Intrusion Detection Based on Swarm Intelligence using mobile agent

Khaled Sellami[1], Rachid Chelouah[2], Lynda Sellami[1], Mohamed Ahmed-Nacer[3]

[1] Université de Bejaia
Route de Targua Ouzemour, 06000, Bejaia , Algérie
skhaled36@yahoo.fr, lynda.sellami@univ-bejaia.dz

[2]EISTI, L@aris, Avenue du Parc,
95011 Cergy-Pontoise Cedex, France
rachid.chelouah@eisti.fr

[3] USTHB, LSI,
BP32 El Alia, 16111, BAB EZOUAR, Alger
anacer@cerist.dz

Abstract

Due to the increase in access of malicious data over the internet resources, intrusions Detection Systems (IDSs) have become the necessary component of the computer and information security framework. Although the field of IDSs is still developing, they are not able to detect all types of intrusions.

New intelligent Intrusion Detection Systems (IDSs) which are based on sophisticated algorithms rather than current signature-base detections are in demand. This work discuss about the ways of implementing a swarm intelligence approach to data clustering to detect intrusions. Mobile agent technology is used to initially collecting data properties. These data are evaluated by the combining of the artificial Immune recognition system and the artificial fuzzy ants clustering systems. Our approach allows us to recognize not only known attacks but also to detect suspicious activity that may be the result on knowledge Discovery and Data Mining (KDDCup 1999) dataset compared to a standard learning schema that use the full dataset.

Key words

Intrusions Detection, Swarm Optimization, mobile agent , fuzzy c-means

1 Introduction

The prevalent use of computers and internet has enhanced the quality of life for many people, but it has also exposed to increasing security threats that originate externally or internally. The security of a computer system is compromised when an intrusion takes place. An intrusion can be defined as “any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource” [1]. Different technologies have been developed and deployed to protect organizations’ computer systems against network attacks, for example, anti-virus software, firewall, message encryption, secured network protocols, password protection, and so on. Despite Intrusion prevention techniques, it is nearly impossible to have a completely secured system.
Various approaches have been proposed in intrusion detection systems which include statistical , Rule based approach , Expert System approach [2], Pattern recognition approach [2, 6], Hybrid approach [2], Artificial neural network approach [2, 4].
Compared with other approaches, a statistical analysis technique involves comparison of specific events based on a predetermined set of criteria. The data was collected from the system and the network. This collected data was tested for attack analysis by statistical models. The models which have been frequently used are Operational Model, Average and Standard Deviation Model, the Multivaried Model, the Markovian Model, and the Time Series Model [2]. The analysis of threats was much laborious and time consuming because first data are collected and then different models are applied.
In this work we construct a prototype of anomaly detection model using mobile agent in the detection stage and we use the artificial Immune recognition system and the artificial fuzzy ants clustering systems in the classification stage to find good partitions of the data.

2 The proposed method

Our contribution to solving the problems of attacks on networks is evolving along two axes:

2.1 The first axis

The first concerns are to propose an intrusion detection system based on the use of the mobile agent technology approach. We first use the mobile agent called *AgentCalcul* for calculating the normal profile of the network during a learning phase. Then, during a detection phase, a classifier is used to improve detection of new attacks, which is accomplished by the mobile agent called *AgentPrinc*.
To make the intrusion detection we need to analyze data, we have chosen for this *audit system* for the data source. These are analyzed in *distributed* according to a *behavioral approach* with a frequency of *continuous* (real time).

2.2 The second axis

In this axis we proceed in the classification of attacks found in the phase of detection, in which we apply an approach of Ant based clustering algorithm defined by [5].
Data is clustered without initial knowledge of the number of clusters. Ant based clustering is used to initially create raw clusters and then these clusters are refined using the Fuzzy C Means algorithm. Initially the ants move the individual objects to form heaps. The centroids of these heaps are taken as the initial cluster centers and the Fuzzy C Means algorithm is used to refine these clusters. In the second stage the objects obtained from the Fuzzy C Means algorithm are hardened according to the maximum membership criteria to form new heaps. These new heaps are then sometimes moved and merged by the ants. The final clusters formed are refined by using the Fuzzy C Means algorithm.

During the experimentation, we processed about preprocessing also handle missing and incomplete data. In second phase, feature selection using artificial Immune recognition system and optimization artificial fuzzy ant clustering for detection group of data. In addition to this process, we manipulated the KDD'99 data set with important attribute for processing. The preprocessing module performs the following tasks:

1. Identifies the attributes and their value.
2. Convert categorical to numerical data
3. Data Normalization
4. Perform redundancy check and handle about null value.

3 Conclusion

In this paper, a method of applying a swarm intelligence optimization for network intrusion detection is presented. Software is implemented for the presented method, and its architecture and operations are described in detail using high level class diagram and pseudo-code. A number of experiments have been carried out using a benchmark data set in order to show the efficacy of the developed software. Although the main purpose of this study is to expect for get higher classification accuracy in intrusion detection problem.

References

[1] R. Heady, G. Luger, A. Maccabe, and M. Servilla. The architecture of a network level intrusion detection system. Technical report, Computer Science Department, University of New Mexico, August 1990.

[2] Pervez, I. Ahmad, A. Akram, and S. U. Swati, "A comparative analysis of artificial neural network technologies in intrusion detection systems," WSEAS Transation on Computers, vol. 6, no. 1, pp. 175–180, 2007.

[3] S. Peddabachigari, A. Abraham, C. Grosan, and J. Thomas, "Modeling intrusion detection system using hybrid intelligent systems," Journal of Network and Computer Applications, vol. 30, no. 1, pp. 114–132, 2007.

[4] I. Ahmad, A. B. Abdullah, and A. S. Alghamdi, "Application of artificial neural network in detection of probing attacks," IEEE Symposium on Industrial Electronics and Applications, pp. 557 – 562, 2009.

[5] Parag M. Kanade and Lawrence O. Hall , "Fuzzy Ants as a Clustering Concept " Proceeding of the 22th International Conference of North American Fuzzy Information Processing Society, NAFIPS, pp. 227 – 232, 2003.

[6] D. Ariu, G. Giacinto, and R. Perdisci, "Sensing attacks in computers network with hidden markov models," Machine Learning and Data Mining in Pattern Recognition, vol. 4571, pp. 449–463, 2007.