Simulateur de propagation de virus et d'antivirus
Mode d'emploi

Yassine Mehmouden

Table des matières

1 Introduction

Ce document présente les spécificités du simulateur de propagation de virus et d'antivirus. Beaucoup d'éléments pouvant être nécessaires à la compréhension sont expliqués dans le mode d'emploi du simulateur de propagation de base avec les honeypots.
Ce document se veut être une mise à jour du document précédent, expliquant les différences entre les deux modèles de simulation.

1.1 Principe général

Cette application permet de simuler la propagation d'un virus au sein d'un réseau. Il est possible d'utiliser une stratégie de défense tout comme dans le simulateur de base mais contrairement à ce dernier, il ne s'agit plus de honeypots ou bien de détections de propagation de virus en surveillant des arêtes mais de diffusion d'un antivirus au sein du réseau après un certain temps.
Le modèle utilisé est, comme pour le précédent simulateur, un modèle SIR avec les changements d'états suivants :

— S $\rightarrow$ I, lors de la contamination d'un noeud susceptible par un noeud infecté. Les noeuds portant l'antivirus ne peuvent plus être infectés par le virus.

— S $\rightarrow$ R ou bien I $\rightarrow$ R, lors de la diffusion de l'antivirus.

Dans la suite, nous allons présenter les principales différences avec le modèle de base.

2 Probabilités de changements d'état

Dans ce nouveau modèle, la priorité est donnée aux changements d'états liés à la propagation du virus et de l'antivirus. Ainsi, il n'est plus possible de voir des changements d'état S $\rightarrow$ R sans diffusion d'antivirus, mais il reste possible de donner une probabilité non nulle de changement d'état de I vers S, c'est-à-dire une probabilité non nulle pour qu'un noeud infecté redevienne susceptible durant chaque tour.

3 Probabilités d'infections

Une nouveauté par rapport au modèle de base est la possibilité de définir les probabilités d'infection.
Les infections, par le virus ou par l'antivirus, ne réussissent plus forcément à tous les coups, l'utilisateur doit choisir des probabilités d'infection pour chacun des deux et les contaminations à chaque tour ne se font qu'avec ces probabilités.

4 Injection de l'antivirus

La différence principale entre ce modèle et le précédent est l'injection dans le réseau d'un antivirus qui se propage à travers les arêtes à la manière du virus. Ainsi, l'utilisateur doit choisir à partir de combien de tours l'antivirus est injecté.
Un tour est composé d'une boucle sur les noeuds du graphe, chaque noeud pouvant diffuser quelque chose, virus ou antivirus, peut alors essayer de contaminer un ou plusieurs voisins. L'utilisateur du simulateur peut alors choisir s'il souhaite que l'antivirus soit injecté au début de la simulation dans un noeud tiré aléatoirement [1] dans le réseau ou bien qu'il soit injecté plus tard.

1. Le noeud tiré peut être susceptible ou infecté.

5 Types de propagation

On ne considère désormais plus que deux types de propagation pour le virus et l'antivirus :

— La *propagation unicast* : chaque noeud infecté peut essayer de contaminer un seul de ses voisins.

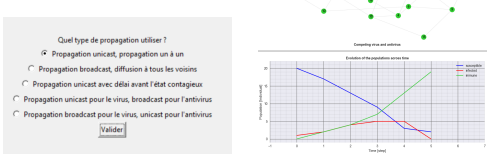
— La *propagation broadcast* : chaque noeud infecté peut essayer de contaminer tous ses voisins. Dans le cadre de la diffusion de l'antivirus, tous les voisins sont concernés mais dans le cadre de la diffusion du virus, seuls les voisins susceptibles peuvent faire l'objet de cette contamination.

6 Informations supplémentaires

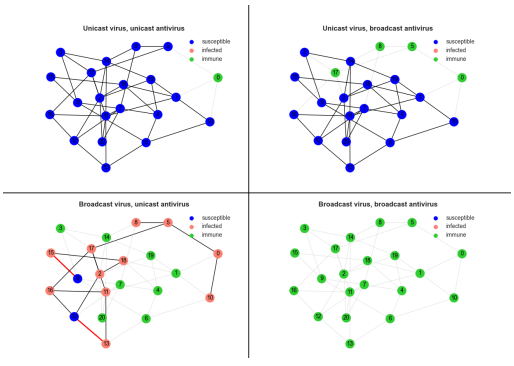
Cette application n'est pas disponible en ligne de commande, seule la version graphique existe. Il est nécessaire d'avoir au minimum **Python 3.10** pour pouvoir la faire tourner. Il sera, tout comme pour le premier simulateur, nécessaire de télécharger quelques bibliothèques comme *Networkx*.

Il existe un dernier type de propagation, contenant 4 états et qui se base sur un modèle SEIR (Susceptible, Exposed, Infectious, Resistant) : après avoir été infecté par le virus, un noeud n'est pas directement contagieux, ce n'est qu'après un tour d'incubation qu'il peut lui aussi commencer à transmettre le virus. Ce dernier mode de propagation permet d'étudier un modèle différent de tous les autres et ainsi de pouvoir observer de nouvelles dynamiques de propagation.

Deux applications sont disponibles pour simuler ce modèle de confrontation entre le virus et l'antivirus. Une première application dans laquelle l'utilisateur peut choisir les types de propagation pour le virus et pour l'antivirus. Et une deuxième application "app_antivirus_4" qui permet d'afficher simultanément les 4 couples de stratégies de propagation pour le virus et l'antivirus (on ne considère pas la propagation avec l'état contagieux ici), soit les couples (virus : unicast, antivirus : broadcast), (virus :unicast, antivirus : unicast)...



(a) Simulateur basique



(b) Simulateur avec les 4 animations

7 Paramètres de la simulation

Pour terminer, un petit récapitulatif des paramètres nécessaires pour lancer une simulation est fait ici :

— Le type de graphe choisi (s'il y a génération de graphe), qui peut être comme pour le précédent simulateur, soit une triangulation de Delaunay, soit un graphe d'Erdos-Rényi, soit un graphe Small World

— Les paramètres liés à la génération de graphe (si on décide de générer un graphe) : le nombre de noeuds, et éventuellement un degré et une probabilité d'activation comme vu plus haut

— Les probabilités liées au modèle : la probabilité de passer de l'état I à S

— Le nombre de noeuds infectés au départ ainsi que leurs indices, le graphe est affiché à côté pour pouvoir faciliter le choix

— Les probabilités d'infection par le virus et l'antivirus

— Le nombre de tours après lesquels est faite l'injection de l'antivirus dans le réseau

— Le type de propagation choisi pour le virus et pour l'antivirus