RBR 기반의 우선 순위 규칙 적용을 통한 네트워크 장애 탐지 및 복구 시스템

김시흥*, 안성진**, 정진욱*
*성균관 대학교 컴퓨터 공학
**성균관 대학교 컴퓨터 교육과
e-mail : shkim@songgang.skku.ac.kr

RBR Based Configuration Fault Management System using Priority rule

shi-hung kim*, Seongjin Ahn**, Jin Wook Chung*
*Dept. of Computer Science, Sung-kyun kwan University
**Dept. of Computer Education, Sung-kyunkwan University

요 약

본 논문은 RBR(Rule-Based Reasoning) 기법과 RBR 기법에 적용될 규칙에 대한 우선순위를 둠으로써 효율적인 네트워크 설정을 만드는 동시에 네트워크 장애 발생시 장애를 진단 검출복구하는 에이전트 시스템에 관한 연구이다. 논문에서 제시하는 시스템은 AS 내에서 동작하는 것을 원칙으로 하며 각 네트워크의 에이전트들은 우선 순위 장애 탐지 및 복구를 위해 우선 순위에 따라 규칙을 적용한다. 장애 발생시 진단 검출 복구를 위해 에이전트는 상호 협력하며 장애 검출 및 진단 도구로써 ping, traceroute 등을 이용한다.

1. 서론

네트워크 기술이 향상됨에 따라 산업 전반의 각 부분에서는 효율성과 편리성을 위해 이를 사용하고 있으며 그 활용도는 날로 증가되는 추세이다. [1, 3, 4] 이와 함께 네트워크 장애의 빈도나 피해 규모도 늘어나고 있으며 장애의 형태도 다양해 지고 있다. 특히 비즈니스 산업에서 네트워크 장애는 업무의 중단으로까지 이어질 수 있기 때문에 이에 대한 해결책이 요구되는 실정이다. [1]

네트워크 장애는 네트워크 내의 복잡 다양한 요인들로 인해 야기 됨으로 네트워크 장애 복구를 위해서는 네트워크에 대한 전문적인 지식을 필요로 한다. 하지만 네트워크 장애 발생시 전문가를 적제 적소에 파견한다는 것은 어려운 일이며, 전문가를 상주 시키는 방법 역시 비용적 측면에서 좋은 방법이라 할수 없다. 이런 측면들이 고려 되어 전문가 시스템을 이용하는 방법이 제기되었으며 이 시스템은 네트워크 내의 장애에 대해 다양하고 폭 넓게 원인을 찾고 분석하기 위해 RBR 기법을 기반으로 하고 있다.[5] RBR 기반의 네트워크 장애 관리 시스템은 하나의 문제에 대하여 다양한 유형의 장애 진단 규칙을 적용하여 비교적 명확한 장애 진단을 수행할 수 있도록 한다. 또한 지속적인 규칙의 갱신은 다양하고 복잡한 네트워크 환경에 쉽게 적응 할 수 있도록 한다. 대표적인 예로 LODES 시스템을 들수 있는데 이 시스템은 LAN 상의 장애 검출 및 위치 확인을 위한 규칙 기반 전문가 시스템으로 장애 발생에 대한 진단이 가능하지만 시스템 스스로 이러한 장애를 복구하지 못한다.[2] 그 밖에 기존의 RBR 기반의 네트워크 장애 검출 진단 복구 알고리즘에서는 정해진 규칙 베이스만을 따라서 원인을 조사하기 때문에 급변하는 네트워크 상황에 맞게 규칙을 적용할 수 없다.

이에 본 논문에서는 RBR 기반의 네트워크 장애 탐지와 복구에 대한 방안을 제시하며 장애 탐지와 복구에 사용되는 규칙들에 대한 효과적인 적용법에 대한 방법을 제시하고자 한다.

2. 네트워크 장애 진단 및 복구

2.1 네트워크 장애 관리 시스템

컴퓨터 네트워크의 활용이 증대됨에 따라 네트워크 장애의 유형이 다양해 지고 발생 빈도도 높아지고 있다. 네트워크에서 발생하는 장애의 증상은 호스트 사이의 연결불능, 의도 되지 않는 비연결성, 느린 전송속도와 과다한 브로드 캐스트 트래픽에 의한 네트워크 혼잡등이 있다. 이들 장애 문제는 파악과 복구에 있어 전문적인 지식을 요구하고 있지만, 비슷한 문제가 자주 발생하고 일정한 절차를 통해 해결될 수 있다. 이러한 네트워크 장애가 갖는 특성으로 인해 시스템적이며 효율적인 네트워크 관리를 위한 장애 진단 전문가 시스템이 등장하게 되었다. 장애 진단 전문가 시스템들은 발생한 장애에 대한 문제를 분석하고 복구될 수 있는 경우라면 장애를 복구하는 기능을 가지고 있다. 그리고 발생한 장애가 전문가 시스템에 의해 자동적으로 복구 될수 없는 경우이면 네트워크 관리자에게 발생한 장애를 분석한 결과를 통보한다. 또한 앞으로 발생할 장애에 대한 진단을 위해 분석데이터를 누적해 놓는다. 대표적인 예로 LODES 시스템을 들 수 있다.

2.2 네트워크 장애 진단 시스템(LODES)

LODES 는 대규모의 인터네트워크에서 장애를 진단하는 장애 전문가 시스템이다. 이 시스템은 복잡하고 이질적인 네트워크 환경에서 일어나는 장애문제를 TCP/IP 에 대한 전문 지식을 바탕으로 하여 해결하는 시스템이다. 이 시스템은 네트워크에 존재하여 장애 문제의 유형을 판별하고 가능하다면 자동적으로 이를 해결 한다. 설령 장애 문제가 해결 되지 않더라도 네트워크에 대한 중요한 정보들을 수집해 줌으로서 네트워크 전문가로 하여금 문제 분석의 유용한 정보를 제공한다. LODES 는 장애 유형 판별을 위해 규칙 베이스를 유지하고 있다. 규칙 베이스 내에는 프로토콜에 대한 지식과 장애 문제의 경험 관리 데이터가 있어 이를 토대로 네트워크 장애에 대한 자동적인 문제 발견과 분석을 수행한다. 문제 발견과 분석은 독립적으로 수행되거나 다른 네트워크에 존재하는 인접 LODES 시스템의 도움을 받아 이루어 진다. 상기한 방식은 네트워크 장애를 해결하는데 있어 한계가 있겠지만 네트워크 문제가 주로 사소하고 유사한 유형이 반복되기 때문에 LODES 는 네트워크의 장애 처리 문제에 대해 적절히 동작할 수 있다.[1]

2.3 RBR 기반의 네트워크 장애 진단 복구 시스템

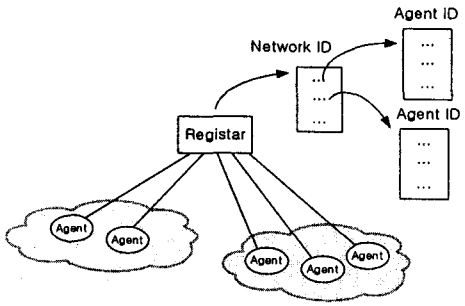
RBR 기반의 네트워크 장애 진단 및 복구 시스템은 에이전트의 상호간의 협력을 바탕으로 네트워크 상황을 진단 및 복구하고 있다. 네트워크간의 에이전트들은 REGISTRA 에게 등록을 하며 REGISTRA 는 각 에이즌트들에 대해 네트워크를 구분하여 관리한다. 그래서 만약 한 에이전트로부터 네트워크 진단에 대한 요구가 있을시 그 요구가 동일 네트워크 내의 이웃 에이전트를 통해 수행이 가능한지 또는 외부 네트워크의 에이전트의 도움이 필요한지 여부를 판단하여 해당 에이전트에 대해 작업 수행을 요청한다. REGISTRA 는 결과를 얻고 이를 요청한 에이전트에게로 전송한다.[1,6]

각 에이전트는 목적지에 대한 장애 분석 모듈, 6 개의 장애 진단 모듈, 그리고 5 개의 장애 복구 모듈로 이루어진며 각 모듈은 모듈의 실행시에 참조하게 되는 지식 베이스를 유지하고 있다. 목적지에 대한 장애 분석 모듈은 네트워크 장애시 가장 먼저 수행되는 모듈로써 목적지의 어플리케이션에 대해 접근 가능성여부를 조사한다. 목적지 어플리케이션의 이상이 없을시 6 개의 장애 진단 모듈을 이용하여 네트워크 장애에 대한 진단을 하게된다. 진단 모듈은 기본 연결 구성 장애 진단(Default Connectivity Configuration Fault Diagnosis, DCCFD), 네트워크 환경 장애 진단(Network Environment Fault Diagnosis, NEFD), 라우팅 구성 장애 진단(Routing Configuration Fault Diagnosis, RCFD), 네임 서비스 구성 장애 진단(Name Service Configuration Fault Diagnosis, NSCFD), 인터넷 데몬 프로세스 구성 장애 진단(Internet Demon Process Configuration Fault Diagnosis, IDPCFD) 및 애플리케이션 데몬 구성 장애 진단(Application Demon Configuration Fault Diagnosis, ADCFD)이 있다. 장애에 관해 진단 모듈이 순서대로 적용되며 모듈별로 미리 정의 된 규칙들에 따라 장애를 진단하게 된다. 장애의 유형을 판별 했을시에는 복구 모듈이 수행되는데 네트워크 환경 장애 같은 종단 시스템에서는 복구를 수행할 여지가 없는 장애를 제외하고는 각 모듈에 대한 복구 모듈이 따로 존재한다.

3. RBR 기반의 Rule 공유 네트워크 장애 진단 복구 시스템

3.1 장애 관리 모델

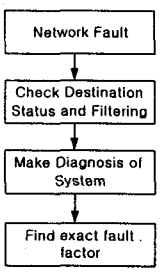
네트워크 장애는 네트워크내의 다양한 요소들이 원인이 될수 있다. 이런 다양한 요소들을 효과적으로 찾아내고 복구를 하기 위해서 4 가지 에이전트 개념을 정의 하였다. 첫번째는 네트워크 장애가 발생하여 다른 에이전트의 도움을 받고자하는 T-Agent 이다. 두번째는 T-Agent 와 동일한 네트워크에 존재하는 N-Agent, 세번째는 다른 네트워크에 존재하는 F-Agent, 네번째는 REGISTRA Agent 로 그림에서와 같이 네트워크 별로 에이전트들을 관리하여 데이터베이스에 저장하고 있다. 데이터 베이스는 이중적인 인덱싱 구조로 되어 있으며 첫번째 테이블에서는 에이전트의 네트워크를 찾을 수 있고 두번째 테이블에서는 해당 네트워크의 에이전트들을 찾을 수 있다. REGISTRA Agent 는 T-Agent 의 요청을 받아 요청에 적절한 Agent 를 찾아 해당 에이전트에게 작업을 요청하며, 결과를 T-Agent 에게로 돌려준다.



<그림 1> 장애 관리 모델

예를 들어 T-Agent 가 목적지에 접속하지 못한 경우 목적지 어플리케이션이 다운 됐는지 여부를 판단하기 위해 REGISTRA Agent 에게 이것의 확인을 요청한다. REGISTRA Agent 는 T-Agent 에 대한 N-Agent 중 ID 값이 가장 낮은 N-Agent 와 F-Agent 를 각각 하나씩 선택하여 목적지 시스템에 대한 테스트를 요구하게 된다. 테스트 결과는 REGISTRA Agent 에게로 되돌려지며 최종적으로 T-Agent 에게로 결과 값이 이동하게 된다. 위와 같은 방식을 통해 T-Agent 는 동일한 네트워크에 있는 에이전트뿐만 아니라 다른 네트워크의 에이전트로부터 도움을 받을 수 있다.

3.2 장애 진단 및 복구 모듈의 흐름



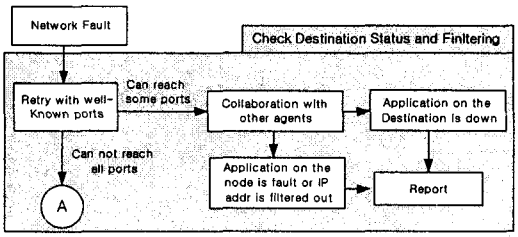
<그림 2> 장애 진단 및 복구 흐름도

<그림 2>은 전체 시스템의 흐름을 도시하고 있다. 네트워크 장애 감지시에 시스템은 장애 진단 및 복구 과정을 진행하게 되며 장애 발생을 판단하는 시기는 어플리케이션으로부터의 통지가 있을시나 REAGISTRA 와의 연결을 잃었을 때 이다. 장애 발생을 인식한 후에는 목적지 상태 판단 및 필터링 점검 단계, 장애 진단 단계, 정확한 장애 요소 판단 단계를 거쳐 장애에 대한 진단 및 복구를 하게 된다.

3.3 모듈별 구성

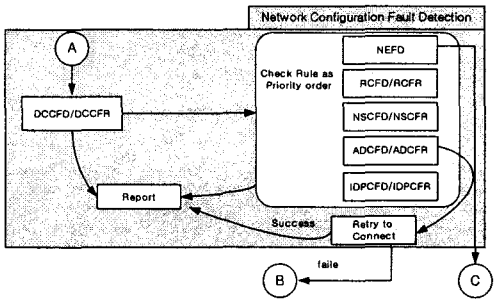
<그림 3>은 흐름도의 두번째 과정에 해당하는 목적지 상태 판단 및 필터링 점검 단계의 세부 모듈을 나타낸 그림이다. 시스템은 장애 발생후 목적지의 well-known port 에 접근을 시도하여 목적지의 어플리케이션이 다운되었는지를 판단한다.

이때 하나 이상의 포트가 열려 있을 경우 T-Agent 에서 목적지까지 경로 상에 다른 문제는 없는 것으로 판단하며 이때 다른 에이전트들에게 목적지로 접근을 요청한다. 여기서 모든 에이전트가 접근이 불가능 할 경우 목적지의 해당 포트를 사용하는 어플리케이션이 다운된 것으로 판단하고 보고한다. 그러나 일부 에이전트들이 접근이 가능하다면 나의 어플리케이션에 문제가 있거나 IP 주소가 목적지에 의해 필터링 되는 것으로 판단하고 보고한다.



<그림 3> 목적지 상태 판단 및 필터링 점검 모듈

모든 well-known 포트로 접근이 불가능한 경우 이것은 목적지가 다운되었거나, 목적지로 가는 경로 상에서 문제가 발생한 것으로 판단하여 다음 모듈로 이동한다.



<그림 4> 장애 진단 모듈

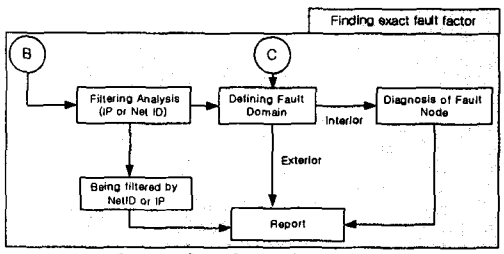
<그림 4>는 장애 진단 모듈로써 총 6 개의 작은 진단 복구 모듈이 시스템 자체의 장애를 진단하고 복구한다. 각 진단 모듈은 아래와 같다.

- 기본 연결 구성 장애 진단(Default Connectivity Configuration Fault Diagnosis, DCCFD)
  시스템의 기본적인 연결 설정 상태를 진단하는 모듈로 NIC 의 상태, 케이블의 상태, IP 주소, 서브넷 마스크, 브로드 캐스트 주소 등의 설정이 올바른지 진단한다.
- 네트워크 환경 장애 진단(Network Environment Fault Diagnosis, NEFD)
  시스템에서 검출된 장애가 시스템 자체의 네트워크 구성장애가 아닌 시스템이 위치한 내부 네트워크 혹은 관리 도메인 상의 다른 네트워크의 장애를 진단하는 모듈이다.
- 라우팅 구성 장애 진단(Routing Configuration Fault Diagnosis, RCFD)
  시스템이 라우팅 기능을 하고 있을 때, 정적 라우

팅 혹은 동적 라우팅 시 나타나는 장애를 진단하는 모듈이다.

- 네임 서비스 구성 장애 진단(Name Service Configuration Fault Diagnosis, NSCFD)
  네인 서비스에 대한 구성 장애를 진단하는 모듈로 시스템이 DNS 로 동작하고 있을 때와 DNS 를 이용하는 Resolver 로 동작하고 있을 때의 구성 장애를 진단한다.
- 인터넷 데몬 프로세스 구성 장애 진단(Internet Demon Process Configuration Fault Diagnosis, IDPCFD)
  인터넷 데몬 프로세스 즉 inetd 프로세스에 대한 장애를 진단한다.
- 애플리케이션 데몬 구성 장애 진단(Application Demon Configuration Fault Diagnosis, ADCFD)
  TCP/IP 관련 어플리캐이션 서비스를 제공하는 각 데몬 프로세스에 대한 장애를 진단한다.

이 6 개의 모듈로써 네트워크 장애의 유형을 판단할 수 있으며 각 모듈은 우선순위를 가지고 있어 우선순위에 따라 진단 순서가 결정된다. 즉 특정 네트워크에서 자주 발생하는 장애에 대한 진단을 먼저하게 된다. NEFD 를 제외한 각 모듈은 해당 장애에 대한 복구 모듈을 갖고 있다. 목적지로 접근이 불가능한 상태에서 DCCFD 모듈은 시스템 및 각종 네트워크 설정 상태를 진단하고 복구 한다. 그 이후 NEFD 에서 장애 유형을 두 가지로 분리하여 RCFD 혹은 NSCFD 로 분기 시킨다. RCFD 는 라우터 의 상태가 정상적인지 판단하여 IDPCFD 로 이동하고 인터넷 데몬 프로세스들이 정상적으로 동작하는지 점검한다. 반면 NSCFD 는 DNS 서버의 상태를 점검하는 것으로 시스템 자체가 DNS 인지 DNS 를 이용하는 Resolver 인지를 판단하여 장애를 진단한다. IDPCFD 와 NSCFD 를 마친 후 ADCFD 에서는 애플리케이션 데몬의 구성 장애를 진단하고 복구한다. 마지막으로 재접속 시도를 한다. 성공하면 보고를 하고 실패하게 되면 다른 지점에서 장애가 발생한 것으로 판단하고 장애 지점을 찾는 <그림 5>의 모듈로 이동한다.



<그림 5> 정확한 장애 요인 분석 모듈

<그림 5>는 시스템 장애를 복구하였거나, 장애가 없었던 경우임에도 불구하고 접속이 안 될 경우 장애가 어디에서 발생하였는지 찾아내는 모듈이다. 처음에는 필터링을 검사한다. 네트워크에 아무런 장애가 없음에도 불구하고 접근할 수 없는 경우는 목적지에서 IP 주소 또는 network ID 를 차단할 목적으로 필터링을 수행한 경우이다. 이러한 경우 다른 에이전트들과 협동으로 필터링에 대한 조사를 실시한다. 필터링이 사실로 판단될 경우 보고하고, 그렇지 않은 경우 네트워크 내에 장애가 발생한 것으로 간주하고 장애 도매인을 정의한다. 장애가 관리영역 외부에서 발생한 경우, 관리자에게 외부의 장애임으로 복구할 수 없음을 알리며, 관리영역 내부의 장애인 경우 어떠한 장비에서 장애가 발생했는지 검사한다. 내부 네트워크에서 장애가 발생한 경우에 본 시스템은 인터페이스가 다운된 경우에 정확하게 장애를 인지할 수 있으며 그렇지 않은 경우 어떠한 장비가 다운 상태인지 파악할 수 있다.

3.4 규칙의 생성과 공유

네트워크 기술이 진보함에 따라 네트워크 장애 요인도 다양하게 변모한다. 그래서 네트워크 장애 요인을 찾아내는 규칙 베이스도 이에 맞는 변화가 있어야 한다. 규칙의 생성은 REAGISTRA Agent 에서만 가능하며, TCP 연결을 통해 REAGISTRA Agent 는 생성된 규칙을 전파한다. 전파된 규칙을 받은 에이전트는 받은 규칙을 규칙 베이스에 저장하며 규칙 베이스의 가장 하위에 위치 시킨다.

4. 결론

본 논문에서는 제시하는 시스템은 규칙기반 베이스를 통해 네트워크내의 장애를 진단하고 복구한다. 시스템은 3 가지의 에이전트로 분류되며 서로의 협력을 통해 완전한 동작을 이끌어 낼 수 있다. 또한 REAGISTRA Agent 를 통해 규칙을 생성하고 파기, 공유할 수 있어 변화하는 네트워크 환경에 적절히 대응할 수 있다.

참고문헌

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

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

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

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

[5] Denise W.Gurer, Irfan Khan, Richard Ogier, Renee Keffer, An Aritficial Intelligence Approach to Network Fault Management, SRI International, Menlo Park, California, USA.

[6] 조규억, 안성진, 정진욱, "RBR 을 이용한 지연 장애 검출 및 진단알고리즘에 관한 연구", 정보처리학회, 제 7 권 제 8 호,pp.2620-2630, 2000