Algorithmes d'extraction et d'interrogation d'une représentation concise exacte des motifs corrélés rares : Application à la détection d'intrusions

Souad Bouasker, Tarek Hamrouni, Sadok Ben Yahia

Département des Sciences de l'Informatique, Faculté des Sciences de Tunis, Tunisie
{tarek.hamrouni, sadok.benyahia}@fst.rnu.tn

Résumé

Nous proposons, dans ce papier [1], l'algorithme RCPRMINER d'extraction de la représentation $\mathcal{RMCR}$ de l'ensemble $\mathcal{MCR}$ des motifs corrélés rares. Les algorithmes d'interrogation de cette représentation et de régénération de l'ensemble $\mathcal{MCR}$ à partir de $\mathcal{RMCR}$ sont aussi introduits. En outre, nous décrivons le processus de classification basée sur les règles génériques corrélées rares et son application dans la détection d'intrusions.

Summary

In this paper, we introduce the algorithm RCPRMINER allowing the extraction of $\mathcal{RCPR}$. We also present dedicated algorithms allowing the query of the $\mathcal{RCPR}$ representation and the regeneration of the whole set $\mathcal{RCP}$ starting from this representation. The effectiveness of the proposed classification method, based on generic rare correlated association rules derived from $\mathcal{RCPR}$, has also been proved in the context of intrusion detection.

1. Une version étendue de ce travail se trouve à l'adresse suivante : `http://arxiv.org/abs/1111.6552`.
Ce travail est partiellement financé par le projet Utique 11G1417.