Rapport final

Matthias Goffette

June 10, 2017

1 Abstract

Networks 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. We model the networks as a graph, each node representing an agent. 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. The simulation show that for the same mean degree of nodes, homogenous networks are more resiliant than scale-free networks.

2 Préambule

Mon objectif a peu changé depuis la MCOT. J'ai donc poursuivi l'étude de l'impact d'une attaque sur les noeuds du réseau, selon sa topologie. Cependant, je ne me suis finalement pas concentré sur la vitesse de transmission des informations. En effet, cette partie m'a semblé moins intéressante. J'ai préféré me concentrer sur l'étude des attaques.

3 Introduction

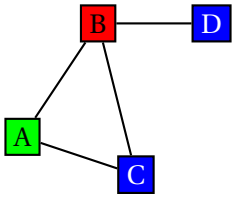
La modélisation prend ici la forme d'un modèle multi-agents. Je traite deux types de réseaux, *scale-free* et *homogène*. Le modèle des réseaux *scale-free* a une importance pratique, puisque beaucoup de réseaux réels, comme Internet, prennent cette forme. Je les ai ici générés par l'agorithme de Barabási–Albert. Les réseaux homogènes sont plus difficiles à mettre en pratique, et donc peu utilisés. Mais il peremettent une base intéressante de comparaison.

4 Corps Principal

4.1 Modalités d'action

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.

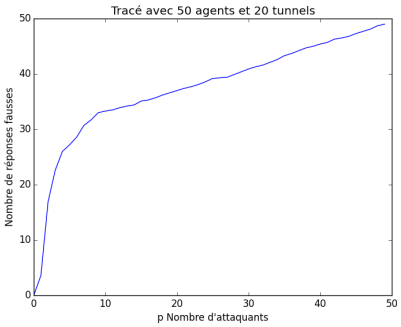
Ensuite, il a fallu définir la manière dont l'attaque allait opérer. Je me suis penché sur une attaque sur les noeuds. C'est là que réside la différence avec le travail de Dimitri Granger, l'autre membre du groupe, qui s'est intéressé à des attaques sur les liens. Ainsi, un noeud peut être soit normal, soit attaquant. Un noeud normal transmettra toutes les informations qu'il reçoit à ses voisins sans les modifier. 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. Cela crée un réseau dans lequel il y a quelques nœuds ayant une forte connectivité, et ue majorité en ayant une faible.

4.2 Restitution des résultats

On obtient des résultats intéressants sur les réseaux homogènes. En effet, conformément à nos attentes, 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, qui correspond à un stade où les seuls nœuds non attaquants sont voisins de l'émetteur.



Pour un réseau *scale-free*, on observe en moyenne le même type de courbe que pour un réseau *scale-free*. Cependant, pour une simulation, on voit qu'il s'agit d'une courbe à palier. En effet, lorsqu'un nœud ayant une forte connectivité devient attaquant, il a un fort impact sur le reste du réseau. Cependant, pour un même degré moyen, on voit que les réseaux homogènes ont en moyenne une plus petite proportion d'informations fausses.

4.3 Analyse - Exploitation - Discussion

Si les résultats sur les réseaux homogènes peuvent être intéressants, ce type de réseau est peu facile à mettre en pratique. C'est un objet principalement théorique. De plus, on a supposé que la probabilité d'être attaquant ne dépend pas de la connectivité. Or en pratique, les serveurs très connectés sont de gros serveurs, généralement plus protégé que les autres. Ils devraient donc être moins souvent infecté.

5 Conclusion générale

Les résultats valident les hypothèses que nous avions formulées. Mais on voit que les réseaux homogènes, bien que plus difficiles à mettre en place, semblent être moins vulnérables que les réseaux scale-free.