Journal of Theoretical and Applied Information Technology
30th April 2015. Vol.74 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NEW ARCHITECTURE OF IDS BASED INTERACTION ON MOBILE AGENTS AND DATA MINING

CHAIMAE SAADI[1], RACHID CHERKAOUI[2] , HABIBA CHAOUI[3] AND HASSAN ERGUIG
Systems Engineering Laboratory, Data Analysis and Security Team
National School of Applied Sciences, Campus Universitaire, B.P 241, Kénitra14000, Morocco
E-mail: [1]chaimaesaadi900@gmail.com , [3]mejhed90@gmail.com

ABSTRACT

Intrusion detection system (IDS) is a very useful tool for the defence of a network against attacks. Nowadays, intruders use a complex attacks towards a target. This make the IDS unable to detect all intrusions and the latter generate two frequent false alarms. The purpose of this paper is to propose a new architecture of an IDS allowing to increase the rate of intrusion detection and to minimize the false positive rate. The proposed architecture is based on mobile agents and data mining algorithms.

Keywords- intrusion, intrusion detection system, mobile agent, data mining algorithms.

1. INTRODUCTION

Intrusion detection systems are an integral part of any complete security package of a modern, well managed system. The intrusion detection system detects if someone tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security [1]. Therefore, an IDS is a security system that monitors computer system and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. Implementation of the IDS by integrating data mining algorithms in mobile agents will offer a new model of intrusion detection system. Indeed, some researchers have been developed an IDS using the mobile agent technology. [2] Uses autonomous agents which work independently (their execution is scheduled only by the operating system and not by another process). [3] Is a set of software entities called mobile agents that can move from one node to another node within a network, and perform the task of aggregation and correlation of the intrusion related data it receives from another set of software entities called the static agents. Mobile agents reduce network bandwidth usage by moving data analysis computation to the location of the intrusion data, support heterogeneous platforms, and offer a lot of flexibility in creating a distributed IDS. In some research the data mining algorithm are also used combined with the mobile agents. [4] Proposed a novel data mining assisted multi agent-based intrusion detection system, particularly with the support of multiclass supervised classification. The agents of this IDS can detect and take predefined actions against malicious activities, and the data mining techniques can help detect them. [5] Uses intelligent agents that collect and analyze the network connections, and data mining techniques that shown to be useful to detect the intrusions. The experiments carried out on this IDS showed superior performance compared to the centralized architecture.

This paper is organized as follows: in section II, we present the work environment. We discuss data mining

algorithms which are used in this work in section III. Section IV will be devoted to the proposed architecture. Finally, a conclusion in section V will be given with work perspectives for improvement.

2. WORK ENVIRONMENT

2.1 Mobile Agents

In our proposed architecture, we had chosen to use mobile agents based on the following criteria [6]:

- ✓ They reduce the network load: Very large volumes of data are stored at remote hosts, mobile agents move to that hosts to compute data locally. Thus,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

we move the computation of the data rather than the data to the computation.

- ✓ They overcome network latency: Mobile agents can be dispatched from a central controller to act locally and execute the controller's directions directly.
- ✓ They encapsulate protocols: Mobile agents can move to remote hosts to establish "channels" based on proprietary protocols.
- ✓ They execute asynchronously and autonomously: After being dispatched, the agents become independent of the process that created them and can operate asynchronously and autonomously.
- ✓ They adapt dynamically: Mobile agents can sense their execution environment and react autonomously to changes.
- ✓ They are naturally heterogeneous: Mobile agents provide optimal conditions for seamless system integration.
- ✓ They are robust and fault-tolerant: Mobile agents can react dynamically to unfavourable situations and events.

2.2 Mobile agents framework

To use mobile agents, we need a framework or platform that allow us to develop agents. The JADE platform was selected after several studies was made on mobile agent platforms. JADE (Java Agent Development Framework) is a software Framework fully implemented in Java language. It answers the constraints of environments with limited resources, and it was already integrated in complex architecture like .NET or J2EE. Our choice is based on [7] as shown in the following figure.

Agent Development Toolkits → / Features ↓	Aglet	Voyager	JADE	Anchor	Zeus
Nature of Produce	Free, Open source	Commercial	Free, Open Source	Available in BSD license	Free, open source
Standard implemented	MASIF	----	FIPA Compliant	SSL, X.509	FIPA compliant
Communication Technique	Synchronous , Asynchronous	All methods	Asynchronous	Asynchronous	Asynchronous
Security Mechanism	Poor	Weak	Good	Strong security	Good
Agent Mobility	Weak	Weak	Not-so-weak	Weak	Do not support
Agent Migration Mechanism	Socket	RMI	RMI	Socket	null

Fig. 1 : Comparison Of Various Mobile Agents' Platforms

3. DATAMINING ALGORITHMS

In the last few years, data mining algorithms have been used widely in intrusion detection field. Actually, the data mining algorithms show performance in discovering consistent and useful patterns of system features that describe program and user behaviour. They use a set of relevant system features to compute classifiers that can recognize anomalies and known intrusions.
In our architecture, we had chosen k-means as algorithm to integrate it in one of the mobile agents. Our choice is based on two comparative studies. [9] As shown in the following figure compare between k-means, EM, DBSCAN and so on.

Journal of Theoretical and Applied Information Technology
30th April 2015. Vol.74 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Name	Number of clusters	Cluster Instances	Number of Iterations	Within clusters sum of squared errors	Time taken to build model	Log likelihood	Unclustered Instances
K-Means Algorithm	2	0:254(42%) 1:346(58%)	4	2016.6752520938053	0.08 Seconds		0
EM Algorithm	6	0:31 (5%) 1:97 (16%) 2:65 (11%) 3:184(31%) 4:92(15%) 5:131(22%)			76.94 seconds	-21.09024	0
DBSCAN	3	0:10 (40%) 1:6 (24%) 2:9 (36%)			1.03 Seconds		575
Hierarchical Clustering	2	0:599(100%) 1:1 (0%)			1.16 Seconds		0
Density based Clusters	2	0:239(40%) 1:361(60%)	4	2016.6752520938053	0.06 Seconds	-22.04211	0
OPTICS	0				1.37 seconds		600

Fig. 2 : Comparison And Results Between Data Mining Algorithms Using WEKA

[10] Is the second comparison study between k-means, k-medoids and clarans. The figure below illustrate the study.

Parameters	k-means	k-medoids	Clarans
Complexity	O (i k n)	O (i k (n-k)2)	O (n^2)
Efficiency	Comparatively more	Comparatively less	Comparatively more
Implementation	Easy	Complicated	complicated
Sensitive to Outliers?	Yes	No	No
Advance specification of No. of clusters 'k'	Required	Required	Required
Does initial partition affects result and Runtime?	yes	yes	Yes
Optimized for	Separated clusters	Separated clusters, small dataset	Separated clusters, large dataset

Fig. 3 : Comparison Between K-Means, K-Medoids And Clarans

4. PROPOSED ARCHITECTURE

In our new architecture, we propose to integrate data mining algorithms in mobile agents as shown in the next figure:

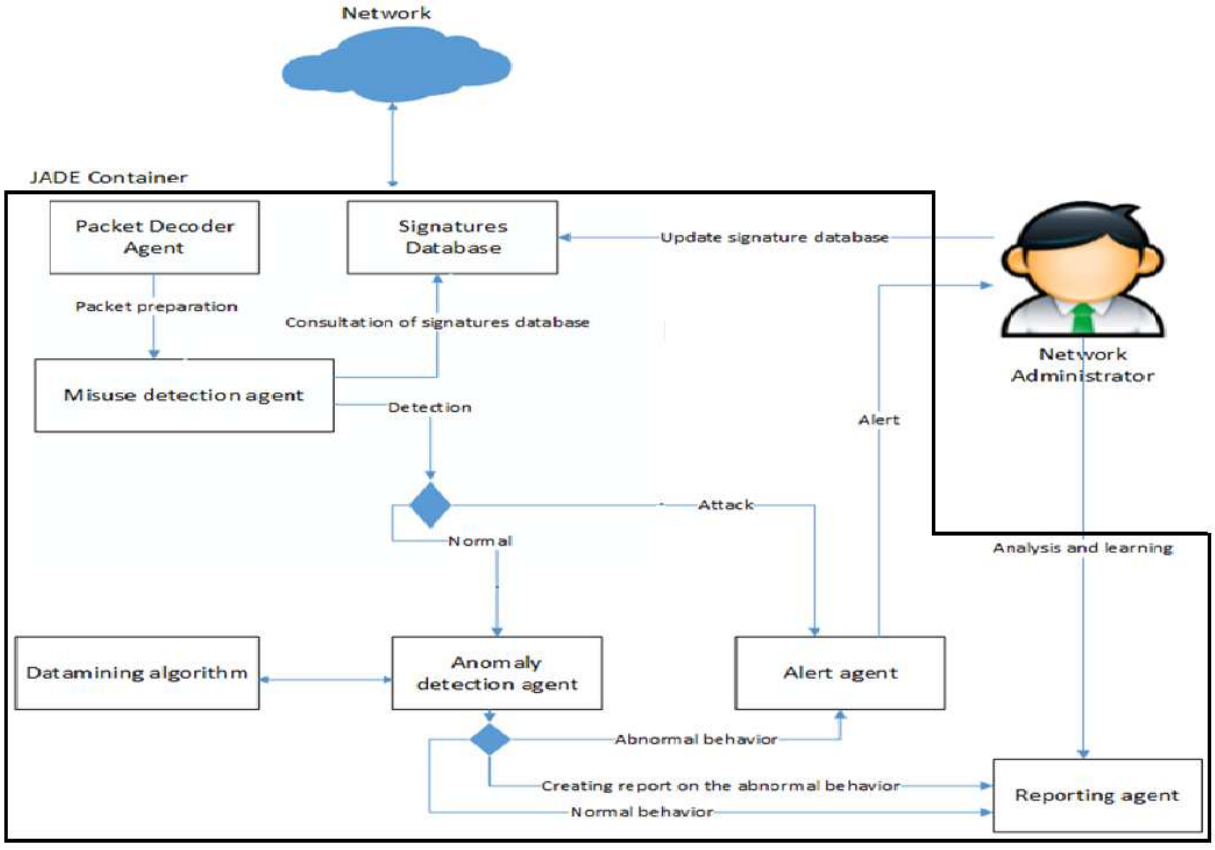

Fig. 4 : Proposed Architecture

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

To use mobile agents in a network architecture, we need to install a JADE server or more on the machines. The JADE server is the environment of creation and execution of the mobile agents. After creation, an agent can move through the network to carry out the tasks for which it was created. This agent can use the results sent by another agent and thus carry out the treatment without moving.

The mobile agents are created to achieve goals while collaborating between them. An agent cooperates with other agents what pushes it to understand the messages of his collaborators. The communication between the agents makes it possible to bind a set of agents and makes it possible to increase the perceptive capacities of the agents while enabling them to profit from information and the know-how of the other agents. Without communication, an agent is isolated and act on itself. The communication thus is based on languages of communication.

In our architecture, after the creation of all the agents, the packet decoder agent recovers the packets since the various network interfaces and prepares the packets to send them to the misuse detection agent. Once the misuse detection agent receives the formatted packets from and packet decoder agent, it uses a signatures database of the intrusions or the already known attacks to detect any type of intrusions.

The misuse detection agent compares the packets received with the existing signatures in the database of signatures (a signature of attack indicate a set of characters or of characteristics which identify the intrusion), if a signature is detected, it sends a message to the alert agent to create an alarm and to inform the administrator that an intrusion is detected. If the result of the treatment of the misuse detection agent is considered normal, it sends the result to the anomaly detection system. The anomaly detection agent applies an algorithm of data mining to the received message from the misuse detection agent to be able to detect the behaviour. A normal behaviour is a profile already creates in a network of test.

After the treatment, the anomaly detection agent by using an algorithm of data mining such as k-means decides and sends a message to the alert agent to inform the administrator that the detected behaviour is abnormal, if not he sends a message to the reporting agent to create a total return on the behaviour. The logs files and the reports created by the reporting agent will be used thereafter by the administrator to try to create new signatures for the abnormal activities or events detected. The administrator must regularly update the database of signatures in an automatic way by using a script or manually.

This architecture is based on another study already done on the integration of mobile agents in an IDS with the use of unsupervised data mining algorithms that led to positive results in terms of intrusion detection and minimization the rate of positive and negative false [11]. The development of this system was using Sun Java Developing Kit 7, the platform 3.7 JADE (Java Development Officer) that simplifies the implementation of multi-agent systems and the open source library JPCAP0.7.

Our work aims to enhance the previous architecture with good modelling of agent behaviour scenario between them and a clarification of the role of the network administrator of the proposed system

5. CONCLUSION

In this paper, we had presented a new architecture of IDS based using mobile agents and data mining algorithms, which make it possible to seize with precision the behaviour of the network traffic in order to detect intrusions.

In future work, we will develop an IDS using the architecture proposed. We will create a new datamining algorithm to performing our study.

REFERENCES

[1] "Intrusion Detection Systems: Definition, Need and Challenges." SANS Institute, 2001.
[2] E. H. Spafford and D. Zamboni, "Intrusion detection using autonomous agents," *Computer Networks*, vol. 34, no. 4, pp. 547–570, Oct. 2000.
[3] P. Kannadiga and M. Zulkernine, "DIDMA: A Distributed Intrusion Detection System Using Mobile Agents," pp. 238–245,2005.
[4] L. Cao, Ed., Data Mining and Multi-agent Integration. Boston, MA: Springer US, 2009.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[5] L. Cao, A. L. C. Bazzan, A. L. Symeonidis, V. I. Gorodetsky, G. Weiss, and P. S. Yu, Eds., Agents and Data Mining Interaction, vol. 7103. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.

[6] D. B. Lange and M. Oshima, "Seven good reasons for mobile agents," Communications of the ACM, vol. 42, no. 3, pp. 88–89, Mar. 1999.

[7] A. Singh, D. Juneja, and A. K. Sharma, "Agent Development Toolkits," CoRR, vol. abs/1111.5930, 2011.

[8] Lee, Wenke, and Salvatore J. Stolfo. "Data mining approaches for intrusion detection." Usenix Security. 1998.

[9] M. Verma, M. Srivastava, N. Chack, A. K. Diswar, and N. Gupta, "A Comparative Study of Various Clustering Algorithms in Data Mining," vol. 2, no. 3, pp. 1379–1384, 2012.

[10] G. Gandhi and R. Srivastava, "Review Paper : A Comparative Study on Partitioning Techniques of Clustering Algorithms," vol. 87, no. 9, pp. 10–13, 2014.

[11] Chaimae Saadi et al, Security Analysis Using IDs Based on Mobile Agents and Data Mining Algorithms / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 597-602, 2015