

Détection d'attaques élémentaires et coordonnées à base de réseaux Bayésiens naïfs

Tayeb Kenaza^{1,2,4}, Karim Tabia³ and Aïcha Mokhtari⁴

¹ Laboratoire de Recherche en Intelligence Artificielle, Ecole Militaire Polytechnique, BP 17 Bordj-Elbahri 16111, Alger
ken.tayeb@gmail.com

² Centre de Recherche en Informatique de Lens (CNRS-UMR 8188), Université d'Artois, rue Jean Souvraz, SP 18 F-62307, Lens Cedex

³ Laboratoire d'Informatique de Nantes Atlantique (UMR 6241), Polytech'Nantes - rue Christian Pauc BP 50609 44306 Nantes Cedex3
tabia@univ-nantes.fr

⁴ Laboratoire de Recherche en Intelligence Artificielle, USTHB, BP 32 El-alia 16111 Bab-Ezzouar Alger aissani_mokhtari@yahoo.fr

Résumé

Les réseaux Bayésiens constituent des outils très puissants de représentation de connaissances et de raisonnement sous incertitude. Cet article montre leur applicabilité avec facilité et efficacité à deux problèmes importants en détection d'intrusions : la détection d'attaques élémentaires et d'attaques coordonnées. Nous commençons par poser les problèmes traités puis définir les variables nécessaires pour les modéliser en utilisant des réseaux Bayésiens naïfs. En plus du fait que la construction de ces modèles est simple et rapide, leurs performances sur des données représentatives concurrencent les outils de classification les plus performants dans la littérature. Enfin, nous montrons comment les règles de décision utilisées dans les classifieurs Bayésiens peuvent être améliorées pour la détection de nouvelles attaques et d'activités anormales nouvelles et nous montrons expérimentalement l'efficacité de ces améliorations sur un trafic Web récent.

Mots-clés : Réseaux Bayésiens, classification, classifieur Bayésien naïf, détection d'intrusion, attaques coordonnées