논문 2011-2-20

지능적 네트워크 장애 판별 및 문제해결을 위한 확률기반 시스템

A Probability Embedded Expert System to Detect and Resolve Network Faults Intelligently

양영문*, 장병윤**

Young-Moon Yang, Byeong-Yun Chang

요 약 현재의 망관리시스템들은 네트워크 장치에서 제공하는 경보의 심각도 정도로만 유효한 정보를 제공해 주며, 장애분석 과정이 주로 기술적인 숙련도가 높은 전문 운용 인력에 의존적이다. 이러한 이유 때문에 발생한 경보에 대하여 실제 장애 여부를 판단하는데 상당한 시간이 소요되며, 비교적 높은 인력 투입비용이 소요되고 있다. 따라서 이러한 문제를 해결하기 위해 본 연구에서는 네트워크 시설의 과거 경보발생 이력 및 장애처리 이력을 기반으로 각 경보에 대한 장애 가능성을 확률적으로 분석하고, 장애에 대한 적합한 조치 방법을 신뢰수준과 함께 안내하는 방법과 이를 실제 자동화된 시스템으로 구현하기 위해 필요한 프로그램 설계를 제시한다. 또한 사례연구를 통하여 제안된 방법이 실제 어떻게 사용될 수 있는지를 보여준다.

Abstract Currently network management systems(NMS) just give useful information about the criticality of the alarms and the process of the fault analysis is mainly dependent on the experts who have many years experiences in the field. Due to these reasons it takes very much time and manpower cost to localize the real root of the fault from the alarm information. Therefore, to solve these problems in this research we analyze the probability of the fault for each alarm and provide how to give the problem solving procedure with confidence level and give idea to build a system to realize the problem solving procedure. In addition, we give a case study to show how to use the proposed ideas.

Key Words : NMS, Fault Management, Fault Analysis, Probability, Autonomous System

Ⅰ. 서 론

현재의 통신사업자들은 인터넷, 전화, 전용회선 등의 통신 서비스를 제공하기 위해 백본망 및 액세스망 등의 통신 인프라를 구축하고 안정적인 통신의 기반이 되는 네트워크 운용을 위해 각종 네트워크 도메인의 경보 감시 업무를 수행하고 있다. 하지만 현재의 네트워크 경보 감시 업무 등 장애관리 업무는 운용자가 직접 각종 도메인의 망관리시스템(NMS:Network Management System)을 활용하여 네트워크 경보를 모니터링하고, 수집된 경보에 대하여 경보의 심각도(Critical, Major, Minor) 등을 참고하여 선별적으로 경보 발생 시설을 점검하여 장애 여부를 판단하고, 장애가 확인되면 장애복구 업무를 수행한다. 따라서, 현재의 망관리시스템들은 네트워크 장치에서 제공하는 경보의 심각도 정도 말고는 장애를 판별할 수 있는 유효한 정보를 제공해 주지 못하고, 장애분석 과정이 주로 기술적인 숙련도가 높은 전문 운용 인력에

*정회원, KT Professional Service 본부 데이터기술팀
**정회원, 아주대학교 경영학부 (교신저자)
접수일자: 2011.1.20, 수정일자: 2011.3.22
게재확정일자: 2011.4.15

의존적이기 때문에, 발생한 경보에 대하여 실제 장애 여부를 판단하는데 상당한 시간이 소요되고, 비교적 높은 인력 투입비용이 소요되는 문제가 있다.

이와 같은 문제점을 해결하기 위하여, 본 연구에서는 네트워크 시설의 과거 경보발생 이력 및 장애처리 이력을 기반으로 각 경보에 대한 장애 가능성을 확률적으로 분석하고, 장애에 대한 적절한 조치 방법을 신뢰수준과 함께 안내하는 방법을 제시한다. 이 방법은 과거 경보 및 장애발생 그리고 장애처리 이력을 기반으로 각각의 경보, 장애발생, 그리고 장애처리 건에 대하여 확률 값을 부여하고 이를 바탕으로 망운용관리 운용자에게 경보 및 장애관련 정보를 제공하고자 한다. 또한 이러한 방법의 자동화된 계산을 위하여 확률기반 네트워크 장애통보 시스템을 제시하며, 이 시스템의 내부 기능구성을 간략하게 설명한다. 이와 같은 방법을 실제 Network Fault Management System에 적용함으로써 비 숙련자인 운용자도 쉽게 경보발생에 대해서 대처할 수 있고 또한 인건비도 줄일 수 있을 것으로 생각된다.

일반적으로 네트워크 관리는 제한된 비용과 인력을 활용하여 네트워크 서비스 품질을 극대화함으로써 네트워크의 효율성과 생산성을 높이기 위하여 복잡한 네트워크를 제어하는 일련의 과정을 말한다. 네트워크 관리 영역중 장애관리는 네트워크 서비스의 비정상적인 운영과정을 인지, 격리, 수정하여 네트워크의 서비스 가동율을 높여 주기 위한 일련의 행위를 말한다. 즉 네트워크 장애관리는 네트워크에 장애가 발생되었을 때, 이를 감지하고 장애의 원인과 위치를 판별하여, 복구하는 기능을 말한다. 이 장애관리를 위하여 서비스 제공자는 일반적으로 fault management system을 사용한다. 이상적으로 fault management system 는 전문운용인력의 도움 없이도 네트워크상에서 일어나는 장애를 찾아내고 해결할 수 있어야 된다. 이와 관련된 연구로Gardner and Harle [2]은 alarm correlation와 alarm correlation시스템의 필요요건들을 제시했다. 또한 Chao et al. [3]은 자동화된 장애진단 시스템을 제안 했으며, 장애관리 및 이와 관련된 연구는 상당히 많은 연구가 진행 되었다 [4-8]. 하지만 현실 네트워크 장애관리에서는 장애관리 시스템은 네트워크 장치에서 제공하는 경보의 심각도 정도로만 유효한 정보를 제공해 주며, 장애분석 과정이 주로 기술적인 숙련도가 높은 전문 운용 인력에 의존적이다. 따라서 본 논문에서는 실제적이고 효과적으로 network operations and management staff들을 도우기 위하여 지능적 네트워크 장애 판별 및 문제해결을 위한 확률기반 시스템을 제안한다.

본 논문은 다음과 같은 순서로 구성되어 있다. 먼저 2장에서는 네트워크 장애관리를 효율적으로 하기 위하여 행하여진 연구들을 살펴보고 제3장에서 실제 현장에서 많은 부분 전문가에 의존적으로 행하여지고 있는 네트워크 장애관리를 비전문가도 쉽게 수행하는데 도움을 줄 수 방법을 소개하고 이를 시스템화 한다. 제 4장에서는 제3장에서 제시한 방법을 실제 네트워크 장애관리 사례에 적용한 예를 살펴보도록 한다. 그리고 마지막 5장에서는 결론 및 향후 연구방향을 제시하도록 한다.

Ⅱ. 관련 논문 연구

본 절에서는 장애관리를 효율적으로 하기 위하여 행하여진 과거의 연구에 대해서 개략적으로 살펴본다. 먼저 Gardner and Harle[2]은 통상적으로 network operations staff들에게 network monitoring 및 fault diagnosis을 어렵게 만드는 다양한 Alarms들을 처리할 수 있는 방법을 제시했다. Alarm Correlation은 다양한 Alarm들을 분석하여 근본원인을 찾는 과정으로 Gardner and Harle[2]의 논문에서 다양한 Alarm을 처리하는 방법으로 제시했다. 이상적으로 이 방법은 네트워크 운용전문가의 도움 없이도 네트워크 문제발생시 그 원인을 알 수 있고 또한 자동적으로 조치 및 정비작업을 할 수 있어야 한다. 하지만 실제 시스템에서는 그렇지 못한 것이 현실이다. 운용자가 직접 각종 도메인의 망관리시스템(NMS:Network Management System)을 활용하여 네트워크 경보를 모니터링하고, 수집된 경보에 대하여 경보의 심각도(Critical, Major, Minor) 등을 참고하여 선별적으로 경보 발생 시설을 점검하여 장애 여부를 판단하고, 장애가 확인되면 장애복구 업무를 수행한다. 따라서, 현재의 망관리시스템들은 네트워크 장치에서 제공하는 경보의 심각도 정도 말고는 장애를 판별할 수 있는 유효한 정보를 제공해 주지 못하고, 장애분석 과정이 주로 기술적인 숙련도가 높은 전문 운용 인력에 의존적이기 때문에, 발생한 경보에 대하여 실제 장애 여부를 판단하는데 상당한 시간이 소요되고, 비교적 높은 인력 투입비용이 소요되는 문제가 있다.

Gardner and Harle[2]이외에도 장애진단 및 문제해결을 위한 다양한 논문 들이 출판 되었다[4-8]. Chao et al.[3] 은 network fault propagation model 의 causality graph 를 기반으로 하여 an alarm correlation system 을 제안 하였으며 실제적이고 효과적인 network fault 진단 시스템의 개발이 중요하다고 역설했다. Bouloutas et al.[4]은 통신 네트워크에서 alarm correlation과 fault identification의 문제를 모델링하고 해결하는 일반적인 Framework을 제시했다. 특히 multiple faults인 경우 fault localization문제는 discrete optimization문제가 되고 이 문제는 실제의 많은 경우 NP-Hard 문제인 경우가 많으므로 이를 해결하기 위하여 heuristic algorithm이 제안 되었다. Stdinder and Sethi[8]은 지난 10년 기간 동안 제안 됐던 network fault localization solution들의 장단점 및 fault localization 문제의 여러 도전들을 설명했다. 이 논문은 network fault management분야에 대한 기본적 개념들을 잘 설명 하였으며, fault localization 기법에 관하여는 AI techniques, Model traversing techniques, Fault propagation models관점에 따라 분류를 하였다. 이 이외에도 현재에는 다양한 통계 기법[9, 10] 및 data mining[11, 12] 기법 등을 활용하여 네트워크 장애진단 및 문제해결을 하려는 여러 연구들이 진행 중이다.

Ⅲ. 확률기반 네트워크 장애 통보 및 문제해결 가이드

여기에 제안한 내용을 입력하세요. 본 연구는 네트워크 시설의 과거 경보발생 이력 및 장애처리 이력을 기반으로 각 경보에 대한 장애 가능성을 확률적으로 분석하고, 장애에 대한 적합한 조치 방법을 안내하여 네트워크 장애처리에 소요되는 인적, 시간적 투입비용을 절감하기 위한 것이다.

이러한 과제를 달성하기 위한 본 연구에서는 확률기반 네트워크 장애통보 시스템을 제안한다. 이 시스템은 네트워크 경보발생 이력 및 장애처리 이력을 분석하여 각 네트워크 경보에 대한 장애확률과 장애에 대한 조치방법 데이터를 구축하는 장애 분석모듈, 네트워크 이상징후 경보를 실시간으로 수집하는 경보 수집모듈, 수집된 경보에 대하여 해당 경보의 장애확률을 파악하고, 장애성 경보인 경우 적절한 조치방법을 안내하는 장애통보모듈, 사용자 인터페이스로부터 입력된 장애에 대한 작업정보에 따라 장애복구 절차를 진행하고, 최종적으로 경보에 대한 처리를 마감하는 장애처리모듈, 사용자가 감시대상 경보의 장애확률 조건 및 장애 조치 안내 신뢰도 조건을 설정할 수 있도록 제공하는 사용자 인터페이스, 경보발생 이력과 장애처리 이력, 그리고 경보별 장애확률과 장애조치 안내 정보를 관리하기 위한 데이터베이스를 포함하고 있다.

그림 1은 확률기반 네트워크 장애통보 시스템의 내부 기능구성을 간략하게 나타낸 블록 구성도이다. 경보 수집부모듈은 네트워크 장치 혹은 외부 네트워크 경보 수집 장치로부터 경보 수집을 위한 연동 인터페이스를 제공하고, 다양한 도메인에서 수집된 경보를 표준 형식으로 변환하여 장애 통보부모듈로 전달하고, 경보내역을 데이터베이스에 저장하는 역할을 수행한다. 장애 통보부모듈은 사용자 인터페이스로부터 장애확률 조건 및 장애조치 안내 신뢰도 조건의 설정을 읽어 들여 데이터베이스의 경보별 장애확률 및 조치안내 정보 테이블에서 상기 조건으로 수집된 경보들에 대한 자료를 조회하여 경보별 장애 가능성을 확률로 표시하고, 장애성 경보인 경우 적합한 장애조치 방법을 각 방법에 대한 신뢰도와 함께 접속된 클라이언트 PC에 통보하는 역할을 수행한다.

장애 처리모듈은 사용자 인터페이스로부터 입력된 작업정보에 따라 데이터베이스에 작업내역을 등록하고, 최종적으로 경보에 대한 장애처리를 마감하는 역할을 수행한다. 장애 분석모듈은 상기 장애처리 활동으로 데이터베이스에 기록되는 경보발생 이력과 장애처리 이력을 분석하여 경보별 장애확률 정보와 장애조치 안내 정보를 구축하는 역할을 수행한다. 장애확률과 조치안내 정보는 정보의 신뢰성을 보장하기 위하여 최근 6개월 기준, 혹은 1년 기준 등의 검출 기준을 정하여 구축하고, 상기 장애분석모듈은 매월 혹은 매주의 특정 주기에 자동으로 실행되어 항상 현행화된 장애확률과 조치안내 정보가 유지될 수 있도록 한다. 데이터베이스는 본 발명의 중요한 데이터인 경보발생 이력, 장애처리 이력, 그리고, 경보별 장애확률 및 조치안내 정보를 포함한다. 사용자 인터페이스는 사용자가 감시 대상 경보의 장애확률 조건(이를 테면, 장애확률이 30% 이상인 경보만 모니터링 하도록 설정할 수 있고, 검출기준을 최근 6개월 기준 또는 최근 1년 기준으로 설정할 수도 있다.)과 장애조치 안내 신뢰도 조건을 설정할 수 있는 인터페이스를 제공한다.

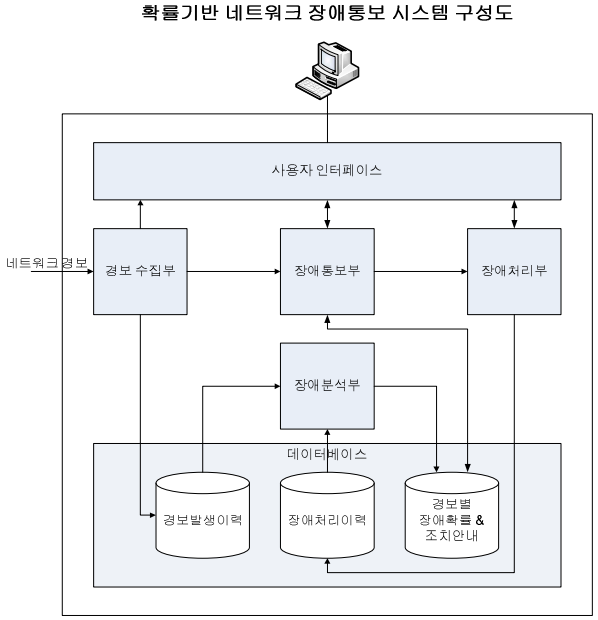

그림 1. 확률기반 네트워크 장애통보 시스템
Fig. 1. Probability based network fault alarm system

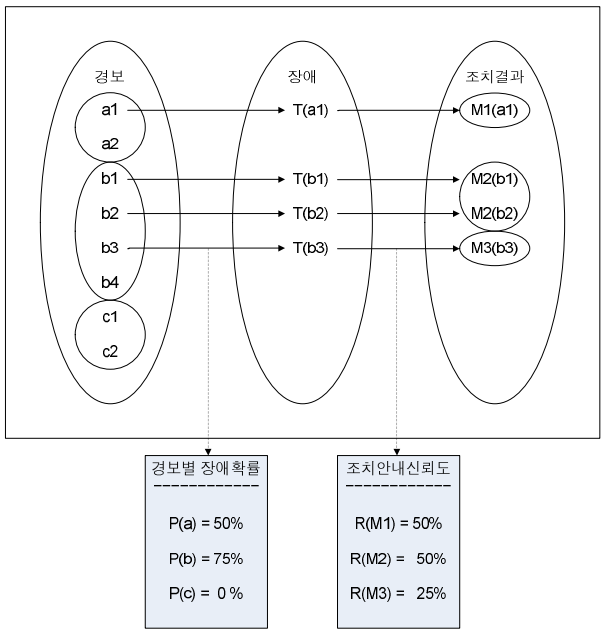

그림 2. 경보별 장애확률 및 조치안내 신뢰도
Fig. 2. Fault probability and problem solving procedure confidence level for each alarm

그림 2는 본 연구의 경보별 장애확률과 장애조치 안내 신뢰도를 도출하는 개념을 설명하는 경보-장애-조치결과 매핑 관계도이다. 그림 2의 경보 그룹에서 알파벳 문자가 같은 것들은 서로 동일 경보이며, 기호 뒤의 숫자는 발생번호를 나타낸다. 즉, 경보 a1과 경보 a2는 같은 a 종류의 경보이며, 두 번 발생했음을 나타낸다. 장애 그룹에 포함된 경보들은 장애로 판정된 경보 이력을 나타낸다. 즉, T(a1)은 경보 a1의 장애이력을 나타내고, T(a2)에 대한 내역은 없으므로 경보 a2는 실제 장애가 아닌 단순 경보였음을 나타낸다. 조치결과 그룹의 내역은 각 장애들에 대한 조치방법을 나타낸다.

즉, M1(a1)은 장애로 판명된 경보 a1에 대하여 M1의 방법으로 장애조치를 한 내역이다. 이러한 경보-장애-조치결과의 매핑 관계로부터 단위 기간 동안 경보별 장애가능성과 장애조치 결과에 대한 신뢰도를 확률적으로 분석할 수 있다. 그림 2의 예에서 경보 b에 대한 장애확률은 75%(경보가 4 번 발생하였고, 3 번의 장애 내역이 있으므로, 75% = 3/4 * 100), 조치결과(안내) 신뢰도는 M2, M3 두 가지 방법이 있는데, M2 방법의 신뢰도는 50% (4번의 동일 경보에 대하여 M2 방법으로 2번 장애조치 했으므로, 50% = 2/4*100), M3 방법의 신뢰도는 25% (4번의 동일 경보에 대하여 M1 방법으로 1 번 장애조치 했으므로, 25% =1/4*100)이다.

아래 그림 3은 경보별 장애확률 정보를 구축하는 과정을 나타낸 로직 순서도이다. 본 프로세스는 매월 또는 매주 등 일정한 주기로 자동 구동되는 형태가 바람직하며, Unix 서버를 운영하는 경우 Cron job으로 등록하여 이를 실현할 수 있다. 본 연구에서 제안하는 장애확률 정보 구축 프로세스가 구동되면 먼저 DB접속을 시도한다. DB접속이 완료되면 기 구축된 장애확률 정보 테이블의 기준일자 컬럼 값을 읽어 시스템의 현재일자와 비교한다. 기준일자가 현재일자와 동일하다면, 해당 일자에 이미 장애확률 정보를 새로 구축한 것으로 간주하여 프로세스를 종료한다. 상기 기준일자와 현재일자가 다른 경우, 경보발생 이력 테이블과 장애조치 이력 테이블의 정보를 조회하여 현재일자로부터 최근 6개월 자료들을 기준으로 장애확률을 계산한 데이터를 장애확률 정보 테이블에 새로 구축한다. 이후 현재일자로부터 최근 1년 자료들을 기준으로 장애확률을 계산한 데이터를 장애확률 정보 테이블에 새로 구축한다. 상기 장애확률 정보 구축이 완료되면 각 기준일자 컬럼을 현재일자로 갱신하고 작업을 종료한다.

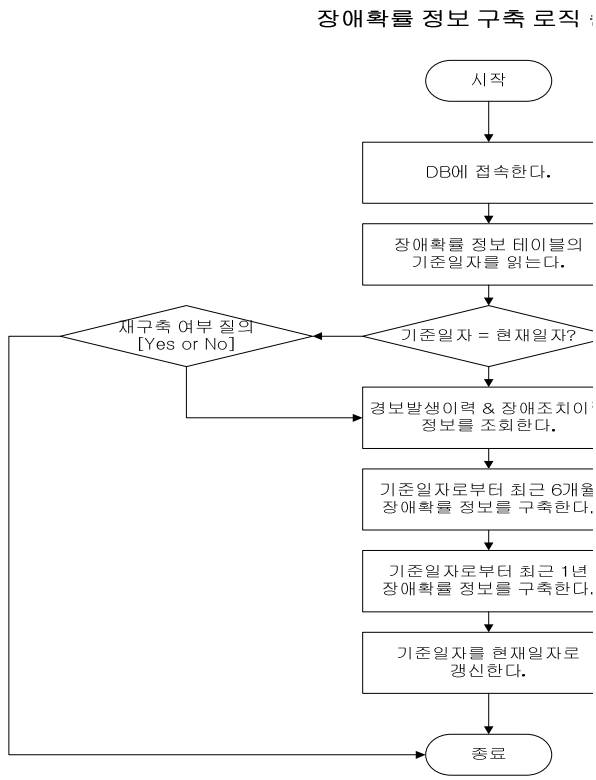

그림 3. 경보별 장애확률 정보 구축 로직
Fig. 3. Fault probability information establishment logic for each alarm

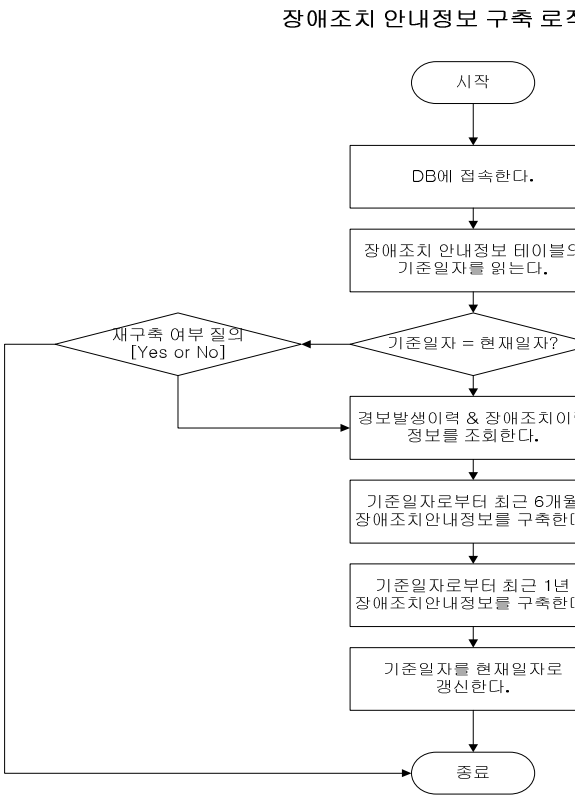

그림 4. 장애조치 안내정보 구축 로직
Fig. 4. Problem solving procedure guidance establishment logic

그림 4은 장애조치 안내정보를 구축하는 과정을 나타낸 로직 순서도이다. 본 장애조치 안내정보 구축 프로세스 역시 그림 3의 장애확률 정보 구축 프로세스와 마찬가지로 동일한 주기로 자동 구동되는 형태가 바람직하다. 장애조치 안내정보 구축 프로세스가 구동되면 먼저 DB 접속을 시도한다. DB접속이 완료되면 기 구축된 장애조치 안내정보 테이블의 기준일자 컬럼 값을 읽어 시스템의 현재일자와 비교한다. 기준일자가 현재일자와 동일하다면, 해당 일자에 이미 장애조치 안내정보를 새로 구축한 것으로 간주하여 프로세스를 종료한다. 위의 기준일자와 현재일자가 다른 경우, 경보발생 이력 테이블과 장애조치 이력 테이블의 정보를 조회하여 현재일자로부터 최근 6개월 자료들을 기준으로 장애조치 안내정보의 신뢰도를 계산한 데이터를 장애조치 안내정보 테이블에 새로 구축한다. 이후 현재일자로부터 최근 1년 자료들을 기준으로 장애조치 안내정보의 신뢰도를 계산한 데이터를 장애조치 안내정보 테이블에 새로 구축한다. 장애조치 안내정보 구축이 완료되면 각 기준일자 컬럼을 현재일자로 갱신하고 작업을 종료한다.

그림 5은 확률기반 네트워크 장애통보 및 장애조치 안내 기능을 제공하는 과정을 나타낸 로직 순서도이다. 위 확률기반 네트워크 장애통보 시스템의 서버 프로세스의 주요 동작을 위주로 설명하면 다음과 같다. 서버 프로세스가 구동되면 먼저 DB에 접속하고 경보의 유입을 기다린다. 이후 경보 수집부에서 경보의 유입이 있으면 해당 경보는 경보발생 이력 테이블에 등록된다. 경보 통보부에서는 상기 유입된 경보가 장애확률 정보 테이블에 등재된 경보인지 확인하여 등재되지 않은 경보인 경우, 비장애성 단순경보로 UI에 표시하여 장애조치가 불필요한 경보임을 표시한다. 위 확인 과정에서 장애확률 정보 테이블에 등재된 경보인 경우, 해당 경보의 최근 6개월 장애확률과 최근 1개월 장애확률을 읽어 온다. 그리고, 장애조치 안내 테이블로부터 해당 경보에 대한 장애조치 안내정보를 최근 6개월, 최근 1년 기준의 신뢰도 정보와 함께 읽어 온다.

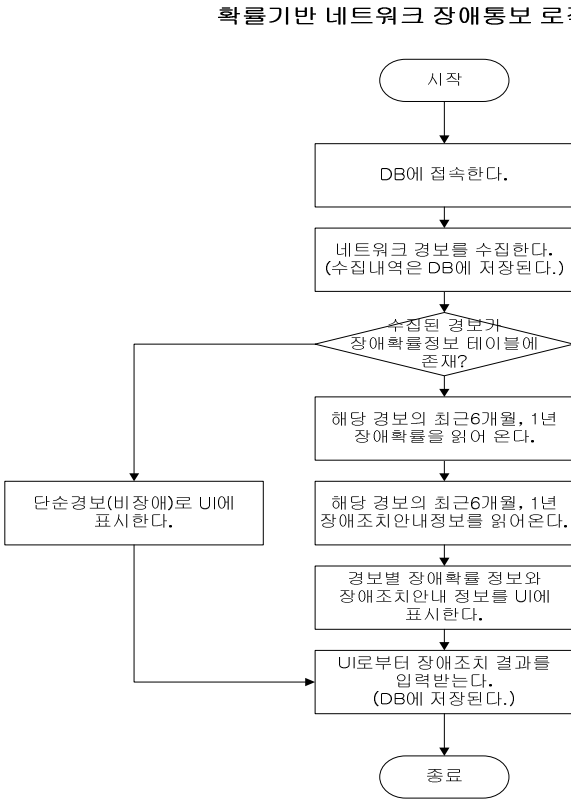

그림 5. 확률기반 네트워크 장애통보 로직
Fig. 5. Probability based network fault alarm logic

그리고 나서, 위 과정에서 도출된 경보별 장애확률 정보와 신뢰도를 포함하는 장애조치 안내 정보를 UI에 표시한다. UI에는 운용자가 설정한 장애확률 검출 조건과 장애조치 안내 신뢰도 조건에 부합하도록 표시된다. 예를 들어 운용자는 장애확률 검출 조건 설정을 통해 장애확률이 30% 이상인 장애만 선별적으로 감시할 수도 있고, 장애조치 안내를 최근 6개월 신뢰도가 높은 순으로 조치방법을 안내 받을 수 있다. 이러한 과정으로 장애성 경보에 대하여 장애확률과 함께 장애조치 방법이 자동으로 안내되므로 기술적으로 전문성이 없는 일반 운용자들도 쉽고 빠르게 장애조치 업무를 수행할 수 있을 것이다. 이후에 사용자 인터페이스로부터 장애조치 결과를 입력받아 장애조치 이력 테이블에 저장하고 경보에 대한 장애처리 업무를 종료한다.

확률기반 네트워크 장애 통보시스템의 업무 로직은 장애조치 이력 테이블에 새로 등록된 내역이 경보 분석 모듈에서 장애확률과 장애조치 안내정보를 갱신하는 데 다시 활용되는 순환적 구조이다. 장애조치 결과가 안내된 장애조치 방법과 다를 수도 있으며, 이런 경우는 장애조치 안내 정보 구축시 해당 경보에 대한 새로운 장애ID를 부여하여 별개의 장애조치 건으로 등록된다.

Ⅳ. 사례 연구

다음페이지 그림 6은 그림 1에서 제시된 확률기반 네트워크 장애통보 시스템을 적용하고자 하는 네트워크 분야의 경보와 장애조치내역 샘플 데이터이다.

각 경보는 도메인, 장치종류, 유니트, 경보종류의 조합으로 유일성을 갖으며, 이 조합이 같은 경우 동일 경보라고 볼 수 있다. 그림 6의 샘플은 경보ID가 B000001, T000001, T000002 인 3가지 종류의 경보가 각각 3번, 3번, 2번 발생한 경우이다. 그리고, 각 경보에 대하여 실제 장애로 판명된 경우는 장애조치 내역이 있고, 장애가 아닌 단순경보인 경우 장애조치 내역이 없다. 그림 3의 샘플에서 B000001 경보는 2번 동일한 방법으로 장애 조치한 내역이 있고, T000001 경보는 두 번 다른 방법으로 장애 조치한 내역이 있다.

그림 7는 장애확률 정보 테이블 구조와 그림 6의 경보 및 장애조치 이력으로부터 분석된 경보별 장애확률 샘플 데이터이다.

장애확률 정보 테이블 구조는 경보와 장애간의 매핑을 위해 경보ID를 Primary Key로 사용하고, 하나의 경보ID는 [도메인+장치종류+유니트+경보종류]의 조합으로 유일한 Key 값을 갖는 구조이다. 그리고, 데이터를 구축한 일자를 관리하기 위해 기준일자 컬럼을 추가하였고, 기준일자로부터 최근6개월 데이터로 추출한 장애확률과 최근 1년 데이터로 추출한 장애확률 컬럼을 두었다. 장애확률 컬럼은 실무 운용환경에 맞게 신뢰성이 보장되는 기간을 고려하여 검출 기간을 조정하거나, 검출기간을 보다 세분화 하여 컬럼을 추가할 수도 있을 것이다. 그림 6의 경보-장애 샘플로부터 도출된 그림 7의 경보ID B000001에 대한 장애확률은(기준일자는 2009. 7. 1) 최근 6개월 기준으로 50% (= 1/2 * 100), 최근 1년 기준으로 67% (= 2/3 * 100) 이다. 나머지 경보들의 장애확률도 같은 방식의 계산으로 그림 7의 결과를 얻을 수 있다.

그림 8는 장애조치 안내정보 테이블 구조와 그림 6의 경보 및 장애조치 이력으로부터 분석된 장애별 조치안내 신뢰도 샘플 데이터이다. 장애조치 안내정보 테이블 구조는 별도의 장애ID를 Primary Key로 사용하고, 경보와

[경보-장애조치 샘플]

	경보내역					조치내역			
	발생일자	도메인	장치종류	유니트	경보종류	장애시설	장애구분	장애원인	조치내역
B000001	2008-09-01	BcN	AccessGateway	111-102	UNIT FAIL	BAGW0071	S/W불량	S/W에러	소프트웨어 버그로 svu 리부팅
	2009-03-05	BcN	AccessGateway	111-102	UNIT FAIL	-	-	-	-
	2009-05-03	BcN	AccessGateway	111-102	UNIT FAIL	BAGW0071	S/W불량	S/W에러	소프트웨어 버그로 svu 리부팅
	…	…	…	…	…				
T000001	2008-11-14	전송망	SM16G	T1E1X	LOS	-	-	-	-
	2009-04-06	전송망	SM16G	T1E1X	LOS	ST16-0510	H/W불량	유니트불량	ERX-OC3 IO 카드 교체
	2009-05-11	전송망	SM16G	T1E1X	LOS	ST16-0510	H/W불량	공통부불량	공통부 UNIT 교체
	…	…	…	…	…				
T000002	2008-10-02	전송망	WDC7	AMX-14-E	ELCV	-	-	-	-
	2009-02-02	전송망	WDC7	AMX-14-E	ELCV	WDC7-01	H/W불량	유니트불량	공통부유니트(PU) 불량/교체
	…	…		…	…				

그림 6. 경보-장애 조치 샘플
Fig. 6. Alarm-Problem Solving Sample

[장애확률 정보 테이블 구조]

경보ID	도메인	장치종류	유니트	경보종류	기준일자	장애확률(최근6개월)	장애확률(최근1년)
B00001	BcN	AccessGateway	111-102	UNIT FAIL	2009-07-01	50%	67%
T000001	전송망	SM16G	T1E1X	LOS	2009-07-01	100%	67%
T000002	전송망	WDC7	AMX-14-E	ELCV	2009-07-01	100%	50%

그림 7. 장애확률 정보 테이블 구조
Fig. 7. Fault probability information table structure

[장애조치 안내정보 테이블 구조]

장애ID	경보ID	장애시설	장애구분	장애원인	조치안내	기준일자	신뢰도(최근6개월)	신뢰도(최근1년)
B000001-1	B000001	BAGW0071	S/W불량	S/W에러	소프트웨어 버그로 svu 리부팅	2009-07-01	50%	67%
T000001-1	T000001	ST16-0510	H/W불량	유니트불량	ERX-OC3 IO 카드 교체	2009-07-01	50%	33%
T000001-2	T000001	ST16-0510	H/W불량	공통부불량	공통부 UNIT 교체	2009-07-01	50%	33%
T000002-1	T000002	WDC7-01	H/W불량	유니트불량	공통부유니트(PU) 불량/교체	2009-07-01	100%	50%

그림 8. 장애확률 정보 테이블 구조
Fig. 8. Fault probability information table structure

의 매핑을 위해서 경보ID를 Foreign Key로 사용한다. 동일 경보이더라도 장애조치 방법이 다를 수 있기 때문에, 이 경우는 경보ID에 순번을 적용하여 장애ID를 생성한다. 그림 6의 경보-장애 샘플로부터 도출된 그림 8의 장애ID T000001-1에 대한 조치안내 신뢰도는(기준일자는 2009. 7.1) 최근 6개월 기준으로 50% (= 1/2 * 100), 최근 1년 기준으로 33% (= 1/3* 100)이다. 나머지 장애들의 조치안내 신뢰도도 같은 방식의 계산으로 그림 8의 결과를 얻을 수 있다.

V. 결 론

본 논문에서는 현재 망관리시스템들이 가지고 있는 주요문제점들을 해결하기 위하여 네트워크 시설의 과거 경보발생 이력 및 장애처리 이력을 기반으로 각 경보에 대한 장애 가능성을 확률적으로 분석하고, 장애에 대한 적합한 조치 방법을 신뢰수준과 함께 안내하는 방법과 이를 실제 자동화된 시스템으로 구현하기 위해 필요한 프로그램 설계를 제시하였다. 또한 사례연구를 통하여 제안된 방법이 실제 어떻게 사용될 수 있는지를 상세하게 설명하였다. 이번 연구를 통하여 현재 전문운용인력에 의존적인 네트워크 장애관리 업무를 비 숙련자라도

쉽게 수행할 수 있도록 하였으며 좀더 사용하기 쉽고 간편하면서 효율적인 네트워크 장애 통보 시스템을 제안하였다.

이 연구와 더불어 네트워크 장애판별 및 문제해결의 다양한 방법론적 검토가 필요할 것으로 보이며 Logistic Regression, Market Basket Analysis등의 다양한 통계[9, 10] 및 Data Mining[11,12]기법의 적용도 좋은 연구 결과를 가져올 것으로 기대된다.

참 고 문 헌

[1] Y.-M. Yang, J.-S. Kim, S. Park, S.-W. Lee, B.-D. Chung, and B.-Y. Chang, "A Probabilistic Approach for Network Trouble Report and Recovery Guide," Proc. of KICS 2009, November, 2009

[2] R. D. Gardner and D. A. Harle, "Methods and systems for alarm correlation," Proc. of GLOBECOM, London, UK, pp. 136 - 140, November 1996

[3] C. S. Chao, D. L. Yang, and A. C. Liu, "An automated fault diagnosis system using hierarchical reasoning and alarm correlation," Journal of Network and Systems management, vol. 9, no. 2, pp. 183 - 202, 2001.

[4] A. T. Bouloutas, S. Calo, and A. Finkel, "Alarm correlation and fault identification in communication networks," IEEE Trans. On Commun., vol. 42, pp. 523 - 533, 1994.

[5] R. N. Cronk, P. H. Callahan, and L. Bernstein, "Rule-based expert systems for network amangement and operations: An introduction," IEEE Network, vol. 5, no. 4, pp. 7 - 21, September 1988.

[6] T. E. Marques, "A symptom-driven expert system for isolating and correcting network faults," IEEE Commun. Mag., vol. 26, no. 3, pp. 6 - 13, March 1988.

[7] C. Melchiors and L. M. R. Tarouco, "Troubleshooting network faults using past experience," IEEE/IFIP Network Operations and Management Symposium, Honolulu, HI, pp. 549-562, Apr. 2000.

[8] M. Steinder and A. S. Sethi, "A survey of fault localization techniques in computer networks," Science of Computer Programming, vol. 53, pp. 165－194, 2004

[9] Gerald Keller. "Managerial Statistics," South Western Cengage Learning, 2009.

[10] J. Neter, M. Kunter, C. Nachtsheim, W. Wasserman, "Applied Linear Statistical Model," Times Mirror Higher Education Group, 1996.

[11] T. Hastie, R. Tibshirani, J. Friedman, "The elements of Statistical Learning, Springer, 2001.

[12] D. Hand, H. Mannila, P. Smyth, "Principles of Data Mining," MIT, 2001.

※ This paper is an updated and extended version of Y.－M. Yang et al. of Ref. [1].

저자 소개

양 영 문(정회원)

- 1997년 동국대학교 전자공학과, 학사
- 1999년 ~ 2009년 KT 네트워크 연구소, 선임 연구원
- 2010년 ~ KT Professional Service본부 Network Consultant

<주관심분야 : 정보통신경영, Operations Research, Optimal Network Design>

장 병 윤(정회원)

- 2000년 Georgia Tech, Operations Research 석사
- 2002년 Georgia Tech, Applied Statistics 석사
- 2004년 Georgia Tech, Industrial and Systems Engineering 박사
- 2004년 ~ 2006년 Georgia Tech, Post-Doc
- 2006년 ~ 2009년 KT 네트워크 연구소, 선임 연구원
- 2009년 ~ 현재 아주대학교 경영학부 교수

<주관심분야 : 정보통신경영, Operations Research, Simulation, Applied Statistics, Production and Operations Management>