PROJET DE THESE

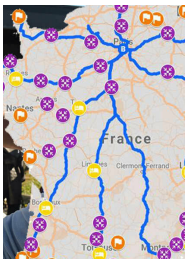
AID IDEES – appel 2026

Matthieu Latapy


manifestation classique


bateau obstruant le canal de Suez


route coupée par un affaissement



saturation des routes par des *anti-pass*


câble internet sectionné


route bloquée par des écologistes

1 Titre ou intitulé de la thèse

Perturbations de Réseaux : Simulation et Gamification

2 Objet de la thèse (5 lignes maximum)

Les réseaux jouent un rôle crucial en défense, et sont donc souvent ciblés par des attaques. L'ampleur potentielle des perturbations est souvent méconnue, ainsi que les points faibles des réseaux et les scénarios catastrophes. Nous proposons de développer un simulateur permettant aux utilisateurs d'être perturbateurs ou défenseurs. La compétition entre les deux permettra d'explorer les vulnérabilités d'une façon inédite, propre à révolutionner l'état de l'art.

3 Descriptif de la thèse (1 page environ)

Qu'il s'agisse de communication, de transport, d'énergie, ou d'autres, les réseaux jouent un rôle crucial pour la société et pour la défense. Or, **la plupart de ces réseaux subissent des attaques**, qu'il s'agisse de sabotages, d'exploitations de failles, de bombardements, ou encore de perturbations géo-politiques. Or, la vulnérabilité de ces réseaux, c'est-à-dire leurs points faibles et l'impact potentiel de telles attaques, est mal connue.

Nous pensons que cette méconnaissance est en grande partie dûe au fait que l'essentiel de la recherche est dédiée à la conception de réseaux fiables et robustes ; **très peu de travaux prennent le parti des attaquants et recherchent activement des vulnérabilités**. On est loin d'une situation comme celle de la cryptologie, par exemple, où beaucoup de recherches sont menées pour mieux coder les échanges (la cryptographie), mais beaucoup de recherches visent également à casser ces codages (la cryptanalyse).

Le but de ce sujet est de concevoir un simulateur permettant d'explorer expérimentalement les vulnérabilités des réseaux. Il s'agira d'abord de lever les verrous méthodologiques soulevés par le développement d'un simulateur générique (s'appliquant à une vaste gamme de cas pratiques). Les résultats obtenus permettront d'implémenter un

logiciel de simulation capable d'interagir avec ses utilisateurs en leur donnant le rôle d'attaquants et/ou de défenseurs. La compétition entre les deux types d'utilisateurs permettra d'explorer réellement les vulnérabilités : une vulnérabilité réelle est décelée par une attaque que les défenseurs ne peuvent pas endiguer.

Notre approche repose sur la gamification : en mettant attaquants et défenseurs face à face, nous espérons donner une dimension ludique à la recherche de vulnérabilité, dans laquelle deux partis s'affrontent et contrecarrent leurs ripostes réciproques. Cette approche a l'avantage de rendre la recherche de vulnérabilités bien plus réaliste que l'application directe d'un algorithme, qui fait souvent abstraction des réactions adverses. Notre simulateur devra donc faire un retour réaliste, temps-réel et lisible sur l'effet des actions des utilisateurs, notamment en affichant un rééquilibrage de l'activité dans le réseau suite à une action utilisateur (en attaque ou en défense).

Toutefois, il ne s'agit pas pour nous de tourner le dos à la vaste littérature disponible pour déceler de potentielles faiblesses dans des réseaux. Au contraire, **le simulateur fournira une assistance algorithmique active aux utilisateurs**. Cette assistance prendra la forme d'un tableau de bord affichant un large éventail d'outils pour la conception d'attaques et pour la défense des réseaux. Ces outils prendront la forme de métriques décrivant l'état du réseau et de ses composantes, mais aussi les caractéristiques structurelles et dynamiques des nœuds et liens du réseau. Par exemple, le simulateur permettra de calculer des coupes dynamiques, des métriques de centralité (comme la *betweenness* ou le *pagerank*, par exemple), ou encore de décomposer le réseau en sous-réseaux (*clusters* ou *communautés*).

Ces ambitions soulèvent plusieurs défis méthodologiques, détaillés dans la prochaine section.

Soulignons auparavant que **le simulateur sera diffusé sous licence libre (*open source*)** et conçu pour encourager la communauté à s'en emparer. Nous espérons ainsi favoriser son développement au-delà de la thèse, notamment via la modélisation plus fine de cas particuliers importants ou l'ajout de davantage d'outils d'aide à l'attaque et à la défense. Ainsi, notre ambition dans cette thèse est seulement de développer un premier prototype, visant à établir une *proof of concept* et fournissant un cadre pour plus de développements.

Soulignons également que **l'approche gamifiée que nous proposons est résolument nouvelle** dans le domaine de la robustesse des réseaux, et elle vient en complément des approches classiques. Nous pensons qu'elle est de nature à faire progresser significativement l'état-de-l'art et même à bouleverser les pratiques.

Enfin, ce sujet est de **nature profondément duale**, avec un intérêt fort en défense des infrastructures et des populations lors d'attaques (notamment cyberattaques) sur les réseaux, et en conception de réseaux robustes ; ces problématiques se posent en contexte défense comme civil. Nous les situons dans la thématique prioritaire de la cybersécurité (maîtrise de l'exposition au risque cyber, maîtrise des impacts des attaques cyber) car les réseaux d'infrastructures sont des cibles privilégiées de cyberattaques, souvent internationales. L'approche scénarisée de la Red Team Defense peut également être concernée (simulation de scénarios).

4 Programme de la thèse (2 à 4 pages)

Le développement du simulateur présenté ci-dessus soulève plusieurs défis que nous présentons ci-dessous. Ces défis constituent les tâches à mener pendant la thèse. Soulignons toutefois que nous les mènerons en parallèle et non en séquence : plutôt qu'apporter une

réponse parfaite à un des défis avant de passer au suivant, nous apporterons une première réponse triviale à chacun d'eux, afin de rapidement obtenir un premier simulateur, certes peu réaliste et peu performant, mais opérationnel. Nous identifierons ainsi les éléments clés et les points bloquants, et adopterons une approche itérative pour affiner les solutions progressivement. Nous obtiendrons ainsi une série de versions du simulateur de plus en plus performantes et réalistes.

Rappelons que, plutôt qu'un simulateur lourd et complexe, **l'objectif est d'établir un premier prototype simple et fonctionnel**, quitte à sacrifier dans une certaine mesure le réalisme. Il s'agit d'établir la faisabilité d'un tel simulateur, et de le rendre suffisament modulaire pour qu'il soit ensuite extensible et permette d'explorer des scénarios variés. Le simuateur devra être suffisament interactif pour mener ces explorations, avec une dimension *gamification* : un utilisateur peut chercher à perturber au maximum le réseau, pendant qu'un autre lutte contre ces perturbations.

Défi 1 : Modélisation du réseau.

L'objectif n'est pas de modéliser précisément un réseau en particulier, mais d'abstraire ce que la plupart des réseaux d'infrastructures ont en commun, et de permettre ensuite la spécialisation au cas par cas, si besoin.

En un premier temps, **nous modéliserons le réseau comme un graphe, dans lequel les nœuds et les liens ont une certaine capacité et une certaine charge**, évoluant au cours du temps. De plus, nous supposerons en un premier temps que les réseaux considérés sont spatialisés : les nœuds ont une position dans le plan, ce qui permet de les visualiser facilement. Le simulateur devra être capable de lire divers réseaux en entrée à partir de fichiers de données.

On considèrera le cas des réseaux urbains comme un exemple paradigmatique en se basant sur les cartes d'OpenStreetMap et la librairie OSMnx, qui permet de les exploiter confortablement. La disponibilité de ces données d'excellente qualité offre déjà une diversité de cas, à travers les différentes villes cartographiées. On considèrera également des réseaux routiers à plus grande échelle, entre les villes d'un pays par exemple.

Défi 2 : Modélisation du trafic.

Il s'agit ensuite de modéliser le trafic sur ce réseau, c'est à dire les demandes de déplacements, et les chemins empruntés pour ces déplacements. Les demandes sont typiquement modélisées par des matrices origine-destination indiquant les points de départ et d'arrivée. Les déplacements peuvent être initialement modélisés par des plus courts chemins, une approximation simple mais qui a fait ses preuves. On enrichira ensuite ces modèles de déplacements avec des modèles de flux ou de transports, avec des modèles de marche aléatoires biaisées, ou encore avec des modèles bio-inspirés, par exemple.

La modélisation de trafic sur un réseau est un domaine vaste et riche en soi. Ici, l'objectif est avant tout d'être capables de rapidement calculer une charge pour chaque nœud et/ou lien du réseau, et ce de façon dynamique. Non seulement un changement dans la structure du réseau (ou dans la capacité de ses éléments) doit avoir des conséquences sur le trafic, mais le trafic lui-même induit une charge et une potentielle saturation d'éléments du réseau, qui à leur tour engendrent une adaptation du trafic. Modéliser ces boucles de rétroaction se fera

via une haute dynamique du modèle, qui recalculera en permanence le trafic en cours. A terme, les matrices origine-destination elles-mêmes seront dynamiques.

Défi 3 : Modélisation des perturbations

Les attaques sont classiquement modélisées par des suppressions de nœuds et/ou liens, choisis par l'attaquant, et nous suivrons cette convention en un premier temps. Toutefois, les nœuds et/ou liens supprimés sont restaurés au bout d'un certain temps, et ils ne sont souvent pas complètement bloqués (supprimés), mais l'attaque a un impact sur leur charge. Les attaques seront donc finalement modélisées par des suppressions (temporaires) de nœuds et/ou liens, mais aussi par des modifications de leurs capacités. C'est sur ces modifications du réseau que l'utilisateur attaquant agira.

Le simulateur devra être capable de rendre compte des conséquences de ces attaques, y compris des effets en cascade potentiellement induits : une perturbation d'un lien peut engendrer une nouvelle répartition de la charge, qui a son tour perturbe des liens, ce qui induit une nouvelle répartition de la charge, et ainsi de suite. La notion de retour à la normale (portentiellement différente de l'état initial) et la caractérisation des conséquences d'une attaque (quel sous-réseau impacté, avec quelle temporalité) sera un des questionnement à aborder : comment décrire une perturbation de réseau ?

Enfin, il s'agira également de modéliser les contre-mesures, c'est à dire les actions des défenseurs du réseau. En un premier temps, celles-ci peuvent consister en le rétablissement de nœuds et/ou liens supprimés. Mais il faudra à terme prendre en compte certaines contraintes réalistes, comme par exemple le fait qu'une intervention suppose un déplacement sur place, et qu'elle a elle-même un impact sur la charge du réseau. Les attaquants pourraient se servir de ces interventions elles-mêmes pour perturber le réseau.

Défi 4 : Assistance algorithmique

Les utilisateurs du simulateur, attaquants comme défenseurs, auront à leur disposition une batterie d'algorithmes permettant de calculer des métriques importantes pour leurs actions. Par exemple, les métriques de centralité (comme la *betweenness* ou le *pagerank*) permettent d'identifier des liens et des nœuds particulièrement importants (car ils sont sur de nombreux plus courts chemins, ou car ils sont eux-mêmes reliés à beaucoup de liens ou nœuds importants, respectivement). Ce sont des nœuds et/ou liens à cibler lors d'attaques.

Mais il est clair qu'une attaque sur un nœud ou un lien change les indicateurs, et peut impliquer qu'un lien auparavant peu important devienne crucial car une grande partie du trafic est redirigé vers lui. Il s'agira donc de mettre à jour les métriques en temps réel, et même de proposer des métriques pouvant quantifier ces changements. Ces métriques sont potentiellement non scalaires : il peut s'agir de courbes ou de distributions, par exemple.

De façon plus générale, le simulateur proposera à l'utilisateur des stratégies d'attaque plus ou moins élaborées, et pré-calculées. L'utilisateur attaquant pourra faire son choix dans ces propositions, ou les combiner à sa guise. L'utilisatuer défenseur pourra contrer ces attaques, ce qui permettra en retour à l'attaquant d'améliorer sa stratégie. Itérer cette boucle vertueuse permettra de découvrir les vraies vulnérabilité du réseau considéré.

Défi 5 : Interface et gamification

Il est crucial, pour que le simulateur soit utilisable, qu'il soit équippé d'une interface agréable, riche mais lisible. En particulier, il doit présenter une visualisation claire du réseau et de son état (charge, congestions, etc). Des indicateurs seront affichés de façon lisible (valeurs mais également couleurs) à côté de cette carte.

En complément, le tableau de bord du simulateur devra afficher une grande quantité d'inforations pour l'aide à l'attaque ou à la défense. Ces affichages pourront être numériques, mais également sous forme de courbes, et de façon plus générale via des moyens plus intuitifs comme des jauges. Les utilisateurs devront en un premier temps indiquer leurs actions en ligne de commande, mais à terme le simulateur permettra une interaction à la souris, via une interface graphique.

Soulignons qu'attaquants et défenseurs n'ont pas nécessairement le même tableau de bord. Ils voient le même réseau et son état, mais n'ont pas besoin des mêmes métriques pour leurs stratégies. Chacun est aveugle aux décisions de l'autre, mais voit leurs effets potentiels.

Planning de thèse

La première année de thèse devrait permettre de produire deux versions complètes du simulateur : une première version implémentée avec les choix de modélisation et les algorithmes les plus simples, permettant de définir l'architecture du simulateur et les structures de données de base ; et une seconde version dans laquelle les choix de modélisation seront un peu moins naïfs et l'attirail algorithmique sera plus élaboré. Ce travail permettra une publication sur la question de la modélisation du triptyque infrastructure–demande–trafic, et une

Outre l'amélioration continue du simulateur, la seconde année mettra l'accent sur la gamification : comment interfacer le simulateur aux différents types d'utilisateurs, comment synchroniser les actions des attaquants et des défenseurs, comment modéliser raisonnablement la capacité des contre-mesures, leur impact sur le réseau, et la capacité d'adaptation des attaquants ? Ici aussi, nous adopterons une approche incrémentale, avec une première version gamifiée du simulateur faisant les choix les plus simples, puis une version plus élaborée.

L'amélioration du simulateur permettra des publications sur l'impact d'une modification sur la nouvelle répartition de charge, sur les effets en cascades produits, ou encore sur l'existence de stratégies d'attaques qu'on ne puisse pas contrer (ou pour un coût prohibitif).

La troisième et dernière année sera consacrée à la finalisation d'une version avancée du simulateur, capable de lire des données de différents réseaux, de proposer une aide algorithmique avancée aux utilisateurs, et de leur fournir une interface permettant une exploration ludique des possibilités d'attaques. Cette année sera également consacrée à la finalisation et la présentation d'articles, et à la rédaction du mémoire de thèse.

5 Références (5 références principales, par exemple)

Nous listons ici cinq de nos publications liées de près au sujet.

1. *Computing Betweenness Centrality in Link Streams.* Frédéric Simard, Clémence Magnien, Matthieu Latapy. Journal of Graph Algorithms and Applications (JGAA) 27(3),

2023.

2. *Weighted, Bipartite, or Directed Stream Graphs for the Modeling of Temporal Networks.* Matthieu Latapy, Clémence Magnien, Tiphaine Viard. Invited chapter in *Temporal Network Theory*, Springer, edited by Petter Holme and Jari Saramäki, 2019.
3. *Stream graphs and link streams for the modeling of interactions over time.* Matthieu Latapy, Tiphaine Viard, Clémence Magnien. Social Network Analysis and Mining (SNAM) 8(1), 2018.
4. *Impact of random failures and attacks on poisson and power-law random networks.* Clémence Magnien, Matthieu Latapy, Jean-Loup Guillaume. ACM Computing Surveys 43(3), 2011.
5. *A radar for the internet.* Matthieu Latapy, Clémence Magnien, Frédéric Ouédraogo. Complex Systems, 20(1), 2011.