

Comment optimiser l'architecture d'un réseau pour résister aux attaques

Matthias Goffette

Lycée La Martinière Monplaisir
Lyon, 18 Mai 2017

Motivations et objectifs

- Réseaux dans tous les domaines : informatique, biologie, sociologie
- Sécuriser les réseaux est un point primordial
 - Base de la communication entre ordinateurs
 - De plus en plus d'attaques pour récupérer les données des utilisateurs
- Objectifs du TIPE
 - Quelle architecture choisir de façon à rendre un réseau le moins vulnérable ?

Travail réalisé

- Modélisation multi-agents d'une diffusion d'information dans deux types de réseaux
- Étudier la proportion d'informations fausses dans le réseau à l'issue de la diffusion
- Paramètres du plan d'expérience :
 - Type de réseau
 - Nombre de noeuds
 - Nombre d'arêtes par noeud

Sommaire

1 Modélisation

- 1 Fonctionnement général
- 2 Les types de réseaux

2 Résultats

- 1 Première modélisation
- 2 Seconde modélisation

3 Conclusion et discussion

Fonctionnement général

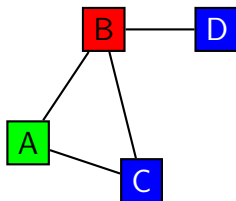
Principe de diffusion de l'information

- Au départ, un agent a une information
- Itération :
 - Parcours des agents un à un
 - Si *normal* : passe son information à tous les voisins qui ne la possèdent pas
 - Si *attaquant* : envoie une information fausse à tous ses voisins qui ne la possèdent pas encore

Plan d'expérience

- Pour chaque jeu de paramètres, on effectue k simulations
- Une simulation consiste en
 - Génération d'un réseau, puis variation du nombre d'attaquants
 - Résultat de la simulation : % d'informations fausses en

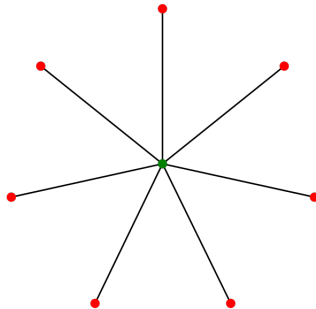
Fonctionnement général



- Initialement, A possède une information vraie
- Itération 1 : B et C reçoivent l'information vraie (B la modifie en faux)
- Itération 2 : D reçoit l'information, fausse, en provenance de B

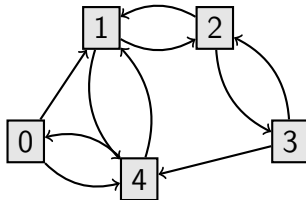
Les types de réseaux - En étoile

- Étoile : Un seul noeud central est connecté avec tous les autres. C'est l'architecture d'un système client-serveur.
- Ce type de réseau est assez facile à étudier.



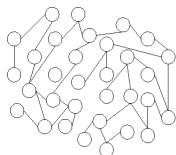
Les types de réseaux - Homogène

- *Homogène* : les degrés sortants de chaque noeud sont égaux
- nous n'étudierons que des réseaux connexes (strictement dans le cas orienté)

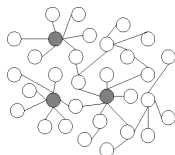


Les types de réseaux - Réseau invariant d'échelle

- *Scale-free*, ou invariant d'échelle : Le nombre d'arêtes par noeud suit une loi de puissance : la probabilité qu'un noeud ait k voisins est $k^{-\gamma}$. Le réseau Internet est de ce type.
- Nous utiliserons l'algorithme de Barabási-Albert, pour lequel $\gamma = 3$.



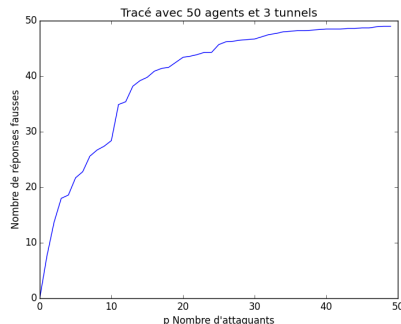
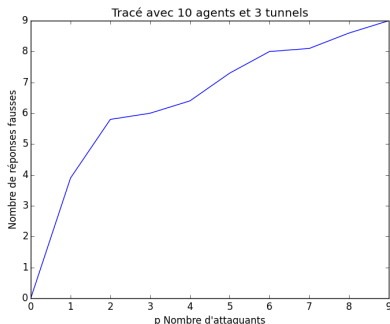
(a) Random network



(b) Scale-free network

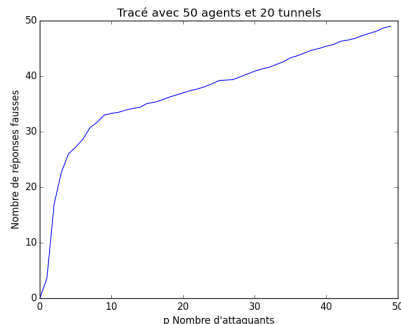
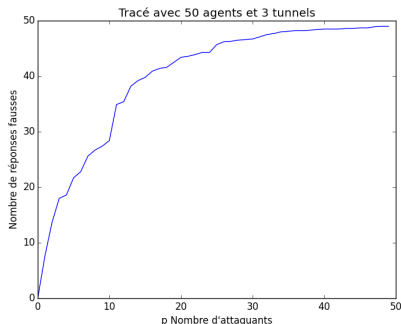


Variation du nombre de noeuds : 10 et 50 noeuds



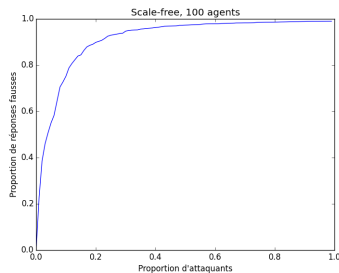
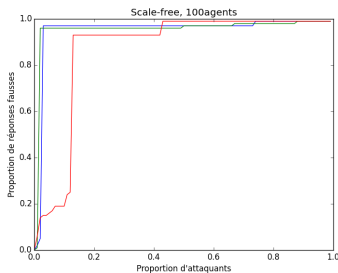
- Nombre de réponses fausses selon le nombre d'attaquants
- Croissant, mais la courbe est concave : plus il y a d'attaquants, et moins l'action d'en ajouter un nouveau est significative

Variation du nombre d'arêtes par agent



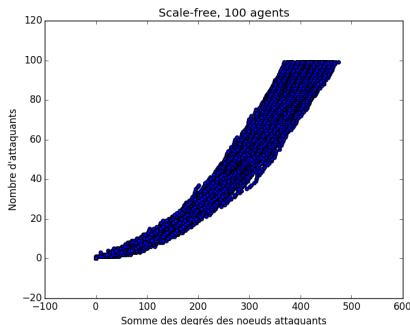
- Variation du nombre d'arêtes par agent
- Courbe se divise en deux parties, la seconde affine
- A l'arrivée sur la dernière partie, les seuls agents ayant des informations vraies sont voisins de l'émetteur

Sur un scale-free network



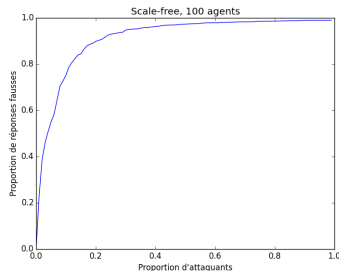
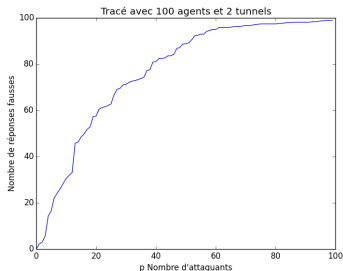
- Présence de paliers : noeuds ayant une forte connectivité deviennent attaquant
- Assez rapidement, la quasi-totalité du réseau reçoit des informations fausses

Sur un réseau invariant d'échelle



- Pour avoir le même nombre de degrés attaquants, le nombre d'attaquants peut varier beaucoup (à une somme de degrés 400, entre 60 et 100 attaquants)

Scale-free et homogène



- Le réseau homogène semble être plus performant, pour une même connectivité moyenne

Conclusion

■ Résultats

- Courbes non linéaires, croissantes
- Pour les graphes homogènes, division en deux parties affines
- Réseaux invariants d'échelle : présence de paliers

■ En pratique

- Le réseau en étoile est peu vulnérable, si le noeud central est non-attaquant
- Réseau homogène difficile à mettre en place
- Dans le réseau scale-free, on a supposé que les noeuds ayant une forte connectivité ont la même probabilité d'être attaquants que les autres. Or en pratique, ce sont souvent des noeuds plus sécurisés.