2005년도 대한전기학회 하계학술대회 논문집 2005. 7. 18 - 20

통합 장애관리 기능 구조에 관한 연구

조동권 KT 운용시스템연구소

Functional Structure for an Integrated Network Management

D. K. Cho KT OSSL

Abstract - 고객 서비스 제공 관점에서 통신 인프라를 감시하고 분석하기 위한 도메인간 장애관리 솔루션의 필요성이 대두되고 있다. 이벤트에 대한 상관관계분석을 통해 근원장애 이벤트를 도출하고 장애 문제에 대한 해결을 신속하게 처리할 수 있는 체계를 구축하는 것이 중요하다. 본 논문에서는 요구기능의 분석을 통해 통합망 상관관계 분석 기능을 수용한 통합 장애관리 시스템의 구조를 제안한다.

1. 서 론

주요 통신망 사업자들은 효과적이고 효율적인 통신망 운용 및 확장을 위해 고객 및 서비스 관점의 종합적인 관리에 주력해 오고 있다. 그러나, 통신망에서의 다음과 같은 어려움으로 서비스 단대단 서비스 제공 현황 감시가 어려운 실정이다. 첫째, 다른 도메인의 장애로 인한 고장인 경우 근본 원인 추적에 많은시간과 노력이 소요되며 도메인 별로 중복된 트러블 티켓 발행 가능성이 크다. 둘째, 대형고장 발생시 고장판단 및 영향범위 예측이 어렵다. 고객에게 망관리시스템의 경보발생 현황만으로는 서비스영향 여부, 대형고장으로의 여부 판단이 곤란하고, 운용자 노하우에 의존한 경보분석으로 기량에 따라 대형 고장 판정 및 초동 조치에 많은 시간이 소요된다. 또한, 전체 통신망 통합감시 불가로 통신망간 연동된 장애개소에 대한 판단이 지연된다. 셋째, 종합적인 통합 상황관리 기능 부재를 들 수 있다. 망관리자 관점에서 전체적인 종합장애를 판단할 수 있는 뷰 및 관리자 관점에서 서비스 영향 지역/범위에 대한 판단 정보 데이터, 장애발생시 신속한 조치 및 전파를 위한 통합 상황관리체계가 필요하다. 이러한 문제점들을 해결하기 위해서는, 대형장애의 발생 가능성 및 영향범위 최소화 방안이 필요하다. 구체적인 내용은 다양한 도메인의 장애 및 구성정보를 수집하여 데이터변환을 수행하고 분석 가능한 형태로 도메인간 상관관계 분석을 기반으로 통합망 관점에서 장애 근본 원인을 찾아내어, 통신망 대형 고장유무를 판단하고 신속한 상황전파 및 피해규모를 산출해야 한다.

통합망 장애관리시스템의 국내외 사례는 다음과 같다. 통합망관리 어플리케이션들은 일반적으로 장애이벤트를 수집하는 수집모듈, 수집된 이벤트에 상관관계 규정 및 변환 처리를 수행하는 엔진모듈, 타 시스템 또는 데이터베이스와 연동을 수행하기 위한 연동모듈, 마지막으로 이들 처리과정 또는 처리된 결과를 보여주기 위한 사용자 클라이언트 모듈의 4가지로 구성된다.

HP OpenView 제품군은 Network Node Manager가 핵심 제품으로 자체적으로 솔루션 기능을 수행할 뿐만 아니라 다른 HP OpenView 제품과 데이터 연동을 통해 네트워크 관리를 위한 종합적인 체계를 구축하는 기반이 되며, NNM은 여러 네트워크 시스템과 어플리케이션을 하나의 네트워크 그래픽 화면에서 관리할 수 있는 통합 도구를 네트워크 관리자에게 제공할 수 있다.

Netcool 시스템은 크게 ObjectServer 모듈, 사용자 뷰 모듈, 이벤트 정보수집 및 연동 지원 모듈, 통계 정보 가공 모듈, 확장 모듈로 구성된다. ObjectServer 모듈은 실시간 장애 이벤트를 각 Probe및 모니터로부터 수신하여 메모리 DB에 저장하고 Desktop 모듈을 통해 장애관리 뷰를 제공하고, 사용자 뷰 모듈은 관리자, 운영자, CNM, 등 관리자의 수준별로 뷰를 구성하고 분산시킬 수 있는 클라이언트 관리 뷰 기능이 있다. 이 외에도 CA Unicenter 및 IBM Tivoli 등과 같은 제품군이 있다. 상관관계분석 기능은 특성화된 단위제품이기보다는 제품내의 제한된 모듈로 기능하고 있다.

2. 통합망 장애관리

통신망 관리에 있어서 심각하면서도, 현실적인 문제는 이벤트가 적절하게 관리되지 못한다는 것이다. 즉, 관리대상이 되는 시스템에 장애가 발생했을 경우, 관리자는 종종 장애의 일부 증상을 알려주는 다소 무의미한 이벤트들의 폭발적 증가 속에 직면한다. 그래서 이벤트 상관관계분석의 주요 목적은 관리자가 신속하고 정확하게 장애 원인을 식별하고 조치할 수 있도록 이벤트의 개수를 줄여 보다 쉽게 분석할 수 있는 정보로 가공하여 제공해주기 위한 것이다. 여기서 이벤트 상관관계분석 이란 두 이벤트 간의 관계 및 처리되어야 할 방식을 정의하고 정의된 조건에 부합되는 이벤트들의 발생시 앞서 정의된 규정에 따라 처리하는 과정을 의미한다. 이벤트 상관관계를 이용함으로써, 중복하여 발생한 이벤트를 제거하고, 인과적 상호관계를 이용하여, 근원 장애를 분석할 수 있다. 따라서, 운용자의 신속한 대처가 요구되는 장애관리, 성능관리, 보안관리 등 여러 어플리케이션 분야에 적용될 수 있다.

가. 장애관리

OSI 환경에서 장애가 발생했을 경우, 순간적으로 수십, 수백개의 이벤트가 발생하게 된다. 순간적으로 발생한

수백개의 이벤트를 하나하나 분석하여 장애 원인을 규명하는 것은 대단히 어려운 일이다. 또한, 이와 같은 장애 조치는 신속히 이루어져야 함으로, 망 관리자는 빠르게 근원 장애를 정확히 분석할 수 있어야 한다. 따라서, 자동화된 모듈이 요구되며, 자동화 모듈의 핵심 기능이 바로 상관관계 구성 및 적용이다. 이벤트 상관관계를 적용함으로써, 망 관리자는 관리해야 할 유효한 이벤트만을 감시하고 조치함으로써, 신속 정확하게 장애에 대처할 수 있다. 이를 정리하면 장애 관리란, 원활한 서비스 제공을 위하여 망에서 발생하는 여러 장애들을 신속히 감지, 분석, 해결하는 기능을 의미하며, 장애 관리의 주요 단계는 다음과 같다. 장애를 인지하는 과정으로 폴링과 트랩이 있다.

수집된 데이터를 바탕으로 장애가 발생한 위치를 찾는 과정이다. 그 방법들은 몇가지 단계로 구성된다. 오류가 발생한 모든 콤포넌트를 감지한 후, 토폴로지 트리 구조를 트레이스하여 원인을 찾는다. 망과 SNMP 툴을 이용하여 장애 위치를 찾는다. 또는 기타 상관관계 기법을 이용한다. 상관관계 기법은 이벤트들 간의 연관관계를 구성하는 것으로써, 장애 관리의 장애 감지 및 식별 단계에 해당된다. 망에서 발생하는 모든 이벤트를 수집하고, 관리 대상이 되는 이벤트만을 처리할 수 있도록 걸러준다. 인공지능 기법을 이용하여 관측된 이벤트들 간의 상관 관계를 구성하여 장애가 발생한 위치를 통신망에서 찾는다.

나. 이벤트 상관관계 분류

(1)인과적 상관관계(Causal correlation)

인과적 상관관계는 비반사적(irreflexive)이며, 추이적(transitive) 성격을 지니고 있으므로, 엄격한 순서(strict order)가 존재한다. 그림1은 인과적 상관관계의 하나의 예를 보이고 있다. 여기서 순번은 원인-결과의 형태를 표현한 것으로 순번12에의하여 다양한 형태의 결과가 일어나는 것을 보이고 있다.

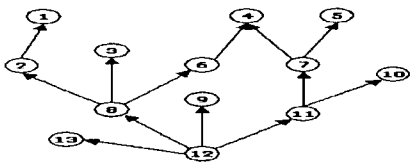

그림1 인과적 상관관계

(2)시간적 상관관계(Temporal correlation)

이벤트 들의 시간 정보를 이용하여 보다 다양하고 구체적인 상관관계를 정의할 수 있다. After, Follows, Proceeds, Before등과 같은 시간적 연산자들을 사용함으로써 보다 다양한 상관관계를 정의하고 활용할 수 있다.(그림2)

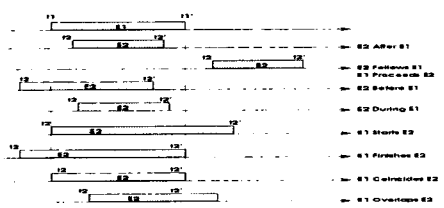

그림 2 시간적 상관관계

(3)이벤트 상관관계 적용 유형

이벤트 상관관계분석 기능의 적용을 위해 처리되어야 할 기능적 요건은 다음과 같다.

중복방지(Compression / De-duplication) : 여러 번 발생한 동일 이벤트를 하나의 이벤트로 표현한다. 인지된 하나의 이벤트만을 관리함으로써 효율적으로 이벤트를 처리한다

계수(Counting) : 유사 이벤트의 개수를 합산한다. 임계치(threshold)를 사용한다.

억제(Suppression) : 우선순위가 높은 상위 이벤트를 대표이벤트로 처리하여 하위 우선순위를 갖는 이벤트를 억제한다.

일반화(Generalization) : 상위 개념의 이벤트로 연결시킨다. 구체적인 장애 이벤트 모두가 감지됐을 때, 일반화된 장애 이벤트(상위 개념의 이벤트)로 대치시킨다. 예를 들어, 라우터/스위치의 모든 포트에서 장애 이벤트가 발생할 때, 라우터/스위치의 장애 이벤트로 처리한.

Temporal Relation : 이벤트 상관관계에 시간을 연관시킨다. 특정 이벤트들이 특정 시간 동안에 발생하면, 그 이벤트들 간에 상관관계가 존재한다.

(4)이벤트 상관관계 처리 기법

이벤트 상관관계 처리 기법은 다음과 같이 여러 방식이 존재한다.

Rule-based Reasoning : 장애를 인지된 후, 그 인지된 사실을 예전의 경험, 또는 학습에 의해 알고 있는 지식과 비교한 한 후, 결정을 내리는 추론 방식이다. 따라서 그 구조를 이해하기 쉽고, 가장 직관적인 방법이다. Rule-based Reasoning 기법을 적용한 시스템을 Rule-based system이라고 하며, Expert system, production system, blackboard system라고도 부른다.

Model-based Reasoning : 국소 지역 망의 모든 정보를 모델로써 구축하고, 모델들 간에 정의된 관계(관계+통신방법)를 이용하여 특정 NE의 장애를 진단하는 기법이다. 이벤트 상관 관계를 모델들 간의 협업 결과로써 알 수 있다. 즉, 망 위상정보, 장비 종류, 라우팅 테이블, 등 국소 지역 망의 모든 정보를 구축하고, 구축된 정보와 IP 패키지가 망을 이동하는 방식을 이용하여 각 NE들의 장애 여부를 판단한다.

Case-based Reasoning : 유사한 문제들은 유사한 해결법이 존재하고, 일정 유형의 문제들이 시간이 지남에 따라 반복적으로 발생하는 경향이 있다. 따라서 한 문제에 적용되었던 해결 법은 유사 문제에서 조금 변경된 후 다시 적용될 수 있다.

Codebook correlation model : 확장되어 가는 망을 관리할 수 있도록 확장성 높은 구조로 되어 있으며, 속도가 빠르다. 또한, 일부 노이즈 이벤트에 대하여 유연하게 대처할 수 있는 모델이다.

3. 통합장애관리 기능구조 제안

이벤트 상관관계 분석에 기반한 통합망관리 기능구조를 그림3과 같이 제안한다. 기본 기능은 이벤트의 수집, 시설정보 관리, 맵관리, Rule 관리, 사용자 관리, 로그 관

리이며, 서비스 기능은 경보관리, 상황관리, 장애이력관리, 정책지원관리, 통계관리, 원인/영향분석, 상황전파 기능으로 구성된다. 본 구조는 다음과 같은 차별화된 기능을 수행할 수 있다.

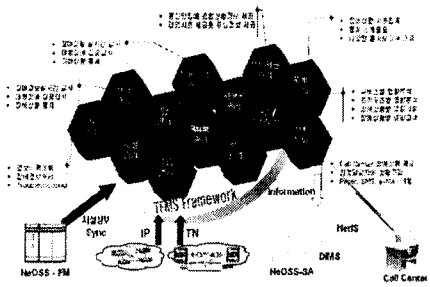

그림 3 통합망관리 기능구조

가. 통합 장애 감시

기존의 장애를 다루는 시스템들과 목적과 역할면에서 뚜렷한 차별성을 가지고 있다. 기존 NMS 시스템은 단일 도메인내 장애관리를 수행하지만 통합망관리 구조는 통합망 관점에서 도메인간 장애관리를 수행하며, 이를 종합망관리 상황실에서 NMS 인터페이스를 통해 통합뷰를 제공한다. 이를 통해 운용자는 자신의 도메인의 장애와 타 도메인의 장애정보와의 연관성을 직관적으로 파악할 수 있으며 경영자 또한 KT 전체 장애상황에 대해 한눈에 파악할 수 있다.

나. 통합 통계의 정확성

기존 통계시스템은 이벤트가 발생하면 해당 도메인을 관리하는 NMS에서 장애가 관리되고 이러한 장애관리 정보를 기반으로 도메인별 장애통계 작성 및 영향고객에 대한 피해회선을 산출하고 재해상황관리 등으로 활용한다. 반면에 통합망관리구조는 도메인간 장애상황 분석을 목적으로 각 NMS에서 올라오는 각종 이벤트 정보를 기반으로 이벤트 상관관계 분석, 중복경보제거 등의 작업을 수행하여 도메인별 장애통계 뿐만 아니라 장애원인으로 인한 도메인별 장애통계 자료 제공이 가능하다. 또한 장애 영향고객 및 시설을 파악할 수 있으므로 영향고객에 대한 피해회선 자료 등 다양하게 가공된 정보를 가공할 수 있다.

다. 통합 실시간 분석집계

그림4는 통합망관리구조 도입 전후 장애로 인한 영향고객 및 피해시설을 분석하는 방안에 대해 도식화하여 나타낸 것이다.

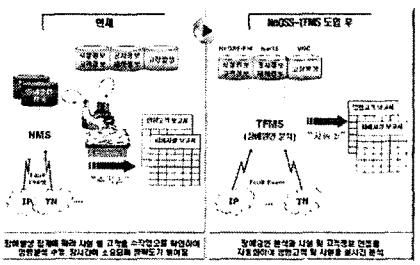

그림 4 장애원인을 통한 실시간 분석집계

도입전 수작업 분석집계는 많은 시간이 소요되며 통신망 운용상황을 실시간으로 파악하는 것을 어렵게 하고 있다. 도입 후에는 장애원인 분석과 시설 및 고객정보 연동을 자동화 함으로써 장애로 인한 영향고객 및 피해시설을 실시간으로 분석이 가능하다. 이는 집중관리가 요구되는 고객에 대해 특별관리가 가능하게 하고 고장상황에 대해서도 고객이 인지할 수 있도록 한다.

라. 빠른 고객응대

기존 고객응대 체계에서는 고객이 고장신고를 접수하게 되면 상담원들은 이를 서비스별 운용자에게 통보하고 각 운용자는 해당 NMS에서 제공하는 기능을 통해 고객의 고장신고를 확인하고 해결한다. 이는 해당 고장에 대해 최소한의 운용자 조치가 이뤄진 후 그 결과를 고객에게 제공할 수 있어 실시간으로 고객 응대하는 것을 어렵게 한다. 시스템 도입 후에는 실시간으로 수집된 장애정보, 공사정보 및 재해성보를 시설 및 고객정보와 연동하여 분석함으로써 영향고객과 피해시설에 대한 정보를 고객의 고장신고가 접수되기 전에 준비가 가능하며 고객의 고장신고 전에 예측된 장애정보 및 고장정보를 미리 고객에게 제공할 수도 있다.

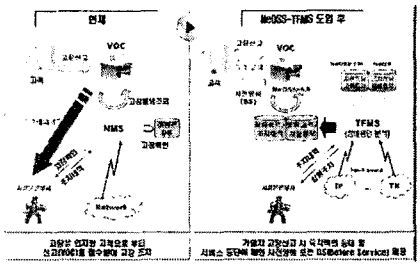

그림 5 고객응대 연계강화

4. 결 론

통합 도메인으로부터 장애정보를 수집하여 상관관계기능을 적용한 장애원인을 분석하기 때문에 장애상황판에 분석된 장애원인에 대해서만 경보를 발생할 수 있다. 운용자들은 발생된 경보에 대한 처리만 수행하게 되어 신속하게 상황을 제어할 수 있다. 또한 장애원인으로 인한 영향고객 및 피해시설을 실시간으로 분석하여 제공함으로 경영자들에게 운용현황을 한눈에 파악하도록 하며 분석된 정보를 고객에게 제공하므로 고객 만족도를 향상시킬 수 있게 된다.

참고문헌

1. A Generic Model for Fault Isolation in Integrated Management Systems, Stefan Katkerl and Kurt Geihs2, 1997
2. Event Relationship Networks: A Framework for Action Oriented Analysis In Event Management, D.Thoenen, J.Riosa, J.L.Hellerstein, 2001
3. Towards Discovery of Event Correlation Rules, L. Burns, J.L. Hellerstein, S. Ma,, D.J. Taylor, 2001
4. A Conceptual Framework for Network Management Event Correlation and Filtering Systems, Masum Hasan, Binay Sugla, Ramesh Viswanathan