Les G-réseaux qui apprennent à détecter et à mitiger les cyber-attaques

Erol Gelenbe*[1]

[1]Polish Academy of Science – Pologne

Résumé

Les G-réseaux, dont les "réseaux neuronaux aléatoires avec signaux négatifs et positifs" (RNN), sont des approximateurs de fonctions continues bornées, et disposent d'algorithmes polynomiaux pour choisir leurs "poids synaptiques" qui permettent d'obtenir des minimaux locaux de "fonctions de cout" sur des ensembles de données. Avec deux architectures distinctes de G-réseaux, et des données réelles, nous montrons qu'avec un apprentissage de type gradient, ils peuvent etre utilisés pour détecter les attaques de type Botnet sur des noeuds de réseaux de communication, et aussi permettre de savoir si le Botnet s'est répandu sur un ensemble de noeuds. Nous montrons aussi qu'un ensemble de RNN répartis sur plusieurs noeuds d'un réseau de communication peuvent - ensemble - utiliser l'apprentissage par renforcement pour modifier les chemins des connexions de communication afin de mitiger une attaque de type "worm" et assurer au moins partiellement la survie des communications.

*Intervenant