Réseau de transmission d'information : Architecture, vitesse et fiabilité

Nous cherchons à modéliser des réseaux informatiques pair-à-pair d'architectures différentes pour étudier comment optimiser la vitesse de transmission des informations, tout en tenant compte de la contrainte que représentent les attaques informatiques.

Les réseaux pair-à-pair occupent aujourd'hui une place importante dans les échanges d'informations. Leur étude a donc des applications concrètes. Ce sujet nous mène à étudier la théorie des graphes et à modéliser des systèmes informatiques multi-agents.

Ce TIPE fait l'objet d'un travail de groupe.

Liste des membres du groupe :

- *GOFFETTE Matthias*

Positionnement thématique

INFORMATIQUE (Informatique Théorique), INFORMATIQUE (Informatique pratique), MATHEMATIQUES (Autres).

Mots-clés

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Système multi-agent	*Agent-based system*
Transmission de l'information	*Data transmission*
Graphe	*Graph*
Connectivité	*Connectedness*
Réseau robuste	*Robust network*

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[1] entre deux participants.

L'un construit un réseau, avec ses noeuds et ses arêtes, et en protège certains. Ces actions ont 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 [2]. 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[1]. Une démonstration de Frank Harary donne le nombre minimal d'arête pour rendre k-connecté un réseau à n noeuds[3].

Il est nécessaire de classer les différents types de réseaux. Gueye[5] introduit des mesures de vulnérabilité d'un réseau en étudiant la connexité de ce réseau après le retrait d'une arête. Une autre topologie[4] 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 noeuds ayant une connectivité fort, les serveurs, sont assez vulnérables aux attaques. selon ce même article, les réseaux bimodaux, dont les noeuds ont soit x, soit y arêtes sortantes sont ceux qui permettent de présenter le meilleur compromis à ce problème.

Problématique retenue

Les réseaux sont susceptibles 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 ?

Objectifs du TIPE

Les différentes recherches trouvées étudient l'évolution de la connectivité d'un graphe soit après le retrait d'arêtes, soit après le retrait de noeuds. Je me propose donc d'étudier la réaction d'un graphe à l'arrivée simultanée de ces évènements, ainsi que l'évolution du diamètre de ce même graphe. Pour cela, je construirai une modélisation informatique permettant de simuler l'attaque d'un réseau, ainsi que l'étude de ses propriétés. Cela me permettra de mener une étude comparative des différentes architectures de réseau, afin de trouver laquelle est la plus robuste.

Références bibliographiques

[1] Marcin Dziubiski, Sanjeev Goyal : Network design and defence : *Games and Economic Behavior - Volume 79, Pages 30-43*

[2] Christophe Bravard, Liza Charroin : Optimal design and defense of networks under link attacks : *Journal of Mathematical Economics - Volume 68, Pages 62-79*

[3] Frank Harary : The Maximum Connectivity of a Graph : *Proceedings of the National*

Academy of Sciences of the United States of America - Volume 48, Pages 1142-1146

[4] KATSUYA SUTO, HIROKI NISHIYAMA, XUEMIN SHEN, NEI KATO : Designing P2P Networks Tolerant to Attacks and Faults Based on Bimodal Degree Distribution : *Journal of Communications - Volume 7, Pages 587-595*

[5] ASSANE GUEYE : Science-Based Metrics for Network Topology Resilience Against Attacks : *Colloque sur la Cryptographie et les Codes Correcteurs d'Erreurs Université Cheikh Anta Diop, Dakar, 2015*