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

Matthias Goffette

Lycée La Martinière Monplaisir

Lyon, 18 Mai 2017

Motivations et objectifs

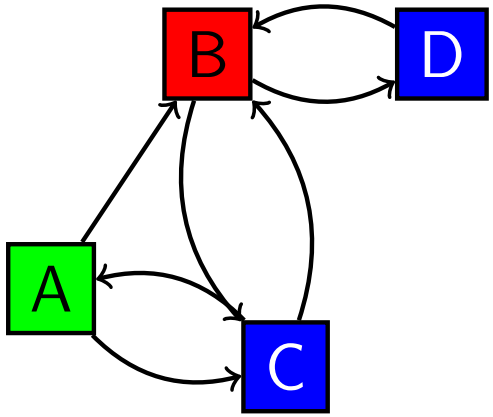
- Réseaux dans tous les domaines : informatique, biologie, sociologie
- Sécuriser les réseau est un point primordial
  - Base de la communication entre ordinateurs
  - De plus en plus d'attaques pour récupérer les données des utilisateurs
  - Un réseau doit pouvoir être résistant
- Objectifs du TIPE
  - Modéliser des réseaux
  - Simuler des attaques, et en faisant varier la topologie du réseau, étudier sa vulnérabilité

Sommaire

Fonctionnement général

- Fonctionnement multi-agents, en effectuant de multiples itérations sur le réseau
- 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 à tous ses voisins qui ne possèdent pas encore l'information une information fausse

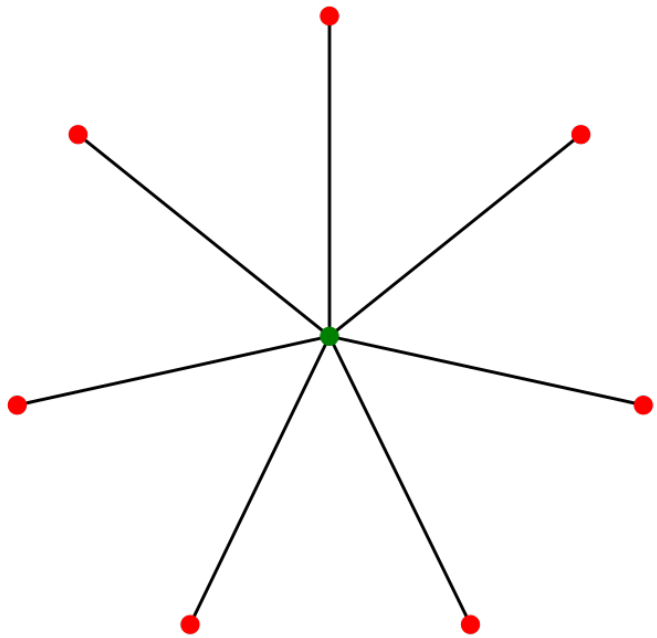
Fonctionnement général



- 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

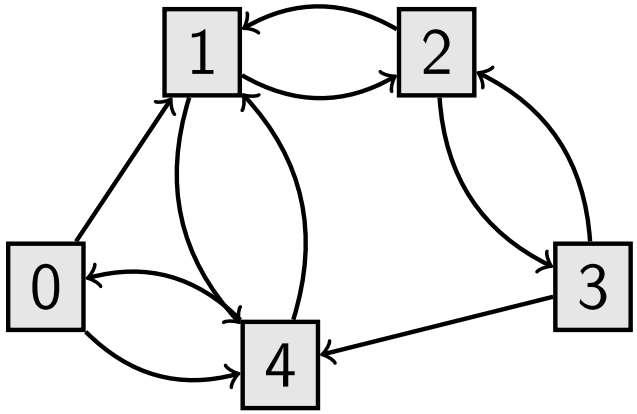
Les types de réseaux - En étoile

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



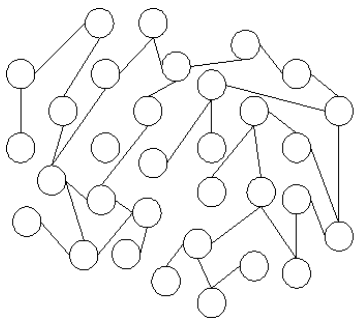
Les types de réseaux - Homogène

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

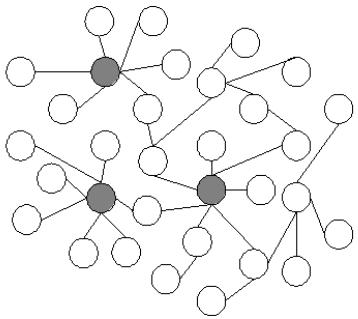


Les types de réseaux - Reseau invariant d'échelle

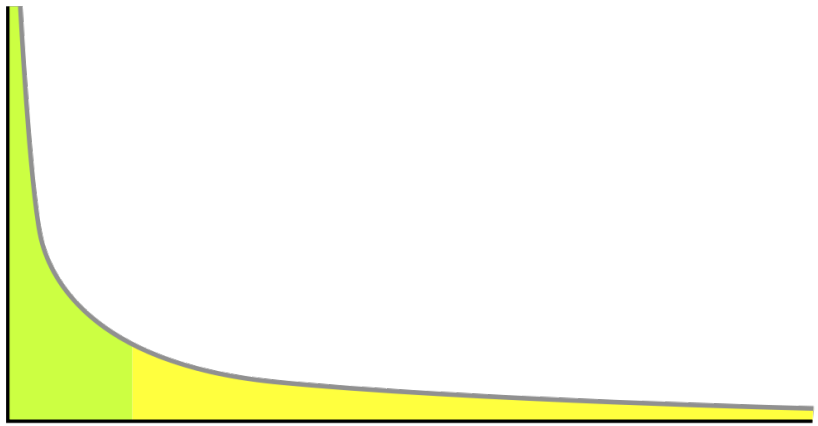
- *Scale-free*, ou invariant d'échelle : Le nombre d'arêtes par noeud suit une loi de puissance : c'est-à-dire que la probabilité qu'un noeud ait k voisins est $k^{-\gamma}$ Le réseau Internet est de ce type.
- Nous utiliserons l'agorithme de Barabási-Albert, pour lequel $\gamma = 3$.



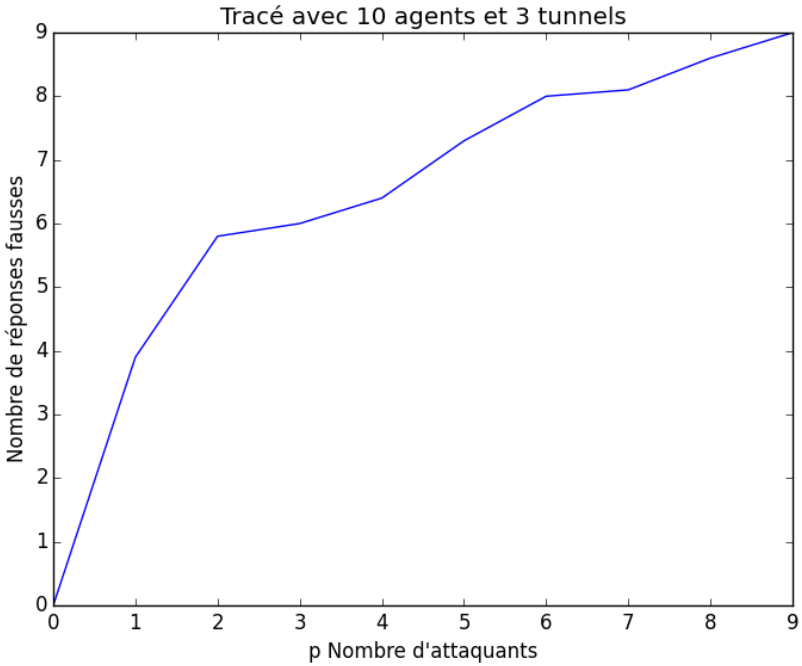
(a) Random network

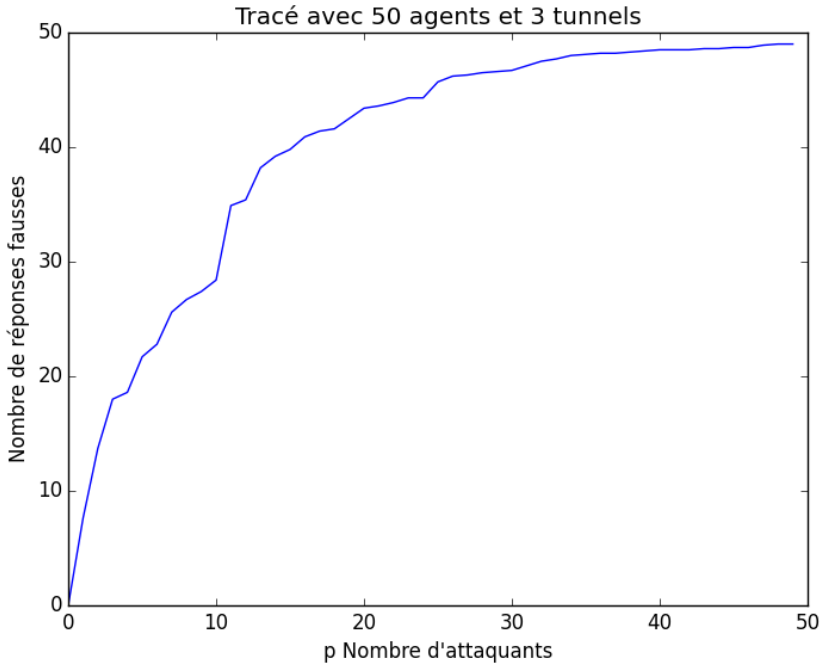


(b) Scale-free network



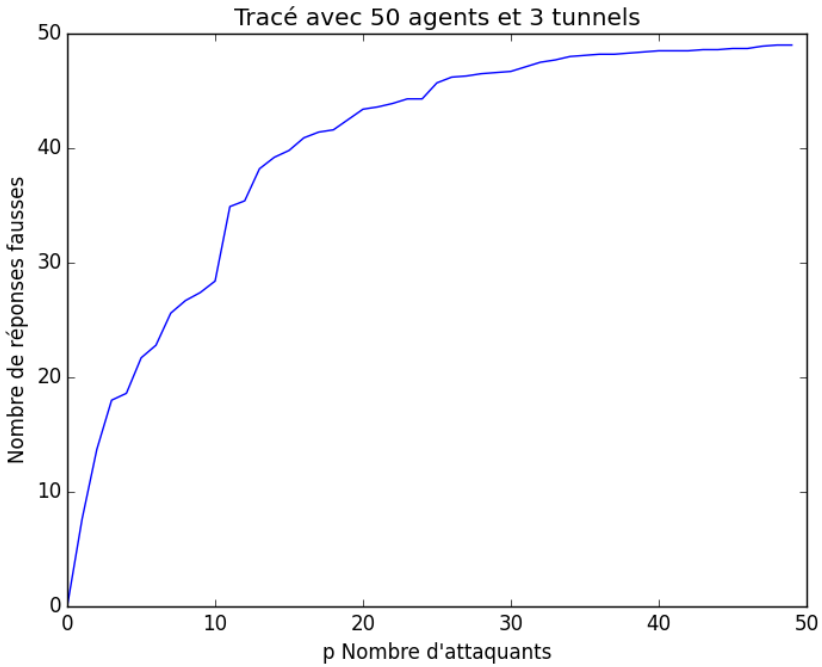
Variation du nombre de noeuds

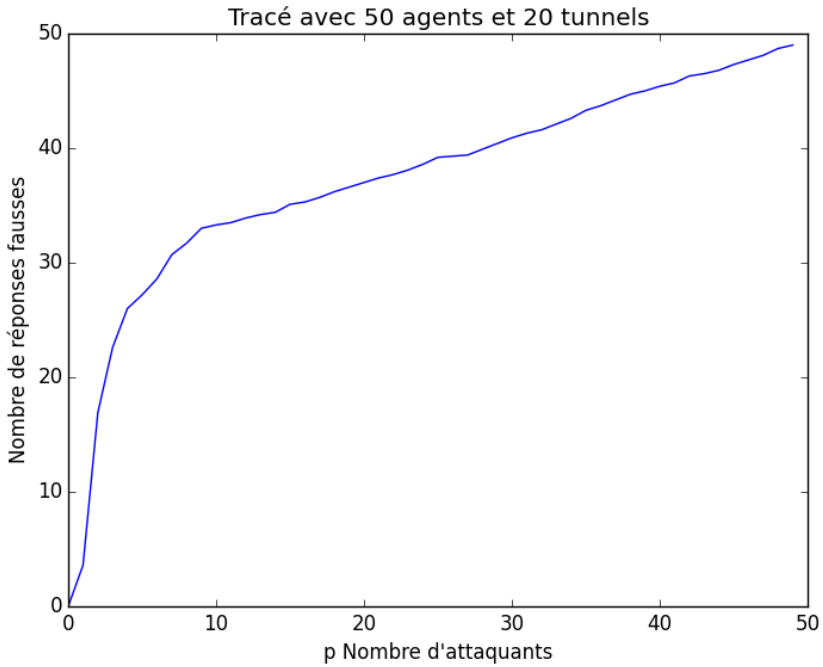




- Nombre de réponses fausses selon le nombre d'attaquants
- Croissant, mais la dérivée seconde est négative : plus il y a d'attaquants, et moins l'action d'en ajouter un nouveau est significative

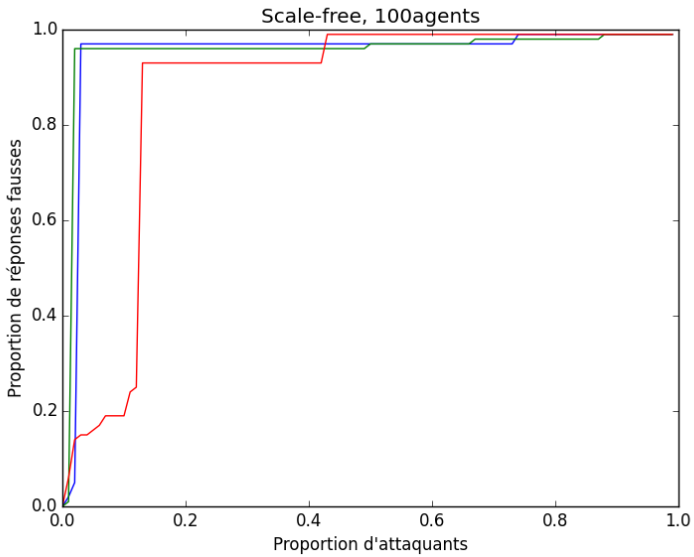
Variation du nombre d'arêtes

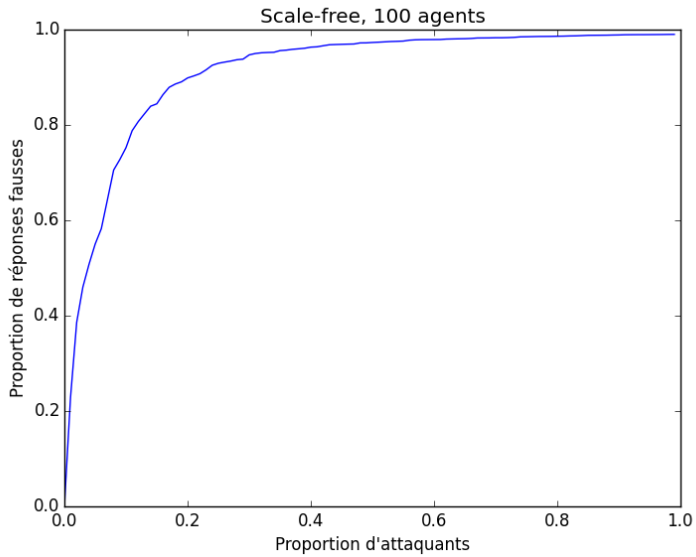




- Variation du nombre de tunnels par agent
- Courbe se divise en deux parties, la seconde affines
- A l'arrivée sur la dernière partie, les seuls agents ayant des informations vrais sont voisins de l'émetteur

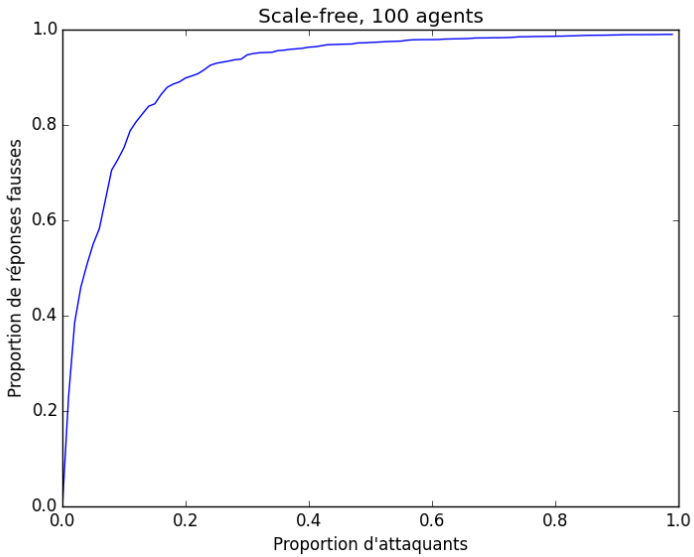
Sur un scale-free network





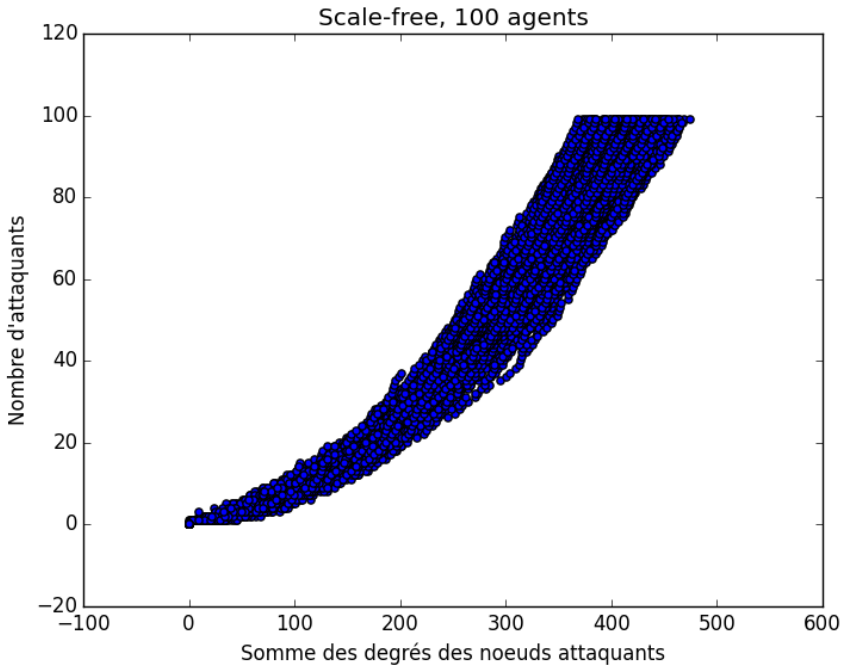
- Présence de paliers : noeuds ayant une forte connectivité deviennent attaquant
- Assez rapidement, la quasi-totalité du réseau reçoit des informations fausses (se confirme sur un grand nombre d'essais)

Scale-free et homogène



- Présence de paliers : noeuds ayant une forte connectivité deviennent attaquant
- Assez rapidement, la quasi-totalité du réseau reçoit des informations fausses (se confirme sur un grand nombre d'essais)

Sur un scale-free network



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

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.