2009

# An agent-based framework for distributed intrusion detections

Dayong Ye
*University of Wollongong*

# 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

*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. $JACK^{TM}$.

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

# List of Tables

# List of Figures