentent le modèle de vulnérabilité, des conséquences et du risque. Enfin nous finissons par une conclusion et les perspectives d'avenir.

B. CONCEPTS ET DÉFINITIONS

Les concepts liés à l'analyse de la vulnérabilité des réseaux sont divers et variés. Face à cette diversité nous présentons ci-dessous notre point de vue. Il repose sur le trio Population, Territoire et Aléa d'une part et sur le duo Risque-Vulnérabilité d'autre part.

1. Population, Territoire, Aléa

L'analyse de la vulnérabilité suppose la présence de

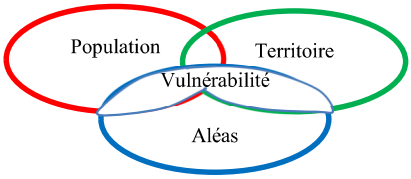

Figure 1: Le trio Population, Territoire, Aléa

phénomènes anthropiques ou naturels non maîtrisés que nous appelons aléas. La spécificité de l'aléa est qu'on ne peut pas prédire sa date d'occurrence et son intensité en même temps. Nous le définissons comme un « phénomène naturel ou anthropique pour lequel on ne peut prévoir l'occurrence et l'intensité à la fois, et susceptible d'affecter un enjeu».

Les conséquences d'un aléa dépendent le plus souvent de la position sociétale de l'endroit d'occurrence [1]. Cette position que nous appelons population est l'ensemble des personnes vivant sur un territoire donné ou susceptible d'être affecté par un aléa.

L'aléa se produit sur un territoire qui est l'élément matériel ou immatériel assurant une fonction dont la détérioration est dommageable ou préjudiciable pour la société.

L'enjeu est l'union entre les ensembles population et territoire. Nous la définissons comme un « élément

matériel ou immatériel assurant une fonction dont la détérioration est dommageable ou préjudiciable pour la société. Les réseaux sont les enjeux auxquels nous nous intéressons dans la suite de ce document. Ils sont souvent appelés systèmes critiques.

2. Risque et Vulnérabilité

La vulnérabilité est « l'incapacité d'un enjeu à résister à l'occurrence d'un aléa et à retrouver efficacement son fonctionnement nominal durant une période de temps donnée». Elle inclue deux composants: Le composant structurel lié à l'organisation physique du réseau (Robustesse), et le composant fonctionnel lié à la circulation des différents flux (Résilience). La robustesse est une propriété statique. Elle définit l'aptitude de résister à une contrainte [2] et signifie que le système va maintenir ses fonctions intactes quand il est exposé aux perturbations [3]. La résilience quant à elle, implique que le système peut s'adapter et retrouver une nouvelle position stable proche de sa situation initiale après l'occurrence de l'aléa [3].

La vulnérabilité est souvent confondue avec le risque. Le risque est la probabilité d'exposition d'un enjeu à un aléa et/ou la probabilité d'avoir des conséquences négatives à un moment donné dans des conditions spécifiées. Comme nous le montrerons, le risque est fonction de la vulnérabilité, et la réduction de l'un entraine celle de l'autre.

L'analyse de la vulnérabilité et du risque sont très peu dissociables. Elle s'applique à un modèle de ou des enjeux considérés. Dans le chapitre suivant, nous présentons la modélisation des réseaux souvent rencontrée dans la littérature.

C. MODÉLISATION DES RÉSEAUX

La modélisation est une représentation du système réelle en vue de l'analyser. Cette représentation peut être mathématique ou graphique. La plupart des systèmes de communication et de transport (réseaux technologiques) peuvent être représenté représentés par un graphe [4]. Dans la littérature les réseaux sont modélisés par des graphes. Un graphe fini $G = (V, E)$ est défini par l'ensemble fini $V = \{V1, V2 \ldots . VN\}$; $(|V| = N)$ dont les éléments sont appelés sommets, et par l'ensemble fini $E = \{E1, E2 \ldots . EM\}$, (|E|=M) dont les éléments sont les arêtes. Nous avons présenté dans [5] les limites d'une telle modélisation. Nous argumentions que :

- Les graphes soient orientés;
- Les graphes soient pondérés;
- Il y ait plusieurs flux (caractérisés par des vecteurs) pour chaque composant;
- Il y ait différents types de sommets. Le type dépend de la fonction réalisée dans le réseau. Cette fonction peut être: Produire, Relayer, Utiliser [6], [3]; auxquels nous ajoutons, Traiter, et Transporter quand il s'agit d'une arête.

A travers le modèle réseau obtenu, on en déduit un modèle de la vulnérabilité. Nous présentons ci-dessous les modèles rencontrés dans la littérature.

D. MODÉLISATION DE LA VULNÉRABILITÉ

Souvent on considère que l'efficacité de la réalisation d'une fonction réseau est affectée par sa structure [7]. À l'occurrence d'un aléa, l'endommagement et les dommages dépendent de l'organisation structurelle et varie d'un réseau à un autre [8]. Analyser la topologie du réseau permet ainsi de comprendre les phénomènes dynamiques qui affectent sa performance [9] et de déterminer ses points faibles [10]. Certains paramètres structurels permettent ainsi une estimation de la vulnérabilité [9], [11].

Dans la littérature, les principaux paramètres de mesure de la vulnérabilité incluent, le degré, le coefficient d'agglomération, la distance moyenne, et le poids [9]. À côté de ces paramètres évidents, on retrouve quatre autres classes : l'efficacité, l'intégrité, les probabilités et les fonctions.

3. Efficacité

[12], [13] et [14] définissent la vulnérabilité comme le manque de performance du réseau. Cette performance appelée aussi efficacité est définie par rapport à la distance moyenne entre les sommets [14] et [13] :

$$\phi(\mathrm{G}) = \mathrm{E}(\mathrm{G}) = \frac{1}{\mathrm{N}(\mathrm{N}-1)} \sum_{\mathrm{i} \neq \mathrm{j} \in \mathrm{G}} \frac{1}{\mathrm{D}(\mathrm{V_i}, \mathrm{V}r_{\mathrm{j}})} \qquad (1)$$

L'efficacité d'un chemin entre deux sommets est la moyenne de l'efficacité de toutes les arêtes constituant le chemin et détermine la fluidité de circulation du flux entre les deux sommets. La résilience qui est une mesure de la vulnérabilité est la baisse de l'efficacité induite par la détérioration d'une arête [14], [15] :

$$\mathrm{V}(\mathrm{E_i}) = \frac{\mathrm{E}(\mathrm{G}) - \mathrm{E}\prime(\mathrm{G})}{\mathrm{E}(\mathrm{G})} \qquad (2)$$

$\mathrm{E}(\mathrm{G})$ est l'efficacité globale du système et $\mathrm{E}'(\mathrm{G})$ est

l'efficacité du réseau après enlèvement de l'arête E_i. La vulnérabilité globale est alors définie par :

$$V(G) = \max[V(E_i)] \qquad (3)$$

4. Intégrité

[16] [17] et [18] définissent la vulnérabilité comme un manque d'intégrité. L'intégrité est le quotient Ng/N0 où Ng est la taille du graphe après endommagement d'une fraction g de sommets par rapport à la taille initiale N0. D'autres auteurs définissent l'intégrité par rapport, au poids, la distance géodésique et la portée (rapport entre la distance et le poids) [12].

5. La probabilité

La vulnérabilité d'un système est mesurée dans [19] et [20] comme la probabilité $P(\max_{t\in T}(X(t)) > x)$ pour une période de temps T, que la conséquence négative $X(t)$ de la perturbation soit plus grande qu'une valeur x.

6. Les fonctions de vulnérabilité

Pour un graphe de N sommets et M arêtes, [8] définit une fonction de vulnérabilité du graphe par:

$$V(G) = \exp\left(\frac{\sigma}{N} + N - M - 2 + \frac{2}{N}\right) \qquad (4)$$

Sa valeur est comprise entre 0 et 1. σ est l'écart type de la distribution du degré.

Les différentes manières de quantifier la vulnérabilité ne tiennent pas compte de certains éléments qui nous semblent importants. Le modèle que nous proposons dans le chapitre suivant essaie de surmonter ces lacunes.

E. MODÈLE RESEAU PROPOSÉ

Le modèle que nous proposons tient compte des limites énoncées dans le chapitre C et inclut les interdépendances entre les composants.

En tenant compte de l'état des composants et du sens des flux, on peut modéliser tous types de liens soit par une dépendance, soit par une influence. La démarche pour y parvenir est explicitée dans les lignes qui suivent.

7. La dépendance

Toute arête entre deux sommets matérialise une dépendance. D'une manière générale b dépend de a s'il existe un flux partant de a à b. La dépendance entre les arêtes et les sommets de mêmes types n'est pas possible. En effet, ce lien s'intègre dans l'architecture du réseau et n'est plus considéré comme une dépendance.

Nous représentons une dépendance par:

8. L'influence

Figure 2: Arête de dépendance

Un composant b est géographiquement dépendant d'un composant a (a influe sur b) s'il n'y a pas de lien fonctionnel entre les deux composants, mais qu'une défaillance de a entraine une défaillance de b. Nous représentons une influence par une arête (en pointillé) de poids nul et ne transportant aucun flux.

Figure 3: Arête influence

Par les arêtes de dépendance et d'influence, nous pouvons modéliser les liens Arête-Arête, Sommet-Arête, Arête-Sommet, et Sommet-Sommet.

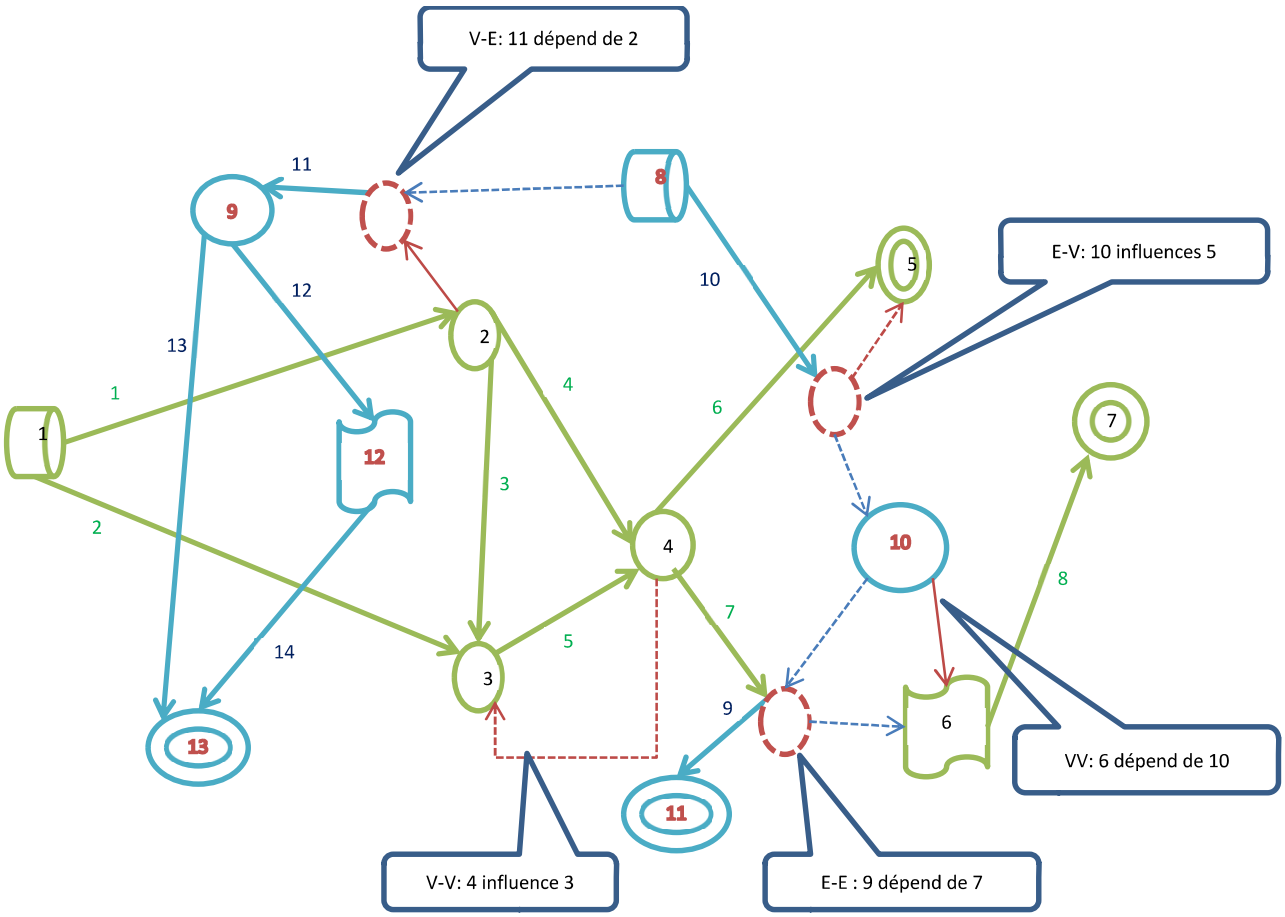

Figure 4: Exemple de Modèle Multi Systèmes Interdépendants

La Figure 3 donne un exemple de modèle. Les sommets virtuels (en pointillé) sont supposés infiniment fiables.

Pour tenir compte de l'influence des éléments du milieu extérieur, nous attribuons à chaque composant une fonction poids. Avec le modèle de réseau obtenu, nous poursuivons notre analyse en présentant le modèle de vulnérabilité ci-dessous.

F. MODELE DU RISQUE ET DE VULNÉRABILITÉ PROPOSE

Il n'y a pas une méthodologie d'analyse de la vulnérabilité admise de tous. Les étapes et les outils sont assez souvent inspirés de l'analyse du risque.

Nous résumons dans les paragraphes suivants les différentes étapes pour l'estimation de la vulnérabilité.

9. La probabilité de l'événement redouté

Nous avons identifié sept types d'aléa susceptibles d'affecter les réseaux (Séisme, Inondation, Volcan, Tsunami, Incendie, Cyclone, Tempête, et Mouvement de terrain). Ceux –ci étant interdépendants, nous utilisons les techniques de Markov pour quantifier leurs probabilités. Cette quantification est basée sur une discrétisation des aléas judicieusement choisis et sur le recueil des données dans les bases telles que celles de l'IGN et de CatNat. Ce qui nous permet d'écrire :

$$P(A) = P\left(\cap E_{\theta\mu}\right) \qquad (5)$$

Où Les $E_{\theta\mu}$ correspondent aux états redoutés

10. La vulnérabilité

En tenant compte des propriétés de la vulnérabilité admises dans la littérature, nous définissons celle-ci par :

$$V = \mathrm{P}(A).\frac{E_F}{E_I} \qquad (6)$$

Où E_F est l'état final du système après l'occurrence de l'aléa, et E_I l'état initial du système avant l'occurrence de l'aléa. $\mathrm{P}(A)$ est la probabilité liée aux aléas considérés.

La vulnérabilité des réseaux dépend ainsi du type de sommet défaillant [2], de la probabilité que les composants ne remplissent pas leurs fonctions ; de la distance entre les sommets sources et cibles ; de l'importance structurelle et fonctionnelle des Sommets Sources et des Sommets Cibles ; et de l'importance relative des flux. L'état initial est calculé par la relation:

$$E_I = \sum_k \sum_l \sum_i \alpha_i P_i \times \beta_l D_{kil} \times \gamma_k C_k \quad (7)$$

Où: α_i est l'importance relative du sommet cible Vi ; P_i : Probabilité que les flux ayant pour cible le sommet

Vi ne soient pas disponibles à ce même sommet ; β_l : Importance relative du flux l ; D_{kil} : Distance entre le sommet cible i et le sommet source le plus proche k, produisant le flux l ; γ_k : Importance relative du sommet source k ; C_k est la centralité du sommet source k ;

L'état final est calculé de la même manière en tenant compte de l'impact des aléas sur le système.

11. Le risque

Le risque est souvent vu comme une entité à deux dimensions: Une Probabilité d'une part et des conséquences d'autre part [23]. Nous l'estimons par:

$$R = P(A) \times \frac{E_F}{E_I} \times C \qquad (8)$$

Où C est l'ensemble des conséquences.

Cet ensemble résulte des impacts du système sur un ou plusieurs enjeux.

$$C = \sum_m \varepsilon_m E_m \qquad (9)$$

Où E_m : Les conséquences relatives à l'enjeu e_m , ε_m l'importance relative de l'enjeu e_m.

$$E_m = \sum_i \alpha_i I_{im} \times P_i + \sum_j I_{jm} C_j \times \sum_l \sum_i \frac{\beta_l F_{ijl} P_{li}}{M_{jl}} \qquad (10)$$

F_{ijl} : La quantité du flux l partant du sommet source $S_i$au dispositif D_j ; I_{im} : L'impact du sommet source S_i sur l'enjeu e_m ; I_{jm} : L'impact du dispositif $D_j$sur l'enjeu e_m ; P_{li} : La probabilité que le flux l soit disponible au sommet S_i ; C_j : La centralité du dispositif D_j ; M_{jl} : La consommation du dispositif D_j en flux l.

G. CONCLUSION ET PERSPECTIVES

Les catastrophes naturelles sont des événements éprouvants pour la société. Par l'intermédiaire des réseaux, elles peuvent affecter un grand nombre de population et conduire à une situation de crise. Dans cette situation, toute décision peut avoir des conséquences parfois irréversibles et mérite d'être justifiée. Elle doit aboutir aux choix rationnels et objectifs. Pour y arriver, avant la prise de décision proprement dite, une formalisation du problème est nécessaire.

Le premier objectif de ce papier était de proposer cette formalisation ainsi que de trouver un moyen de modéliser les réseaux d'une manière générique. Le traitement des décisions nécessitant une analyse du risque, le second objectif était de modéliser ce dernier à travers la vulnérabilité et les conséquences.

Nous avons défini les différents types d'interdépendances et proposer un modèle compatible avec la théorie des graphes. Nous avons également proposé une démarche pour estimer la vulnérabilité, les conséquences et le risque.

Avec notre modèle, on peut en déduire entre autres : le temps de remise en état ; la courbe de réponse en fonction des scénarii; les zones critiques etc.

Par ailleurs, les décisions proprement dites reposent sur des critères. L'identification des ceux-ci et l'agrégation des certains d'eux seront notre prochain terrain d'investigation. Nous envisageons également l'usage des agents cognitifs pour la gestion de la crise.

RÉFÉRENCES

[1] S. Einarsson et M. Rausand, « An Approach to Vulnerability Analysis of Complex Industrial Systems », *Risk Analysis*, vol. 18, n°. 5, p. 535-546, oct. 1998.

[2] J. Johansson, H. Jonsson, et H. Johansson, « Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions », *International Journal of Emergency Management*, vol. 4, n°. 1, p. 4 - 17, 2007.

[3] F. Petit, B. Robert, et J. Rouselle, « Une nouvelle approche pour la caractérisation des aléas et l'évaluation des vulnérabilités des réseaux de support à la vie », 2004.

[4] R. Albert, H. Jeong, et A.-L. Barabasi, « Error and attack tolerance of complex networks », *Nature*, vol. 406, n°. 6794, p. 378-382, juill. 2000.

[5] D. Kamissoko, P. Zaraté, et F. Pérès, « Infrastructure Network Vulnerability (regular paper) », http://www.computer.org, 2011, p. 305–312.

[6] H. Jönsson, J. Johansson, et H. Johansson, « Identifying critical components in technical infrastructure networks », *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 222, n°. 2, p. 235 -243, juin 2008.

[7] S. H. Strogatz, « Exploring complex networks », *Nature*, n°. 410, p. 268-276, 2001.

[8] R. Criado, J. Flores, B. Hernández-Bermejo, J. Pello, et M. Romance, « Effective measurement of network vulnerability under random and intentional attacks », *Journal of Mathematical Modelling and Algorithms*, vol. 4, n°. 3, p. 307-316, nov. 2005.

[9] A. Yazdani et P. Jeffrey, « A note on measurement of network vulnerability under random and intentional attacks », *1006.2791*, juin 2010.

[10] B. C. Ezell, « Infrastructure Vulnerability Assessment Model (I-VAM) », *Risk Analysis*, vol. 27,

n°. 3, p. 571-583, juin 2007.
[11] P. Crucitti, V. Latora, M. Marchiori, et A. Rapisarda, « Error and Attack Tolerance of Complex Networks », 2004.
[12] V. Latora et M. Marchiori, « Vulnerability and protection of infrastructure networks », *Physical Review E*, vol. 71, n°. 1, p. 015103, janv. 2005.
[13] P. Crucitti, V. Latora, et M. Marchiori, « A topological analysis of the Italian electric power grid », *Physica A: Statistical Mechanics and its Applications*, vol. 338, n°. 1-2, p. 92-97, juill. 2004.
[14] S. Arianos, E. Bompard, A. Carbone, et F. Xue, « Power grids vulnerability: a complex network approach », *0810.5278*, oct. 2008.
[15] E. Bompard, M. Masera, R. Napoli, et F. Xue, « Assessment of Structural Vulnerability for Power Grids by Network Performance Based on Complex Networks », in *Critical Information Infrastructure Security*, vol. 5508, Springer Berlin / Heidelberg, 2009, p. 144-154.
[16] L. Dall'Asta, A. Barrat, M. Barthelemy, et A. Vespignani, « Vulnerability of weighted networks », *physics/0603163*, mars 2006.
[17] L. Zhao, K. Park, et Y.-C. Lai, « Attack vulnerability of scale-free networks due to cascading breakdown », *Physical Review E*, vol. 70, n°. 3, p. 035101, 2004.
[18] A. Jamakovic et P. Van Mieghem, « On the robustness of complex networks by using the algebraic connectivity », Berlin, Heidelberg, 2008, p. 183–194.
[19] A. J. Holmgren, « Using graph models to analyze the vulnerability of electric power networks », *Risk Analysis: An Official Publication of the Society for Risk Analysis*, vol. 26, n°. 4, p. 955-969, août 2006.
[20] Å. J. Holmgren, « A Framework for Vulnerability Assessment of Electric Power Systems », in *Critical Infrastructure*, Springer Berlin Heidelberg, 2007, p. 31-55.
[21] Y. Y. Haimes, « On the Definition of Vulnerabilities in Measuring Risks to Infrastructures », *Risk Analysis*, vol. 26, n°. 2, p. 293-296, avr. 2006.
[22] J. Agarwal, D. Blockley, et N. Woodman, « Vulnerability of structural systems », *Structural Safety*, vol. 25, n°. 3, p. 263-286, juill. 2003.
[23] A. Leroy et J.-P. Signoret, *Le risque technologique*. France: Presses Universitaires de France (PUF), 1992.