실시간 네트워크 트래픽의 예측을 이용한 성능관리 시스템 연구

°정상준*, 최혁수*, 권영헌**, 임인택***, 권은영*, 김종근*
* 영남대학교 컴퓨터공학과
** 세경대학 컴퓨터정보통신과
*** 미래대학 멀티미디어정보과학과

A Study on Performance Management System Using a Realtime Network Traffic Prediction

°Sangjoon Jung*, Hycksu Choi*, Younghun Kwon**, Inteak Leem***, Eunyoung Kwon*, Chonggun Kim*
* Dept. of Computer Engineering, Yeungnam University
** Dept. of Computer Information & Network, Seakyung College
*** Dept. of Multimedia Information Science, Daegu Mirae College

요 약

네트워크에서 실시간으로 통신 트래픽의 변화량을 감시하고 시계열 분석을 이용해 변화량의 추이를 모형화한다. 트래픽의 변화량을 모형화하게 되면 트래픽에 대한 예측이 가능하게 되므로 트래픽 예측을 이용하여 성능관리를 수행할 수 있다. 본 연구에서는 실시간 트래픽을 이용한 성능관리 시스템에 대해 다룬다. 기존의 성능관리 시스템은 SNMP를 이용한 MIB-II 정보를 바탕으로 하는 분석 방법으로 이는 누적 데이터를 기본으로 하는 관리 방법으로 이상 징후의 판단이 즉각적이지 않았고 또한 모니터링을 수행하기 위해서는 통신 트래픽의 증가를 가져왔다. 대부분의 성능관리 시스템은 단순히 망에서의 트래픽이나 에러율 등을 관리자에게 보고하는 데 그치고 있어 능동적인 성능관리가 이루어지지 않는다. 따라서, 본 논문에서는 실시간 트래픽 감시를 위해 네트워크에 들어오거나 나가는 트래픽의 양을 측정하여 분석하고, 이 정보를 바탕으로 특정 시점 이후의 트래픽 추이를 모형화하여 미래의 트래픽 양을 예측하고, 예측된 정보를 바탕으로 하는 성능관리 시스템에 대해 연구한다. 예측 알고리즘으로는 시계열 분석을 통해 시계열 자료의 예측을 가능하게 하는 알고리즘으로 설계한다. 이 성능관리 시스템을 바탕으로 망 관리자가 전체 통신 네트워크의 부하 상태를 예측하여 신속하게 대응을 할 수 있다.

1. 서론

인터넷을 선두로 전세계적으로 다양한 통신망이 구축, 운용되고 있으며 이들 통신망을 이용하여 다양한 종류의 서비스가 제공되고 있다. 이 통신 서비스에 대해 가입자들은 고품질의 서비스를 요구하고 있으며, 이러한 사항을 충족하기 위해서는 통신망 운용의 관리가 필수적이다[1-2]. 인트라넷에서 네트워크를 효과적으로 관리하기 위해서는 다양한 방법이 있으나, 사용자가 신뢰할 수 있는 성능을 제공하기 위해서는 네트워크 트래픽의 추이를 분석하고 대응하는 것 또한 중요하다. 일반적으로 망관리에 있어서 성능관리 분석은 네트워크 자원들의 운영 형태와 통신 활동의 효율성을 평가하는 일이다[3]. 실제적으로는 네트워크 사용자의 요구사항을 충족시킬 수 있도록 하기 위해 관리자는 망을 효율적으로 관리한다. 네트워크 자원들을 관리하기 위해서는 인트라넷에서의 특정 서비스가 중지되었는지를 관리 시스템이 자동으로 파악함으로써 중단 없는 서비스 구조를 가질 수 있으며, 네트워크의 트래픽 분석을 통해 네트워크 침입 등의 징후에 대비하여 붕괴된 부분을 최대한 빨리 복구하도록 하는 체계가 필요하다.

기존의 연구로는 MIB(Management Information Base) 정보를 활용한 관리 구조나 성능관리에 대한 연구[6-8], SNMP를 이용한 관리 기법 연구[7], MIB-II에서 제공하는 정보를 기준으로 한 성능 분석

파라미터 도출에 관한 연구[8] 등이 있다. 또한 유사 연구로는 누적된 HTTP 패킷을 기반으로 Web 네트워크 트래픽의 양을 측정하는 방법과 실제 전화 교환기 상의 트래픽 이용을 예측 알고리즘이 제시되기도 하였다[9].

효율적인 성능관리의 한 방법으로 트래픽의 양을 측정하는 것이 중요하지만 이보다 진일보한 방법으로 시계열 분석을 통해 특정 시점에서의 트래픽을 예측하는 것도 아주 유용하다[10-11]. 각각의 패킷을 예측하게 되면 TCP, UDP, SMTP, RTP 등의 패킷에 대한 예측이 가능하여 각각의 통신 부하가 서버에 미치는 영향을 예측 가능하게 함으로, 서버를 보호하기 위한 데이터베이스를 종료하는 등의 성능관리를 할 수 있다. 이는 사이버 시위 등과 같은 특정 호스트의 서비스를 방해하는 트래픽 증가를 대비할 수 있어 능동적인 성능관리를 수행할 수 있다는 장점을 가진다. 본 논문에서는 실시간 네트워크 관리 체계 하의 사용자 노드에서 보다 빠른 성능관리를 수행할 수 있는 실시간 트래픽을 예측하고 대응하는 성능관리 시스템을 제안한다.

2. 관련 연구

현재까지의 네트워크 성능관리는 단위 네트워크 및 인터넷을 대상으로 라우터나 게이트웨이에 들어오고 나가는 트래픽의 양, 종류, 특성 등을 분석하여 네트워크의 성능을 파악하고 장애의 위험성을 분석하고 있다. 또한, 각각의 네트워크 장비의 효율성 및 이용율을 관리자에게 알려주고 있으며 이 정보를 토대로 네트워크 관리가 이루어지고 있다.

2.1 SNMP 기반의 성능 관리 시스템

기존의 망 관리 시스템에서의 성능관리 방법은 네트워크 자원 내의 에이전트가 수집한 MIB 정보를 관리국에서 수집하여 사용자 인터페이스를 통해 관리자에게 보여줌으로써 네트워크 관리를 수행된다[1-3]. 그림 1은 SNMP 기반의 망관리 시스템을 보이고 있다.

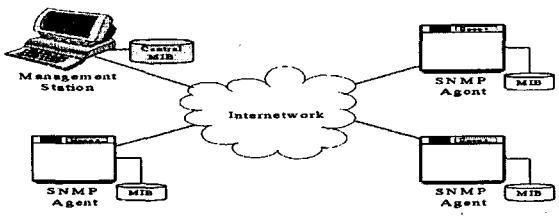

그림 1 SNMP 기반의 망 관리 시스템

이와 같은 방법은 모든 네트워크 구성 요소가 SNMP 에이전트를 탑재하고 있어야 하고, MIB 정보를 갖는 호스트에 한해 관리를 수행할 수 있으며 관리국이 각 에이전트에 주기적인 정보 요청을 하고, 에이전트가 이에 응답하는 형태의 관리 방법이 이루어지고 있다.

2.2 실시간 트래픽 모니터링 시스템

네트워크 관리를 위한 관리국과 에이전트간의 정보 교환으로 야기되는 통신량 증가의 단점을 해소하기 위한 관리방법으로 네트워크 관리국에서 실시간으로 네트워크 내의 패킷들을 받아들여 어떤 정보가 흘러가는가에 대한 감시를 수행한다[10-11]. 그림 2는 실시간 트래픽 모니터링 시스템의 구조와 위치를 보이고 있다.

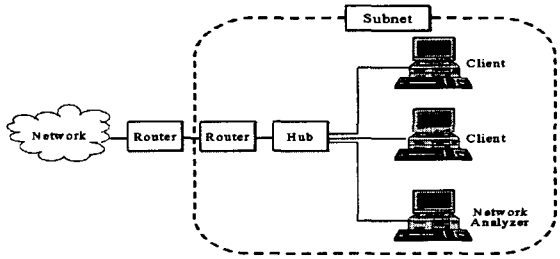

그림 2 실시간 트리픽 모니터링 시스템

이 방법은 특정 서브네트워에 모니터링 시스템을 설치하여, 네트워크 내의 패킷을 읽어들여 분석하고 사용자 인터페이스를 통해 관리자에게 정보를 제공한다.

2.3 시계열 분석을 이용한 트래픽 예측 방법

성능 분석을 수행하기 위해서는 시간의 흐름에 따라 패킷의 양이 변화하는 특징을 가진다. 이 형태의 자료를 시계열 자료라 하고, 이러한 시계열 자료는 시간의 흐름에 따라 일정한 패턴을 나타내는 경우가 많다[4-6]. 즉, 관찰되는 시점에 따라 이산적인 형태의 자료를 얻을 수 있고, 체계적인 분석 과정을 통해 자료의 성격을 파악할 수 있으며, 이를 토대로 특정 시점의 트래픽을 예측할 수 있다.

3. 트래픽 예측을 통한 성능 관리 방안

SNMP 기반의 성능관리 시스템이 가지는 폴링(Polling)의 요청으로 인해 통신량이 증가하는 단점을 보완하기 위해서는 요구 메시지를 최소화하는 방법으로 네트워크 관리가 이루어져야 한다. 네트워크 관리

국에서 실시간으로 서브네트워크 내의 패킷들을 받아들여 어떤 정보가 흘러가는가에 대한 감시를 수행하면 관리의 요구시간 및 수집 시간을 최소화할 수 있다. 뿐만 아니라 이 정보를 바탕으로 트래픽을 예측하게되면 과부하 상태가 발생하기 전에 적절한 조치를 취함으로써 사용자에게 중단없는 서비스를 제공할 수 있는 하나의 방안이 될 수 있다. 예측을 수행함으로써 망 관리자가 통신 네트워크의 부하 상태를 예상할 수 있게 하여 신속하고 예방적인 대응을 수행할 수 있다.

3.1 성능 관리 방안

트래픽은 시간의 흐름에 따라 패킷의 양이 변화하는 특징을 가진다. 패킷의 양은 시간의 흐름에 따라 일정한 패턴을 가지는데 체계적인 분석 과정을 통해 시계열 모형을 얻을 수 있다. 시계열 모형 이용하게 되면 특정 시점 이후의 자료를 예측할 수 있다.

실시간 네트워크 관리의 장점은 누적 데이터를 통한 관리 정보를 얻는 것이 아니라 서브네트워크 내의 패킷에 기반하여 직접적인 관리를 수행할 수 있다는 것이다. 특정 패킷의 양에 의해 트래픽을 예측하게 되면 사용자 입장에서 서비스를 받고 있는 특정 애플리케이션의 사용 여부를 확인할 수 있다. 웹 서버, 메일 서버, 스트리밍 서버 등의 중단없는 서비스가 사용자가 요구하는 최적의 서비스이다. 따라서, 각 패킷의 양을 예측하여 적절한 대응 조치를 강구하는 것이 예측을 이용한 성능관리 방안이 될 것이다. 그림 3은 각 패킷의 양을 모형화하여 예측하고 이에 따른 대응조치를 할 수 있는 방안을 설명하고 있다.

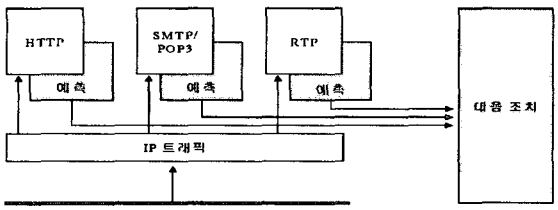

그림 3 예측을 이용한 성능관리 방안

패킷 분석 단계에서 각 패킷을 분류하게 되면 패킷의 양을 시계열 모형으로 형식화하게 되어 각 패킷의 양을 예측할 수 있다. 이는 특정 서버에서 서비스 되는 웹서버, 메일서버, 스트리밍 서버의 부하 여부를 예측 가능하게 함으로 각 서버의 중단없는 서비스를 제공할 수 있으며, 특정 서버가 메일을 통한 바이러스 또는 사이버 시위와 같은 무한정의 트래픽 증가를 가져오는 서비스 방해를 사전에 인지하여 특정 서버를 보호할 수 있는 하나의 성능관리 방법이다

3.2 성능 관리 체계

예측을 이용한 성능 관리 방안은 크게 패킷 수집과정과 예측과정으로 나눌 수 있으며, 패킷 수집은 실시간 모니터링을 수행한다. 예측 과정은 수집된 패킷을 읽어들여 월, 일, 요일별 트래픽을 분류하게 되고 트래픽의 양을 시계열 모형으로 정립하여 특정 시간에 대한 예측을 수행한다. 단순히 예측된 트래픽을 사용자에게 알려주는 것이 아니라, 특정 임계값을 설정하여 임계값 이상의 경우일 때 트래픽이 증가하는 서버를 보호하기 위한 절차를 수행하도록 관리자에게 알려 주도록 한다. 그림 4는 성능관리를 수행할 수 있는 체계를 보이고 있다.

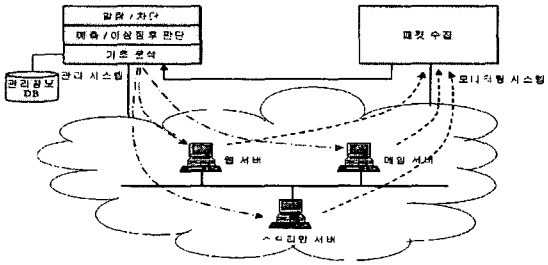

그림 4 예측을 이용한 성능관리 체계

특정 서브네트워크에 위치하는 패킷 모니터링 시스템은 크게 패킷 수집 단계와 패킷 분석 단계로 나눌 수 있으며, 패킷 수집 단계에서는 서브네트워크의 모든 패킷을 받아들여 분석단계로 넘기게 된다. 패킷 분석 단계는 프로토콜별로 패킷을 분류하여 날짜별, 시간별로 분류를 하게 된다. 이 자료를 바탕으로 트래픽을 예측하게 되어, 특정 임계값에 도달할 경우 관리자에게 공지하여 성능 관리를 수행할 수 있도록 한다.

4. 예측을 이용한 실시간 네트워크 성능관리 시스템

예측을 이용하여 성능관리를 수행하기 위해서는 보다 정확한 트래픽의 예측이 필요하며, 이 정보를 관리자에게 알리어 관리자는 적절한 조치를 취할 수 있도록 한다. 서비스를 제공하는 서버는 여러 개의 서버로 구성하는 것이 일반적인데, 가장 중요한 것은 데이터베이스가 강제 종료되는 경우는 서비스 제공에 치명적인 결과를 가져올 수 있다. 따라서, 특정 서버의 트래픽이 임계값을 넘어서 계속적으로 증가할 경우, 관리자가 데이터베이스를 관리하며, 이에 따른 특정 서버를 차단하여 사이버 시위 등과 같은 서비스 방해에 능동적으로 대처할 수 있도록 한다.

4.1 트래픽의 분석 및 예측

성능관리가 이루어지기 위해서는 먼저 트래픽의 양을 예측하는 것이 중요하다. 트래픽을 예측하기 위해서는 먼저 패킷 수집 단계와 분석 단계로 나누어 수행한다. 그림 5는 트래픽의 수집 및 예측 단계를 보이고 있다.

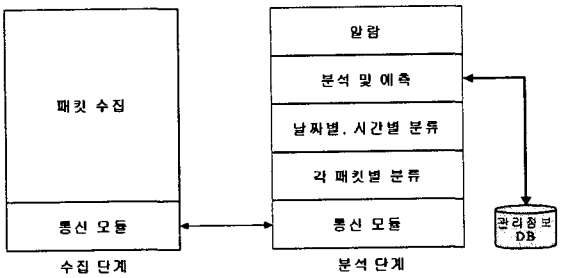

그림 5 트래픽의 분석 및 예측

트래픽의 분석 단계는 성능관리 시스템에서 가장 중요한 과정으로 패킷을 프로토콜별로 분류하고, 이 패킷을 날짜별, 시간별로 분류하여 분석 및 예측 과정으로 넘겨주게 된다. 시계열 모형을 이용하여 특정 시점의 트래픽을 예측하게 되면, 트래픽의 증가에 대한 예방적 관리가 이루어질 수 있다.

4.2 예측을 이용한 성능 관리 시스템

트래픽의 분석 및 예측 단계를 거쳐 네트워크의 상태를 관리자에게 알려주면 관리자는 특정 서버의 중단없는 서비스를 제공하기 위한 관리를 수행한다. 그림 6은 트래픽 예측을 통한 성능관리 시스템의 전체 구조를 보이고 있다.

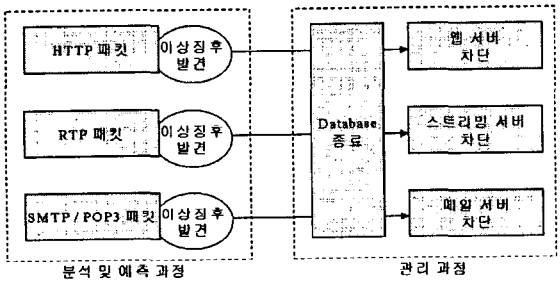

그림 6 트래픽 예측을 이용한 성능관리 과정

각 패킷별로 분류하여 예측을 수행한 후 이상 징후를 발견하게 되면, 특정 서버의 데이터베이스를 보호하는 것이 가장 중요하다. 데이터베이스가 비정상적으로 종료할 경우 서비스 제공에 치명적인 장애를 가져옴으로 데이터베이스 보호와 함께 각 서버를 안전하게 종료하도록 한다. 이는 요즘 많이 발생하는 메일을 통한 바이러스와 사이버 시위와 같은 서비스 방해로부터 안전하게 시스템을 보호할 수 있는 장점을 가진다.

5. 결론

본 논문에서는 트래픽의 예측을 이용한 성능관리 시스템을 제안하였다. 이 성능관리 시스템은 기존의 성능관리 항목을 단순히 관리자에게 보여주는데 그치지 않고, 관리자가 능동적인 관리를 수행할 수 있도록 하여 트래픽의 폭주 등에 대비할 수 있어 서버의 중단없는 서비스를 제공할 수 있다는 장점을 가진다. 또한 데이터베이스의 비정상적인 종료를 막을 수 있어 정보에 대한 손실을 막을 수 있으며, 시스템 자체의 안정성에 크게 기여할 수 있다. 향후 연구 과제로는 보다 정확한 트래픽의 증감 및 이상 징후 예측 방법을 연구하는 방안과 보다 효율적인 성능관리 방안에 대해 연구하는 것이다.

[참고문헌]

[1] William Stallings, "SNMP, SNMPv2, SNMPv3, and RMON 1 and 2", Addison Wesley, 1999.

[2] Mark A. Miller, "Managing Internetworks SNMP", M&T books, 1998.

[3] Kyung Hyu Lee, "An Agent-Manager Scheme for the Integrated Transfort Network Management", IEEE International Conference on Communications, pp.1017-1021, 1999,6.

[4] 최기헌, 이종협, "SAS/ETS를 이용한 시계열 분석과 그 응용", 자유아카데미, 1994.

[5] Yantai Shu, Zhigang Jin, Lianfang Zhang, Lei Wang, "Traffic Prediction Using FARIMA Models", IEEE International Conference on Communications, pp.891-895. 1999,6.

[6] 홍원택, 안성진, 정진욱, "시계열 분석을 이용한 SNMP MIB-II 기반의 회선 이용률 예측 기법", 한국정보처리학회 논문지 제6권 제9호,

[7] 안성진, 정진욱, "SNMP MIB-II를 이용한 인터네트 분석 파라미터계산 알고리즘에 관한 연구", 한국정보처리학회 논문지 제5권 제8호, pp.2102-2116, 1998,8.

[8] 김동수, 정태명, "실시간 네트워크 관리를 위한 SNMP 확장에 관한 연구", 한국정보처리학회 논문지 제6권 제2호, pp.449-458, 1999,2.

[9] 이강원, 김태윤, "효율적인 통신망 설계를 위한 예측 시스템 설계", 한국정보과학회 논문지, 제25권 제1호, pp.76-82, 1998,1.

[10] 정상준, 권영헌, 최혁수, 이정협, 김종근, "실시간 망 관리를 위한 패킷 분석 시스템의 설계 및 구현", 한국멀티미디어학회 춘계학술발표대회 논문집. 2001,5.

[11] 정상준, 권영헌, 최혁수, 김종근, "시계열 분석을 이용한 실시간 네트워크 트래픽 예측 시스템의 설계", 한국정보처리학회 추계학술발표대회 논문집. 2001,10.