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

Dimitri Granger Matthias Goffette

March 16, 2017

1 Positionnement thématique

Informatique pratique, Informatique théorique, Mathématiques - Autres Domaines

2 Mots-clefs

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

3 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 protège certains de noeuds ou arêtes, ces actions ayant 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[**?**].

Gueye[**?**] introduit des mesures de vulnérabilité d'un réseau en étudiant la connexité de ce réseau après le retrait d'une arête. Cela lui permet d'étudier le comportement d'un attaquant du réseau et d'un défenseur avec la théorie des jeux. Il est nécessaire de classer les différents types de réseaux. La classification actuelle [**?**] 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.

Lorsqu'un membre d'un réseaux reçoit plusieurs informations contradictoire, laquelle privilégier ?

4 Problématique retenue

Les réseaux sont suscptibles 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 ?

5 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.

References