Cari 2008+ 22/08/08 17:20 Page 667

IDS-GARC : Détection d'intrusions basée sur les règles associatives génériques de classification

I. Brahmi, S. Ben Yahia, Y. Slimani

Faculté des Sciences de Tunis, 1060, Tunis, Tunisie
{sadok.benyahia, yahya.slimani}@fst.rnu.tn

RÉSUMÉ. En réponse aux problèmes posés par la complexité croissante des réseaux et des attaques informatiques, les systèmes de détection d'intrusions (SDIs) constituent une bonne alternative pour mieux sécuriser un réseau ou un système informatique. Cependant, les SDIs existants présentent des lacunes en terme de génération excessive de fausses alarmes. Dans ce papier, nous proposons une nouvelle approche de détection d'intrusions, dont le but est la réduction de fausses alarmes et l'amélioration de détection de vraies attaques. Ainsi, nous proposons un nouveau système de détection d'intrusions basé sur les règles associatives génériques de classification. En effet, l'extraction de règles génériques permet de minimiser le nombre de règles de détection, tandis que la classification associative permet la concentration sur les règles utiles. En outre, un classifieur est construit pour améliorer le mécanisme de détection de nouvelles attaques. L'étude empirique, que nous avons menée, montre la robustesse et l'efficacité du nouveau système proposé *vs* ceux de la littérature.

ABSTRACT. A long with the development of computer network technology, intrusion detection used to capture malicious activities occurring in computer network systems is becoming more and more important. So, Intrusion Detection Systems (IDS) mainly aim to guarantee high immunity to networks from external attacks. However, the existing IDS present some shortages in term of excessive generation of false alarms. In this paper, we introduce a new approach of intrusion detection based on generic association rules. Indeed, the generic basis rules minimize the number of detection rules, while the associative classification permits the concentration on the useful rules. Carried out experiments showed the efficiency of the introduced system *vs* those of the literature.

MOTS-CLÉS : Détection d'intrusions, règles d'association, Base générique, Classifieur.

KEYWORDS : Intrusion Detection, Association Rules, Generic Basis, Classifier.

1. Introduction

Le revers de la médaille de l'ouverture de l'entreprise sur Internet réside dans une éventuelle vulnérabilité face au nombre croissant d'intrusions. Pour cela, la mise en place d'une politique de sécurité, autour de ces systèmes, est donc primordiale afin d'aboutir à un système de détection d'intrusions (SDI) efficace et robuste. En effet, la détection d'intrusions consiste à analyser les informations collectées afin de rechercher d'éventuelles attaques. Ainsi, un SDI est un outil qui automatise les processus de surveillance des évènements système et d'analyse des applications réseau [4]. Nous pouvons distinguer deux approches pour la détection d'intrusions : l'approche par scénarios détectant des intrusions connues et l'approche comportementale détectant des intrusions inconnues [4].

De nos jours, plusieurs SDIs commerciaux sont disponibles. Cependant, les SDIs de détection comportementale ont des limites, puisqu'ils souffrent d'une génération abandante des faux positifs [12].

Récemment, diverses techniques de fouille de données ont été utilisées pour construire des SDIs automatiques et efficaces. Parmi ces techniques, nous pouvons mentionner les réseaux de neurones [3], les arbres de décision [5], les algorithmes génétiques [9], le regroupement [13], etc.

En particulier, plusieurs approches de détection d'intrusions, basées sur les règles associatives, ont été proposées pour découvrir les caractéristiques de connexions fortement corrélées et simplifier ainsi la tâche de détection d'intrusions. Une connexion est un paquet capturé qui porte des informations sur (service port-source port-destination IP-source IP-destination). En effet, Les données d'audit sont des données de détection d'intrusions contenant des attaques identifiées par des experts en sécurité informatique et résulte de l'écoute sur un réseau informatique avec des dispositifs spéciaux. Ces données d'audit peuvent être représentées dans une table de base de données où chaque ligne référence une connexion et chaque colonne indique une caractéristique de connexion [10]. En outre, les règles associatives de détection sont générées par application de l'algorithme APRIORI [1]. Cependant, le très grand nombre de règles associatives de détection générées représente un handicap de taille, car le nombre élevé de règles diminue l'efficacité du SDI, puisqu'il augmente les fausses alarmes et abaisse la détection de vraies intrusions [11].

Pour pallier ces limites, nous proposons dans ce papier, un nouveau système de détection comportementale d'intrusions, visant la diminution de génération des faux positifs 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.

Le reste de l'article est organisé comme suit. La section 2 présente une revue des SDIs basés sur les règles associatives. La section 3, propose un nouveau SDI basé sur les règles associatives génériques de classification. Les résultats des expérimentations menées sur un jeu de données d'audit sont décrits et analysés dans la section 4. La section 5 conclut ce papier et présente quelques perspectives d'extension du présent travail.

2. Les SDIs basés sur les règles associatives

Le problème d'extraction des règles associatives a été introduit par [1]. En effet, les règles associatives ont pour but de découvrir des expressions de corrélation causales entre deux ensembles d'attributs. L'extraction des règles d'association consiste à déterminer les règles dont le support (*i.e.*, fréquence d'apparition) et la confiance (*i.e.*, force d'une règle) sont au moins égaux, respectivement, à un seuil minimal de support *minsupp* et un seuil minimal de confiance *minconf*, prédéfinis par l'utilisateur.

Lee et *al.* [10] ont été les premiers qui ont fait appel au concept des règles associatives dans le cadre de détection d'intrusions. De plus, Barbara et *al.* [2] ont introduit un système de détection d'intrusions dit ADAM (*Audit Data Analysis and Meaning*), qui utilise une combinaison de règles associatives et de classification pour découvrir les attaques. En outre, Chan et *al.* [7] ont proposé un algorithme appelé LERAD (*LEarning Rules for Anomaly Detection*), qui génère des règles associatives de détection d'anomalies particulières, de la forme $X \Rightarrow Y$. LERAD vise à générer le minimum possible de règles associatives de détection comportementale.

Cependant, dans ces approches, la principale limite qui peut être mise en exergue réside dans le nombre très élevé de règles de détection comportementale. Par conséquent, la gestion de ces règles devient lourde, ainsi qu'une augmentation de génération de fausses alarmes et une diminution de détection de vraies intrusions. Pour pallier les limites de ces approches, 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.

3. Le système IDS-GARC

Le nouveau système de détection d'intrusions IDS-GARC, que nous proposons dans ce papier, repose sur l'utilisation d'**une base générique** de règles associatives et d'une technique de classification, lors d'une phase d'apprentissage, afin de minimiser le nombre de règles de détection. Ensuite, durant une phase de détection, un classifieur est utilisé pour améliorer la détection de nouvelles attaques.

Le système IDS-GARC dérive de l'application d'un processus, qui peut être résumé dans les quatre étapes suivantes, que nous allons développer dans la suite de cette section :

1) Pré-traitement des données d'audit, en les discrétisant automatiquement,

2) Génération de la base générique de règles associatives $\mathcal{IGB}$ de détection d'intrusions,

3) Sélection de règles associatives génériques de détection contenant un libellé d'intrusions dans leur partie conclusion,

4) Construction d'un classifieur des règles associatives génériques de détection permettant la découverte et la classification des nouvelles intrusions.

Ainsi, l'architecture du système de détection d'intrusions IDS-GARC peut être décrite par la figure 1.

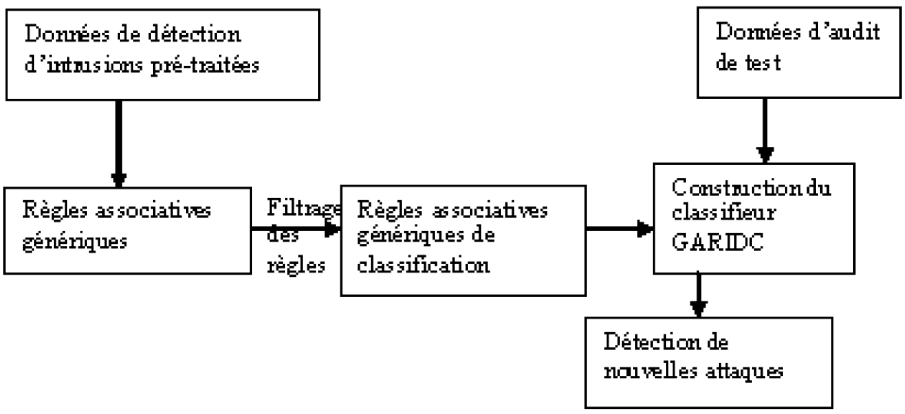

Figure 1. *Architecture du IDS-GARC*

La base de données d'audit contient plusieurs attributs quantitatifs, qui engendrent par conséquence, une grande quantité des données de dimension très élevée [10]. Pour réduire la quantité, Lee et *al.* [10] ont utilisé une notion dite "*attribut axial*". Par conséquent, nous utilisons la discrétisation automatique des données d'audit comme tâche de pré-traitement.

Dans ce qui suit, nous allons mettre le focus sur les trois dernières étapes du processus permettant d'aboutir au nouveau SDI cité ci-dessus.

3.1. Génération de règles associatives génériques de détection d'intrusions

Afin de minimiser le nombre de règles associatives de détection d'intrusions, notre approche se base sur **les bases génériques** et en particulier les règles génériques extraites de la base $\mathcal{IGB}$ (*Informative Generic Basis*). La base $\mathcal{IGB}$ a un intérêt particulier, puisqu'elle présente le meilleur rapport compacité/informativité [8].

Bien que le nombre de règles associatives ait été minimisé par utilisation de la base générique $\mathcal{IGB}$ au cours de la détection d'intrusions, il reste néanmoins le problème de génération des règles inutiles. Pour pallier ce problème, nous nous sommes intéressés à la classification associative.

3.2. Génération de règles associatives de classification

Lors de l'extraction de règles associatives, parfois les règles extraites ne sont pas utiles, spécialement au cours de la détection d'intrusions. Considérons par exemple, la règle Service(http) $\Rightarrow$ Port(80). Même si la confiance de la règle est de 100%, elle n'est pas utile, puisqu'elle n'apporte pas d'information intéressante et augmente inutilement le nombre de règles de détection. Par conséquent, ces règles inintéressantes ont une mauvaise influence sur le SDI, puisqu'elles contribuent à diminuer la précision de la détection d'intrusions.

Anisi, pour minimiser d'avantage le nombre de règles de détection et se concentrer seulement sur les règles les plus utiles, nous proposons l'utilisation de la classification associative. La base de règles générique, extraite de la base de détection d'intrusions d'apprentissage, devrait être filtrée en ne retenant que les règles contenant un libellé d'intrusion dans leur partie conclusion.

Pour se faire, nous avons recours à un mécanisme d'inférence, via l'axiome de *décomposition droite*, afin d'obtenir de nouvelles règles de détection. Par exemple, soit la règle R' : service = frag, IP-src = 209.030.071.165 $\Rightarrow$ attaque = pod, IP-dest = 172.016.118.080. En utilisant l'axiome de décomposition droite, R' est transformée en R" = service = frag, IP-src = 209.030.071.165 $\Rightarrow$ attaque = pod.

L'application de la base $\mathcal{IGB}$ permet d'extraire les règles génériques ayant une prémisse minimale. Ceci apporte un avantage certain, puisqu'il permet le choix de la règle de détection la plus générale de prémisse minimale et de conclusion contenant un libellé d'intrusion, pour une bonne et efficace détection d'intrusions. L'ensemble de règles génériques de classification de détection d'intrusions ainsi obtenu contient seulement des règles utiles et intéressantes, permettant d'améliorer le mécanisme de recherche des attaques.

3.3. Détection de nouvelles intrusions

Une fois les règles de détection extraites de la base générique $\mathcal{IGB}$ et filtrées lors de la classification associative, il nous faut définir à un classifieur permettant de classer les nouvelles connexions et détecter ainsi les nouvelles attaques. Ainsi, nous utilisons le classifieur GARIDC (*Generic Association Rule for Intrusion Detection based Classifier*), inspiré des travaux de [6].

Le classifieur GARIDC permet de couvrir la base de données d'audit. En effet, GARIDC commence par la première connexion de cette base, il parcourt l'ensemble de règles génériques de classification, afin de chercher la règle, dont la prémisse est incluse ou égale aux attributs de la connexion courante, et dont la conclusion est égale à l'étiquette de la connexion courante qui indique une attaque. La règle en question est ajoutée au classifieur. Ensuite, le classifieur peut passer à la deuxième connexion et ainsi de suite avec même processus jusqu'à toute la base d'audit soit couverte.

Dans ce qui suit, nous désignons par connexion C_x une ligne de données de détection d'intrusions étiquettée par une attaque (intrusion) identifiée par des experts en sécurité informatique. En effet, en disposant d'une nouvelle connexion C_x, la détection de nouvelle intrusion consiste à utiliser la première règle rencontrée dans le classifieur, dont la prémisse correspond (*i.e* incluse ou égale) aux caractéristiques (*i.e.*, attribut) de la connexion C_x et la conclusion est égale l'étiquette de la connexion C_x, qui indique une classe d'intrusion.

Ainsi, notre nouvelle approche propose une amélioration de la détection comportementale, puisque le classement de nouvelles intrusions correspond au classement des nouveaux comportements.

4. Évaluation éxperimentale

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[1], fréquemment utilisée pour évaluer les performances des SDIs. La base DARPA 98 recense 38 attaques possibles, qui peuvent être regroupées en quatre catégories :

– Déni de Service (Denial-Of-Service (DOS))

– Les attaques de type Remote to Local access" (R2L)

1. Disponible à l'adresse http ://www.ll.mit.edu/IST/ideval/data/data-index.html

– Les attaques de type "User to Root attacks" (U2R)

– Les attaques de reconnaissance (Probing)

Nous représentons dans la figure 2 les proportions de détection des nouvelles classes en fonction de la variation des valeurs de seuil du support. L'analyse de la figure 2 montre que l'augmentation du seuil du support engendre la diminution de la détection de nouvelles attaques. De plus, même si le seuil est fixé à 0, 9%, les quatres catégories d'attaques restent détectables avec des taux élevés. Ceci s'explique par la bonne classification des attaques avec la technique de règles génériques de classification.

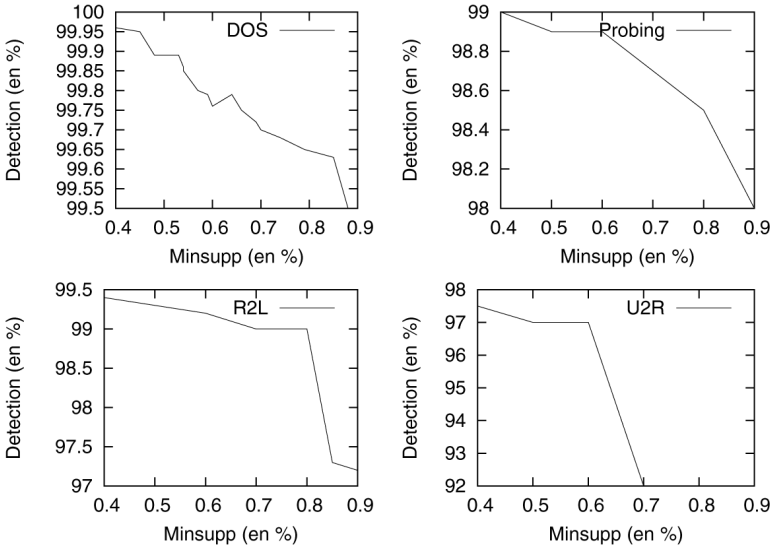

Figure 2. *Détection de nouvelles attaques en fonction de la variation des valeurs de seuil du support avec un minconf = 50%.*

Le tableau 1 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 daudit DARPA 98.

	Arbre de décision	Clustering	Algorithmes génétiques	Règles associatives	IDS-GARC
Normale	100,00%	98,92%	99,73%	74,60%	100,00%
DOS	96,83%	100,00%	99,95%	99,90%	99,28%
Probing	99,86%	63,01%	99,89%	96,70%	99,66%
U2R	68,02%	66,70%	64,05%	78,40%	91,41%
R2L	95,56%	50,00%	99,47%	65.90%	98,99%

Tableau 1. *Comparaison de la précision de classification correcte.*

En comparant les résultats du tableau 1, 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%.

Le tableau 2 présente les résultats obtenus en termes de taux de détection et de fausses alarmes. L'analyse du tableau 2 permet de conclure que la technique de règles génériques de classification permet dobtenir le meilleur taux de détection de vraies intrusions (97,86%). De plus, elle engendre peu de fausses alarmes, soit 2,00%. 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%
Regroupement (clustering)	75,72%	10,00%
Algorithmes génétiques	92,60%	3,62%
Règles associatives	83,10%	2,50%
Règles génériques de classification	**97,86%**	**2,00%**

Tableau 2. *Comparaison des taux de vraies et de fausses détections.*

5. Conclusion

Les approches de détection d'intrusions actuelles, basée sur les règles associatives, souffrent de l'augmentation du nombre de règles de détection,. Ceci a pour effet d'engendrer une génération excessive de fausses alarmes et la diminution de détection de vraies intrusions. Pour remédier ces insuffisances, nous avons proposé une nouvelle approche de détection d'intrusions qui se base sur la stratégie d'extraction de règles associatives génériques de classification. Nous avons ensuite implémenté cette stratégie dans un nouveau système de détection d'intrusions appelé IDS-GARC. Ce système utilise une approche comportementale, puisqu'il est capable de détecter de nouvelles attaques et de caractériser ainsi les nouveaux comportements. Les expérimentations réalisées sur des bases de données d'audit ont montré que le système IDS-GARC est plus efficace et robuste, puisqu'il génère peu de fausses alarmes et détecte plus de vraies intrusions. Comme perspectives de prolongement de ce travail, nous proposons d'examiner le contenu sémantique des alertes produites avec les règles génériques de classification, en les rendant plus riches en information conçernant le diagnostic d'attaque (localisation, dégâts, catégorie, etc.).

6. Bibliographie

[1] R. AGRAWAL, T. IMIELINSKI AND A. SWAMI, « Mining association rules between sets of items in large databases. », In *Proceedings of the ACM SIGMOD International Conference on Management of Data, Washington, D.C.*, pages 207-216, 1993.

[2] D. BARBARA, J. COUTO, S. JAJODIA, AND N. WU, « ADAM : Detecting intrusions by data mining », In *Proceedings of the IEEE SMC Information Assurance Workshop, West Point, NY*, pages 11-16, 2001.

[3] V. BOBOR, « *Efficient Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms* » PhD thesis, Royal Institute of Technology, 2006.

[4] K. BOUDAOUD, « *Détection d'intrusions : Une nouvelle approche par systèmes multi-agents* » Thèse de Doctorat, École Polytechnique Fédérale de Lausanne, 2000.

[5] Y.BOUZIDA, « *Principal Component Analysis for Intrusion Detection and Supervised Learning for New Attack Detection* » PhD thesis, National High Institute of Brittany, 2006.

[6] I. BOUZOUITA, S. ELLOUMI AND S. BEN YAHIA, « GARC : A new associative classification approach », In A Min Tjoa and J. Trujillo, editors. In *Proceedings of the 8th International Conference on DaWaK 2006 ; Krakow, Poland*, pages 554-568 : Springer-Verlag, 2006.

[7] P. K. CHAN, M. V. MAHONEY AND M. H. ARSHAD, « *Learning Rules and Clusters for Anomaly Detection in Network Traffic* ». Managing Cyber Threats : Issues ; Approaches and Challenges ; V. Kumar, J. Srivastava and A. Lazarevic editors, Kluwer, 2003.

[8] G. GASMI, S. BEN YAHIA, E. MEPHU NGUIFO AND Y. SLIMANI, « $\mathcal{IGB}$: une nouvelle base générique informative des règles d'association ». *Revue I3 (Information, Interaction et Intelligence)*, 6(1) :31-67, 2006.

[9] R. H. GONG, M. ZULKERNINE AND P. ABOLMAESUMI, « A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection ». In *Proc. of the 6th International Conference on SNPD/SAWN'05, Washington, DC, USA* ; pages : 246-253, 2005.

[10] W. LEE AND S. J. STOLFO, « Data Mining approaches for intrusion detection ». In *Proc. of the 7th Conference on USENIX Security Symposium ; San Antonio, Texas*, page 6, 1998.

[11] T. R. LI AND W. M. PAN, « Intrusion Detection System Based on New Association Rule Mining Model ». In *Proc. of the International Conference on Granular Computing, Beijing, China* ; pages : 512-515, 2005.

[12] L. MÉ, « *Détection d'intrusions dans les systèmes d'information : la nécessaire prise en compte des caractéristiques du système surveillé* ». Habilitation à diriger des chercheurs, Université de Renne 1 ; 2003.

[13] V. RAMOS AND A. ABRAHAM, « ANTIDS : Self-organized anti-based clustering model for intrusion detection system ». In *4th IEEE International Conference on Soft Computing as Transdisciplinary Science and Technology ; Muroran, Japan* ; pages 977-986 : Springer-Verlag, 2005.