IA-BASED FUALT DETECTION SYSTEM

"Mohammad Jehad" Baeth "Ahmad Fawzi"

UNIVERSITI UTARA MALAYSIA
2010

IA-BASED FAULT DETECTION SYSTEM

This thesis submitted to the Graduate School in partial fulfillment of the requirements for the degree Master of Science (Information Technology) University Utara Malaysia

By

"Mohammad Jehad" Baeth " Ahmad Fawzi" (802379)

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

MOHAMED JEHAD BAETH "A. FAWZI"
(802789)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

INTELLIGENT AGENT BASED FUALT DETECTION SYSTEM

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **PROF. DR. KU RUHANA KU MAHAMUD**

Tandatangan
(Signature) : _____

Tarikh
(Date) : 28 April 2010

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from University Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the Graduate School.

It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part should be addressed to:

Dean of Graduate School

University Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman.

ABSTRACT

The current IP-network management systems normally utilize the centralized (client–server) architecture. Researchers have stated that, those systems may cause serious efficiency defects, when the complexity and size of the network increases. Automated network monitoring systems have some limitation. They are known of making a huge overload on the network bandwidth due to their unnecessary message transaction between the server and the monitored hosts. Moreover, the lack of getting appropriate information that describes the malfunction makes it hard for the administrational team to identify the source of reported error. An innovative distributed intelligent agent based fault detection system that operates on Windows platform was presented, to capture abnormal and faulty behaviors on both application and system levels. The design process of the intelligent agent utilized the ability of reactive operating and independent decision taking. The system has a web based graphical user interface to facilitate the accessibility to such vital information. Several evaluation scenarios were conducted to evaluate the trustworthiness and performance criterion of the proposed system.

DEDICATION

In the name of Allah, the most merciful and compassionate.

All praise is due to Allah, the most Generous and loving, the source of all blessings.

To the symbol of wisdom, my mentor, and the source of my existence. To my father "Ahmad".

Heaven lies under your feet along with my happiness and success in this life and the afterlife, there are no words that can honor you enough. To my mother "Sahar".

To Eyad, only Allah can pay off my debt to you, thank you for turning me from a JGDAF into me.

To my sisters Bara'a, Tayma, Thara'a, Yousr.

To my friends Fadi, Alla, Ahmad, Hamzeh, Dia'a, Osama, Zyad, Hussam, Faisal, Chris, Hashem, Rony, Samer, Mohamad, Homam, Morhaf, Taha, AbdulGhani and All those I have not mentioned, thank you for your continuous support.

ACKNOWLEDGEMENT

At the beginning of my speaking, I thank Allah for helping me in my study and guiding me to continue what I have started in my educational life. I thank Allah in every day for giving me the ability and motivation to continue this work...

After thanking Allah, I would like to convey my regards to my supervisor Prof. Dr. Ku Ruhana for the benefit and precious information that she gave me as one of her students. I thank and honor her for helping me to complete my study in a good way...

Finally, I would like to say thankfulness word for the lecturers in the Information Technology Department at University Utara Malaysia (UUM)...

Thank you UUM...

"Mohammad Jehad" Baeth "Ahmad Fawai"

2010

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

The development and growth of computer networks concepts and technology have paved the way for developing new applications in this field of study. Considering the high demand of business organizations for improvements in network management, the wave of development was directed towards creating more advanced network management systems this is to simplify and speed up administrational responsibilities as well as observing network hosts in a real-time basis in order to protect the network from faults. Generally, network management system can handle problems concerning network configuration, tune reliability and efficiency issues, even more increase security standards (Cisco Systems, 2004). In other words, network management system is concerned with monitoring, analyzing and controlling a network, serving the purpose of smoother operation.

Network monitoring is the portion of network management, which is concerned with detecting symptoms of failure and analyzing the status and behavior of the managed network devices. It is getting vital for computer networks to perform in the best manner (Boutaba and Xiao, 2002). A typical network management system consists of two parts as shown in Figure1.1.

The contents of the thesis is for internal user only

REFERENCES

Anne, C., & Alexis, D. (1998). USING THE CASSIOPEIA METHOD TO DESIGN A ROBOT SOCCER TEAM. *Applied Artificial Intelligence, 12*(2/3), 127.

Baldini, A., Benso, A., Chiusano, S., & Prinetto, P. (2000, 2000). *BOND: An interposition agents based fault injector for Windows NT.* Paper presented at the Proceedings. IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, 2000, Yamanashi, 387-395.

Bianchini, C. d. P. (2003). *Intelligent management of network devices aided by a strategy and a tool.* Paper presented at the Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research, La Paz, Bolivia,141-151.

Boutaba .R and Xiao. J. (2002). Network Management: State of the Art, *IFIP, 220*, 127 146.Cooperative Network Management Architecture. *IEEE Network, 10 April, 1-3.*

Buschmann, F. (1998). *pattern-oriented software architecture a system of patterns.* Chichester: Wiley.

Cisco Systems, I. (2004). *Internetworking technologies handbook.* Indianapolis, IN: Cisco Press.

Dong-Liang, L., Sheng-Yuan, Y., & Yi-Jen, C. (2009, 3-5 Dec. 2009). *Developing an active mode of network management system with intelligent multi-agent techniques.* Paper presented at the Joint Conferences on Pervasive Computing (JCPC) 2009, 77- 82, Tamsui, Taipei.

Franklin, S., & Graesser, A. (1997). *Is it an Agent, or Just a Program?: A Taxonomy for Autonomous Agents.* Paper presented at the Proceedings of the Workshop on Intelligent Agents III, Agent Theories, Architectures, and Languages, Verlag, 21-35.

Gavalas, D., Greenwood, D., Ghanbari, M., & O'Mahony, M. (2000). Advanced network monitoring applications based on mobile/intelligent agent technology. *Computer communications., 23*(8), 720.

Gavalas, D., Tsekouras, G. E., & Anagnostopoulos, C. (2009). A mobile agent platform for distributed network and systems management. *J. Syst. Softw., 82*(2), 355-371.

Ibrahim, M. A. M. (2006). *Distributed Network Management with Secured Mobile Agent Support*. Paper presented at the Proceedings of the 2006 International Conference on Hybrid Information Technology,Cheju Island, 244-251.

Kendall, E. A., Krishna, P. V. M., Suresh, C. B., & Pathak, C. V. (2000). An application framework for intelligent and mobile agents. *ACM Comput. Surv., 32*(1es), 20.

Kim, B. U., Al-Nashif, Y., Fayssal, S., Hariri, S., & Yousif, M. (2008). *Anomaly-based fault detection in pervasive computing system.* Paper presented at the Proceedings of the 5th international conference on Pervasive services, Sorrento, Italy, 147-156.

Kuechler, W., Vaishnavi, V., & Kuechler, W. L. (2007). *Design [Science] Research in IS: A Work in Progress.* Paper presented at the 2nd International Conference on Design Science Research in Information Systems and Technology, USA, California, 234-239.

Liotta, A., Pavlou, G., & Knight, G. (2002). Exploiting Agent Mobility for Large-Scale Network Monitoring. *IEEE NETWORK, 16*, 7-15.

Pugazendi, R., & Duraiswamy, K. (2009, 27-28 Oct. 2009). *Mobile Agents - A Solution for Network Monitoring.* Paper presented at the ARTCom '09. International Conference on Advances in Recent Technologies in Communication and Computing, 2009, Kottayam, Kerala, 579-584.

Ray, J., Hoe, J. C., & Falsafi, B. (2001). *Dual use of superscalar datapath for transient-fault detection and recovery.* Paper presented at the Proceedings of the 34th annual ACM/IEEE international symposium on Microarchitecture, Austin, Texas, 214-224.

Reinhardt, S. K., & Mukherjee, S. S. (2000). Transient fault detection via simultaneous multithreading. *SIGARCH Comput. Archit. News, 28*(2), 25-36.

Sakai, M., Matsuba, H., & Ishikawa, Y. (2007, 17-19 Dec. 2007). *Fault Detection System Activated by Failure Information.* Paper presented at the 13th Pacific Rim International Symposium on Dependable Computing, 2007. PRDC 2007., Melbourne, Qld, 19-26.

Satoh, I. (2002, 2002). *A framework for building reusable mobile agents for network management.* Paper presented at the Network Operations and Management Symposium, 2002. NOMS 2002. 2002 IEEE/IFIP, Tokyo, Japan, 51-64.

Staff, M. C. (1992). *The Basics Book of OSI and Network Management*: Addison-Wesley Longman Publishing Co., Inc.

Stallings, W. (1999). *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.* Reading, Mass.: Addison-Wesley.

Utton, P., & Scharf, E. (2004). A fault diagnosis system for the connected home. *Communications Magazine, IEEE, 42*(11), 128-134.

Vaishnavi, V. and Kuechler, W. (2004). "Design Research in Information Systems" January 20, 2004, last updated January 18, 2006. URL: http://www.isworld.org/Researchdesign/drisISworld.htm

Wooldridge, M. (2002). *An introduction to multiagent systems*. Chichester: Wiley.

Wu, F., Zhao, Z., & Ye, X. (2008, 20-22 Dec. 2008). *A New Dynamic Network Monitoring Based on IA.* Paper presented at the International Symposium on Computer Science and Computational Technology, 2008. ISCSCT '08,, Shanghai, 637-640.

Zambonelli, F., Jennings, N. R., & Wooldridge, M. (2003). Developing Multiagent Systems: The Gaia Methodology. *ACM transactions on software engineering and methodology., 12*(3), 317.

Zhang, S., Cohen, I., Symons, J., & Fox, A. (2005). *Ensembles of Models for Automated Diagnosis of System Performance Problems*. Paper presented at the Proceedings of the 2005 International Conference on Dependable Systems and Networks, CA, USA, 644-653.