Simulateur de propagation de virus
Mode d'emploi

Yassine Mehmouden

Table des matières

1 Introduction

Ce document explique le fonctionnement et le principe du simulateur de propagation de virus qui a été développé au sein du LIA. Il détaille entre autres les fonctionnalités du simulateur ainsi que les différents paramétrages disponibles.

1.1 Principe général

Cet outil permet de simuler la propagation d'un virus au sein d'un réseau. Le graphe utilisé pour modéliser le réseau peut être généré à l'aide de différentes manières. On peut également réutiliser le même graphe plusieurs fois ou encore importer un graphe. Pour l'importation des graphes seuls les fichiers *'gexf'* sont autorisés.
Le modèle de propagation utilisé est un modèle SIR, trois changements d'états sont possibles :

1. $S \rightarrow I$, lorsqu'un noeud susceptible est infecté par un noeud déjà infecté.
2. $S \rightarrow R$, lorsqu'un noeud susceptible est directement considéré comme rétabli. Dans le contexte d'un virus informatique, cela peut être considéré lors d'une mise à jour de l'antivirus par exemple.
3. $I \rightarrow S$, lorsqu'un noeud infecté est libéré du virus, il redevient alors susceptible.

1.2 Informations pratiques

Le simulateur peut permettre l'enregistrement des animations, pour cela il faut cependant avoir installé le logiciel **FFmpeg**. [1].
Pour faire fonctionner l'outil de simulation, il est nécessaire d'avoir au moins la **version 3.10 de Python**, et d'installer quelques bibliothèques comme *Networkx* par exemple. La version de l'application en ligne de commande peut fonctionner avec une version antérieure de *Python*, mais il est tout de même recommandé d'installer au moins la version 3.10.

2 Types de graphes

Différents types de graphes peuvent être générés à l'aide de l'outil. Pour tous les types de graphes il est tout d'abord demandé de choisir le nombre de noeuds souhaité. Tous les graphes générés devront être connexes, ainsi, il sera parfois demandé de renseigner de nouveaux paramètres.

2.1 Graphe aléatoire

La première méthode proposée consiste en la génération de points aléatoires sur lesquels est appliquée une triangulation de Delaunay pour obtenir un graphe connexe.
paramètres à compléter : nombre n de noeuds du graphe

2.2 Graphe de Erdos-Renyi

Cette deuxième méthode consiste à générer un graphe aléatoire binomial selon le modèle imaginé par Erdos et Rényi. Ce modèle consiste à considérer un graphe complet d'ordre n (n étant le nombre de noeuds choisi) dont chaque arête sera conservée avec une probabilité p. Cette probabilité devra être renseignée par l'utilisateur, mais il faudra prêter attention à la connexité du graphe.
paramètres à compléter : nombre n de noeuds du graphe, probabilité p de conserver une arête

1. Pour l'installation de FFmpeg sur Windows, un tutoriel est disponible ici

2.3 Graphe Small World

La dernière méthode de génération de graphe s'appuie sur les modèles Small World. Il est demandé de renseigner un degré d de départ pour chaque noeud du graphe ainsi qu'une probabilité p. Et à partir d'un graphe d-régulier, c'est-à-dire un graphe où chaque noeud est relié à d plus proches voisins, chaque arête est modifiée avec une probabilité p. Ce qui donne alors un autre graphe avec une distance moyenne inversement proportionnelle à la probabilité de modification des arêtes : plus la probabilité de modifier une arête donnée est élevée, plus la distance moyenne dans le graphe est faible.
paramètres à compléter : nombre n de noeuds du graphe, degré d de chaque noeud au départ, probabilité p de modifier chaque arête

3 Types de propagation

Différents types de propagation sont disponibles pour les simulations. Ils sont détaillés ci-dessous.

3.1 Propagation un à un classique

Ce type de propagation est assez classique. Pour chaque noeud infecté, un voisin, c'est-à-dire un noeud auquel il est relié par une arête, est tiré aléatoirement pour être infecté. Le voisin tiré peut être dans n'importe quel état (S, I ou R) mais l'infection ne sera effective que si ce dernier est susceptible, soit dans l'état S.

3.2 Multipropagation

Ce type de propagation reprend le type de propagation classique un à un. Seulement désormais, l'utilisateur doit choisir la proportion des voisins qui seront infectés. Ainsi, au lieu de pouvoir infecter un seul de ses voisins, le noeud infecté pourra en infecter une certaine proportion.
paramètres à compléter : proportion p de voisins à infecter

3.3 Multipropagation complète

Avec ce type de propagation, chaque noeud infecté va tenter d'infecter la totalité de ses voisins.

3.4 Propagation un à un intelligente

Avec ce type de propagation, chaque noeud infecté va essayer d'infecter son voisin susceptible de plus haut degré.

3.5 Multipropagation mixte

Avec ce type de propagation, chaque noeud infecté va infecter la totalité de ses voisins susceptibles de plus haut degré, ainsi qu'un nombre aléatoire de ses autres voisins susceptibles.

3.6 Multipropagation : plus haut degré

Ce dernier type de propagation est moins viral que la propagation précédente, ici chaque noeud infecté va "seulement" infecter tous ses voisins susceptibles de plus haut degré.

4 Méthodes de défense

Le simulateur permet également de modéliser une stratégie défensive face à la propagation du virus. Pour cela, il se repose sur le système de IDS (Intrusion Detection System), que l'on appelera ici "honeypots". Deux stratégies de défense sont envisagées et peuvent être également utilisées conjointement. Le principe de base consiste à sélectionner des arêtes à surveiller, si lors d'un tour le virus se propage à travers une arête surveillée alors à la fois le noeud transmetteur du virus et le récepteur redeviendront susceptibles.
paramètres à compléter : nombre n de honeypots total

4.1 Stratégie naïve

Cette première approche consite à placer les "honeypots" aléatoirement sur les arêtes non résistantes. Sont considérées résistantes les arêtes reliées à un noeud résistant car il n'y a plus de danger étant donné que ces noeuds là ne peuvent plus être contaminés.

4.2 Stratégie intelligente

Avec cette seconde approche, les arêtes choisies pour y placer des "honeypots" sont choisies parmi les arêtes liées à un noeud qui a transmis le virus durant le tour précédent car le noeud ayant transmis le virus a des chances de transmettre à nouveau le virus à un de ses voisins sur le tour d'après. Le choix est alors fait avec une pondération selon le degré des voisins.
paramètres à compléter : nombre n_s de honeypots qui adoptent la stratégie intelligente, les autres honeypots adopteront automatiquement la stratégie naïve

5 Paramètres de la simulation

Pour lancer la simulation, il faut remplir les paramètres suivants :

— Le type de graphe choisi (s'il y a génération de graphe)

— 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 et la probabilité de passer de l'état S à R

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

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

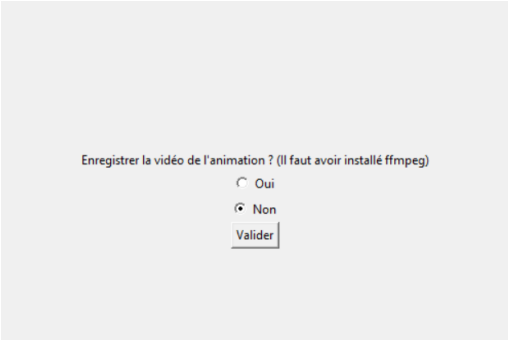
— Le nombre de "honeypots" voulu et le nombre de ces "honeypots" qui adoptent la stratégie intelligente

— Le type de propagation choisi

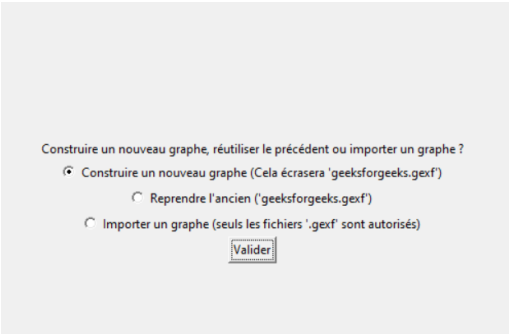
6 Tutoriel pas à pas

Dans cette dernière partie, un tutoriel est fait pas à pas illustré de captures d'écran pour faciliter la prise en main de l'outil de simulation.

Dans un premier temps, il est donné le choix de l'enregistrement, suivi d'un choix sur le graphe :

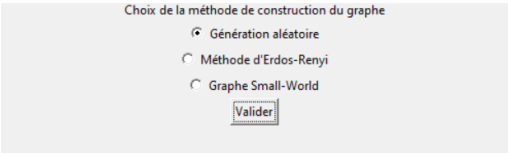


(a) Ecran de choix pour l'enregistrement

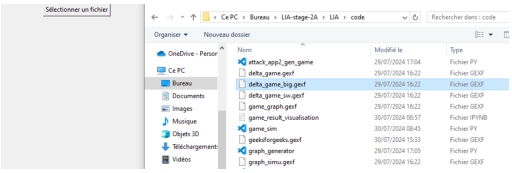


(b) Ecran de choix pour le graphe

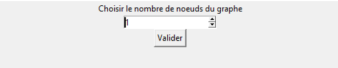
Plusieurs choix sont possibles pour le graphe, il peut être généré via diverses méthodes et écrasera alors le graphe *"graph.gexf"* (s'il existe). L'utilisateur peut également avoir le choix de récupérer l'ancien graphe généré *"graph.gexf"* ou alors d'importer un graphe.



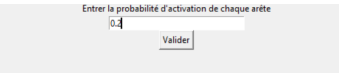
(a) Ecran de choix de la méthode de génération de graphe



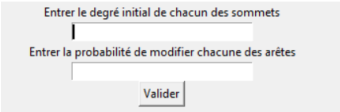
(b) Ecran d'import de graphe



(c) Ecran de choix du nombre de noeuds

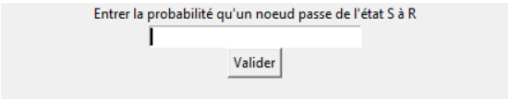


(d) Ecran de choix des paramètres pour un graphe d'Erdos-Renyi

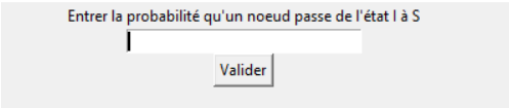


(e) Ecran de choix des paramètres pour un graphe Small World

L'utilisateur doit par la suite entrer les probabilité des changements d'états.

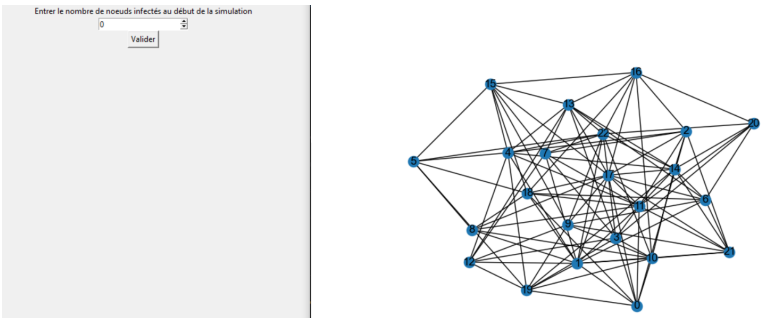


(a) Ecran de choix de la probabilité S → R

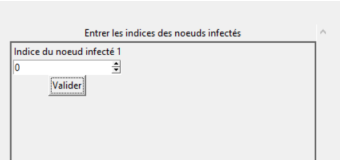


(b) Ecran de choix de la probabilité I → S

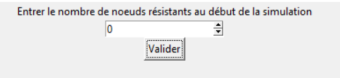
L'utilisateur est alors invité à renseigner le nombre et les indices des noeuds infectés et résistants, le graphe est affiché à côté pour faciliter les décisions.



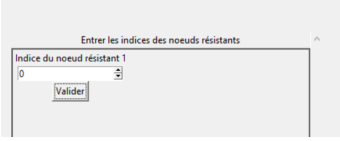
(a) Ecran de choix du nombre d'infectés



(b) Ecran de choix des indices des noeuds infectés

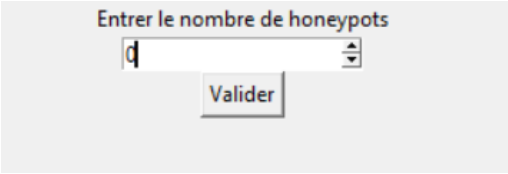


(c) Ecran de choix du nombre de résistants

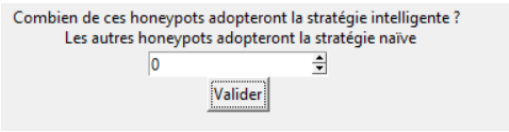


(d) Ecran de choix des indices des noeuds résistants

Ensuite, il faut renseigner le nombre de honeypots et de honeypots qui adopteront la stratégie intelligente.

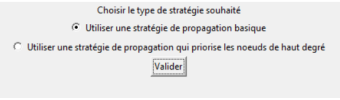


(a) Ecran de choix pour le nombre de honeypots

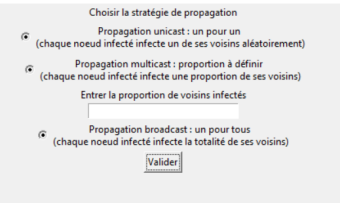


(b) Ecran de choix pour le nombre de honeypots intelligents

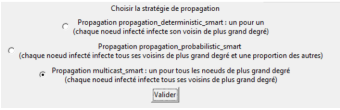
Enfin, il reste à choisir le type de la propagation.



(a) Ecran de choix des types de propagation



(b) Propagations basiques



(c) Propagations avec les hauts degrés

Il ne reste plus qu'à visualiser l'animation de la simulation.
Une légende est affichée sur la figure concernant la couleur des noeuds. Pour la couleur des arêtes, elles deviennent épaisses lorsqu'un honeypot/IDS y est mis en place, si elles détectent la propagation du virus elles deviennent bleues et lorsqu'elles deviennent résistantes, c'est-à-dire qu'elles sont liées à un noeud résistant, elles deviennent grises.