

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique  
Université M'hamed BOUGARA de BOUMERDES



Faculté des Sciences  
Département d'Informatique

## MEMOIRE DE MAGISTER

**Spécialité : Informatique**  
**Option : Spécification de Logiciel et Traitement de l'Information**

**Présenté par :**

M<sup>elle</sup> Ghenima BOURKACHE

### Thème

---

---

Un IDS réparti basé sur une société d'agents  
intelligents

---

---

Soutenu devant le jury:

Mr. M. Mezghiche  
Mr. Y.M. Djouadi  
Mr. Y. Challal  
Mr. K. Tamine

Pr à l'université de Boumerdes  
M.C à l'université de Tizi-Ouzou  
M.A à l'université de Bab ezzouar  
HDR. à l'université de Limoges

Président  
Examinateur  
Examinateur  
Rapporteur

Année Universitaire : 2006/2007

<b>Introduction générale.....</b>	<b>1</b>
<b>Chapitre I : Sécurité réseaux et systèmes de détection d'intrusions</b>	
I. Introduction à la sécurité informatique.....	5
I.1. Services de sécurité.....	6
I.2. Classification des attaquants.....	6
I.3. Les différents types d'attaques.....	8
I.3.1. Les attaques réseaux.....	8
I.3.2. Les attaques applicatives.....	12
I.3.3. Les attaques par Déni de service.....	13
I.3.4. Les attaques virales.....	16
II. Système de détection d'intrusions.....	16
II.1. Contexte.....	16
II.2. Définitions.....	17
II.2.1. Intrusion.....	17
II.2.2. Détection d'intrusion.....	17
II.2.3. Définition d'un IDS.....	18
III. Caractéristiques des systèmes de détection d'intrusions.....	19
IV. Classification des systèmes de détection d'intrusions.....	20
IV.1. La méthode de détection.....	21
IV.1.1. L'approche comportementale.....	21
IV.1.2. Approche par scénarios.....	22
IV.2. Le comportement de la détection (réponse).....	25
IV.2.1. Les réponses actives.....	25
IV.2.2. Les réponses passives.....	26
IV.3. L'emplacement des sources d'audits.....	27
IV.3.1. NIDS (Network-Based IDS).....	27
IV.3.2. HIDS (Host-Based System).....	28
IV.3.3. IDS d'application.....	29
IV.3.4. IDS hybrides.....	30
IV.4. La fréquence d'utilisation (La synchronisation).....	30
V. Les imperfections des systèmes de détection d'intrusions actuels.....	31
Conclusion.....	33

**Chapitre II : Systèmes multi-agents : SMA**

I. Introduction.....	36
II. Concepts de base.....	36
II.1. Définitions.....	38
II.2. Propriétés d'un agent intelligent.....	39
II.3. Intelligence des agents.....	40
II.3.1. Les agents cognitifs.....	40
II.3.2. Les agents réactifs.....	42
II.3.3. Les agents hybrides.....	43
III. Systèmes multi-agents (SMA).....	44
III.1. Qu'est-ce qu'un SMA ?.....	44
III.2. Les systèmes multi-agents à base de colonie de fourmis.....	45
III.3. propriétés des systèmes multi-agents.....	46
III.3.1. La coopération.....	46
III.3.2. La coordination.....	47
III.3.3. La communication.....	48
IV. Efficacité de la détection des attaques de sécurité et les propriétés des agents intelligents.....	49
Conclusion.....	51

**Chapitre III : Systèmes de détection d'intrusions à base d'agents**

I. Introduction.....	53
II. Aperçu sur les agents mobiles.....	53
III. Avantage de la mobilité dans les systèmes de détections d'intrusions.....	54
IV. Les caractéristiques d'un système de détection d'intrusions à base d'agents mobiles.....	58
V. Les travaux relatifs.....	59
Conclusion.....	75

**Chapitre IV : Notre contribution**

I. Introduction.....	78
II. Nos motivations initiales.....	78
II.1. L'influence des systèmes naturels.....	78
II.2. La vie artificielle.....	79

III. Ce que font les fourmis réelles.....	80
IV. Ce que font les fourmis artificielles.....	81
V. Présentation de ANTClass.....	83
V.1. Principe de fonctionnement.....	83
V.2. Hybridation avec les centres mobiles.....	88
V.2.1. L'algorithme des centres mobiles.....	91
VI. Validation de la méthode ANTClass.....	92
VI.1. Présentation de la base KDD'99.....	92
VI.2. Application de la méthode ANTClass sur la base KDD'99.....	94
VII. La recherche d'un SDI furtif mobile collectif.....	96
VII.1. Notre modèle.....	97
VII.1.1. L'étape de l'apprentissage.....	99
VII.1.2. L'étape de la détection d'anomalies.....	101
VII.1.3. Détection d'attaques par les réseaux bayésiens.....	103
Conclusion.....	106
<b>Conclusion générale.....</b>	<b>107</b>
<b>Bibliographie.....</b>	<b>109</b>
<b>Annexe A : Les réseaux bayésiens</b>	
A.1. Introduction.....	117
A.1.1. Probabilité conditionnelle.....	117
A.2. Réseaux bayésiens.....	117
A.2.1. Loi de Bayes.....	118
A.2.2. D- séparation.....	118
A.3. Inférence dans un réseau bayésien.....	119
A.4. Apprentissage.....	120
<b>Annexe B : La plate-forme Aglets™</b>	
B.1. Présentation de la plate-forme Aglets.....	121
B.2. La sécurité dans la plate-forme Aglets.....	126

## ملخص

يكون أمن شبكات الإعلام الآلي عرضة لشتى الإختلالات التي تتمثل خاصة في الازدحامات، التداخلات الغير السليمة والهجمات. لهذا فإنه من الضروري تزويد هذه الأنظمة بوسائل وآليات قادرة على منع هذه الظاهرة.

من أجل الكشف على كلّ محاولة لخرق سياسة الأمن يجب القيام بمراقبة الأنظمة بطريقة مستمرة ومنتظمة و ذلك باستعمال طرق الكشف عن التعدّيات.

أصبحت أنظمة و طرق الكشف عن التعدّيات منتشرة في أنظمة المعلومات التي حُضيت بمكانة هامّة في تصميم إستراتيجية الأمن.

على الرغم من سمعة هذه الوسائل، فإنّ غالبية أنظمة كشف التعدّيات أحادية ومركزية، بينما جمع المعلومات في الشبكة يكون موزّعا. لهذا فإنّ هدفنا يتمحور في الكشف الموزع والذكي للتعدّيات.

في هذا الصدد، نقترح نموذجا لتحقيق نظام لكشف التعدّيات، الذي يكون موزعا وسلوكيا، وهذا باستعمال طريقة التصنيف القائمة على سير النمل التي تعمل على مبدأ مجموعة من العملاء المتنقلين الذين يتصفون بميزة ردّ الفعل، حيث تكون هذه المجموعة مكرسة للكشف الموزع، والذكي على التعدّيات في الشبكة.

يهدف هذا النموذج إلى حلّ المشاكل الناتجة عن الأنظمة المركزية للكشف على التعدّيات.

**الكلمات الرئيسية:** شبكة الإعلام الآلي، الأمن، أنظمة كشف التعدّيات، عملاء متنقلين، أنظمة متعددة العملاء.

## Abstract

The networks are increasingly susceptible to be a target of various disorders, against their security, such as the congestions, malevolent accesses and the attacks. To this end, it becomes inescapable to provide these systems of tools and mechanisms able to inhibit these disordered states.

The intrusion detection systems are became very largely deployed in the information systems and they gained an important place in the design of the strategy of security.

In spite of the reputation of these tools, the majority of intrusion detection systems are monolithic and centralized whereas the data-gathering on network is distributed. To this end, our objective lies in the scope of distributed and intelligent intrusion detection.

In this spirit, we propose a model for build a distributed and behavioural intrusion detection system by using a method of classification based on the functioning of ants -ANTClass- and functioning on the principle of a society of reactive mobile agents dedicated to the distributed and intelligent intrusion detection in a network.

This model aims at solving the problems included by the centralized intrusion detection systems.

Keywords: data-processing networks, security, intrusions detection systems, IDS, reactive mobile agents, Multi-agents systems, MAS.

## Résumé

Les réseaux informatiques sont de plus en plus susceptibles d'être la cible de dérèglements divers, à l'encontre de leur sécurité, tels que les congestions, les accès malveillants et les attaques. A cet effet, il devient inéluctable de munir ces systèmes d'outils et de mécanismes capables d'inhiber ces dérèglements.

Afin de détecter toute tentative de violation de la politique de sécurité, une surveillance permanente ou régulière des systèmes peut être mise en place : ce sont les Systèmes de Détection d'Intrusions (IDS).

Les systèmes de détection d'intrusions sont devenus très largement déployés dans les systèmes d'informations et ils ont gagné une place importante dans la conception de la stratégie de sécurité.

Malgré la réputation de ces outils, la plupart des systèmes de détection d'intrusions sont monolithiques et centralisés alors que la collecte des données sur le réseau est distribuée. A cet effet, notre objectif s'inscrit dans le cadre d'une détection d'intrusions distribuée et intelligente.

Dans cet esprit, nous proposons un modèle pour construire un système de détection d'intrusions réparti comportemental en utilisant une méthode de classification basé sur le fonctionnement des fourmis – ANTClass – et fonctionnant sur le principe d'une société d'agents mobiles réactifs dédiée à la détection d'intrusions distribuée et intelligente dans un réseau.

Ce modèle vise à résoudre les problèmes induits par des systèmes de détection d'intrusions centralisés.

Mots clés : réseaux informatiques, Sécurité, système de détection d'intrusions, IDS, agents mobiles réactifs, systèmes multi-agents, SMA.