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

Matthias Goffette

June 11, 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 moins vulnérable ?

Travail réalisé

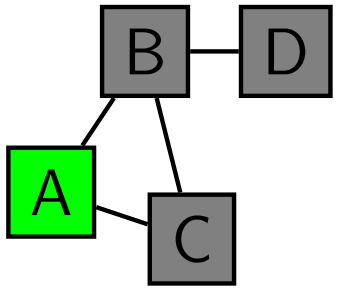
- Modélisation multi-agents d'une diffusion d'information dans deux types de réseaux
- Étudier la proportion d'informations fausses dans le réseau à l'issue de la diffusion
- Paramètres du plan d'expérience :
  - Type de réseau
  - Nombre de noeuds
  - Nombre d'arêtes par noeud

Sommaire

1. Modélisation
   1. Principe de diffusion de l'information
   2. Les types de réseaux
   3. Plan de l'expérience
2. Résultats
   1. Réseau homogène
   2. Réseau invariant d'échelle
   3. Comparaison
3. Conclusion et discussion

Principe de diffusion de l'information

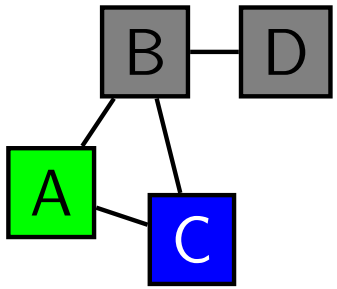
- Au départ, un nœud a une information



- Initialement, A possède une information vraie

Principe de diffusion de l'information

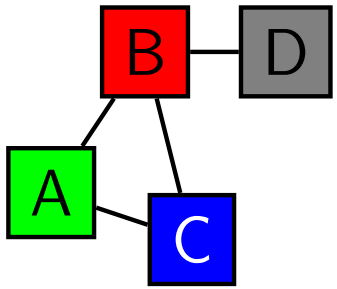
- Itérations
  - Parcours des nœuds un à un, chacun passe son information à ses voisins qui ne la possèdent pas
  - Si le voisin est *normal*, l'information passe inchangée



- Itération 1 : C reçoit l'information vraie

Principe de diffusion de l'information

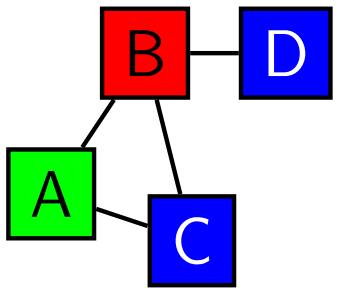
- Itérations
  - Parcours des nœuds un à un, chacun passe son information à ses voisins qui ne la possèdent pas
  - Si il est *attaquant*, l'information passe à Faux



- Itération 1 : B reçoit l'information et la modifie en faux

Principe de diffusion de l'information

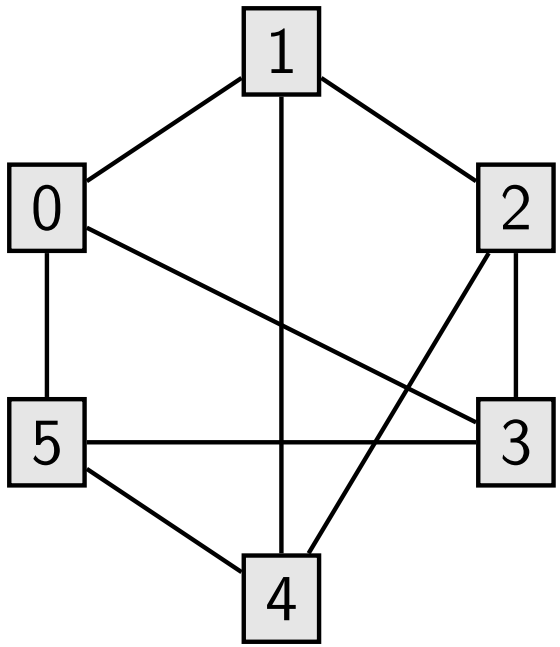
- Itérations
  - Parcours des nœuds un à un, chacun passe son information à ses voisins qui ne la possèdent pas
  - Fin lorsque tous les nœuds ont reçu une information



- Itération 2 : D reçoit l'information, fausse, en provenance de B

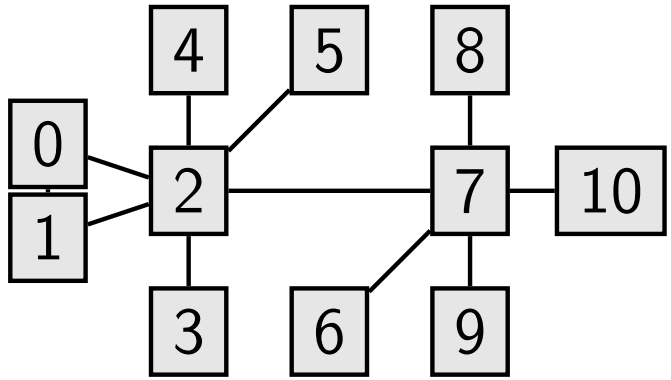
Les types de réseaux - Homogène

- *Homogène* (ou régulier) : tous les nœuds ont le même degré
- Nous n'étudierons que des réseaux connexes



Les types de réseaux - Réseau invariant d'échelle

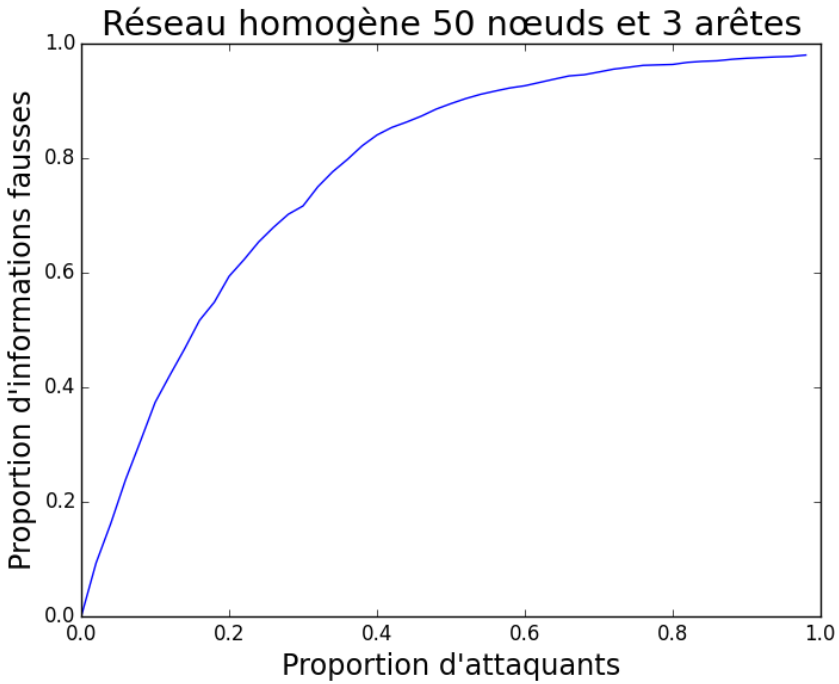
- *Scale-free*, ou invariant d'échelle
  - La probabilité qu'un noeud ait k voisins est $\alpha k^{-\gamma}$
  - Le réseau Internet est de ce type.
- Nous utiliserons l'algorithme de Barabási-Albert, pour lequel $\gamma = 3$ et $\alpha \approx 0.83$.

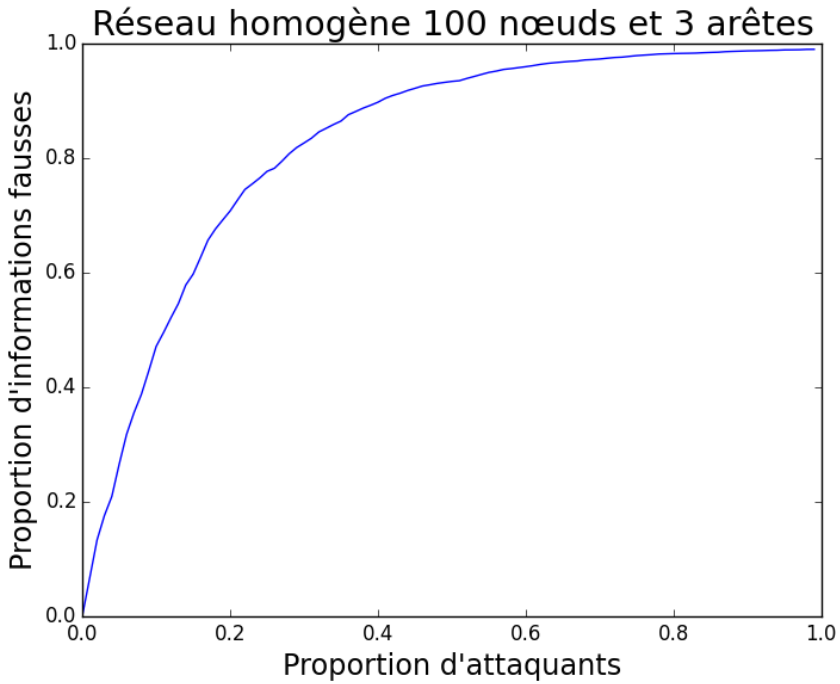


Plan d'expérience

- Pour chaque jeu de paramètres, on effectue k simulations
- Une simulation consiste en
  - Génération d'un réseau
    - Variation du nombre d'attaquants n
    - Diffusion de l'information pour chaque valeur de n
  - Résultat de la simulation : proportion d'informations fausses en fonction du nombre d'attaquants

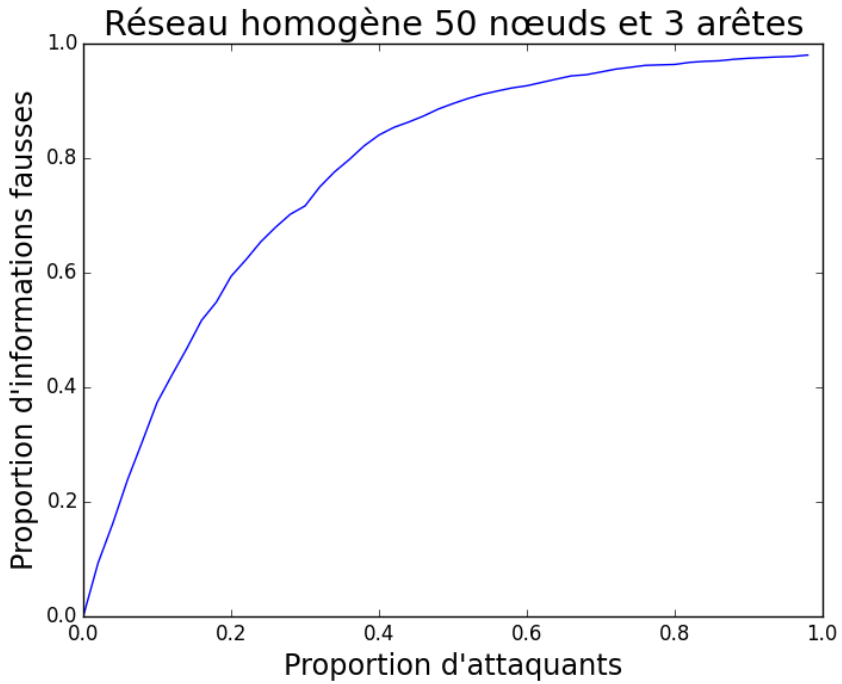
Variation du nombre de nœuds : 50 et 100 noeuds

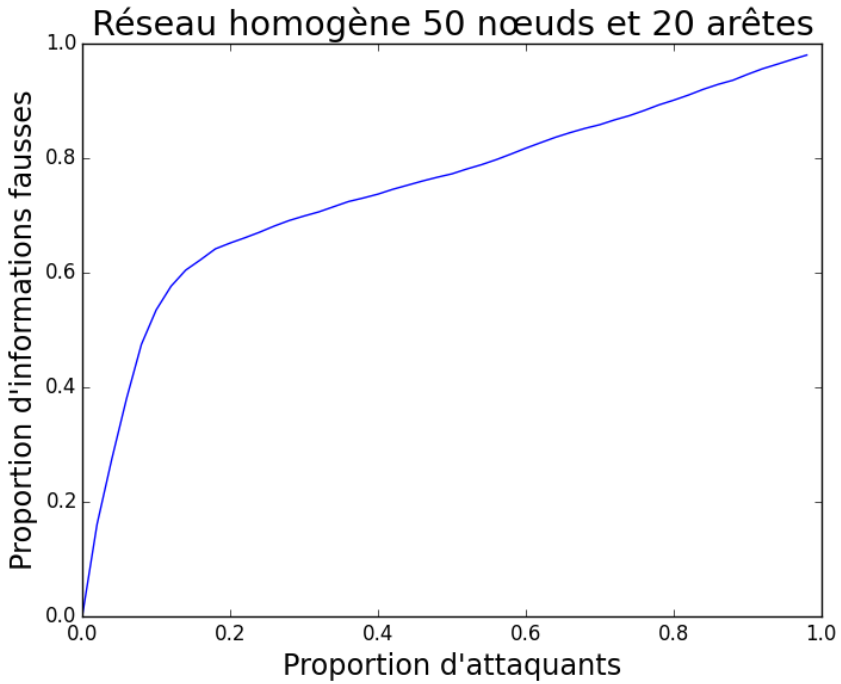




- Plus il y a de nœuds et plus le réseau est vulnérable
- Courbe concave : plus il y a d'attaquants, et moins l'action d'en ajouter un nouveau a un effet important

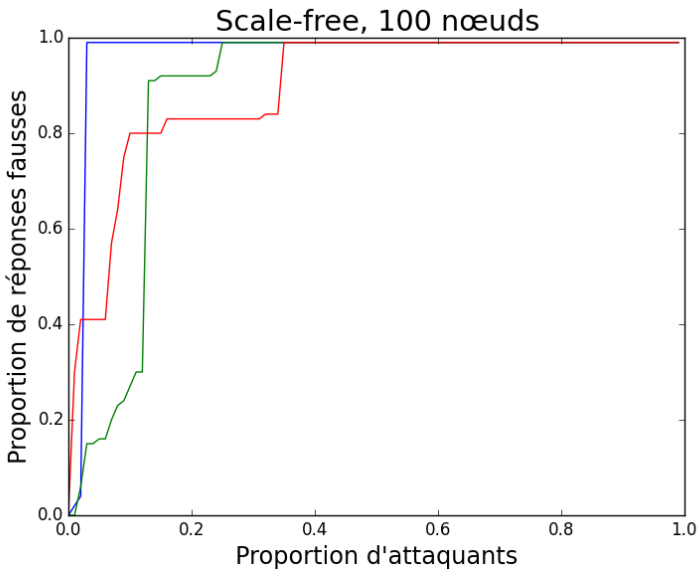
Variation du nombre d'arêtes par nœud

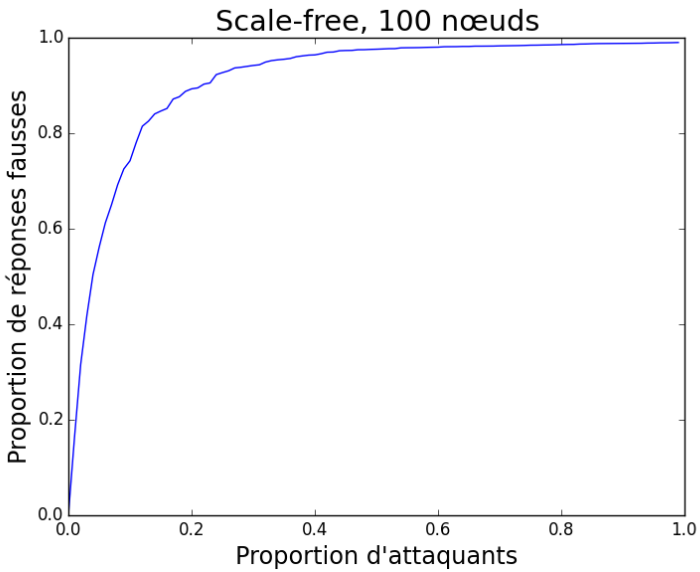




- Courbe se divise en deux parties, la seconde affine
- A l'arrivée sur la partie affine, les seuls nœuds ayant des informations vraies sont voisins de l'émetteur

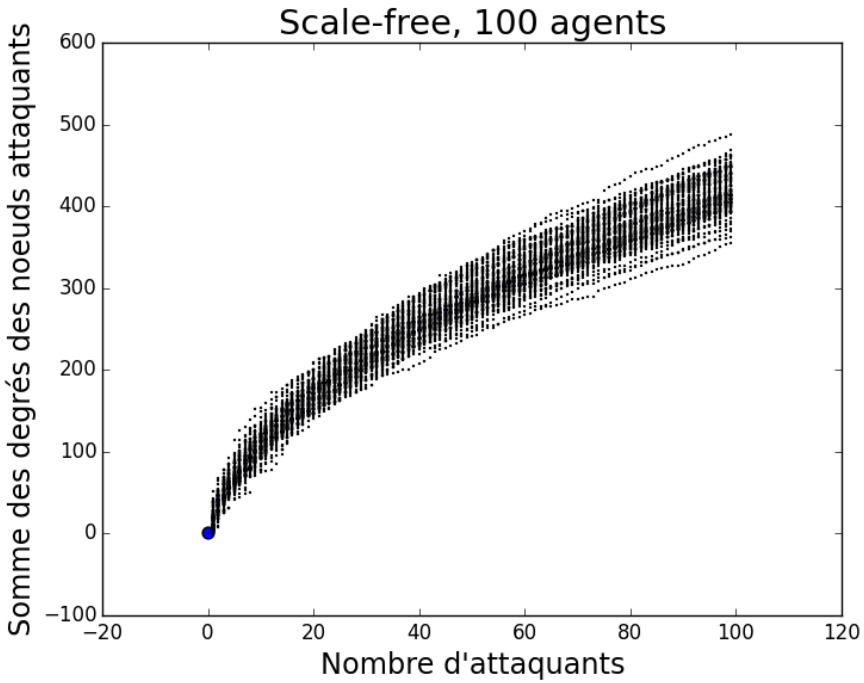
Sur un réseau invariant d'échelle





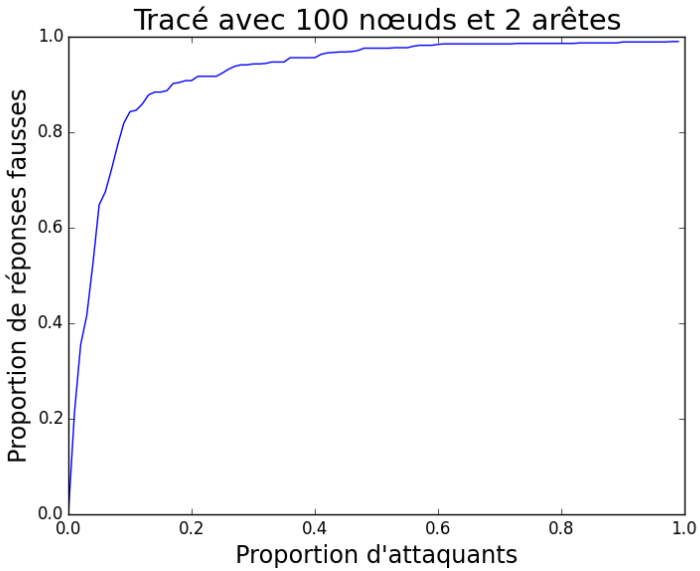
- Présence de paliers : noeuds ayant une forte connectivité deviennent attaquants
- Assez rapidement, la quasi-totalité du réseau reçoit des informations fausses

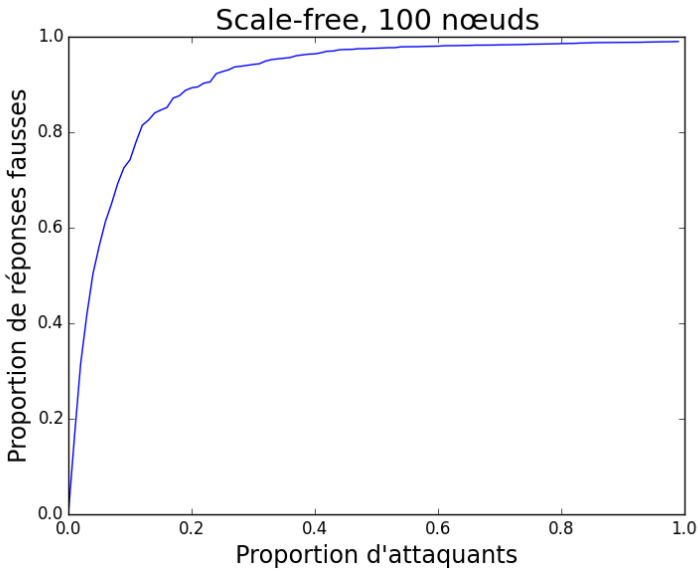
Sur un réseau invariant d'échelle



- Pour un même nombre de degrés attaquants, le nombre d'attaquants peut varier beaucoup (pour somme de degrés 300, entre 40 et 80 attaquants)

Scale-free et homogène





- Le degré moyen d'un nœud pour un réseau invariant d'échelle est 2.
- A degré moyen égal, le réseau invariant d'échelle semble légèrement plus sûr

Conclusion

- Résultats
  - Courbes non linéaires, croissantes
  - Pour les graphes homogènes, division en deux parties, l'une affine
  - Réseaux invariants d'échelle : présence de paliers
- En pratique
  - 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.