KSIAM IT series Vol.10, No.1, 83-93, 2006

규칙 기반의 네트워크 장애 자기 복구 시스템*
(Rule-based network fault self-recovery system)

이재욱, 안성진**, 정진욱
(Jaewook Lee, Seongjin Ahn, Jinwook Chung)

요 약

본 논문에서는 유비쿼터스 컴퓨팅 환경에서 규칙 기반의 네트워크 장애 복구 시스템을 제안한다. 이 시스템은 유비쿼터스 컴퓨팅 환경에서 네트워크에 장애가 발생하였을 때, 정해진 규칙을 기반으로 장애를 스스로 복구할 수 있는 장애 관리 시스템이다. 시스템에 적용되는 규칙들을 네트워크 장애의 원인으로 분류하여 제시하였다. 그리고 본 논문에서는 네트워크 장애 복구 시스템이 각 상황에 맞게 규칙이 적용됨을 시뮬레이션을 통해 증명하였다.

Abstract

This paper introduces rule-based reasoning (RBR) based self-recovery system for network fault in ubiquitous computing. This system is fault management system for fault recovery of rule-based for self-recovery in ubiquitous computing environment. We proposed rules of network fault recovery applied the system as a distinguished reason of network fault. And, in this paper, the network fault self-recovery system proved the rules that applied each situatpion through the simulation.

1. 서 론

근래에는 유비쿼터스 컴퓨팅 (ubiquitous computing) 기술이 각광을 받으며 언제 어디서나 누구라도 어떤 대상이든 네트워크를 형성할 수 있게 되면서 네트워크는 점진적으로 복잡해지고 있다.[1] 또한 유비쿼터스 컴퓨팅 환경에서 디지털 기기들과 통합된 컴퓨터들

* This work was supported by grant No. R01-2004-000-10618-0 from the Basic Research Program of the Korea Science and Engineering Foundation.
** Corresponding author.
Key Words: Rule-based, Network fault recovery, RBR

은 센싱과 트래킹을 통해 장소나 시간에 따라 변화하는 상황을 인식하여 인간의 개입 없이 자율적으로 관리/복구되는 특성을 갖는다.[2] 현재는 이러한 네트워크 관리 및 장애 관리 및 탐지, 복구 문제를 전문가의 견해가 축적된 전문가 시스템(Expert System)을 통해 관리하고 있다.[3] 그러나 이러한 방법은 전문가가 시스템 혹은 네트워크의 모든 상황을 파악하는데 있어서 발생하는 한계로 인해 그 역할이 제한적일 수밖에 없다.[3,5,6,7]

특히 시스템의 네트워크 구성 장애에서는 장애 발생 원인을 명확히 판단하기는 더욱 어렵다. 시스템의 네트워크 구성 관련 장애는 그 장애 발생 원인이 다양하지만 실제 나타나는 장애 증상이 동일한 경우가 많기 때문이다. 예를 들어 인터넷이 되지 않는다고 해서 시스템의 네트워크 구성의 장애라고 단정하기는 어렵다. 이러한 장애는 네트워크 자체의 다운, 시스템의 네트워크 인터페이스 장치의 고장 혹은 네트워크를 구성하고 있는 네트워크 장비의 다운 등과 같은 다양한 장애의 원인이 존재할 수 있기 때문이다.[4]

따라서 시스템의 네트워크 구성 장애를 시스템 자체에서 판단하는 것은 많은 한계가 있다. 즉 외부 혹은 내부 네트워크의 상황을 해당 시스템 혼자서 판단하기는 어려운 일이다. 따라서 이러한 장애의 원인을 명확하게 판명하기 위해서는 네트워크의 구성 장애를 복구하기 위해 네트워크에 분포되어 있는 다양한 에이전트들 간의 통신을 통한 협력이 필요하다.

이에 본 논문에서는 유비쿼터스 컴퓨팅 기술을 통해 언제 어디서든 가능한 모든 에이전트들 간의 유기적인 협력을 통하여 시스템 자체적으로 파악할 수 없는 내부 혹은 외부네트워크의 상황을 정확히 파악함으로써 정확한 장애의 진단뿐만 아니라 효율적인 장애 복구를 위한 방법을 제공하고자 한다. 그리고 신속한 장애 복구를 위해 결정 트리를 적용하여 시스템의 성능 향상을 통해 장애를 복구하는데 걸리는 시간을 단축하고자 한다.

2. 네트워크 장애 복구 규칙

네트워크 장애 복구 규칙은 장애가 발생하면 그 증상을 진단하여 장애를 복구할 수 있는 특정 행동을 취하기 위한 일련의 규칙 집합(Rule Set)이다. 이러한 규칙 기반의 장애 복구 모델은 전문가 시스템을 구축하는데 있어서 가장 강력하고 구현하기 쉬운 툴로써 작용한다. If~then 형식의 가정은 설정된 상황에 대해서는 순조로운 수행을 하게 한다. 또 많은 상황에 대한 정보를 가지고 있을수록 RBR 기반의 전문가 시스템은 더 우수한 성능을 보이게 된다. 그래서 규칙 기반의 구조는 규칙이 추가될 수 있는 확장 구조를 필요로 하게 된다. 이를 위해서 가정들을 세분화하여 5개로 구분하여 규칙들을 의미 별로 구성하였으며 이를 통해 규칙의 확장을 쉽게 할 수 있게 하였다.[6,7,8]

2.1. 목적지에 의한 장애 진단

목적지에 의한 장애 진단(FBDD: Fault by destination detection)에서 에이전트 간의 협력은 well-known port와 해당 어플리케이션에서 사용하는 포트에 대한 접속 시도를 통해 목적지 장비 혹은 목적지 어플리케이션이 정상적으로 동작하고 있는지 아니면 목적지 장비에 의해서 협력을 요청한 에이전트가 필터링 되고 있는지 점검하는 것이다.

RS11 (Rule Set 11)

Rule 1101: IF Q1101 = fail THEN F1101 Rule 1102: IF Q1102 = fail THEN F1101 Rule 1103: IF Q1103 = fail THEN F1101 Rule 1104: IF Q1104 = fail THEN F1101 Rule 1105: IF Q1105 = fail THEN F1101 Rule 1106: IF F1101 THEN R21 ELSE R31 Rule 1107: IF Q1107 THEN RS31	
F1101: The Destination has some problems	Q1101: try to connect to the application Q1102: try to connect to [echo (7)] Q1103: try to connect to [discard (9)] Q1104: try to connect to [daytime (13)] Q1105: try to connect to [web (80)] Q1107: No response from any host

RS11에는 목적지에 대한 장애를 판단하는 과정에서 다른 에이전트의 협력이 필요하다고 판단되는 경우 RS21을 수행한다. RS21에서 목적지 장애 여부 확인은 목적지에 의한 필터링이나 목적지의 다운, 응용 프로그램이 이상으로 분류된다. 그러나 다른 에이전트들과의 협력이 불가능 한 경우, 즉 협력을 요청한 모든 에이전트들로부터 응답이 오지 않는 경우는 기본 연결 구성의 장애나 네트워크 환경 장애, 인터페이스 구성 장애로 보고 일단 기본 연결 구성의 장애로 분기하여 규칙을 적용한다.

RS21

Rule 2101: IF (Q2101 AND ~Q2102) THEN D2101 Rule 2102: IF (Q2101 AND Q2102 AND ~Q2103 AND ~Q2104) THEN D2102 Rule 2103: IF (Q2101 AND Q2102 AND Q2103 AND ~Q2104) THEN D2101 Rule 2104: IF (Q2101 AND Q2102 AND Q2103 AND Q2104) THEN D2103	
D2101: Report "Check whether your application is working normally or IP address is filtered out by the destination." D2102: Report "network ID is filtered out by the destination." D2103: Report "The application on the destination is down."	Q2101: Some agents can reach the destination port. Q2102: All agents in the same network failed. Q2103: Some of the agents in the other network can reach the destination port Q2104: All agents failed

2.2. 기본 연결 구성 장애

기본 연결 구성 장애 진단(DCCFD: Default Connection Configuration Fault Detection)은 시스템의 기본적인 연결 설정 상태를 진단하는 모듈이다. 장애 발생 시 시스템 자체의 장애인지를 판단하는 모듈로 네트워크 환경 구성요소인 IP주소, 서브넷 마스크, 브로드캐스트 주소, DNS 주소 등의 설정에 장애가 있는지 진단한다.

RS31

Rule 3101: IF Q3101 = different THEN F3101	
Rule 3102: IF Q3102 = different THEN F3102	
Rule 3103: IF Q3103 = different THEN F3103	
Rule 3104: IF Q3104 = different THEN F3104	
Rule 3105: IF Q3105 = no response THEN F3105	
Rule 3106: IF F3101 OR F3102 OR F3103 OR F3105 THEN RS32	
F3101: IP address setup failure	Q3101: check the state of IP address setup (Comparing to IP address in other L-Agent and backup file)
F3102: Subnet mask setup failure	Q3102: check the state of subnet mask setup (Comparing to subnet mask in other L-Agent)
F3103: Broadcast address setup failure	Q3103: check the state of broadcast setup (Comparing to broadcast address in other L-Agent and one of broadcasting ICMP router solicitation message.)
F3104: Default gateway setup failure	Q3104: check the default gateway address. (comparing to default gateway address in other L-Agent)
F3105: Interior network failure	Q3105: check the responses from L-Agent for Q3104

기본 연결 구성 장애 복구(DCCFR: Default Connection Configuration Fault Recovery)는 로컬 네트워크에 있는 정상적으로 동작하고 있는 L-Agent를 이용하여 네트워크 환경 정보를 다시 설정한다. 기존의 시스템이나 논문에서는 백업 파일 또는 ICMP 메시지를 이용하였으나, 본 논문에서는 이전 방법과 현재 정상동작을 하고 있는 에이전트의 네트워크 정보를 이용한다. 그리고 'address mask request' 메시지를 브로드캐스트하여 복구하는 방법도 병행하고 있다.

RS32

Rule 3201: IF F3101 AND Q3201 = success THEN R3201 Rule 3202: IF F3102 AND Q3202 = success THEN R3201 Rule 3203: IF F3103 AND Q3203 = success THEN R3201 Rule 3204: IF F3104 AND Q3204 = success THEN R3201 Rule 3205: IF F3105 THEN D3101	
R3201: Completion of the Default Connectivity Configuration Fault Recovery D3101: Report "Interior network failure"	Q3201: check the result after replacing the current IP address with the one in backup file Q3202: check the result after replacing the current subnet mask with the one obtain by L-Agent collaboration model or the other obtained by broadcasting ICMP message. Q3203: check the result after replacing the current broadcast address with the one obtained by L-Agent collaboration model. Q3204: check the result after replacing the current default gateway with the one obtain by L-Agent collaboration model or the other obtained by broadcasting ICMP message.

2.3. 네트워크 환경 장애

네트워크 환경 장애 진단(NEFD: Network Environment Fault Detection)은 PING 테스트를 수행하여 ICMP 메시지 중 'unknownHost'가 나타나는지를 조사한다. 'unknownHost'는 일반적으로 DNS에서 목적지를 알아 낼 방법이 없을 때 나타나는 것으로 DNS의 설정이 잘못 되었을 가능성이 있다. 이 경우 네임 서비스 구성 진단을 수행한다. 그러나 그 이외의 ICMP 메시지에 대해서는 라우팅 구성 장애로 판단한다.

RS41

Rule 14 : IF Q4101 = yes THEN R4201 Rule 15 : IF Q4102 = yes THEN R4202	
R4201 : reporting the result of diagnosis, which is the fault of interior network, to network manager R4202 : reporting the result of diagnosis, which is the fault of exterior network, to network manager	Q4101: checking whether the diagnosis result, which is obtained by agent collaboration model, is the fault of interior network Q4102: checking whether the diagnosis result, which is obtained by agent collaboration model, is the fault of exterior network

2.4. 인터페이스 구성 장애

인터페이스 구성 장애 진단(ICFD: Interface Configuration Fault Detection)은 시스템의 네트워크 인터페이스의 장애를 점검하고 NIC의 업/다운 상태, NIC의 드라이버 설치 상태, 케이블 접속 상태를 확인하여 장애를 진단한다.

RS51

Rule 5101: IF Q5101 = down THEN F5101 Rule 5102: IF Q5102 = fail AND ~F5101 THEN F5102 Rule 5103: IF Q5103 = disconnect THEN F5103	
F5101: The interface is down F5102: The operation of interface drive has fault F5103: The cable is disconnected	Q5101: check the state of NIC (up/down) Q5102: check running state of NIC drive Q5103: check the state of cable connection

인터페이스 구성 장애 복구(ICFR: Interface Configuration Fault Recovery)는 다운 상태의 인터페이스를 업 상태로 바꾸거나 인터페이스 카드의 드라이버를 다시 설치한다. 또한 끊어진 상태의 케이블을 복구할 수 있도록 사용자나 관리자에게 신속히 알려 장애를 복구한다.

RS52

Rule 5201 : IF F5101 AND Q5201 = success THEN R5201 Rule 5202 : IF F5102 AND Q5202 = success THEN R5201 Rule 5203 : IF F5113 AND Q5203 = success THEN R5202	
R5201: Completion of the Interface Configuration Fault Recovery R5201 : reporting the result of diagnosis, which is the fault of interface, to network manager or user.	Q5201: check the result after changing down-state interface into up-state one Q5202: check the result after re-install the interface drive Q5203: check the result after recovering the disconnected cable

2.5. 보안성 취약 탐지

보안성 취약 탐지(SWPD: Security Week Point Detection)는 시스템의 상태와 열려진 포트와 ARP Request 모니터링을 통해 알려진 백도어 프로그램이나 웜 바이러스의 포트를 조사하거나 악의적인 사용자에 의한 ARP 스푸핑과 같은 공격을 탐지하여 이를 네트워크 관리자에게 신속히 알려 네트워크 보안 사고에 의한 장애를 복구한다.

RS61

Rule 6101 : IF F9101 = abnormal ports open THEN F9101 Rule 6102 : IF F9102 = rate high THEN F9102 Rule 6103 : IF F9103 = rate high THEN F9103 Rule 6104 : IF F9104 = rate high THEN F9104 Rule 6105 : IF F9105 = rate high open THEN F9105 Rule 6106 : IF F9106 = true THEN F9106 Rule 6107 : IF F9107 = true THEN F9107	
F6101 : inform abnormal port number F6102 : inform abnormal CPU rate F6103 : inform abnormal DNS query rate (there could be worm virus attack) F6104 : inform abnormal ARP request rate(there could be worm virus attack) F6105 : inform that there could be DDoS attack F6106 : Inform that there could be attack F6107 : Inform that there could be TCP-SYN attack	Q6101 : checking whether abnormal ports open Q6102 : checking CPU rate Q6103 : checking DNS query rate Q6104 : checking ARP request rate Q6105 : checking specific host requested repeatedly Q6106 : checking if IP addresses in shared media is in deniable IP address set Q6107 : checking TCP-SYN packets are abnormal

3. 실험 및 고찰

3.1. 구현 환경

본 논문에서 제시하고 있는 유비쿼터스 환경에서 각 기기들간의 네트워크 상태에 대한 장애 복구 모델과 에이전트간 협력 모델, 네트워크 장애 복구 규칙모델이 탑재된 L-Agent, R-Agent, T-Agent를 각각 〔표 1〕과 같이 설치한다.

여기에서 system1, system2, system3는 같은 내부 네트워크에 연결된 상태이며 system4는 다른 네트워크에 연결되어 있는 시스템이다.

〔표 1〕 실험 대상

시스템	IP 주소	모델	OS
default gateway	203.252.53.1	Xylan omni Switch	ROM
system1(T-Agent)	203.252.53.41	LG XNOTE LS50a	Windows XP
system2(L-Agent)	203.252.53.45	PC Intel P4 2.3	Windows 2003
system3(L-Agent)	203.252.53.42	HP RW6100	PocketPC 2002
system4(R-Agent)	203.252.45.161	HP 5450	WinCE 4.1

3.2. 시나리오에 따른 실험 결과

아래 세 가지 시나리오는 장애 복구 모듈을 탑재한 에이전트의 네트워크 장애 복구를 테스트하기 위한 시나리오이다.

(1) 시나리오 1: system1의 NIC을 Down 상태로 설정하고 테스트

Seq	Rule Set	Status and Action	Result
1	-	T-Agent fault occurred	
2	RS51 (Q5101)	check the state of NIC (up/down)	Fail
3	RS52 (R5201)	check the result after changing down-state interface into up-state one	Completion of the Interface Configuration Fault Recovery

(2) 시나리오 2: system1의 네트워크 구성 정보 중 default gateway 정보를 삭제하고 테스트

Seq	Rule Set	Status and Action	Result
1	-	T-Agent fault occurred	
2	RS31 (Q3101)	check the state of IP address setup (Comparing to IP address in other L-Agent and backup file)	Success
3	RS31 (Q3102)	check the state of subnet mask setup (Comparing to subnet mask in other L-Agent)	Success
4	RS31 (Q3103)	check the state of broadcast setup (Comparing to broadcast address in other L-Agent and one of broadcasting ICMP router solicitation message.)	Success
5	RS31 (Q3104)	check the default gateway address. (comparing to default gateway address in other L-Agent)	Fail
6	RS32 (Q3204)	check the result after replacing the current default gateway with the one obtain by L-Agent collaboration model or the other obtained by broadcasting ICMP message.	Completion of the Default Connectivity Configuration Fault Recovery

(3) 시나리오 3: default gateway를 다운시키고 테스트

Seq	Rule Set	Status and Action	Result
1	-	T-Agent fault occurred	
2	RS41 (Q4101)	checking whether the diagnosis result, which is obtained by agent collaboration model, is the fault of interior network	reporting the result of diagnosis, which is the fault of interior network, to network manager

3.3. 결과 및 분석

본 논문의 실험은 유비쿼터스 컴퓨팅 환경에서 우리 생활 속 곳곳에 컴퓨터들이 편재되어 센싱과 트래킹을 통해 장소나 시간에 따라 변화하는 상황을 인식하여 인간의 개입 없이 자율적으로 관리/운영되어지는 특성을 갖게 하기 위해 각 기기에 네트워크 상태에 대한 장애 복구 모델과 에이전트간 협력 모델, 네트워크 장애 복구 규칙모델을 이용한 에이전트를 탑재하여 인간의 개입 없이도 네트워크 장애를 복구를 할 수 있는지 테스트 하였다. 본 논문에서는 네 가지의 실험에서 다양한 결과를 얻었으며 각각의 네트워크 장애 시나리오에 대해 에이전트가 정상적으로 복구를 수행하는 것을 확인하였다.

4. 결 론

본 논문은 유비쿼터스 컴퓨팅 환경에서 디지털 기기들과 통합된 컴퓨터들은 자율적으로 관리되는 특성을 위한 네트워크 장애에 대해 기존의 규칙 기반 장애 진단 및 복구 시스템에서 에이전트가 장애 복구 모델을 통해 어떤 장애가 발생했는지 파악하고 해당 장애를 진단하기 위해 필요에 따라 다른 에이전트들과 협력 모델을 통해 정확한 장애를 진단하고 이를 규칙 기반의 네트워크 장애 복구 규칙 모델을 통해 장애를 복구하는 세 가지 모듈을 제안하였다.

기존의 [1], [2], [3]와 같은 시스템들은 각각의 규칙을 SOR로 수행하여 네트워크 장애 특성 파악이 힘들고 그 특성에 따른 차별적인 장애 진단 및 복구 작업을 수행할 수 없다. 그러나 본 논문에서 제시하는 장애 복구 모델을 통해 시스템의 장애 특성을 파악하고 이 특성을 바탕으로 에이전트 협력 모델과 네트워크 장애 복구 규칙 모델을 적용하여 정확하고 신속한 장애 진단 및 복구 규칙을 수행한다.

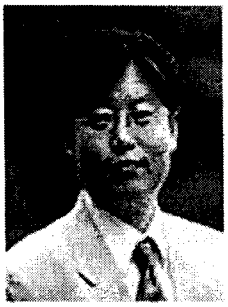
유비쿼터스 컴퓨팅 기술은 시간과 장소에 상관없이 자유롭게 네트워크에 접속할 수 있고 언제 어디서나 누구라도 어떤 대상이든 네트워크를 형성할 수 있게 하면서 네트워크는 점진적으로 복잡해지고 있다. 이러한 환경에서 우리 생활 속 곳곳에 컴퓨터들이 편재되어 센싱과 트래킹을 통해 장소나 시간에 따라 변화하는 상황을 인식하여 인간의 개입 없이 자율적으로 관리/운영되어지는 특성을 적용하기 위해서 본 논문에서는 각 디지털 기기에 네트워크 장애에 대처할 수 있는 에이전트를 탑재하여 네트워크 장애에 대한 자율적 관리/운영

의 특성을 증명할 수 있는 시스템을 제안한다.

참 고 문 헌

1. B. N. Schilit, "Context-aware Computing Applications," in Proc. of IEEE Workshop on Mobile Computing Systems and Applications, 1994.
2. The ubiquitous service-oriented network (USON)-an approach for a ubiquitous world based on P2P technology Takemoto, M.; Sunaga, H.; Tanaka, K.; Matsumura, H.; Shinohara, E.; Peer-to-Peer Computing, 2002. (P2P 2002). Proceedings. Second International Conference on 5-7 Sept. 2002.
3. Kang Hong Cho, Seongjin Ahn, Jin Wook Chung, Rule-based Agent system for Fault Detection and Location on LAN, KIPS, vol. 7-7 pp.2169-2178, 2000.
4. Taein Hwang, Seongjin Ahn, Jin Wook Chung, A study on the rules and algorithm for the diagnosis and recovery of routing configuration, SCI 2000, World Multiconference on Systemics, Cybernetics and Informatics 4(2000) 137-141.
5. T. Sugawara, Acooperative LAN diagnosistic and observation expert system, computers and communications, Proceeding of the Ninth Annual International Phoenix Conference, 1990, pp. 667-674.
6. Taein Hwang, Seongjin Ahn, Jin Wook Chung, Design and Implementation of Rule-Based network Configuration Fault Management System, Thesis of master's course, Sungkyunkwan Univ.
7. J.-M. Yun,, S.-J. Ahn, J.-W. Chung, Web Server Fault Diagnosis and Recovery Mechanism Using INBANCA, 2000, PP. 2467-2504.
8. K. Ohta, T.Mori, N.Kato, H.Sone, G.Mansfield, Y.Nemoto, Divideand Conquer Technique for network Fault Management, Proceedings of ISINM97, 1997.

이 재 욱(Jaewook Lee)
· e-mail : jwlee@songgang.skku.ac.kr
· 2005년 성균관대학교 정보통신공학부 졸업(학사)
· 2005년~현재 성균관대학교 컴퓨터공학부 대학원 석사과정
· 관심분야 : IPv6, 네트워크 보안, VoIP



안 성 진(Seongjin Ahn)
· e-mail : sjahn@songgang.skku.ac.kr
· 1988년 성균관대학교 정보공학과 졸업(학사)
· 1990년 성균관대학교 대학원 정보공학과 석사
· 1990년~1995년 시스템공학연구소 연구 전산망 개발실 연구원
· 1998년 성균관대학교 대학원 정보공학과 박사
· 1999년~현재 성균관대학교 컴퓨터교육과 부교수
· 관심분야 : 네트워크 관리, 트래픽 분석, 보안 관리

정 진 욱(Jinwook Chung)
· e-mail : jwchung@songgang.skku.ac.kr
· 1974년 성균관대학교 전기공학과 학사
· 1979년 성균관대학교 대학원 전자공학과 석사
· 1991년 서울대학교 대학원 계산통계학과 박사
· 1982년~1985년 한국과학기술 연구소 실장
· 1985년~현재 성균관대학교 전기전자 및 컴퓨터공학부 교수
· 관심분야 : 컴퓨터 네트워크, 네트워크 관리, 네트워크 보안