Proposition d'une nouvelle approche de détection d'intrusions basée sur les règles associatives génériques de classification

Imen Brahmi, Sadok Ben Yahia, Yahya Slimani

Département des Sciences de l'Informatique
Faculté des Sciences de Tunis
Campus Universitaire 1060 Tunis, Tunisie
{sadok.benyahia, yahya.slimani}@fst.rnu.tn

Résumé. Les systèmes de détection d'intrusions (SDIs) ont pour objectif la sécurité des réseaux informatiques. Dans ce papier, nous proposons une nouvelle approche de détection d'intrusions basée sur des règles associatives génériques de classification pour améliorer la qualité de la détection d'intrusions.

1 Introduction

Dans ce papier, nous proposons un nouveau système de détection d'intrusions, visant la diminution de génération de fausses alarmes et l'augmentation de détection de vraies intrusions. Nous montrons que l'utilisation des règles associatives génériques, de taille très compacte, permet d'atteindre ce double objectif. Les expérimentations que nous avons menées, montrent que l'approche proposée permet d'obtenir un SDI robuste avec un taux très élevé de détection de vraies intrusions.

2 Le système de détection d'intrusions IDS-GARC

Peu de travaux ont fait appel au concept des règles associatives dans le cadre de détection d'intrusions. Pour améliorer la qualité de détection d'intrusions, nous proposons un nouveau SDI appelé IDS-GARC (Intrusion Detection System based on Generic Association Rule with Classifier), dont l'objectif est de minimiser la génération de fausses alarmes et surtout l'augmentation de détection de vraies intrusions.

Le nouveau système IDS-GARC, dont l'architecture du IDS-GARC est décrite par la figure 1, dérive de l'application d'un processus, qui peut être résumé dans les quatre étapes suivantes :

- Pré-traitement des données : Nous discrétisons automatiquement des données de détection d'intrusions identifiées par des experts en sécurité informatique
- Génération de la base générique des règles associatives : En particulier, nous utilisons les règles génériques extraites de la base IGB (Gasmi et al., 2006)
- Sélection des règles associatives génériques de détection : Pour se faire, nous avons recours à la classification associative.
- Construction d'un classifieur : Pour détecter les nouvelles attaques, nous utilisons un classifieur appelé GARIDC (Generic Association Rule for Intrusion Detection based Classifier).

3 Evaluation expérimentale

Afin d'évaluer les performances du IDS-GARC, nous avons mené une série d'expérimentations sur une base de données orientée détection d'intrusions DARPA 98. Le choix de cette base s'explique par le fait puisqu'elle est fréquemment utilisée pour évaluer les performances des SDIs. Le tableau 1 présente les résultats obtenus en termes de taux de détection et de

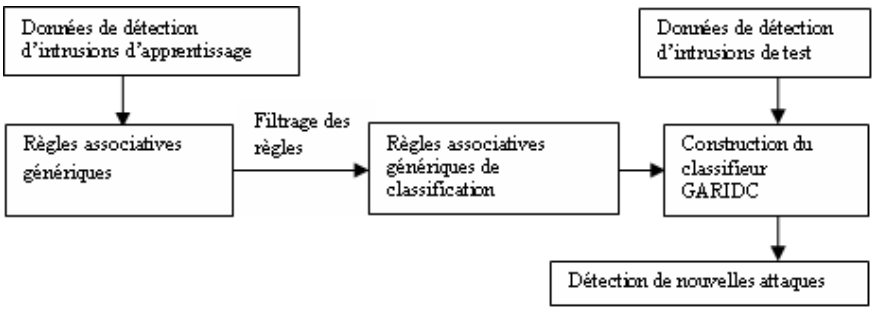

FIG. 1 – *Architecture du système IDS-GARC*

fausses alarmes. L'analyse du tableau 1 permet de conclure que la technique de règles génériques de classification permet d'obtenir le meilleur taux de détection de vraies intrusions $(97,86\%)$. De plus, elle engendre peu de fausses alarmes, soit $2,50\%$. Ainsi, les deux taux TD et TF permettent de montrer la robustesse et l'efficacité du SDI que nous avons proposé dans ce papier.

Approche	Taux de détection (TD)	Taux de fausses alarmes (TF)
Arbre de décision	92,05%	$2,50\%$
Algorithmes génétiques	$92,60\%$	$3,62\%$
Règles génériques de classification	$97,86\%$	$2,50\%$

TAB. 1 – *Comparaison des taux de détection de vraies intrusions et de fausses alarmes*

Le tableau 2 montre les taux de Pourcentage de Classification Correcte (PCC) obtenus avec notre approche par rapport à celles trouvées avec des approches de la littérature de la fouille de données, pour la base d'audit DARPA 98.

	Arbre de décision	Algorithmes génétiques	Machines SVM	IDS-GARC
Normale	100,00%	99,73%	99,64%	100%
DOS	96,83%	99,95%	100,00%	99,28%
Probing	99,86%	99,89%	98,57%	99,66%
U2R	68,03%	64,10%	40,23%	91,41%
R2L	95,56%	99,47%	56,05%	98,99%

TAB. 2 – *Comparaison de la précision de classification correcte*

En comparant les résultats du tableau 2, pour la catégorie normale, nous constatons que les règles génériques de classification donnent le meilleur taux i.e., 100%. De plus, cette stratégie présente le taux de PCC le plus élevé, pour la catégorie U2R, avec 91,41%.

Summary

Intrusion Detection Systems mainly aim to guarantee high immunity to networks from external attacks. In this paper, we introduce a novel approach for intrusion detection based on the use of generic basis of association rules. Preliminary carried out results showed the efficiency of such an approach.
Keywords : Intrusion Detection Systems, Association rules, generic basis