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 les différentes fonctionnalités du simulateur ainsi que les différents paramétrages disponibles.

1.1 Principe général

L'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 ré-utiliser le même graphe plusieurs fois. Le modèle utilisé est un modèle SIR classique, 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.

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. Nous ne nous intéressons qu'aux graphes connexes.

2.1 Graphe aléatoire

La première méthode proposée consiste en la génération de points aléatoires dont on calcule la triangulation de Delaunay. On obtient alors un graphe connexe.

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) et on conserve chaque arête du graphe complet avec une probabilité p. Cette probabilité devra être renseignée par l'utilisateur du simulateur mais il faudra faire attention à ce que le graphe obtenu soit bien connexe.

2.3 Graphe Small World

La denière 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.

3 Types de propagation

Différents types de propagation sont disponibles pour les simulations.

3.1 Propagation un à un classique

Ce type de propagation est assez classique, pour chaque noeud infecté, un de ses voisins est tiré aléatoirement pour être infecté à son tour, ce dernier pourra être dans les 3 états (S, I, R), mais l'infection ne sera réalisée que s'il est susceptible (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.

3.3 Multipropagation totale

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 Propagation multi intelligente

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

3.6 Propagation un pour tous les plus hauts degrés

Ce dernier type de propagation est moins viral que la propagation précédente, ici chaque noeud infecté va 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 sytem), que l'on appelera ici "honeypots". Deux stratégies de défense sont envisagées et peuvent être également utilisées conjointement. Le principe de base consiste à choisir des arêtes à surveiller, si lors d'un tour il y a propagation à travers une arête surveillée alors à la fois le noeud transmetteur du virus et le récepteur redeviendront susceptibles.

4.1 Stratégie naïve

Cette première approche consite à placer les "honeypots" aléatoirement sur les arêtes non résistantes. Sont considérées résistantes les arêtes reliés à un noeud résistant car il n'y a plus de danger, ces noeuds là ne pouvant 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 retransmettre à nouveau le virus à un de ses voisins sur le tour d'après. Le choix est fait avec une pondération selon le degré du voisin de l'autre côté de l'arête.

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 Informations diverses

L'outil permet également d'enregistrer la vidéo de la simulation mais il faut avoir installé le logiciel FFmpeg au préalable.