온톨로지 모델을 활용한 네트워크 장애 탐지 및 진단 방법

한윤선 [1], 서신석 [2], 홍원기 [1]

[1] 포항공과대학교 정보전자융합공학부

[2] 포항공과대학교 컴퓨터공학과

{seon054, sesise, jwkhong}@postech.ac.kr

요 약

인터넷 사용량이 증가함에 따라 서비스 공급자들은 서비스 자원을 효율적으로 관리하기 위하여 복잡하고 거대한 네트워크 인프라를 구축하게 되었다. 이로 인해 네트워크 장치들의 장애의 진단 및 복구는 더욱 어려워졌다. 복잡하고 거대한 네트워크 인프라 구조로 인하여 경보신호의 개수는 급격하게 증가하고 그들 사이의 관계도 매우 복잡해졌다. 따라서 경보신호들을 보고 현재 네트워크에서 발생한 장애의 원인을 신속히 파악하는 것은 매우 어려운 실정이다. 이러한 문제를 해결하기 위하여 본 논문에서는 온톨로지 모델을 활용하여 발생된 경보신호들 사이의 관계를 파악하고 네트워크에서 발생한 장애를 진단하는 방법을 제안한다.

1. 서론

인터넷 기술의 발전 및 인터넷에 접근 가능한 장치들의 보급과 함께 인터넷의 사용량은 꾸준히 증가해왔다. 인터넷 서비스 공급자들은 꾸준히 증가하는 수요에 대응하고 자원들을 효율적으로 관리하기 위해 복잡한 네트워크 시스템을 도입하였다. 이에 따라 네트워크 시스템에서 발생하는 장애들을 관리하는 것은 더욱 어려워 졌다. 장애 관리는 네트워크에서 발생하는 장애 대응에 관한 전반적인 방법들을 지칭하며, 네트워크 모니터링, 장애 진단, 장애 요인 분석, 장애 복구, 장애 기록 등의 세부 활동을 포함한다. 장애 관리를 위해서는 네트워크를 구성하고 있는 장치들의 상태를 파악하기 위한 방법이 필요하다. 현재 각 네트워크 장치의 상태를 파악하는 방법으로 경보신호 (Alarm)를 바탕으로 장애 관리 시스템을 구축하고 있다. 본 논문에서는 온톨로지 모델을 활용하여 경보신호들로부터 의미 있는 정보를 추출하여 장애 진단의 효율을 높이기 위한 새로운 방법을 제안하려고 한다.

2. 관련 연구

경보신호는 각 네트워크 장치에서 의도치 않은 행동들이 탐지 되었을 때 발생하는 신호이다. 하지만, 현재 네트워크는 다양한 장치들이 매우 복잡한 형태로 구성이 되어 있어 모든 경보신호를 수집하고 분석하는 것은 쉬운 일이 아니다. 경보신호의 개수를 줄여 빠르게 장애의 원인을 파악하기 위해 잘 알려진 방법으로는 경보신호 필터링(Filtering)과 연관성을 통한 정보 추출(Correlation)이 있다.

경보신호 필터링 방법은 중복된 신호들을 제거하는데 초점을 맞춘 방법이다. 경보신호들은 다른 형태로 표현되어 있지만 실제로는 동일한 원인으로부터 발생한 경우가 많다. 경보신호 필터링은 이러한 중복 경보신호의 제거를 통해 장애 진단의 효율성을 높인다. 경보신호들의 연관성을 이용한 정보 추출 방법은 발생한 경보신호들이 가지고 있는 정보를 통합하여 새로운 형태의 경보신호를 생성하는 방법을 지칭한다. 이 방법의 경우 다양한 경보신호를 단일 장애 경보로 통합하기 때문에 경보의 개수를 줄이고 통합된 정보를 이용하여 장애의 원인을 쉽게 파악 할 수 있는 장점이 있다. 가장 잘 알려진 방법은 규칙에 기반한 추론 [1], codebook 방법 [2], 그리고 인공 지능을 활용한 방법 [3]이다.

3. 장애 관리기의 구조 및 구성 방법

본 논문에서 제안하는 온톨로지 모델을 활용한 경보신호의 연관성을 통한 정보 추출 기법을 위한 장애 관리기(Fault Manager)는 계층적으로 구성되어 있는 네트워크의 구조를 효율적으로 이용할 수 있도록 설계되었다. 계층적 네트워크 구조를 위한 참조 모델로 ITU-T 에 의해 제안된 TMN 모델[4]을 바탕으로 하였다. 각 장애 관리기는 자신이 속한 계층의 장애 및 하위 계층의 장애들을 관리하는 역할을 수행하게 된다. 이를 위하여 각 장애 관리기는 하위 계층으로부터 장애를 보고 받을 수 있는 인터페이스와 상위 계층으로 장애를 보고 할 수 있는 인터페이스를 가지게 된다. 그림 1 은 각 장애 관리기의 내부 구조 및 상위와 하위 계층의 장애 관리기와 어떻게 연결되는지를 표현하고 있다. 각 계층에 존재하는 장애 관리기는 온톨로지 모델을 가지고 있으며, 온톨로지 모델은 자신이 관리하고 있는 네트워크 요소에 대한 정보를 제공한다. 이러한 구성을 통하여 가장 상위에 존재하는 장애 관리기는 관리 네트워크 전체와 가장 상위 계층과 관련된 장애에 관한 정보를 가질 수 있다.

본 연구는 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU)으로 부터의 지원 (R31-2010-000-10100-0) 및 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원 (No. 2011-0020518)을 받아 수행된 연구임.

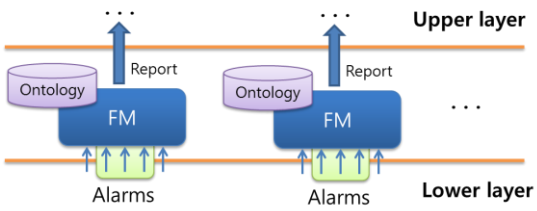

그림 1. 장애 관리기의 구조

4. 온톨로지 모델 설계 및 연관성 추출 방법

온톨로지 모델은 관심 영역(Domain)에 존재하는 개념과 개념들 사이의 관계를 표현하기 위하여 고안되었다. 본 논문에서 온톨로지 모델은 장애 진단에 필요한 개념들과 그들 사이의 관계를 정의하기 위해 사용된다. 장애 진단에 필요한 가장 필수적인 정보는 장치(Device), 경보신호(Alarm), 장애(Fault), 그리고 경보신호 관계자(Alarm Correlator)이다. 그림 2 는 장애 진단을 위해 필요한 온톨로지 모델 내에 존재 하는 개념들의 관계를 보여주고 있다. 장애와 경보신호 사이에는 다양한 특성들이 존재 할 수 있는데, 단일 관계로는 이러한 특성들을 표현 할 수 없다. 이러한 복잡한 관계를 모델로 표현할 수 있도록 경보신호 관계자를 도입하였다.

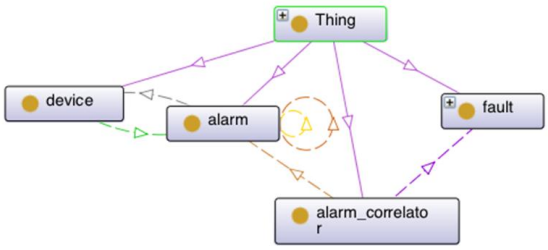

그림 2. 온톨로지 모델 내 클래스 사이의 관계

온톨로지 모델의 큰 장점 중 하나는 추론 규칙(Inference Rule)의 활용이다. 본 논문에서 제안하는 경보신호들 사이의 연관성을 통한 정보 추출 방법의 핵심은 온톨로지 모델과 추론 규칙의 활용에 있다. 제안하는 온톨로지 모델을 활용한 장애 진단 방법은 표 1 의 과정들을 따른다.

1. 빈 온톨로지 모델을 생성
2. 관리 네트워크에서 발생하는 경보 신호를 온톨로지 모델 내에 단일의 객체(Individual)로 할당
3. 단위 시간 동안 수집된 경보신호를 바탕으로 추론 규칙을 적용
4. 추론된 정보를 포함하는 온톨로지 모델 생성
5. 생성된 온톨로지 모델을 상위 계층으로 전송

표 1. 온톨로지 모델을 활용한 장애 진단 과정

5. 실험 설계 및 결과

현재 실제 네트워크에서 수집할 수 있는 자료의 부재로 인하여 실제 경보신호와 장애 사이의 관계를 파악 할 수 없다. 따라서, 실험은 가상의 장애 발생 시나리오를 토대로 하여 설계되었다. 그림 3 은 가정된 시나리오를 도식화한 것이다. a1 과 a2 는 의미적으로 동일한 경보신호, a2 와 a4 가 포함하고 있는 정보는 a3 가 포함 하고 있는 정보와 동일하다. 또한 a2 와 a3 은 손실된 경보신호로 가정하였다.

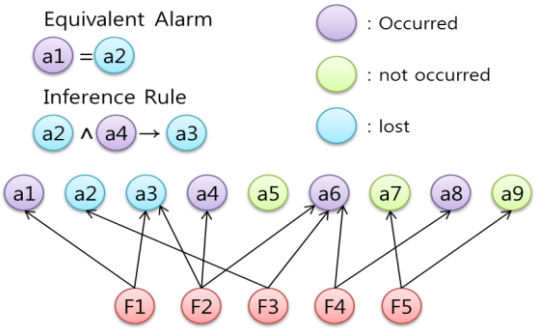

그림 3. 가정된 실험 시나리오

가정된 시나리오를 바탕으로 설계한 온톨로지에 추론 규칙을 적용하여 손실된 경보신호의 관계와 현재 네트워크에서 발생한 장애들을 추론 할 수 있다. 그림 4 는 추론 규칙 적용 후 생성된 온톨로지 모델의 상태로써 유실된 경보신호가 유추되고 장애들이 탐지되었음을 보여주고 있다.

```
| alarm | occurence                                                  | | fault |
| NS:a8 | "1"^^<http://www.w3.org/2001/XMLSchema#int>                | | NS:F1 |
| NS:a6 | "1"^^<http://www.w3.org/2001/XMLSchema#int>                | | NS:F4 |
| NS:a3 | "1"^^<http://www.w3.org/2001/XMLSchema#int>                | | NS:F3 |
| NS:a4 | "1"^^<http://www.w3.org/2001/XMLSchema#int>                | | NS:F2 |
| NS:a2 | "1"^^<http://www.w3.org/2001/XMLSchema#int>                |
| NS:a1 | "1"^^<http://www.w3.org/2001/XMLSchema#int>                |
```

그림 4. 추론 규칙 적용 후 온톨로지 모델 상태

7. 결론 및 향후 계획

본 논문에서는 경보신호 사이의 관계를 통한 정보 추출에 기반한 새로운 네트워크 장애 탐지 방법을 제안하였다. 이를 구현하기 위하여 온톨로지 모델의 설계, 추론 규칙 명세, 그리고 이들을 통합한 실행 가능한 코드를 작성하였다. 또한 가상의 시나리오를 통하여 제안된 방법이 올바르게 작동함을 보였다.

8. 참고문헌

[1] C. S. Chao, D. L. Yang, 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, June 2001.

[2] S. A. Yemini, S. Kliger, and E. Mozes, "High speed and robust event correlation," IEEE Communications Magazine, Vol. 34, No. 5, pp. 82-90, May 1996.

[3] J. F. Huard, “Probabilistic reasoning for fault management on XUNET,” Technical Report, Center for Telecommunications Research, Columbia University, New York, 1994

[4] A. Mayer, S. Kliger, and S. Yemini, “Event modeling with the MODEL language: A tutorial introduction,” 1998. Available: http:/ / versed.smarts.com.