제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

에이전트들 간의 협력을 통한 RBR 기반 네트워크 장애 관리 시스템

장윤석*, 안성진**, 정진욱*
*성균관대학교 정보통신 공학부
**성균관대학교 컴퓨터 교육과
e-mail : ysjang@songgang.skku.ac.kr

A Study on the RBR Based Network Fault Management System using Agent Collaboration

Yunseok Jang*, Seongjin Ahn**, Jin Wook Chung*
*Dept. of Information and Communication Engineering, Sungkyunkwan University
**Dept. of Computer Education, Sungkyunkwan University

요 약

본 논문은 네트워크 장애 발생시 에이전트들 간의 협력을 통해 RBR(Rule-Based Reasoning)을 기반으로 장애의 진단 및 검출, 복구를 수행하도록 하는 시스템에 관한 연구이다. 본 시스템은 하나의 관리영역 내에서 동작하는 것을 원칙으로 하고 있으며 각 에이전트는 관리영역 내의 다른 에이전트들과 협력한다. 장애검출 및 진단을 위해 사용하는 도구로는 PING, Traceroute, SNMP가 있다. 또한 각 에이전트는 관리영역의 네트워크 관리를 위해 설치되어 있는 NMS(Network Management System)로부터 네트워크의 토폴로지를 얻어 토폴로지를 바탕으로 장애관리를 수행한다. 본 시스템은 네트워크 도메인을 크게 관리영역 내부 네트워크와 외부 네트워크로 나누어 토폴로지를 바탕으로 관리영역 내부 네트워크에 대해서는 어떠한 노드로부터 장애가 발생되었는지 규명할 수 있다

1. 서론

컴퓨터 네트워크의 발전으로 현대의 네트워크는 점차 방대하고 복잡하게 되었다. 이러한 구조 속에서 네트워크를 구성하고 있는 시스템 혹은 네트워크에 장애가 발생하였을 때 장애를 검출하고 관리하는 일은 상당히 난해하다. 대부분의 네트워크는 관리자에 의해서 장애의 검출 및 진단, 복구가 이루어지고 있다. 관리자들은 대부분 전문가의 견해가 축적된 전문가 시스템을 사용하고 있다. 그러나 네트워크의 규모나 복잡도에 따라 인력으로 해결할 수 없는 부분이 발생되기 마련이다. 이러한 경우에 RBR을 기반으로 하는 네트워크 장애의 검출, 진단 및 복구가 필요하다.[1, 2, 3]

RBR 기반의 네트워크 장애 관리가 적용된 시스템으로는 LODES(Large Internetwork Observation and Diagnostic Expert System)가 있다[4]. 이 시스템은 LAN 상의 장애 검출 및 위치 확인을 위한 규칙 기반 전문가 시스템으로 장애 발생에 대한 진단은 가능하지만 시스템 스스로가 장애를 복구하지는 못한다. 또한 패킷들을 수집하여 분석하고, 분석을 위해 TCP/IP의 상당수 프로토콜에 대한 지식이 필요하다.[1, 4] 그러나 본 논문에서 제시하는 방법은 몇 가지 장애에 대하여 스스로 복구할 수 있으며, 내부 네트워크 장애에 대해서는 정확한 원인을 파악할 수 있도록 한다. 그럼에도 불구하고 각종 프로토콜에 대한 지식 없이도 원활히 동작할 수 있다.

2. 시스템의 전제조건

본 시스템은 하나의 에이전트가 동일한 관리영역 내의 또 다른 에이전트와 협력하기 때문에 상호간의

등록정보가 있어야 한다. 일단 최초의 에이전트는 단독으로 장애의 검출, 진단 및 자신의 장애 복구가 가능하다. 등록정보에는 이미 설치되어 있는 에이전트 중 최소한 하나의 에이전트에 대한 IP 주소가 있어야 한다. 이 IP 주소를 이용하여 새로운 에이전트는 다른 에이전트들에게 자신의 등록사실을 알릴 수 있다. 새로운 에이전트는 등록되어 있는 하나의 에이전트에게 자신의 IP주소를 보낸다. 새로운 노드의 등록 사실을 통보받은 에이전트는 자신이 저장하고 있는 에이전트들의 주소 리스트를 새로 등록된 에이전트에게 전송한다. 이것으로 새로운 에이전트는 동일 관리영역 내의 모든 에이전트 주소 리스트를 얻게 된다. 이 주소 리스트를 이용하여 새로운 에이전트는 나머지 에이전트들에게 자신의 등록사실을 알릴 수 있다.

에이전트는 자신이 속해 있는 관리영역의 토폴로지를 알고 있어야 한다. 이 토폴로지는 관리영역을 관리하고 있는 NMS로부터 획득되며 에이전트는 이 토폴로지를 이용하여 보다 정확한 장애 위치를 파악할 수 있다.

에이전트는 Ping, Traceroute, SNMP 관리자의 역할을 수행할 수 있어야 한다. 에이전트는 Ping 테스트를 통해 목적지의 활성화여부를 알 수 있으며, 목적지 접속 실패 시에 Traceroute를 통해 관리영역 내부 문제인지 외부 문제인지 판단할 수 있다. 또한 내부문제로 판단된 경우 SNMP를 이용하여 어떠한 노드의 인터페이스가 다운상태인지 분석할 수 있다.

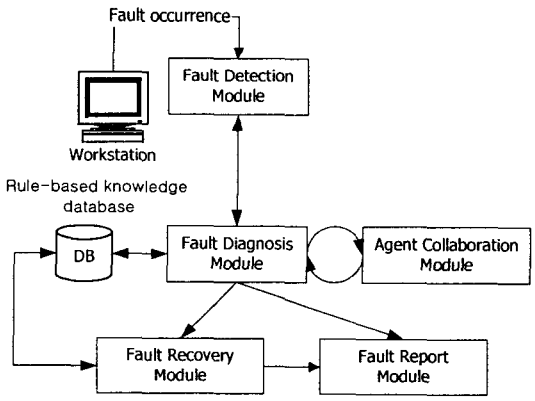
위와 같은 네트워크 도구들은 네트워크 관리자들이 장애를 검출하고, 진단하여 복구하는데 일반적으로 사용되는 도구들이다.

3. 시스템의 모듈구성

네트워크 상에서 발생할 수 있는 장애에는 여러 가지가 있다. 본 논문에서 정의하는 장애의 유형에는 다음과 같은 것이 있다.

(1) 자신의 NIC(Network Interface Card) 오류
(2) 회선연결 오류
(3) NIC 구동 드라이버 오류
(4) IP 주소 설정 오류
(5) 서브넷 마스크 설정 오류
(6) 디폴트 게이트웨이 주소 설정 오류
(7) DNS(Domain Name Server) 주소 설정 오류
(8) 네트워크 포화상태
(9) 디폴트 게이트웨이 다운
(10) DNS 다운
(11) 목적지까지의 경로상의 장비 다운
(12) 목적지까지의 경로상의 인터페이스 다운
(13) 목적지에서의 필터링으로 인한 접근 불가
(14) 목적지의 특정 포트(응용프로그램) 다운
(15) 목적지 다운

본 논문에서 장애 발생가능 영역은 크게 두 가지로 나뉘어 진다. 관리영역 내부 네트워크와 관리영역 외부 네트워크이다. 이 중 본 시스템이 정의한 위의 15가지의 장애항목은 내부 네트워크에서 발생한 장애에 대한 것으로 에이전트가 설치되어있는 시스템의 장애(1~7) 및 네트워크 상태에 따른 장애(8), 관리영역 내의 치명적인 게이트웨이와 DNS의 장애(9, 10), 목적지까지의 경로 상에서 발생할 수 있는 장애(11, 12)를 포함하고 있으며 목적지 자체에서 발생할 수 있는 장애항목(13~15)까지 총괄하고 있다. 그러나 외부 네트워크의 장애에 대해서는 에이전트의 제어가 사실상 힘들기 때문에 단순히 외부 네트워크상의 문제라는 것으로 정의하였다. 본 시스템의 모듈은 [그림 1]과 같이 구성되어 있다.



[그림 1] 시스템의 모듈구성 및 흐름도

[그림 1]의 모듈의 흐름을 보면 최초 장애 검출 모듈(Fault Detection Module)이 장애 발생 사실을 인지하고 장애 진단 모듈(Fault Diagnosis Module)에게 장애 사실을 알린다. 장애 진단 모듈은 규칙기반 지식 데이터베이스 (Rule-based knowledge database)에서 규칙들을 적용한다. 이때 디폴트 게이트웨이 혹은 DNS 주소 설정 오류 및 필터링 사실

판단 여부 등은 에이전트 협력 모듈(Agent Collaboration Module)을 이용하여 관리영역 내의 다른 에이전트들과 협력하여 장애의 진단 및 복구를 수행한다.

장애 진단 모듈은 관리영역 내부의 장애인지 관리영역 외부의 장애인지 장애 도메인을 판단하게 되는데 장애 도메인이 외부 네트워크로 판단한 경우, 다른 에이전트들과 협력하여 목적지 자체의 장애인지 IP 필터링으로 인한 접근 불가인지 판단 할 수 있다. 또한 장애 진단 모듈이 관리영역 내부 네트워크 장애로 판단한 경우 1번부터 15번까지의 규칙기반 지식 데이터베이스에서 장애 유형을 선택해서 복구 가능한 장애라면 장애 복구 모듈(Fault Recovery Module)을 수행하여 장애를 복구한 후 관리자에게 통보하며 그렇지 않은 장애에 대해서는 다른 에이전트들과 협동으로 정확하게 어느 지점에서 장애가 발생했는지 판단하여 관리자에게 통보한다. 관리자에게 통보하는 것은 장애 보고서 모듈(Fault Report Module)이 수행하게 된다.

장애 유형 15가지 중 장애 복구 모듈이 복구 할 수 있는 유형으로는 4~7번으로 이들은 다른 에이전트들과 협동으로 복구가 가능하다. 그 이외의 장애에 대해서는 관리자에게 알려준다.

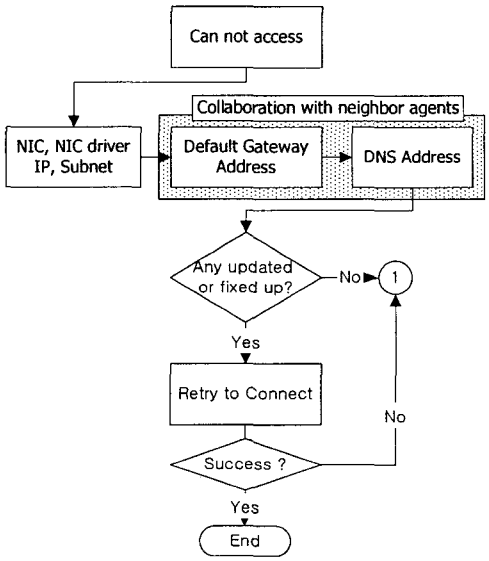
4. 에이전트들 간의 협력

에이전트들 간의 협력은 장애 진단에 있어 매우 중요하다. 네트워크라는 것은 다수의 네트워크 요소들이 유기적으로 연결되어 있는 집합체다. 그 안에서 발생하는 장애는 지극히 국소적일 수 있지만, 몇몇 장애들은 집합체 전체에 걸친 장애일 수 있다. 예를 들어 기술지원팀에 있는 PC에서 인사팀의 서버로 접속하려 할 때 특정 포트와 같은 것은 다른 팀에게 개방이 되어 접근할 수 있지만 그렇지 않은 것들도 있을 것이다. 이때 기술지원팀의 PC에서 접근이 제한된 포트로 접속하려 할 경우 접속이 불가능 할 것이고, 이것을 단순히 인사팀 서버의 장애로 볼 수만은 없을 것이다. 이때 필요한 것이 인사팀의 에이전트에게 접속해 보라고 협력을 요청하는 것이다. 인사팀 내에서는 접속이 가능하여 인사팀 에이전트로부터 접근 가능하다는 응답을 받게 될 것이다. 그러면 기술지원팀 에이전트는 재접속 시도를 하게 된다. 이때 역시 접속이 불가능하다는 것을 알게 되고 자신의 IP 혹은 네트워크 ID가 필터링 되어 접속할 수 없게 되어 있다는 것을 알게 된다.

이밖에도 디폴트 게이트웨이의 주소나 DNS 주소가 변경되었는데, 사용자 혹은 관리자가 에이전트가 설치된 어떤 PC에 설정을 변경하지 않았을 경우 에이전트는 다른 에이전트와 협력을 통해 변경된 주소로 해당 PC의 설정을 변경하여 통신이 가능하도록 한다.

5. 장애 진단 과정

장애 진단 과정은 장애 진단 모듈이 규칙기반 지식 데이터베이스에서 장애유형을 하나씩 비교하면서 정확한 장애를 진단하는 것이다. 장애 유형에 따라 진단 방법이 다르기 때문에 이러한 과정은 필수적이다. 일단 장애가 발생하면 에이전트는 자신이 설치된 시스템 자체의 장애인지 진단하여 이를 수정하고 목적지로 재접속 시도를 하게 된다. [그림 2]는 이 과정을 나타낸다.

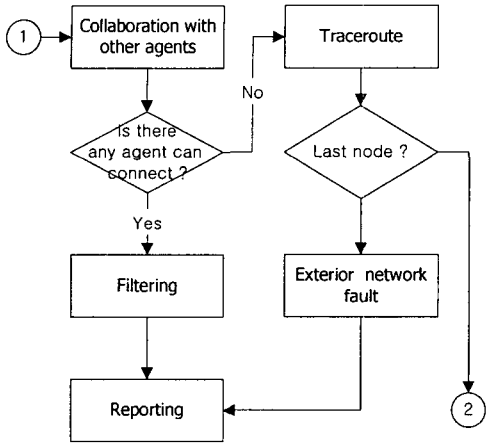


[그림 2] 시스템 자체의 장애 진단

[그림 2]에서 디폴트 게이트웨이 주소와 DNS 주소의 확인 및 변경은 인접한 다른 에이전트들에게 협력을 요청한다. 즉, 인접한 다른 에이전트들에게 그들이 갖고 있는 각각의 주소를 응답해 달라는 요청을 하고, 이를 받아서 자신이 갖고 있는 주소를 변경하고 재접속 시도를 하게 된다. 재접속 시도 후 성공하게 되면 에이전트의 장애 진단 과정은 끝나며 실패하는 경우에는 ①로 분기하게 된다.

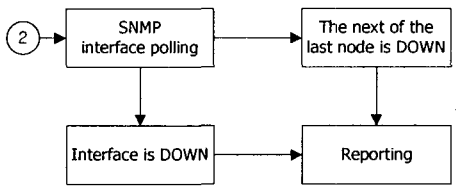
또한 시스템 자체의 장애가 아닌 경우에도 위와

같은 과정을 거치고 ①로 분기하게 된다. [그림 3]은 ①이후의 과정을 나타내는 것이다.



[그림 3] 필터링과 장애 도메인의 결정

[그림 3]은 ①에서 분기하여 시스템 자체의 문제라기보다는 필터링에 의한 접근 통제나 다른 네트워크 요소에 의한 장애로 판단하고 장애의 도메인을 규정하는 과정이다. ①에서 에이전트는 다른 에이전트들에게 자신이 접속하고자 했던 목적지로 접속 요청을 한다. 여기서 접속 가능한 에이전트가 있다면, 이 장애를 필터링에 의한 것으로 판단하고 사용자 또는 관리자에게 보고한다. 그러나 모든 에이전트가 접속이 안 되거나 일부 에이전트에게 접속 실패라는 응답조차 오지 않은 경우 에이전트는 목적지로 Traceroute를 수행한다. Traceroute결과 최종 도달 가능한 노드를 알아내고, 이것이 관리영역 내부인지 외부인지를 판단하여 외부인 경우 사용자(관리자)에게 통보하고, 그렇지 않은 경우는 ②로 분기하여 [그림 4]와 같은 과정을 수행한다.



[그림 4] 장애 노드 진단

[그림 4]는 관리영역 내부 네트워크 장애로 판단한 이후에 어떠한 노드에서 어떠한 장애가 발생했는지 진단하는 것이다. SNMP를 이용하여 Traceroute의 마지막 노드를 진단한다. SNMP가 설치되어 있지 않은 노드는 그 노드의 인터페이스가 다운된 것으로 규정하고 보고한다.

SNMP 에이전트가 활성화되어 있는 노드에 인터페이스 리스트를 폴링하여 목적지로 가는 인터페이스의 업/다운 여부를 판단하여 인터페이스 다운으로 보고할 것인지 다음 노드가 다운된 것으로 보고할 것인지 결정한다.

6. 결론

본 논문에서 제시하는 장애 관리 시스템은 기존의 RBR 시스템들과 유사한 방법으로 장애 검출 및 진단에 접근한다. 규칙기반의 지식 데이터베이스를 활용하며, 관리도구로는 Ping과 SNMP를 이용하여 보다 정확한 장애 진단이 가능해 졌다. 또한 기존 시스템들이 TCP/IP에 대한 구체적인 지식을 보유하여야 하고 전송되고 있는 패킷들을 수집해야 하는 번거로움과 부하를 갖고 있는 반면[4] 본 시스템은 별도의 TCP/IP에 대한 지식 없이 에이전트들 간의 상호 작용으로 일부장애에 대해 자동 복구를, 몇몇 장애에 대해서는 장애 발생 노드를 찾아내어 관리자에게 알리는 역할을 수행할 수 있다. 그 범위는 하나의 AS 내부로 정하여 AS 관리자의 장애에 대한 부담을 줄일 수 있다.

참고문헌

[1] 조광종, 안성진, 정진욱, "에이전트들 간의 협력을 통한 RBR 기반의 네트워크 구성 장애 관리 알고리즘", 한국정보처리학회 논문지C, pp497-504, 2002

[2] Wesley W.Chu, "System Management Research via Behavior Characterization", Proceedings of the IEEE First International Workshop on, pp.1-6, 1993

[3] Kohei Ohta, Takumi Mori, Nei Kato, Hideaki Sone, Glenn Mansfield, Yoshiaki Nemoto, "Divide and Conguer Technique for Network Fault Management", Proceedings of ISINM97, 19

[4] Toshiharu Sugawara, "A Cooperative LAN Diagnostic and Observation Expert System, Computers and Communications", Conference Proceeding of the 9th Annual International Phoenix Conference, pp.667-674, 1990