통합 NMS 환경에 장애 이벤트 관리 방법의 구현

염우섭* · 강희조*

*목원대학교 컴퓨터공학부

Total NMS (Network Management System) Environment for Event Fault Management Method Development

Wu-seob Yeom* · Heau-Jo Kang*

*Division of Computer Engineering, Mokwon University

E-mail : kissyws@mokwon.ac.kr

요 약

오늘날의 네트워크 환경은 다기능, 멀티 벤더(Multi-Vendor)의 분산 환경으로 장비 및 프로토콜의 다양성, 네트워크 구조의 복잡성, 지역적 분산 등 광대하고 복잡한 네트워크로 구성되어 있다. 따라서 기존의 Vendor NMS를 사용한 NMS가 일부 이루어지고 있으나 복잡한 네트워크 구성에 부합하는 신속한 장애 파악이 어려운 실정이다. 본 논문 에서는 복잡하고 다양한 멀티 네트워크 환경 에서 이벤트 상관관계 장애관리에 구현기법을 기술하고자 한다.

키워드

이벤트 상관관계, Rule-based Reasoning, 상관관계 Rule, 시차적관계

Ⅰ. 서 론

장애관리는 보편적으로 "장애감시 > 장애인지 >장애 복구조치 > 원인분석 > 문제해결"의 단계로 업무 프로세스를 구성하며 운영자의 기술적인 조치를 제외한 대부분의 영역을 시스템으로 구현하고 있다. 멀티 네트워크 환경 에는 많은 양의 네트워크 알람이 발생하여 실제로 발생한 개별 event들 로부터 주요 event 인지를 구별 하는데 어려움이 있다. 또한, Event의 발생시간에 차이로 중요한 event 을 너무 늦게 알거나 모르고 지나칠 수 있는 문제가 있다.

동시에 여러 알람이 발생할 경우 분석에 오류를 할 가능성도 있으며 다수의 event가 아닌 한 event를 가지고 판단할 경우 나중에 발생한 event가 진짜 원인(Root Cause)이 되어 장애원인 판정에 오류를 범할수 있다. event에 유기적인 관계를 규명하는데 어려움이 있기 때문에 네트워크의 현재 상태와 추세(Trend)를 예측하는 데는 운영자에 노력이 필요하다. 이상의 문제들에 요구되는 것은 주요 Event를 가시적으로 확인할 수 있어야 되며, 중요 event에 대해 신속하게 파악하고, 원인 분석이 가능하도록 event에 관리 방안이 제공 되어야 한다.

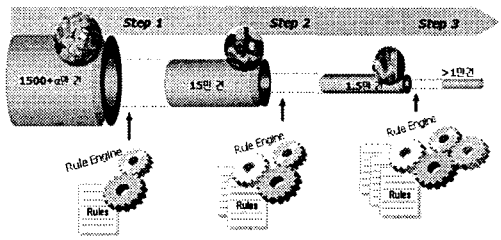

그림 2. Data 처리량 흐름

이를 달성하기 위한 방안에 하나로 이벤트 상관관계 기법을 적용 할 수 있다.

이벤트 상관관계란 Event pattern matching rule을 사용하여 어떤 event에 새로운 의미를 부여하는 실시간 event 분석 과정으로 이벤트 상관관계 기법의 적용은 운용 및 경보처리 속도 향상, 운용자 Knowledge의 부분적인 자동화 (Pattern 자동화) 및 이를 통한 시스템적인 정확성 보장, 운용자의 주요 장애 집중 기반 마련 (중요고장 등), 고장 처리 프로세스의 단계적 표준화 등을 이끌어내기 위한 것이다[1]. 그림 1은 이벤트 상관관계 rule 엔진을 거치면서 최종적으로 관리 대상이 되는 이벤트 수가 감소되는 과정을 나타낸다.

장애관리에서 장애 감지, 장애 식별, 원인 분석 등이 상관관계의 역할 또는 목표가 되며, 이를 위해 네트워크에서 발생한 각 이벤트 간의 관계를 분석하고, 상호간의 관계유형을 구성하여 이벤트를 통해 장애의 근원을 빠르게 규명하는 목적을 갖는다. 구체적으로, 두 이벤트 간의 발생위치, 이벤트 내용, 시간 등을 비교하고 개별 이벤트들의 특성에 적합한 조건으로 상호 관계를 정의함으로써 이 내용을 코드화하여 이벤트에 대한 자동화 처리를 제공한다[2].

본 논문에서는 이벤트 상관관계 처리 시스템에 구성 방안 및 프로세스 내에서 각 모듈별 처리 과정을 논의 한다.

II .Alarm correlation

네트워크 장애관리는 자원의 비정상적인 수행에 대한 검출, 분리 및 수정을 수행하는 관리 기능으로 네트워크상에 발생하는 문제를 찾아내서 수정하고 네트워크의 현재 상태를 나타내는데 필요한 정보를 제공한다.

장애 관리과정은 장애의 식별, 원인 격리 그리고 장애의 수정의 단계로 이루어진다. 장애식별 과정은 회선 장애, 장치 재작동, 호스트로부터의 불충분한 반응과 같은 위험 수준 과 네트워크 이벤트 로깅을 적절한 시간 간격으로 폴링을 통해 확인 한다. 장애 원인 격리는 장애 원인을 식별하면 장애의 우선순위를 결정한다. 이때 네트워크 관리의 범위와 네트워크의 크기를 고려하여 원인을 격리한다. 장애 수정은 격리된 장애에 대한 수정을 수행한다.

Event 상관관계는 문제의 Event 집합으로부터 근원 event를 추적 하고 근원 event에 영향을 받은 event를 선별하는 과정이다. event 상관관계는 현재 시간에 종속적인 객체를 다루고 있다. event 란 상태가 변하는 과정을 지칭하여 시간과 밀접한 관계가 있다. 시간 계념을 가지고 있는 event에 추적은 현재 시간에 종속적일 수밖에 없다. event 객체의 원인을 분석하는 동안 이전 상황이 바뀌어 원인분석을 무의미하게 만들 수도 있다. Correlation 과정은 Context에 매우 종속적이다. (Context의 한 예로 네트워크 토폴로지를 들 수 있다) 일반적으로 correlation 과정은 실시간이며 매우 빨라야 한다. 즉 초당 수백 건 이상의 Event를 처리할 수 있어야 한다. 고장이 발생하지 않는 것이 event correlation 시스템의 일반적인 요구사항이다.

event correlation에서 중요 한것은 근원 이벤트를 추적하고 근원 이벤트와 주변 이벤트 사이에 관계를 규명 하는 것이다. 이벤트들 속에서 근원 이벤트를 추적하는 방법에는 장애발생시 수신되는 이벤트에 대한 공통의 발생유형을 정리하여 코드화 하여 패턴으로 정의 하는 rule 방식이 있다[3]. rule 기반의 접근 패턴에는 "중복방지(Compression/ De-duplication)", 임계치(Threshold) 를 정해놓고 조건에 부합되는 경우 유사 이벤트 개수를 합산하는 "계수(Counting)", 우선순위를 적용하여 상위 우선순위를 갖는 이벤트로 대치하는 "억제(Suppression)", 구체적인 장애 이벤트가 감지되었을 때 일반화된 장애 이벤트로 대치하는 "일반화(Generalization)", 이벤트 발생시간을 이용하는 "시차적 관계(Temporal Relation)" 등으로 분류 및 적용된다.

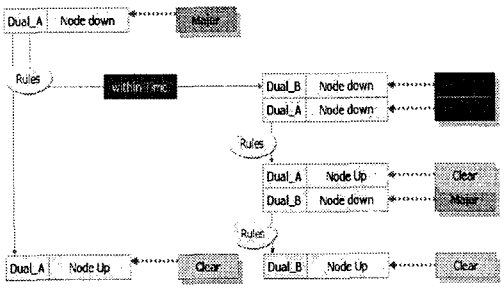

그림 5. 복합적인 Correlation

그림 2는 복합적인 Correlation (Macro Level Correlation) 사례로 각 장애 사이에 rule에 패턴이 적용 방법을 보여준다[4].

event correlation 을 시스템화 하기 위해서는 먼저 각 벤더별 NMS 로부터 이벤트를 수집하는 과정이 필요하다. 수집 된 event는 서로 다른 format 으로 되어 있어 rule 을 적용하는 데는 무리가 있다 그러므로 수집된 이벤트에 표준화 작업이 필요하다. 표준화된 event를 통해 이벤트 사이에 관계 분석 하여 이벤트간 상관관계 패턴을 도출 한다. 도출한 패턴은 상관관계 Rule 기반 구조 및 실제 패턴 매칭에 적용 하여 근원이 되는 이벤트와 주변이벤트를 추출한다.

각 단계를 모듈화 하면 NMS 로부터 이벤트를 수집하는 수집모듈, 수집된 이벤트를 표준화 하는 이벤트 표준화 모듈, 표준화 이벤트를 통해 이벤트 사이에 관계를 규명하는 이벤트 상관관계 모듈, 상관관계를 결과를 사용자에게 전달하는 이벤트 상관관계 모니터링 모듈로 구분한다.

III. Event processing step

이벤트를 상관관계 rule에 적용하는 과정을 도식화 하면 그림3와 같이 나타낸다. 최초 이벤트가 발생되어 이벤트 상관관계를 하기위한 첫 단계는 수집모듈부터 시작 된다. 수집모듈은 하부 NMS 들로부터 발생된 이벤트를 실시간으로 수집하여 이벤트를 표준화하기 위한 최적화 작업을 수행한다. (주석 : 본 논문에서는 NMS로부터 수집한 이벤트를 source 이벤트, 표준화 과정을 거친 이벤

트를 format 이벤트, 상관관계를 통해 나온 이벤트를 이벤트 특성을 고려하여 근원 이벤트와 파생 이벤트라 명칭 하겠다.) 최적화 작업에는 source 이벤트에 대한 garbage discard, 정의된 관리대상 외 event Discard를 한다. 표준화 모듈에서는 source 이벤트를 정의된 표준 format 에 맞게 각 Data 타입에 대한 converting, data field 에 따른 분할, 관리 대상이 아닌 data 삭제 및 통합을 하여 event correlation에 효율성을 높인다.

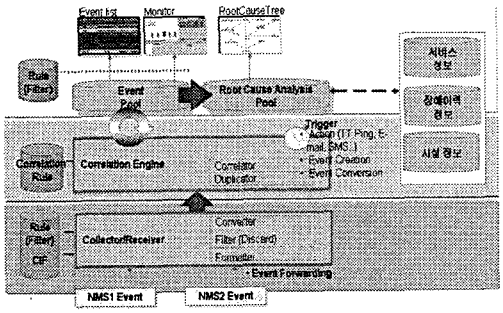

그림 6. Event correlation 구성

event correlation은 format event 패턴을 분석한다. 패턴 분석은 Event의 각 필드 비교를 통해 Rule에 선-정의된 연관성을 부여 하거나, 특정 Event 및 Group에 대해 규정된 Role을 적용하며 이러한 패턴 적용은 Merge, Grouping, Separate 등등에 방법을 사용한다. 상관관계 모니터링 모듈은 GUI 기반 MAP 등과의 연동을 통한 Easy View 환경 구성 하여 근원 이벤트와 파생이벤트를 표현 하고 관리자/사용자에 의해 (CNM Concept) 관련된 Event control과 운용 현황 모니터링 및 통계 처리 정보를 제공한다.

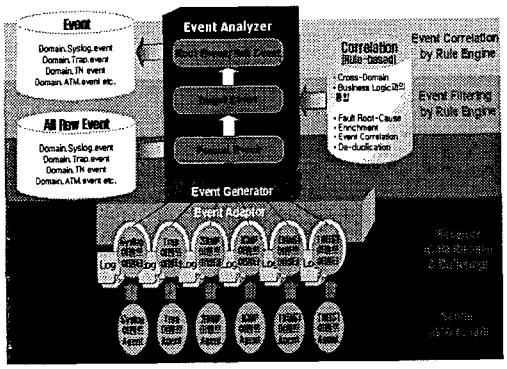

그림 7. Event 순환 흐름

그림 4는 처음 이벤트 발생에서 각 NMS별 이벤트를 Event adaptor에서 수신하여 이벤트를 변환하고 변환한 이벤트를 필터링 하여 format 이벤트를 생성하고 format 이벤트를 각 모듈별 가공을 통해 근원 이벤트와 파생이벤트로 correlation 하는 과정을 나타낸 것이다.

IV. Correlation engine 구성

event correlation 에 핵심은 format 이벤트로부터 근원 이벤트와 파생이벤트에 관계를 도출하는 correlation engine 이다. correlation engine은 실시간 성격을 가지고 있어야 하므로 성능에 대한 이슈가 고려되어야 한다. 또한 rule 적용에 있어서도 correlation engine 에 가변적으로 확정성을 가지고 적용 하도록 해야 한다. correlation engine은rule 이라는 패턴들에 정의 내용을 loading 하여 패턴에 해당하는 정의를 format 이벤트에 할당하고 이런 이벤트를 grouping 하여 근원 이벤트와 파생이벤트에 관계를 도식화 한다. Rule 기반 장애 관리시스템에서 가장 주요한 부분이 Rule 적용 영역이다. Rule 기반 시스템의 구현 완료 후에 Rule이 지속적으로 추가됨으로 인해 Rule 의 확장을 예측하기 어렵다는 것은 고려되어야 할 문제점이다. 시스템에 적용될 Rule 은 도메인 상의 장비, 회선, 서비스 등의 문제로 인해 발생되는 이벤트를 시스템 또는 회선의 관계에 따라 그룹으로 묶고 이들 이벤트 들간의 우선순위(회선계위, 유니트등급, 경보등급, 발생시간 등) 를 설정하며, 이로부터 도출된 정보들을 이용하여 코드를 생성한다. 이를 시스템 상에 Rule로 등록하여 처리과정을 자동화하기 위해 Rule을 구동할 correlation engine에 업로드 함으로써 앞서 정의된 내역과 관련된 이벤트 그룹이 발생되면 Rule 기반의 처리를 통해 운용 로직을 시스템화 하게 된다[1].

rule은 특정 조건에 대해 부합되는 동작을 취하도록 정의된 내용이다. 이렇게 정의된 rule에 나열을 rule list라고 하며 이벤트에 특성 및 네트워크 특성에 따라 성격이 유사한 rule set으로 그룹화 한다. 그룹화한 rule set은 correlation 과정에서 단계적으로 적용하게 된다. rule set에 적용은 시스템 및 운영/유지보수에 구조적으로 관리하도록 하는 장점이 있다. correlation 과정에 rule set에 적용 단계를 Phase 단위로 나누어 보면 Phase 4단계로 구분 된다. Phase 1 단계는 이벤트 수 최적화를 위해 둘 이상의 동일 이벤트 영역을 하나로 표현 하여 반복 수행되어야 하는 correlation 작업을 최소화하고 모니터링 할 이벤트의 수를 최적화 하며 관계 규명에 부적절하거나 선정의 영역을 벗어난 이벤트에 대한 예외처리를 한다. Phase 2 단계는 이벤트 그룹에 대한 correlation 처리할 방법을 시스템화한 Rule로 단일망 및 복합망 으로부터 발생한 무수한 복합적 이벤트 처리의 부분적 자동화 한다. Phase 3 단계는 이벤트의 정보에 대한 이해를 돕기 위해 관련 정보를 추가한다. 이벤트에는 장비, 유니트, 이벤트 유형, 시간, 이벤트 등급 등의 단편적인 정보

만 존재한다. 이벤트 사이에 정확한 관계 규명을 위해서는 각 네트워크 특성을 모두 포함하는 장비유형, 장비개수, 장비로부터 발생되는 장애의 유형 등에 대한 정보를 종합하여 비교 하여야 하며 이런 부가정보에 대한 연결을 한다. Phase 4 단계는 고장 또는 문제의 근원이 되는 최적화된 이벤트 영역으로 집약한다.

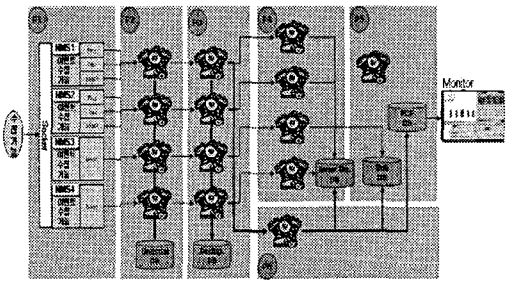

그림 5. correlation 프로세스 구성도

각 단계는 하나의 고유한 프로세스영역 이며 프로세스는 작업 과정이나 작업 결과에 대한 기록을 남기고 결과 정보에 대해서는 다음 단계에 프로세스에 정보달이 이루어 져야한다. 이런 정보들은 최종적으로 시스템 사용자가 열람하고 문제에 이벤트 처리에 대해서 추적하도록 하여 각 프로세스 영역에 결과물에 대한 검증이 가능토록 해야 한다. 프로세스에 내에서 이벤트에 흐름은 전 단계 모듈 또는 프로세스로부터 이벤트를 수신하고 수신 이벤트에 대한 정보 기록 후에 룰 처리 엔진을 통하여 이벤트에 룰 적용 결과 및 필터정보를 추가 기록 한다. 각 프로세스에 유기적인 결합과 정보 전달 과정을 도식하면 그림5와 같은 구성이 된다.

표 1. rule example

```
Rule IXC-DOWN-RULE
Condition
        LINK $link
        LINK-ID $link-id
        LINKSTATE 'Up'
    MESSAGE
        LINK-ID $link-id
        ALARM 'SS7-Link-Failure'
        Action
    Set $link LINK-STATE 'Down'
```

표 1은 rule 정의 예이다. rule은 적용대상이 되는 이벤트 상태에 대한 정의와 적용 이벤트에 대한 작업 내용으로 구성되어 있다.

그림 6. 근원이벤트 도출 Example

V. 결 론

단일망 및 복합망에서 발생한 이벤트 사이에 관계규명을 통해 근원 이벤트와 파생 이벤트를 도출하는 event correlation 기법은 대용량에 시설 및 참고 정보와 이벤트 들을 실시간으로 처리해야 하는 성능관련 이슈가 제기된다. 또한 처리정보에 대용량으로 시스템 리소스 관리에 대한 이슈가 있다. 네트워크에 발달과 복잡성은 단순 이벤트 관리로는 네트워크 관리에 문제가 있으며 더욱더 event correlation 기법을 적용하는 사례는 증가할 것으로 보인다. 향후 서로 다른 네트워크 사이에 rule 도출 및 도출한 rule에 대한 확장성 있는 correlation engine 적용 방안에 대해서 연구하며 성능 및 시스템 리소스에 대한 연구 도 이루어 져야 한다.

참고문헌

[1] In-Soo Lee, Byung-Wook Lee, Dong-Hyeun Shin, Do-Hyun Kim,"The method of Event Correlation in Transmission Network",pp1~3

[2] G. Jakobson, M. Weissman, "Alarm correlation," IEEE Network, Vol.7, Issue 6, pp. 52-59, Nov. 1993.

[3] T.A.M. De Castro, J.M.S Nogueira, "An alarm correlation system for SDH networks," Telecommunications Symposium, 1998. ITS '98 Proceedings. SBT/IEEE InternationalVol. 2, pp.492 497, Aug. 1998.

[4] R. N. Cronk, P. H. Callahan, "Rule-based Expert System for Network Management and Operation: An Introduction," IEEE Network, Vol.12, Issue 5, pp.7-21, Sep. 1988