

University of Wollongong - Research Online

Thesis Collection

Title: An agent-based framework for distributed intrusion detections

Author: Dayong Ye

Year: 2009

Repository DOI:

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Research Online is the open access repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

2009

An agent-based framework for distributed intrusion detections

Dayong Ye
University of Wollongong

Follow this and additional works at: <https://ro.uow.edu.au/theses>

University of Wollongong

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

Recommended Citation

Ye, Dayong, An agent-based framework for distributed intrusion detections, M.Comp.Sc.Res. thesis, School of Computer Science and Software Engineering, University of Wollongong, 2009.
<http://ro.uow.edu.au/theses/797>

NOTE

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

UNIVERSITY OF WOLLONGONG

COPYRIGHT WARNING

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

An Agent-Based Framework for Distributed Intrusion Detections

A thesis submitted in fulfillment of the
requirements for the award of the degree

Master by Research

from

UNIVERSITY OF WOLLONGONG

by

Dayong Ye

School of Computer Science and Software Engineering
May 2009

© Copyright 2009

by

Dayong Ye

All Rights Reserved

*Dedicated to
Zhen Ye and Tonghua Wang*

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Dayong Ye
May 25, 2009

Abstract

Network application has become a part of our everyday life. With the increasing of convenience and popularity of network, more and more malicious users utilize network to obtain their vicious intentions. In order to protect network users' information security and privacy, various intrusion detection systems were proposed and developed in the last decade. Intrusion detection as an emerging technology has made great achievements in theory and practice, whose aim is to protect the confidentiality, integrity or availability of a system or resource. As a complex system, the development of an intrusion detection system includes many aspects, such as system architecture design, design and implementation of system components, system test in real cases, and so on.

Though many intrusion detection systems have been presented, most of them mainly focus on one or two aspects of intrusion detection systems. This thesis aims at providing a rudimentary solution for an agent-based Peer-to-Peer distributed intrusion detection framework. The major contributions of this thesis include the following five aspects.

1. Introducing a novel Peer-to-Peer framework which involve different agents on different peers;
2. Designing functionalities of each agent in the framework by using JACK/UML approach;
3. Representing knowledge of each agent about intrusion and detection according to employing ontology;
4. Developing an efficient task allocation protocol which is used to coordinate different hosts in the system to collaboratively detect distributed attacks;
5. Implementing and testing the framework in a reasonable manner by utilizing an agent development environment, i.e. *JACKTM*.

In summary, this framework integrates agent technology, Peer-to-Peer architecture, ontology technique and a task allocation protocol. Implementation and experiments

show the potential applicability of this framework to real cases. In addition, this framework could help in development of a good intrusion detection system in open and complex environments.

Acknowledgements

Studying abroad is a tedious and tired journey. Without the help and support of many people, I cannot complete my research.

I am indebted to my supervisors, Associate Professor Minjie Zhang and Dr. Quan Bai. Their constant commitment and guidance was instrumental in the completion of this thesis, and in making it a fulfilling experience. I am grateful to Dr. Quan Bai for his kind help, encouragement and patient proofreading my thesis and research papers. I am also delightful for Associate Professor Minjie Zhang's enthusiasm for my everyday life. Furthermore, I thank the School of Computer Science and Software Engineering and the University of Wollongong for the financial support of conference attendance.

My thanks are extended to Mr. Shaojie Yuan, who often discusses with me in the lab and enriches my knowledge; and Mr. Guohua Yao, my house mate, who chats with me during our dinner time everyday and brings me a lot of fun.

I would like to express my deepest gratitude to my parents, Zhen Ye and Tonghua Wang, who always make their financial support, encouragement, understanding and love. Without their help, this thesis would not be finished. Thanks too, to my wife, Yun, for her constantly tolerating my selfishness and her delicious food. I hope she could forgive me for what I have done. I have dedicated this thesis to my parents and my wife for their patience, understanding and unconditional love.

Finally, thanks to all the anonymous reviewers of my research papers, and all my other dear friends and relatives who have supported me.

Publications

The followings are list of my research papers that have been already published during my Master study that is to be ended by the completion of this thesis.

- Dayong Ye, Quan Bai, and Minjie Zhang. BDI agent-oriented design for distributed intrusion detections. *Communications of SIWN*, 4:11-17, Jun. 2008.
- Dayong Ye, Quan Bai, and Minjie Zhang. Ontology-based knowledge representation for a p2p multi-agent distributed intrusion detection system. In *Proceedings of the 2008 IFIP International Workshop on Network and System Security (NSS 2008)*, pages 111-118, Shanghai, China, Oct. 2008.
- Dayong Ye, Quan Bai, and Minjie Zhang. P2P distributed intrusion detections by using mobile agents. In *Proceedings of the seventh IEEE/ACIS International Conference on Computer and Information Science (ICIS 2008)*, pages 259-265, Portland, Oregon, US, May 2008.
- Dayong Ye, Quan Bai, and Minjie Zhang. A mobile agent based peer-to-peer framework for distributed intrusion detections. In *Proceedings of the Eighth International Conference on Intelligent Technologies (InTech'07)*, pages 45-55, Sydney, AU, Dec. 2007.

Contents

Abstract	v
Acknowledgements	vii
Publications	viii
1 Introduction	1
1.1 Intrusion and Intrusion Detection	2
1.1.1 Intrusion	2
1.1.2 Intrusion Detection	7
1.2 Agent-Based Intrusion Detection Systems	9
1.3 Research Concerns	12
1.4 Thesis Structure and Outcomes	14
2 Related Research and Literature Review	16
2.1 Architecture and Design of Agent-Based Intrusion Detection Systems .	16
2.2 Intrusion Detection Language	18
2.3 Task Allocation Protocols and Resource Search Mechanisms	23
2.3.1 Task Allocation in Distributed Environments	23
2.3.2 Resource Search in P2P Environments	25
2.4 Summary	27
3 A Novel P2P Agent-Based Framework for Distributed Intrusion De-	
tections	28
3.1 Framework Architecture	28
3.1.1 Monitor Agent	28
3.1.2 Analysis Agent	29
3.1.3 Executive Agent	29
3.1.4 Manager Agent	30

3.1.5	Retrieval Agent	31
3.1.6	Result Agent	31
3.1.7	Agent working process	31
3.2	Detailed Design of the Framework	32
3.2.1	Overview of BDI agents	32
3.2.2	JACK TM Agent Development Environment	33
3.2.3	Monitor Agent	34
3.2.4	Analysis Agent	36
3.2.5	Executive Agent	38
3.2.6	Manager Agent	39
3.2.7	Retrieval Agent	41
3.2.8	Result Agent	42
3.3	Summary	42
4	Ontology-Based Knowledge Representation for Distributed Intrusion Detection	43
4.1	Overview of Ontology	43
4.2	Ontology Implementation	45
4.2.1	Knowledge of Monitor Agent	46
4.2.2	Knowledge of Analysis Agent	47
4.2.3	Knowledge of Executive Agent	48
4.2.4	Knowledge of Manager Agent	49
4.2.5	Knowledge of Retrieval Agent	50
4.2.6	Knowledge of Result Agent	50
4.3	Example	51
4.4	Summary	52
5	Task Allocation in the P2P Framework	53
5.1	Problem Description	53
5.2	Principle of ETAP	55
5.3	Test of ETAP	58
5.3.1	Gnutella Algorithm	58
5.3.2	Greedy Distributed Allocation Protocol	59
5.3.3	Test Setting	59
5.3.4	Test Results	62
5.3.5	Discussion of ETAP	66

5.4	Summary	66
6	Test and Discussion	67
6.1	Test Metrics of Intrusion Detection Systems	67
6.2	Test of the Framework	68
6.2.1	Test Setting	68
6.2.2	Detection of <i>Doorknob-Rattling Attack</i>	68
6.2.3	Detection of <i>Chain/Loop Attack</i>	71
6.2.4	Detection of <i>Mitnick Attack</i>	73
6.3	Discussion of the Test	75
6.4	Summary	77
7	Conclusion	78
7.1	Major Contributions of this Thesis	78
7.1.1	Architecture of the Agent-Based P2P Framework	79
7.1.2	Knowledge Representation of Agents	79
7.1.3	A Task Allocation Protocol	80
7.2	Remaining Problems and Future Work	80
	Bibliography	82

List of Tables

3.1	UML High Level Stereotypes for JACK TM	34
3.2	UML Association Level Stereotypes for JACK TM	34
4.1	An Example of N-Triples	47
4.2	N-Triples Notation for Suspicious Doorknob-Rattling Attack	51
4.3	Query for Suspicious Doorknob-Rattling Attack	52

List of Figures

1.1	Attack Classification with Ontology	4
1.2	A Paradigm of Doorknob-Rattling Attack	6
1.3	A Paradigm of Chain/Loop Attack	7
1.4	A Paradigm of Mitnick Attack	8
1.5	A Standard Architecture of IDS	10
3.1	Architecture of the Framework	29
3.2	Retrieval Process	32
3.3	A Simple Example of Designing JACK TM Agent with UML	35
3.4	Design of Monitor Agent with JACK/UML	35
3.5	Design of Analysis Agent with JACK/UML	37
3.6	Design of Executive Agent with JACK/UML	38
3.7	Design of Manager Agent with JACK/UML	40
3.8	Design of Retrieval Agent with JACK/UML	42
3.9	Design of Result Agent with JACK/UML	42
4.1	RDF relationship graph	44
4.2	Ontology representation of agent knowledge in each peer	45
4.3	Monitor Agent Knowledge	46
4.4	Analysis Agent Knowledge	48
4.5	Executive Agent Knowledge	49
4.6	Manager Agent Knowledge	50
5.1	Interaction Process Between <i>Initiator</i> and a <i>Participant</i>	56
5.2	Performance of different protocols on distinct average number of neighbors	62
5.3	Performance of different protocols on distinct <i>TTL</i> value	63
5.4	Performance of different protocols on distinct number of agents	64
5.5	The performance of ETAP with different number of walkers	66

6.1	An example P2P network which has been attacked by <i>Doorknob-Rattling</i>	69
6.2	Detection of <i>Doorknob-Rattling Attack</i> with different mechanisms . . .	70
6.3	An example P2P network which has been attacked by <i>Chain/Loop</i> . . .	72
6.4	Detection of <i>Chain/Loop Attack</i> with different mechanisms	73
6.5	An example P2P network which has been attacked by <i>Mitnick</i>	74
6.6	Detection of <i>Mitnick Attack</i> with different mechanisms	76