

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

Abstract

Bayesian networks are powerful tools for knowledge representation and reasoning under uncertainty. This paper shows their applicability with ease and efficiency to two major problems in intrusion detection : the detection of elementary attacks and coordinated ones. We propose two models beginning with stating the problems and defining the variables necessary for model building using naive Bayesian networks. In addition to the fact that the construction of these models is simple and efficient, performance of naive Bayesian networks on representative data is competing the most efficient state of the art classification tools. Finally, we show how the decision rules used in Bayesian classifiers can be improved to detect new attacks and new anomalous activities and we show experimentally the effectiveness of these improvements on a recent web traffic.

Key-words: Bayesian networks, classification, naive Bayes classifier, intrusion detection, coordinated attacks