

혼합형 상관관계 적용방안에 관한 연구

*이인수, *김진식, *이성우, *이병욱

*KT 시스템연구소

*{gazette, jinsikkim, sungwoo, leebw}@kt.co.kr

A study on Hybrid Alarm Correlation Analysis Scheme

*In-Soo Lee, *Jin-Sik Kim, *Sung-Woo Lee, Byeong-Wook Lee

* KT Network Technology Laboratory

요 약

동기식 전송망에서 발생하는 장애는 장비마다 설정된 구성정보에 따라 여러 종류의 알람을 발생시킨다. 이들 장애 알람은 장애의 근원을 추정 할 수 있는 알람과 장애로 인해 파생된 알람들로 분류할 수 있다. 본 고는 이들 분류체계를 기반으로 근원알람과 파생알람으로 분류하고 알람 상관관계 기법을 적용한 장애관리시스템 구현 사례를 제시한다. 알람 상관관계 분석에 사용된 방법은 시스템의 구현시 계산 복잡도를 최소화하기 위해 Rule 기반의 접근방법 및 Codebook 기반의 접근방법을 접목한 hybrid 상관관계 방법을 적용하였고, End-to-End 회선 장애에 대한 알람 grouping 기법을 사용하였다.

1. 서론

통신망 서비스에 대한 수요 증가로 망의 크기 및 복잡성, 대역폭이 놀랄 정도로 성장했다. 통신망 노드는 다양한 제조업체의 장비들로 구성된다. 이러한 통신망에 장애, 문제가 발생하면 많은 양의 알람 메시지가 발생한다. 이러한 알람 중에 장애(Fault)를 파악할 수 있는 중요한 정보를 지닌 알람을 가려내야만 하는데 이를 위해서 알람 데이터 필터링 기술이 요구된다.

국내에서는 현재 통신 시장 규제완화 정책으로 인해 통신 사업자간 경쟁이 치열하게 됨에 따라 통신망 운용자로 하여금 수준 높은 서비스 제공에 대한 필요성이 생겼다. 알람 상관관계 기술은 망 운용자가 알람[1] 정보 분석, 장애의 위치 및 특성을 파악하는데 도움을 줌으로써 네트워크 서비스 정지 시간을 현저히 줄일 수 있다.

알람 상관관계[4] 기술은 많은 양의 이벤트 메시지를 다루는데 가장 중요한 기술 중의 하나이다. 이러한 상관관계는 불필요한 알람을 필터링 함으로써 운용자에 제공되는 정보의 양을 줄여 주며, 동시에 근본적인 장애원인을 분석하는데 도움을 준다.

알람 상관관계는 장애관리 기능에 의해 수집된 데이터를 기준관점에서 해석하고, 분석하는 과정이다. 이러한 과정들에 의해 장애를 인지하는 시간을 줄일 수가 있고, 서비스 질을 향상시키고, 운영 비용을 줄일 수 있다.

통신망 장애는 서비스에 악영향을 끼치는 비정상적인 상태를 말하며, 장애는 소프트웨어의 에러나 장비의 고장으로 발생한다. 장애관리 목적은 정상적인 네트워크 운영을 방해하는 장애의 영향을 최소화 하는 것이다.

기능적 측면에서 통신망 장애관리는 장애를 감지하고, 격리시키고, 회복시키는 것이다. 장애관리를 자동화하기 위한 알람 상관관계 기법은 운용자가 장애를 감지하고 원인을 분석하는 과정을 시스템화하기 위한 방법으로서 많이 이용되고 있다

장애관리에서 장애 감지, 장애 식별, 원인 분석 등이 상관관계 분석의 목표가 된다. 이를 위해 네트워크에서

발생한 각 알람 간의 관계를 분석하고, 상호간의 관계유형을 구성하여 알람을 통해 장애의 근원을 빠르게 규명한다. 즉, 두 알람 간의 발생위치, 알람 내용, 시간 등을 비교하고 개별 알람들의 특성에 적합한 조건으로 상호 관계를 정의한다. 이 내용을 코드화함으로써 알람에 대한 자동화 처리를 제공한다. 이런 역할을 수행하는 프로세스를 상관관계 엔진으로 구성하는데 본 고에서는 동기식 전송망에 대한 상관관계 시스템을 구축할 때 고려되는 여러 이슈 중 시스템 자원의 효율적인 운용에 도움이 될 수 있는 상관관계 전처리 기법에 대한 방안을 제시하고자 한다.

본고의 2 장에서는 망 관리 관점에서 SDH 망의 특성[2], 상관관계를 위한 SDH(동기식 전송망)에 적용된 grouping 방법, Rule 기반의 접근방법[3] 및 Codebook 기반의 접근방법[5]을 접목한 hybrid 상관관계 방법을 제안하였다. 3 장에서는 상관관계 시스템의 구현 측면에 대해 기술하였으며, 마지막 4 장에서는 결론을 맺도록 한다.

II. Family 기반 그룹핑을 활용한 Hybrid 알람 상관관계 분석 방안

본 논문은 SDH 망에서 Topology 정보를 활용하여 알람을 그룹핑함으로써 기존 상관관계 분석에 비해 개선된 성능과 정확성을 제공하는 방안을 제시한다. 운용자들이 장애관리를 효과적으로 할 수 있도록 하기 위해서는 실제 장애를 유발한 알람(근원알람)과 이로 인해 파생된 알람 (파생알람)으로 구분이 제공되어야 한다. 즉, 모든 는 상관관계 분석 후 하나의 근원알람을 갖는 그룹으로 분류되며, 그 중 근원과 파생알람으로 구분된다. 하지만, 장애 상황별 상이한 알람 발생 패턴과 발생 순서와 일치하지 않은 알람의 수집 환경을 고려할 때 현실적으로 제약이 많다. 또한, 그 소실과 시간 정보의 비동기화 등의 기본적인 문제점도 보유하고 있다. 따라서, 본 논문에서는 SDH 망에서 를 분석하는데 효율적인 그룹핑 방안과 상관관계 분석 방안을 제시한다. 이때, 그룹핑 방안은 SDH 망의 End-to-End 회선은 하나의 서비스를 구성하고, End-to-End 회선 상의 장애는