네트워크 사용자를 위한 장애진단시스템 설계

김홍주* 이태경
동국대학교 전자계산학과

Design Approach of Fault Diagnosis System for Network User

Hong Ju Kim* Tae Kyung Lee
Dept. of Computer Science, Dongguk University
k2@wonhyo.dongguk.ac.kr tklee@wonhyo.dongguk.ac.kr

요 약

현재 네트워크 환경과 컴퓨터시스템 환경에서의 고장 또는 장애에 의해서 통신이 않되는 경우에는 사용자들의 불편이 가중되고 있는 실정이다. 네트워크의 확장으로 인하여 네트워크를 관리하기 위한 도구들이 개발되어 왔다.

이 문제를 해결하기 위해서 본 논문에서는 네트워크 및 컴퓨터시스템 환경에서 발생하는 장애에 대한 원인 분석과 이에 따른 장애의 진단과 처치를 위하여 전문가시스템의 기법을 도입하였다. 장애의 원인을 탐색하기 위하여서는 추론기관과 지식베이스를 구성하였으며, 장애요인에 대한 지식은 장애를 하나의 객체로 하는 기법을 사용하였다.

1. 서 론

컴퓨터 네트워크는 다른 컴퓨터 시스템이나 네트워크에 접근하기 위한 것으로 중요시 여겨왔다. 네트워크의 확장으로 인하여 시스템은 더욱 복잡하게 되며, 관리상의 문제점은 점점 증가하고 있다. 네트워크에 대한 컴퓨터 시스템의 구조는 회사나 연구소 등에 의하여 많은 구조가 제안되었다. 이런 관심으로 인하여 네트워크를 관리하기 위한 소프트웨어 도구들이 개발되어 왔으며 사용되고 있다. 그러나, 통신 프로토콜의 차이점으로 인하여 관리 정보의 교환은 상당히 어려운 점으로 나타났다. 장애 관리 시스템은 컴퓨터 네트워크의 잘못된 기능들을 발견하고 진단 그리고 회복하는 과정을 말한다[6].

ISO에서 제안한 네트워크 관리의 기본적인 기능은 구성 관리, 장애 관리, 성능 관리, 계정 관리, 보안 관리로 나뉜다. 장애 관리는 네트워크 자원과 자속성 그리고 자원의 설정값을 결정하고 장애를 발견하며 고침으로 성능을 향상시켜, 네트워크의 효율을 증가시키기 위해 필요한 것이다. 장애 관리의 전반적 요구 사항을 파악하고, 서비스와 프로토콜을 연구하며, 표준화에서 명시하고 있지 않는 부분과 관련하여 장애 관리 시스템은 단순히 피관리자 시스템으로부터 제공된 경보를 바로 관리자 시스템의 사용자에게 제공하였다. 따라서, 관리자 시스템의 기능에 진단(diagnosis)과 회복(recovery)의 절차를 수행하기 위하여 관리 대상의 장애에 따른 지식 베이스 시스템을 유지하고 추론 시스템의 개념을 사용한다. 특히 처방을 위해 제공되는 정보의 부족으로 인하

여, 장애의 원인이 되는 요소를 파악함으로 효과적인 관리 활동을 수행할 수 있다. 전문가 시스템에서의 장애를 보고 처방을 내릴 수 있는 혼합형 기법에서 장애 요인들을 각각의 객체로 보고 객체 지향 방식을 이용하는 것을 제안하고 장애 요인에 대한 처방을 내리는 전문가 시스템을 설계하여 장애의 근원을 추적과 처방을 내릴 수 있다[1].

본 논문의 2장은 전문가 시스템을 이용한 장애 발생에 대한 처리를 위한 진단 시스템의 필요성, 3장에서는 장애 요인 분석, 4장은 장애 요인 분석에 대한 전문가 시스템 구조, 5장은 결론으로 구성되어 있다.

2. 장애 발생 처리를 위한 진단 시스템의 필요성

사용자들은 전산망에 대해 다양한 기능을 요구할 수 있으나 무엇보다도 필요할 때 올바르게 동작되어야 할 것이며 이러한 사용자 요구사항을 만족시키기 위해서는 전산망에서 발생할 수 있는 각종 장애를 효과적으로 감시 및 제어하여야 한다. 사용자들이 기대하는 서비스 수준을 만족시켜 주면서 전산망에서 발생할 수 있는 각종 장애에 대해 지속적으로 신뢰할 수 있는 운용을 보장하는 감시 능력이 없다면, 복잡한 시스템들로 구성된 전산망이 유지 및 관리될 수가 없다. 또한 전산망의 구성 성분들 이 제대로 동작하지 않을 때도 신속하고 안정성 있는 서비스가 이루어져야 함은 물론이며 이러한 제반 기능을 수행하기 위해서는 장애관리에 관한 연구가 필수적으로 수행되어야 한다[2].

전문가 시스템은 방대한 감사 기록을 수작업으로 조사하여 공격자를 확인한다는 것은 매우 힘든 일이며, 또한 즉각적인 확인 및 대처 능력을 제공하지 못하게 된다. 이에 효율적으로 검사할 수 있는 자동화된 시스템 요구되었고, 전문가 시스템 기법은 효율적인 발견-기반 정보 보호 시스템 개발의 이정표가 되었다[7]. 전문가 시스템은 전문가의 지식을 encode한 규칙의 집합으로 구성되며, 이 규칙은 침입 발견 시스템에 의해 도출되는 자료에 대해 결론을 내리기 위해 사용된다. 광범위한 경험을 컴퓨터 응용으로 활용하여 어떠한 행동이 정의된 오용이나 공격 특성과 일치하는가를 판단하기 위한 정보로 이용하는 전문가 시스템은 감사 자료의 검사 능력을 향상시키지만, 수정에 자유롭지 못하거나 혹은 관리자에 의해서만 수정되는 단점이 있다[3].

3. 장애 요인 분석

3.1 네트워크 환경에서의 장애

(1) 네트워크의 하드웨어, 연결 문제
(2) 네트워크의 소프트웨어 문제

증상	처방
LAN상의 다른 서버, 라우터로의 ping의 작동 불능	* TCP/IP 세팅 확인 * 자신의 IP(다른 호스트와의 중복) * 네트워크 마스크 확인 * 게이트웨이, HUB 확인
라우터, HUB와의 ping 작동 불능	* 라우터의 Ethernet 포트가 다운되었는지 확인 * 라우터와 허브의 연결에 문제 * 라우터가 정상 동작하는지 확인 * 허브와의 연결 케이블이 불량하지 않은가 확인

표 1 네트워크 환경에서의 증상, 처방 예

3.2 사용 컴퓨터 시스템 환경에서의 장애

(1) 컴퓨터 하드웨어
사용자가 도달하려고 시도하려는 특정 호스트가 자체 부팅 과정의 오류, 잠정적인 과부하 혹은 다른 원인으로 인해 작동 불능 문제
(2) 소프트웨어
원격 호스트에 도달될 수 없는 원격 호스트의 소프트웨어 설치 상의 문제

3.3 DNS, WWW상의 설정 장애

1. DNS에서의 장애

도메인명으로는 접속이 안되고 IP 주소로는 접속이 된다.

(1) 유닉스 네임 서버
(named 프로세스 확인 .config파일에 name server의 IP address의 확인)

(2) 윈도우즈-NT네임 서버
("DNS 관리자"가 실행 중인지 확인, 세팅이 올바른가에 대한 점검)

증상	처방
사용자가 도달하려고 시도하는 특정 호스트가 자체 부팅 과정의 오류, 잠정적인 과부하, 다른 원인으로 인해 작동 불능	* TCP/IP 세팅 확인 * 자신의 IP(다른 호스트와의 중복) * 네트워크 마스크 확인 * 게이트웨이, HUB 확인
특정 서비스가 이용될 수 없는 상태	* 라우터의 Ethernet 포트가 다운되었는지 확인 * 라우터와 허브의 연결에 문제 * 라우터가 정상 동작하는지 확인 * 허브와의 연결 케이블이 불량하지 않은가 확인

표 2 사용 컴퓨터 시스템 환경에서의 증상, 처방

(3) 윈도우즈95
(네트워크->TCP/IP에서 찾을 DNS주소 목록이 name server의 IP address 확인)

2. WWW에서의 장애

(1) 자신의 웹 서버만 접속이 되고 외부웹 사이트는 연결 불능
(2) 외부 웹 사이트는 연결되는데 자신의 웹 사이트만 접속 불능
(3) 자신이 구축한 웹 서버가 접속 불능

(1)(2)(3)에 대한 조치 사항은 다음과 같다.

① LAN상의 장비들은 제대로 접속 가능한 상태 확인
② 외부로 통하는 장비, 라우터가 제대로 동작 점검

③ 라우터 및 DSU장비를 reset

④ 웹 서버가 잘못된 경우이거나, LAN에 붙린 케이블이 잘못 되었거나 name server가 동작을 제대로 하지 못하는 경우이다. 이 경우는 대체로 name server에 문제가 있기 때문이다.

⑤ ps 명령어를 이용해서 web 프로그램이 올바르게 실행되고 있는지를 점검

⑥ 서버가 정상적으로 수행중이면, name server에 웹 서버 데이터가 바르게 추가되었는지 점검 (nslookup)

3.4 네트워크의 장애 해결 방안 제시

1. 사용자 개입이 없는 단계

사용자 개입이 없는 단계에서의 해결방안은 다음과 같다.

(1) 네트웍, H/W 장애의 해결방안 제시
(2) 각 영역별 체크포인트 제시
(3) 역할을 분담하고 있는 서버들간의 조정방법 제시
(4) 장애 예상 영역을 줄여나가는 질의 응답식 체크리스트 제시
(5) 장애가 발생한 기계의 응급 복구방법 제시
(6) 하드웨어 설정 가이드라인 제시
  ① S/W 장애의 해결방안 제시
  ② 문제가 발생한 계층의 복구방안 제시
  ③ 타이머나 기타 파라메터의 최적해 제시
  ④ H/W와 S/W간의 설정법 제시

2. 사용자 개입이 있는 단계

사용자 개입이 있는 단계에서의 해결방안은 다음과 같다.

(1) 네트워크 장애진단

① 1차 진단의 결과대로 시행했으나 적중하지 못한 경우
  · 처방이 틀렸음을 지식베이스에 추가(사용자 입력)
  · 사용자가 판단한 원인을 입력 (2차 추론)
  · 처방과는 약간 틀리지만 사용자의 경험을 추가하여 공장을 해결했을 경우(사용자 입력)
  · 미해결 과제의 입력 (개발자에게 연락하기 위한)

② 2차 진단이 필요한 경우
  · 부분적으로 해결을 하여 복구는 됐으나 완전하지 못 할 경우의 2차 추론시

(2) OSI장애 진단

① 프로그램의 재 설치가 필요한 경우
② 특수한(범용적이지 못한) 프로토콜의 경우(지식베이스 추가)
③ 개발된 시스템이 전혀 동작하지 못할 정도의 계층간 통신 불량

4. 네트워크 장애진단 시스템의 구성 설계

장애진단 전문가 시스템의 구성은 크게 지식 베이스 모듈, 사용자 인터페이스 모듈, 추론엔진 모듈, 주요 모듈 통합으로 구성한다.

4.1 지식베이스 모듈 설계를 위한 모델

1. 모델 I

시스템을 주요 서브 시스템으로 구분하고 이들 각 주요 부분을 구성하는 모듈과, 모듈을 서브 모듈, 서브 모듈의 주요 요소별로 구분하여, 지식 베이스를 구축하는 방법이다(그림 1).
이 모델은 사용자로부터 서브 시스템에 대한 장애현상을 입력받아 장애 요소를 찾아낸다.

2. 모델 II

시스템을 특정한 문제영역으로 구분하고, 각 특정 문제영역에는 장애를 발생시키는 모듈과 예하의 서브 모듈을 구분하는 지식베이스를 구축하는 방법이다(그림 2).
사용자로부터 특정한 문제영역에 대한 장애현상을 입력받아 장애구성 요소를 찾아낸다. 이것은 문제영역을 구분할 수 있을 때 이 방법을 사용하면 효율적이다.

3. 모델 III

시스템을 주요 관련 서브시스템으로 먼저 구분하고, 각 서브시스템을 주요 장애현상과 관련 있는 특정 문제영역으로 분류하고, 각 주요 장애현상과 관련된 특정 문제영역은 장애를 발생시키는 모듈과 그 이하의 서브 모듈로 구성되며, 서브 모듈은 주요 요소별로 구분하여 지식베이스를 구축한다.
사용자로부터 주요 부분에 대한 장애현상을 입력받아 주요 요소를 찾아내는 방법이다. 이 모델은 시스템을 구분할 때 하드웨어 요소, 시스템 작동시 나타나는 장애현상을 쉽게 구분할 수 있다면 이 모델이 효율적인 지식베이스 모듈 구축방법이다(그림 3).

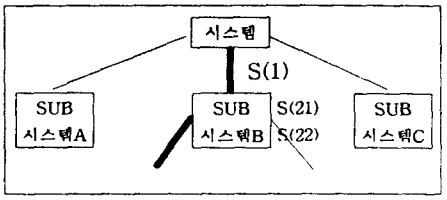

그림 1 모델 I의 구조

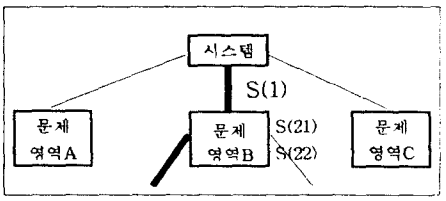

그림 2 모델II의 구조

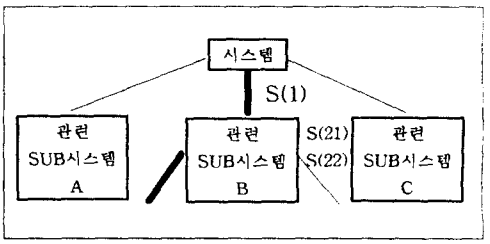

그림 3 모델 III의 구조

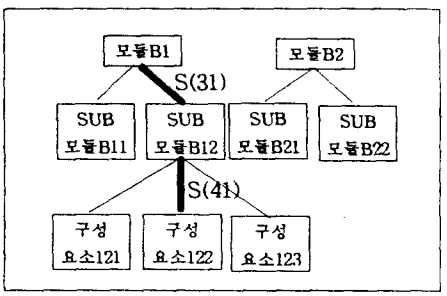

그림 4 모델 I ,모델II, 모델III의 하위 모듈

4.2 사용자 인터페이스

사용자 요구사항 분석 즉 시스템 개발 환경 사용자요구 사항, 시스템 특징으로 구분하고 (그림 5)와

같이 설계한다.

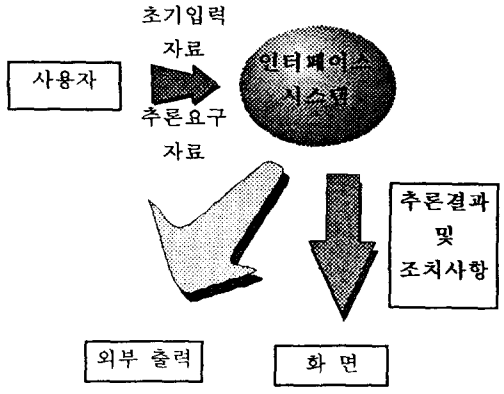

그림 5 사용자 관점에서의 시스템 구조

4.3 추론엔진 모듈

일반적으로 Backward chaining, Forward chaining, Hybrid chaining으로 구분하는데 본 논문의 추론엔진은 3가지 추론제어 기법을 이용하며, 추론을 시작할 것인가에 대한 방법과 실행할 규칙들 사이에 충돌이 발생할 때 해결방법을 가져야 하는데, 본 논문에서 설계한 도구는 이러한 문제를 해결하도록 지원해 준다. 전체적인 추론 절차는 아래와 같다(그림 6).

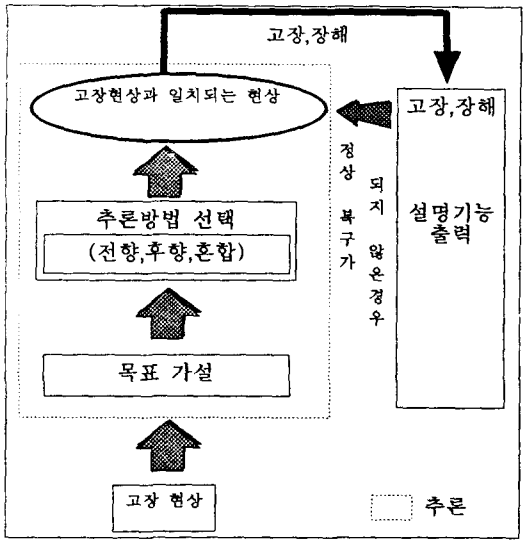

그림 6 추론 절차

4.4 주요 모듈 통합

모듈 통합은 도구를 이용하여 설계된 지식베이스 모듈, 사용자 인터페이스 모듈, 추론엔진 모듈을 도구에서 지원하는 라이브러리를 이용하여 그림 7과 같이 하나의 통합된 형태로 만드는 과정을 의미한다.

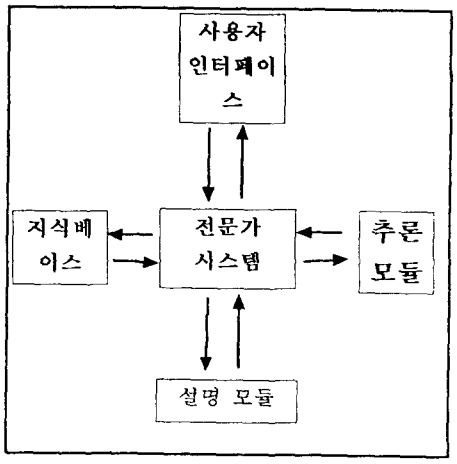

그림 7 시스템 통합 구조

5. 결론

장애 발생 처리를 위한 진단 시스템의 필요성과 그에 대한 여러 형태의 장애에 대한 분석을 3장까지 기술하였고 그것에 의한 장애진단 시스템의 전문가 시스템에서 네트워크 장애진단 시스템의 구성 설계의 여러 형태의 모델 제시와 추론 절차를 제안하였고 향후 연구 방향은 네트워크상의 구체적인 범위에서의 장애 요소와 그에 대한 여러 가지 처방, 추론엔진의 구체화가 되어야 할 것이다.

참 고 문 헌

[1] 권영미, 김종상, ATM 점대다점 연결망에서의 자기치료, 정보과학회논문, 1996, 7

[2] 김건웅, 김익배, 진명숙, 송병권, 안순신, SNMP를 이용한 전산망 관리시스템, 정보과학회논문, 1995, 3

[3] 김일곤, 유석인, 지식 베이스의 구성: 영역 분할

과 혼합 추론을 이용한 통합 기법, 정보과학회논문, 1991, 9

[4] 김화수, 조영범, 최종욱, 전문가 시스템, 집문당, 1995

[5] 양성욱, 실시간 지리정보 추론을 위한 객체지향 접근, 동국대학교 대학원 석사학위 논문, 1997

[6] 이재오, 한순희, 조국현, OSI 장애 관리를 위한 경보보고 기능의 구현 모델, 정보과학회논문, 1993, 8

[7] Adam Beguelin, Erik Seligman, Peter Stephan, "Application Level Fault Tolerance in Heterogeneous",CMU-CS-96-157, August 1996.

[8] Dan W. Patterson, Introduction To Artificial Intelligence And Expert Systems, 1995

[9] Efraim Turban, Expert system And Applied Artificial Intelligence, 1992