1 Problème

On étudie un parc de machine qui se fait attaqué par des virus. Face à l'augmentation du nombre d'attaque sur machines, il devient urgent de s'intéresser à une méthode de protection plus efficace qu'actuellement. Ce modèle permettra d'une part de comprendre comment constituer une attaque intelligente sur un réseau et ensuite, comment s'en défendre. Cela a aussi pour but d'introduire la formation d'une équipe au loria qui a pour objectif de protéger les objets connectés. Nous utiliserons le système immunitaire de Jerne pour tenter de résoudre de problème, dont l'implémentation informatique permet de sélectionner une fonction optimale parmi un ensemble concordant avec un environnement à un instant donné.

2 Modèle

L'environnement est constitué par les agents qui sont les machines et les virus. Les machines dans une première approche sont passives et n'ont d'autres but que de se faire infecter. Les virus, quant à eux, sont capables de contaminer les machines, de communiquer entre eux et de se propager sur le réseau constitué par les machines. Ils auront tous la même constitution et leur objectif final est de restituer un booléen à l'ensemble du groupe qui jugera alors la meilleure stratégie à adopter. Cette meilleure stratégie peut être définie selon plusieurs critères : la perte d'energie globale machines, l'augmentation du coût imposé sur les composants par les virus ou encore le nombre de machines contaminées et la vitesse de contamination. Nous voulons faire une attaque évolutive capable de s'adapter en temps réel au réseau de machines.

Ce qu'on recherche dans l'approche par système immunitaire c'est d'avoir un système ayant une capacité d'apprentissage, de mémoire, d'adaptabilité et de décision.

Détaillons à présent les différentes phases du projet.

2.1 Lancement

On envoie les virus sur une machine du réseau sein.

2.2 Attaque

On considère que l'effet d'un virus sur une machine est le même que l'effet de plusieurs virus sur la même machine. Ce virus va sélectionner une fonction parmi celle possible qui doit être adapté à la situation.

Les attaques possibles sont les attaques de type *«Worms»* soit que le virus infecte la machine pendant un certain temps puis décide de se dupliquer pour aller contaminer la machine. Une attaque de type *«Trojan»*, soit que le virus attaque la machine, et la contrôle tant qu'il est en train de l'infecter. La notion de contrôle consiste en le blocage de la machine ainsi que des machines adjacentes.

Avant cela, des virus *«trouveurs de brèches»* sont nécessaires pour permettre de créer une brèche sur la machine. Une brèche doit être présente sur la machine pour que les deux autres types de virus puissent l'attaquer, cependant, cette faille ne bloque pas la machine, c'est-à-dire qu'on peut toujours l'utiliser sans noter le moindre problème.

2.3 Mise en commun

Les virus après l'attaque vont communiquer entre eux les données. Ils renvoient chacun un booléen visant à enrichir le comportement local de chacun des virus.

3 Simulation