Mise en cohérence des objectifs du TIPE — Réseau de transmission d'information : Architecture, vitesse et fiabilité

Dimitri Granger Matthias Goffette

June 4, 2017

1 Abstract

Nowadays, networks are everywhere, used by firms to organize themselves, by people to communicate. In computer science, network is a central field. They need to be efficient, in terms of communication speed, and reliable, so that they can resist to accidents and attacks. We focus on two types of networks : homogenous and scale-free. On these, attacks are performed. The methodology is the following : an agent has an initial true information. Then, it passes it to its neighbours. If they are normal agents, they repeat the process, but if they are attackers, they falsify the information before spreading them.

2 Préambule

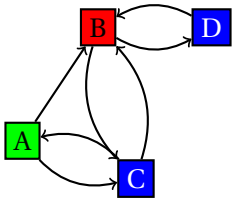
Mon objectif a peu changé depuis la MCOT. J'ai donc poursuivi le travail engagé, c'est-à-dire l'étude de l'impact d'un type d'attaque sur un réseau, selon sa topologie. Cependant, je ne me suis finalement pas concentré sur la vitesse de transmission des informations.

3 Introduction

Conformément à la littérature, la modélisation prend ici la forme d'un modèle multi-agents. Je vais me pencher sur deux types de réseaux, *scale-free* et *homogène*. L'étude d'un réseau *scale-free* est importante, puisque beaucoup de réseaux réels, comme Internet, prennent cette forme. Je les ai ici modélisé par l'agorithme de Barabási–Albert. Cependant, j'ai comparé ce type de réseau avec des réseaux homogènes.

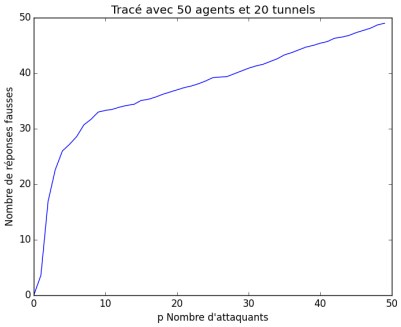
4 Corps Principal

Je me suis dans un premier temps intéressé à la représentation des objets qui seront utiles pour la modélisation d'attaques sur un réseau. Pour cela, j'ai utilisé des objets Pythons : les agents qui représentent les noeuds du réseau, les tunnels qui représentent les arêtes, et un objet qui rassemble les deux premiers, le réseau. Un dernier objet, l'information, est utilisé pour observer la propagation d'informations faussées par les attaquants. Ensuite, il a fallu définir la manière dont l'attaque allait opérer. C'est la que réside la différence avec le travail de Dimitri, qui s'est intéressé à des attaques sur les liens. Je me suis penché sur une attaque sur les noeuds. Ainsi, un noeud peut être soit normal, soit attaquant. Dans le premier cas, il transmettra toutes les informations qu'il reçoit sans les modifier à ses voisins. Mais un attaquant, avant de transmettre des informations, les faussera.



J'ai concentré mon étude sur les réseaux homogènes, et *scale-free*. Pour générer des réseaux *scale-free*, j'ai utilisé l'algorithme de Barabási–Albert. Il consiste à prendre un graphe initial, et à ajouter des nœuds. A chaque ajout d'un nœud i, on le lie à un nœud j avec une probabilité proportionnelle à la connectivité de j.

On obtient des résultats intéressants sur les réseaux homogènes. En effet, conformément à nos attente, on voit que le nombre d'informations fausses dans le réseau va croître avec le nombre d'attaquants. Cependant, cette croissance ralentit, car il va y avoir une redondance d'informations fausses. Avec un grand nombre de tunnels par agent, on observe l'apparition d'une partie affine de la courbe,



* Sur homogène : - dérivée seconde négative - palier * Sur scale-free : - en moyenne, un peu pareil - mais paliers !

*

5 Conclusion générale

Informatique pratique, Informatique théorique, Mathématiques - Autres Domaines

6 Mots-clefs

- *Graphe | Graph*
- *Système multi-agent | Agent-based systm*
- *Réseau robuste | Robust network*
- *Connectivité | Connectivity*
- *Transmission de l'information | Data transmission*

7 Bibliographie commentée

Les réseaux, qu'ils soient physiques ou informatiques, sont vulnérables aux des attaques, qu'elles soient intelligentes ou non. Il convient donc de chercher comment protéger les protéger de telles attaques. Les réseaux permettant la circulation d'informations et de biens, le but de la défense est de garantir, dans un réseau informatique, la véracité des informations qui circulent, et, de manière

générale, la connexité du réseau, pour qu'il reste possible de le parcourir. Notre modélisation retient deux sortes d'attaques : la première étant celle d'un utilisateur malveillant qui chercherait à prendre le contrôle d'un réseau informatique pour répandre de fausses informations, la seconde étant la suppression d'arêtes ou de noeuds composant le réseau. La structure même d'un réseau peut être mise en danger, par exemple par une catastrophe naturelle qui détruirait les câbles ou les centrales électriques. La question est alors de trouver comment organiser un réseau pour qu'il reste fonctionnel, c'est à dire connexe, même après la destruction de certains de ses composants, tout en minimisant le prix de sa construction.

La modélisation de ce problème prend souvent la forme d'un jeu[**?**] entre deux participants. L'un construit un réseau, avec ses noeuds et ses arêtes, et en protège certains. Ces actions ont un coût. L'autre participant, l'attaquant, choisit certains noeuds ou arêtes et les supprime s'ils ne sont pas protégés. Dans une modélisation plus fine, les noeuds et arêtes protégés peuvent aussi être supprimés, avec une certaine probabilité [Bravard-Charroin]. Les résultats montrent que si la protection d'un noeud est peu coûteuse par rapport à la création de liens, le réseau optimal est prend la forme d'une étoile dont le centre est protégé. Au contraire, si la création de liens est moins chère, le réseau optimal sera très dense[**?**]. Le nombre minimal d'arête pour rendre k-connecté un réseau à n noeuds est $\lceil (k*n)/2 \rceil$ selon une démonstration de Frank Harary[**?**].

Il est nécessaire de classer les différents types de réseaux. Gueye[**?**] introduit des mesures de vulnérabilité d'un réseau en étudiant la connexité de ce réseau après le retrait d'une arête. Une autre topologie[**?**] nous permet d'observer les avantages et inconvéniants de certains réseaux. En particulier, les *scale-free networks*, modèle présnt dans de nombreuses situation, sont efficaces pour propager rapidement des données, mais les nœuds ayant une connectivité fort, les serveurs, sont assez vulnérables aux attaques. selon ce même article, les réseaux *bimodaux*, dont les nœuds ont soit x, soit y arêtes sortantes sont ceux qui permettent de présenter le meilleur compromis à ce problème.

8 Problématique retenue

Les réseaux sont susceptibles de subir deux types d'attaques. Les unes détruisent des composants du réseau, les autres cherchent à propager de fausses informations.

Quelle architecture choisir pour rendre un réseau le moins vulnérable possible à ces deux types d'attaques ?

9 Objectifs du TIPE

Notre but consiste à créer un réseau permettant une transmission des informations rapides, tout en résistant efficacement aux attaques, lors desquelles un attaquant prendrait possession de plusieurs nœuds.