韓國 컴퓨터情報學會 論文誌
第11卷 第3號, 2006. 7.

2006-11-3-2-1

이동 에이전트 기반 지능형 네트워크 weather map 프레임워크

강 현 중*, 남 흥 우**

A intelligent network weather map framework using mobile agent

Hyun-Joong Kang*, Heung-Woo Nam**

요 약

오늘날 네트워크는 전 세계적으로 광범위하게 퍼져있으며, 기업 서버에서부터 심지어 가정의 가전제품까지 우리 생활의 대부분의 기기들이 네트워크로 연결되는 상황에 이르렀다. 따라서 실시간으로 네트워크 상태를 파악하고 계획, 관리할 수 있는 프레임워크의 중요성이 날로 증가하고 있다. 네트워크 상황을 실시간으로 파악하고 지속적으로 최적의 상태를 유지할 수 있는 기술은 네트워크 운영의 고도화 측면에서 가장 근본적이며 핵심적인 요소이다. 고속도로 교통관제 센터의 역할과 유사하게 그물처럼 연결된 네트워크를 한눈에 파악할 수 있는 네트워크 상태보고 프레임워크가 효과적으로 구축되어 있다면 바이러스나 웜으로 인한 급격한 트래픽의 증가 또는 서비스 거부공격 등의 긴급 상황에 빠르게 대처할 수 있고, 트래픽 통계 데이터의 분석을 통해서 네트워크의 확장이나 병목구간 등을 미리 파악할 수 있을 것이다. 본 논문에서는 네트워크 트래픽과 성능 상태를 실시간으로 모니터링하고, 동적으로 보고를 해주는 네트워크 상태보고 시스템의 구조를 제시하였다. 이를 위해서 각 네트워크 세그먼트 단위에 이동성을 제공하는 지능형 에이전트를 구축하고 이를 통하여 전체 네트워크의 상태를 효과적으로 제공하는 프레임워크를 제안하였다.

Abstract

Today, Internet covers a world wide range and most appliances of our life are linked to network from enterprise server to household electric appliance. Therefore, the importances of administrable framework that can grasp network state by real-time is increasing day by day. Our objective in this paper is to describe a network weather report framework that monitors network traffic and performance state to report a network situation including traffic status in real-time. We also describe a mobile agent architecture that collects state information in each network segment. The framework could inform a network manager of

• 제1저자 : 강현중
• 접수일 : 2006.04.14, 심사일 : 2006.05.13, 심사완료일 : 2006.06.10
* 서일대학 인터넷정보과 교수 ** 서일대학 정보통신과 시간강사
※ 본 논문은 2005년 서일대학 학술 연구비에 의해 연구되었음

the network situation. Through the framework, network manager accumulates network data and increases network operating efficiency.

▸ Keyword : 모바일 에이전트(Mobile Agent), 네트워크 모니터링(Network Monitoring), Weather Map

I. 서 론

오늘날 네트워크는 전 세계적으로 광범위하게 퍼져있으며, 기업 서버에서부터 가정의 가전제품까지 우리 생활의 대부분의 기기들이 네트워크로 연결되는 상황에 이르렀다. 따라서 실시간으로 네트워크 상태를 파악하고 계획, 관리할 수 있는 프레임워크의 중요성이 날로 증가하고 있다. 네트워크 상황을 실시간으로 파악하고 지속적으로 최적의 상태를 유지할 수 있는 기술은 네트워크 운영의 고도화 측면에서 가장 근본적이며 핵심적인 요소이다.

고속도로 교통관제 센터의 역할과 유사하게 그물처럼 연결된 네트워크를 한눈에 파악할 수 있는 네트워크 상태보고 프레임워크가 효과적으로 구축되어 있다면 효과적인 관리는 물론 바이러스나 웜으로 인한 급격한 트래픽의 증가 또는 서비스 거부공격 등의 긴급 상황에 빠르게 대처할 수 있고, 트래픽 통계 데이터의 분석을 통해서 네트워크의 확장이나 병목구간 등을 미리 파악해서 개선해 나갈 수 있다.

최근 IP-TV와 같은 통합 서비스의 등장으로 데이터 전송량이 급격하게 늘어나고 백본 네트워크 처리성능 또한 급속도로 향상되고 있다. 또한 개인 사용자용 인터넷 접속 서비스에 있어서도 음악이나 동영상 데이터의 송수신 서비스의 일반화는 네트워크 성능에 대한 요구수준으로 이어져 케이블 모뎀이나 기존의 전화회선을 사용한 ADSL (Asymmetric Digital Subscriber Line) 서비스와 같은 광대역 인터넷 접속 서비스가 크게 늘어나고 있다. 따라서 네트워크의 신뢰성, 안정성, 그리고 효율성 보장에 대한 요구도 증가하고 있다.

이를 위해 네트워크 관리자들은 네트워크가 항상 일정한 수준의 전송 효율을 유지할 수 있도록 관리하여야 한다. 아울러 네트워크에 문제가 발생 했을 때, 어디서 발생한 문제이며 원인이 무엇인지 즉시 파악할 수 있어야 한다. 금융권이나 대형 ISP 네트워크처럼 회선단절이나 병목구간이 발생하지 않도록 미리 상황을 예측하고 계획을 세우는 것이 무엇보다도 중요하게 되었다. 이를 위해 네트워크 트래픽의 특성을 파악하고 상태를 실시간으로 점검하는 네트워크 모니터링/측정 기술은 네트워크의 가장 핵심적인 요소라고 할 수 있다.

네트워크 Weather 보고 시스템은 네트워크 상황을 지속적으로 모니터링 하여 문제발생 시 관리자로 하여금 신속한 대응을 가능하게 하는 시스템을 의미한다. 네트워크 weather map 시스템에서 관리자는 에이전트를 이용하여 네트워크 구간별 상태정보를 수집할 수 있고 다양한 분석을 통하여 트래픽이 집중되는 시간대와 상황, 문제가 발생할 소지가 있는 병목구간을 사전에 인지할 수 있게 된다. 결과적으로 문제가 발생하기 전에 시스템의 업그레이드, 회선의 증설과 같은 예방작업을 수행해서 신뢰성 있는 네트워크를 구축할 수 있다 [1][2].

본 논문에서는 이동형 에이전트를 기반으로 네트워크 트래픽과 성능 상태를 모니터링하고, 동적으로 보고하는 네트워크 상태보고 시스템의 구조를 제시하였다. 이를 위해서 각 네트워크에 이동성을 제공하는 지능형 에이전트를 구축하고 이를 통하여 전체 네트워크의 상태를 효과적으로 파악하고 네트워크의 안정적인 운영과 신뢰성 향상을 제공할 수 있는 프레임워크를 제안하였다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 네트워크 측정과 모니터링 핵심 기술에 대해서 상세히 기술한다. 3장에서는 본 논문에서 제안하고 있는 이동형 에이전트 기반 네트워크 weather map 프레임워크 개념과 상세 내용을 기술하며, 마지막으로 4장, 결론에서는 제안된 기술의 응용과 파급 효과, 그리고 앞으로 추가적으로 연구되어야 할 내용을 기술한다.

II. 네트워크 측정과 모니터링 기술

2.1 네트워크 성능 측정

네트워크 트래픽 측정은 트래픽 특성분석, 모니터링, 이상 유무 탐지 등 다양한 목적을 위해 사용 된다. 대형 ISP (Internet Service Provider)에서는 네트워크 용량 설계, 과금 등을 위해서 주로 네트워크 트래픽을 측정하고, 사용자

들은 서비스 성능 모니터링, 최적화, 서비스 협상 등을 위해서, 기업들은 사내 네트워크 설계 및 성능 개선 등을 위해서 사용한다. 현재까지 다양한 측정 방법들이 연구 및 사용되고 있으며 네트워크 측정방식은 크게 네트워크의 트래픽 특성을 파악하는 수동측정 (passive measurement)과 네트워크 상태를 파악하는 능동측정 (active measurement)으로 분류할 수 있다 [3][4].

능동 측정은 네트워크 종단 단말들 간을 경유하는 데이터 패킷이 전송 중에 어떠한 형태의 서비스를 제공받는지를 검사해서 네트워크 상태를 진단하는 목적으로 사용된다. 능동적인 측정은 종단 호스트인 능동 감시자 (active monitor)가 측정패킷 (measurement packet)을 주기적이거나 무작위로 네트워크에 생성하여 측정구간에서 지연시간과 손실 정도를 측정하여 네트워크 상태를 파악하는 방법이다.

능동측정 방식은 테스트 패킷을 생성하기 때문에 네트워크에 부가적인 트래픽을 발생시킬 수 있고 따라서 네트워크의 성능이 저하될 수 있다. 그리고 동적 라우팅 특성 때문에 측정 성능이 실제 네트워크의 성능보다 더 우수하게 또는 더 저하되어 나타날 수 있다는 단점이 있다. 능동측정을 통하여 문제가 되는 경로를 발견해 라우팅 테이블 수정, 라우터 교체, 링크 용량 증대 등과 같은 적절한 조치를 취해 원활한 서비스를 제공할 수 있다.

한편 <그림 1>에서와 같이 인터넷에서 패킷이 전달되는 경로가 항상 동일하다는 보장이 없고 경로에 위치한 시스템들의 버퍼 크기와 처리 능력이 상이할 수 있다는 특징을 갖고 있다. 이러한 인터넷의 비대칭성으로 인해서 단방향 측정이 자주 사용된다. 측정 메트릭으로는 단방향 지연시간 (one way delay), 지연시간 편차(delay variation), 단방향 패킷 손실(one way packet loss), 패킷 손실 패턴 (packet loss pattern) 등이 있다. 이러한 단방향 측정은 능동적인 트래픽 측정에 속한다 [5].

수동측정 방식은 추가적인 패킷 발생 없이 네트워크를 통해 전달되는 트래픽을 수집하고 트래픽의 특성을 분석하는 방식이다. 수동측정 방식은 네트워크의 사용량 변화, 패킷 분석을 통한 네트워크 제어, 트래픽 사용량 측정, 용량 설계, 트래픽 특성 분석 등을 위해 주로 사용된다. 수동측정을 통하여 네트워크 트래픽의 종류와 양을 정량적으로 측정해 네트워크 특성을 정확히 파악하고 최적으로 서비스 할 수 있는 라우팅 정책, 스케줄링 및 버퍼관리 기법 등을 선택할 수 있다. 수동측정 방식에는 SNMP (Simple Network Management Protocol) MIB (Management Information Base)를 통한 링크 트래픽 측정과 NetFlow와 같은 플로우 기반 트래픽 측정방식이 있다. 그러나 수동측정 방식은 사생활 침해 가능성 등의 문제점이 있으며, 대용량 데이터의 분석에 많은 자원을 필요로 하고 네트워크 고속화에 대한 대응이 쉽지 않다는 단점이 있다 [6].

또 다른 관점에서 측정방법은 상시측정과 수시측정으로 나눌 수 있다. 기존에는 트래픽의 상세한 분석을 위한 방법으로 패킷을 수집하고 이를 오프라인으로 분석하는 방법이 많이 사용되었다. 이는 임시로 측정 장비를 네트워크에 장착하여 일정 기간 동안 트래픽을 수집하고 차후 분석을 통해서 트래픽 특성을 분석하는 것으로, 주로 연구나 장기적인 측면의 네트워크 설계에 필요한 정보를 얻기 위해서 사용되었다.

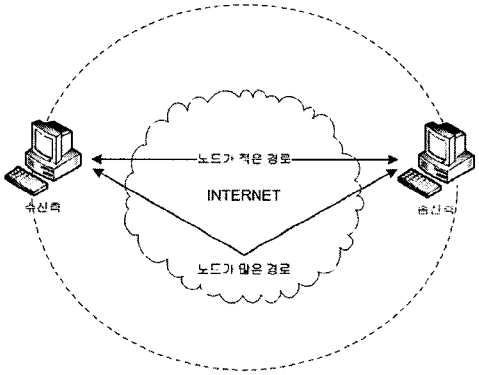

그림 1. 인터넷 시간 관련 파라미터 측정 문제
Fig. 1. A problem of transmission time related measurement

2.2 네트워크 모니터링

트래픽 증가로 인해 네트워크 회선 용량의 부족이나 응답 시간의 저하 등과 같은 문제가 발생할 수 있다. 네트워크 자원 (Network Resource)을 안전하고 효율적으로 이용하기 위해서는 네트워크 상태를 측정할 수 있는 도구가 필요수적이며 네트워크 모니터링은 네트워크 관리를 위해서 네트워크의 트래픽 정보를 수집, 분석하는 것을 말한다.

네트워크 모니터링 시스템이란 OSI (Open System Interconnection) 7계층별로 패킷 및 비트 열을 분석하여 네트워크의 문제점 및 해결책을 찾기 위한 도구이다. (그림 2)에서와 같이 모니터 역할을 하는 프로그램을 네트워크 분석기 (Network Analyser) 또는 네트워크 에이전트 (Agent), 네트워크 프루브 (probe)라고 한다. 네트워크 분석기는 크게 미러(mirror) 포트에 네트워크 분석 하드웨어를 연결해서 모니터링 하는 하드웨어 분석기와, LAN상에서 네트워크 분석 소프트웨어를 사용해서 모니터링 하는 소프트웨어 분석기가 있다. 분석기는 네트워크의 충돌횟수, 길이초과 패킷 개수, 그리고 전송오류가 발생한 패킷의 개수 등과 같은 네트워크의 상태 정보를 인터페이스로부터 얻어내고, 네트워크에 돌아다니는 패킷들을 분석하여 패킷의 개수, 길이별 패킷 분포, 그리고 호스트 통계 정보 등을 수집한다. [7][8]

한편 네트워크 모니터링 시스템은 단순히 네트워크 상태를 수집하는 기능에서 좀 더 적극적인 형태로 발전하고 있다. 특히 네트워크 프로토콜의 취약성을 보완하여 네트워크 생존성과 안정성을 향상 시킬 수 있는 기능을 제공하기도 한다. 인터넷 자체가 TCP/IP라고 할 수 있을 만큼 인터넷 표준 프로토콜인 TCP/IP는 시스템이나 네트워크 분야에서 많이 사용되고 있지만 그 내부를 들여다보면 TCP/IP는 본질적으로 많은 취약성을 가지고 있다는 것을 알 수 있다 [9][10]. 시스템을 패치하고 보안 설정을 한다고 하더라도 네트워크 자체의 취약성에 대한 근본적인 대응에는 한계가 있다. 따라서 이를 악용한 공격 역시 끊이지 않고 있으며 이러한 형태의 공격은 특별한 로그도 남기지 않고 마땅한 모니터링 방법도 없어 인지하기가 쉽지 않다.

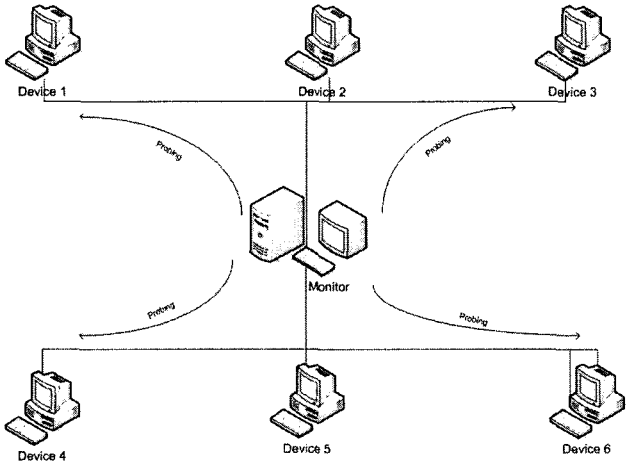

그림 2. 네트워크 모니터링
Fig. 2. Network monitoring architecture

악의적인 공격을 당한 시스템의 경우 대량의 트래픽을 유발하거나 다른 시스템의 정상적인 동작을 방해할 수 있다. 이러한 경우 네트워크를 공유하는 다른 시스템에도 심각한 영향을 미치게 된다. 특히 대량의 패킷이 유발되는 경우 해당 트래픽을 처리하는 스위치나 라우터와 같은 네트워크 장비 또한 심각한 영향을 받게 된다. 이를 대비하고 네트워크 자원을 안전하고 효율적으로 이용하기 위해서는 네트워크의 상태를 측정할 수 있는 도구가 필요하다 [11][12].

이처럼 네트워크 트래픽 모니터링은 네트워크는 물론이고 시스템의 문제를 인지하고 문제의 원인을 발견하여 신속한 대처를 하기 위해서 반드시 필요한 핵심기능이라 할 수 있다. 즉 네트워크의 보안뿐만 아니라 효율성을 고려하여 최상단 핵심 네트워크에서부터 말단 네트워크까지 통합적이고 일관적인 모니터링 체계를 유지하는 것이 필요하다.

III. 이동형 에이전트 기반 네트워크 weather map 프레임워크

본 절에서는 관리노드의 SNMP 정보를 수집하여 관리 네트워크의 노드 상태를 한눈에 파악할 수 있는 네트워크 Weather map 프레임워크에 대해서 기술한다. 네트워크 Weather map 프레임워크에서는 관리 노드에 대한 실시간 상태표시, 노드 상태에 따른 필터링 기능, 노드 정보 표시, 관리노드를 표시하는 네트워크 Weather Map 편집기능, Weather Report 제공 등의 기능을 제공한다.

기존의 SNMP를 기반으로 네트워크를 관리하는 시스템과 달리 본 논문에서 제안하고 있는 시스템은 이동형 에이전트를 사용하고 있다. 이동형 에이전트는 네트워크 상황에 따라 SNMP 에이전트가 설치된 관리 노드간을 이동할 수 있다. 또한 적절한 네트워크 상황 판단을 위하여 이동형 에이전트간에 직접적으로 통신을 수행할 수 있다.

(그림 3)에서 도시하고 있는 바와 같이 프레임워크의 핵심인 중앙 관리 서버에서는 SNMP 매니저가 동작하면서 주기적으로 이동형 SNMP 에이전트가 설치된 노드로부터 관리 정보들을 실시간으로 수집하여 관리 서버에 축적한다. 이렇게 축적된 정보를 관리 서버에 동작하는 여러 가지 CGI (Common Gateway Interface) 모듈들이 웹 서버를 통해서 관리자에게 관리 기능을 제공한다. 또한. 웹을 통해 접속한 관리자에게 관리 네트워크 상태를 손쉽게 파악할 수 있는 인터페이스를 제공함과 동시에 웹을 통하여 Weather Map의 관리를 가능하게 함으로서 관리자에게 네트워크 관리의 편의성을 제공한다.

네트워크 Weather Map 시스템의 동작은 다음과 같다.

관리자는 관리 콘솔에서 웹브라우저로 관리 노드에 대한 네트워크 Weather Map 정보를 관리서버에 요청한다. 관리서버는 네트워크 상태를 웹서버를 통하여 주기적으로 갱신한다.

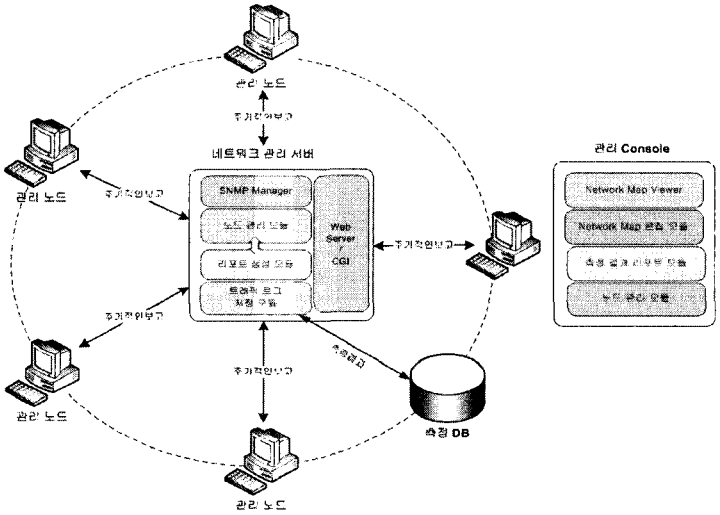

그림 3. Weather map 프레임워크 구성
Fig. 3. The Conceptual architecture of weather map framework

관리자는 관리 콘솔을 통해서 관리 네트워크의 노드를 추가하거나 삭제하고, 정보를 편집하고, 노드를 Network Map 상에서 이동하거나, Network Map을 관리자가 원하는 다른 Map으로 교체 하는 등의 관리 행위를 원격에서 수행한다.

관리서버는 설정파일을 통해서 관리 노드의 리스트를 관리한다. 이 리스트는 관리 서버에서 직접 설정파일을 수정하거나 원격에서 관리 콘솔의 요청에 따라서 수정된다.

관리노드는 설정된 주기에 따라서 관리 노드의 네트워크 상태 정보를 주기적으로 전송한다.

관리 서버는 관리 노드에서 받은 측정결과를 로그에 저장한다. 관리서버는 저장된 로그파일을 주기적으로 측정 DB에 저장한다.

관리서버는 측정 결과가 저장된 로그 파일을 이용하여, 네트워크 상황 보고서를 생성하였다가 관리 콘솔에서 요청하면 웹서버와 웹브라우저를 통해서 제공한다.

관리 콘솔은 관리 노드를 좀 더 자세하게 관찰하기 위해서 노드에 설정된 레벨이나 상태에 따라서 노드를 필터링한 후 노드 상태를 표시할 수 있다.

3.1 Weather map 프레임워크 기능

네트워크 Weather map 시스템은 관리자가 원격에서 관리 콘솔을 통하여 관리 노드의 상태를 파악하고 관리 노드를 표시하는 기능과 네트워크 Weather Map을 편집할 수 있는 기능을 제공한다. 관리 서버는 네트워크 Weather Map의 초기화, 관리 노드의 편집, 노드 상태의 표시 기능

표 2. 네트워크 Weather map 시스템 노드 관리 기능
Table 2. Node management function of network weather map system

	항 목	설 명
네트워크 노드 관리 기능	관리 노드의 관리 정보 표시 기능	관리 노드를 생성할 때 입력한 관리 노드의 관리정보를 표시해주는 기능이다. 관리 노드의 위치, IP, 총 네트워크 인터페이스의 개수, 네트워크 인터페이스 번호, 관리자 정보, 관리자 연락처 등을 표시해 준다.
	관리 노드 관리 기능	관리 서버에 SNMP 매니저를 설치하여 SNMP 에이전트 관리한다. 관리자는 노드 편집기능을 사용하여 SNMP 에이전트 리스트를 편집할 수 있다.
	관리 노드의 설정된 레벨에 따른 필터링 기능	관리 노드를 추가할 때 입력받은 노드의 레벨에 따라서 노드를 그룹화해서 표시할 수 있다.
	관리 노드의 대역폭 사용률에 따른 필터링 기능	관리 노드의 네트워크 인터페이스 상태에 따라서 노드를 다섯 단계로 구분해서 필터링한 후 표시할 수 있다.

표 1. 네트워크 Weather map 시스템 기능
Table 1. The functions of network weather map system

항 목	설 명
웹 기반 관리자 인터페이스 기능	웹 브라우저를 통하여 관리 노드들의 상태를 쉽고 편리하게 모니터링 할 수 있는 인터페이스 제공 관리 서버의 CGI로 요청을 보내고 관리 서버의 응답 수신
관리노드의 실시간 트래픽 상태 표시 기능	Weather Map상의 관리 노드 상태 정보를 미리 설정된 주기에 따라 갱신 자세한 정보 제공을 위하여 관리 노드의 인터페이스별 트래픽 보고서를 제공 일정 시점부터 현재까지의 트래픽 상황을 그래프로 표시한 상태 그래프를 웹브라우저를 통해서 제공
네트워크 노드 관리 기능	관리 노드 상태 실시간 갱신 기능 관리 노드의 인터페이스(IP)에 따른 트래픽 상태 그래프로 표시 기능 관리 노드의 관리 정보 표시 기능 관리 노드의 설정된 레벨에 따른 필터링 기능 관리 노드의 대역폭 사용률에 따른 필터링 기능
네트워크 Weather Map 관리 기능	관리 노드의 추가 관리 노드의 삭제 관리 노드 정보 편집 관리 노드 위치 이동 및 저장 Weather Map 변경
측정한 트래픽 저장 및 보고서 생성 기능	관리 노드에서 주기적으로 전송하는 트래픽 정보를 로그 파일로 저장 관리 노드의 인터페이스에 따라서 보고서를 생성

을 웹서버의 CGI를 사용해서 제공한다. 관리 콘솔은 관리 노드에 대한 실시간 정보를 표시하고 네트워크 Weather Map에서 관리 노드 정보를 표시 할 수 있는 기능을 제공한다.

관리 노드는 관리서버에서 설정된 주기에 따라 관리 노드의 트래픽 정보를 관리 서버로 전송한다. 측정 DB에는 관리 서버에서 받은 관리 노드에 대한 정보를 에이전트 리스트 테이블로 관리하며 관리 노드의 인터페이스 IP별로 테이블을 생성하여 트래픽 정보를 저장한다. 네트워크 Weather map 시스템의 구성요소별 기능은 (표 1)과 같다.

네트워크 Weather map 시스템은 (표 2)에서와 같이 웹 브라우저를 통하여 네트워크 Weather Map 구성을 관리 할 수 있는 기능을 제공한다. 네트워크 Weather Map 관리 기능은 네 가지 종류가 있다.

첫째, 네트워크 Weather Map 상에서 관리 노드를 추가하고 상태 정보를 표시할 수 있는 기능이다. 관리 노드를 추가할 때는 노드 이름, 노드의 위치, 관리자 연락처, 관리 IP 정보 및 노드에 설치된 네트워크 인터페이스 정보 등 관리 노드 정보에 표시되는 모든 관리 정보를 입력할 수 있다. 또한 관리 노드의 레벨을 설정하며 설정된 레벨에 따라서 관리 노드의 표시 아이콘이 달라진다.

둘째, 관리 노드를 삭제하는 기능이다. 웹브라우저의 관리 인터페이스는 선택된 노드의 정보를 관리 서버의 CGI로 전송하여 측정 DB에 관련된 노드 정보를 삭제할 수 있다.

셋째, 관리 노드의 정보 편집 기능이다. 관리서버는 관리 노드의 이름을 제외하고 관리 노드를 추가할 때 입력했던 정보를 모두 수정할 수 있다. 새로운 IP가 입력이 되면 측정 DB에 테이블을 생성하고 데이터를 입력받으며, 기존에 있던 IP가 지워졌으면 DB 테이블에서 관련된 인터페이스 정보를 삭제한다.

넷째, 관리 노드 이동 메뉴를 선택하면 선택한 관리 노드의 위치 값을 이동할 수 있다. 이동이 끝난 후에 네트워크 Weather Map 상에서 노드의 위치 값을 측정 DB의 노드 정보 테이블에 입력한다.

3.2 Weather map 프레임워크 구조

네트워크 Weather map 프레임워크 구축을 위해서 본 논문에서는 (그림 4)에서와 같이 Weather Map 시스템과 MRTG (Multi Router Traffic Grapher) 시스템, 측정 DB 시스템 그리고 관리 콘솔측 Weather Map 인터페이스 시스템으로 이루어진 구조를 제안하였다. Weather Map 시스템에서는 Map 초기화 모듈, 관리 노드 상태와 그래프 데이터 전송 모듈, 관리 노드 위치 저장 모듈, 관리 노드 편집 모듈, 트래픽 정보를 측정 DB로 저장하는 모듈로 구성되어 있다. Map 초기화 모듈은 최상위 모듈로 설계 되었다. 관리 노드가 편집된 다음에 항상 Map 초기화 모듈이 실행된다.

MRTG 시스템은 SNMP 매니저 시스템을 기반으로 구현되어 있다. 관리 노드 관리 모듈을 이용해 SNMP 에이전트들을 관리하고 트래픽 정보를 수집한다. 수집된 트래픽 정보는 IP별로 로그로 저장한 뒤에 Weather Map 시스템의 일정한 주기의 요청에 의해서 측정 DB에 IP 테이블별로 저장된다. 그리고 네트워크 인터페이스(IP) 별로 보고서를 생성해놓고 Weather Map 시스템에서 요청이 올 때 관리 콘솔의 웹 브라우저를 통해서 제공해준다.

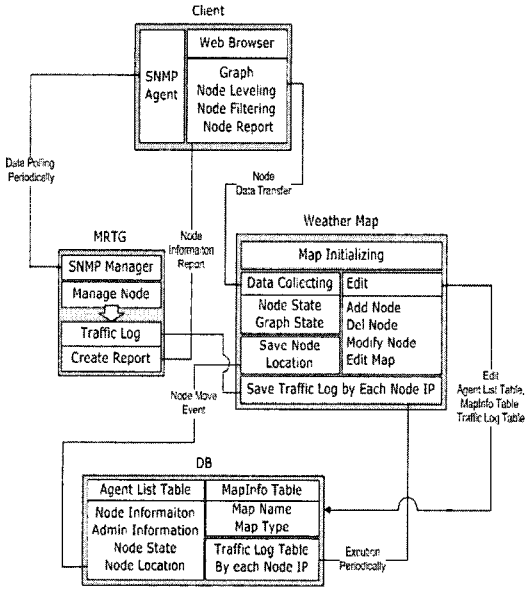

그림 4. Weather map 프레임워크 전체 구성
Fig. 4. The Conceptual architecture of weather map framework

측정 DB 시스템은 관리 노드의 모든 정보와 Weather Map 파일 정보, 관리 노드의 IP별 트래픽 정보를 저장하는 시스템이다. 관리자는 관리 콘솔의 웹 브라우저를 이용하여 관리 서버의 CGI를 통해서 측정 DB에 접근할 수 있다. 또한 MRTG 시스템의 트래픽 로그는 관리 서버의 주기적인 CGI의 호출에 의해서 측정 DB의 IP 테이블로 저장이 된다.

관리 콘솔측 Weather Map 인터페이스 시스템은 웹브라우저에서 동작하며 관리 서버의 Weather Map 시스템과

전송 변수들을 주고받는다. 관리 노드의 상태 표시, 관리 기능의 인터페이스를 제공하며 관리 서버로부터 전송받은 노드 정보를 이용해서 관리 노드의 레벨과 사용률에 따라서 필터링 하는 기능을 제공한다.

3.3. Weather map 시스템 구조

네트워크 Weather Map 시스템은 (그림 5)에서와 같이 크게 세 가지 시스템으로 구성되어 있다. 네트워크 Weather Map 시스템은 관리자에게 네트워크 상황을 쉽게 파악하고 편리하게 노드의 관리 기능을 제공하는 Map Viewer 시스템, 트래픽 로그와 보고서를 만드는 MRTG 시스템, 그리고 중간에서 데이터 전송과 편집, 관리자 요청을 처리하는 Weather Map 시스템으로 구성되어 있다.

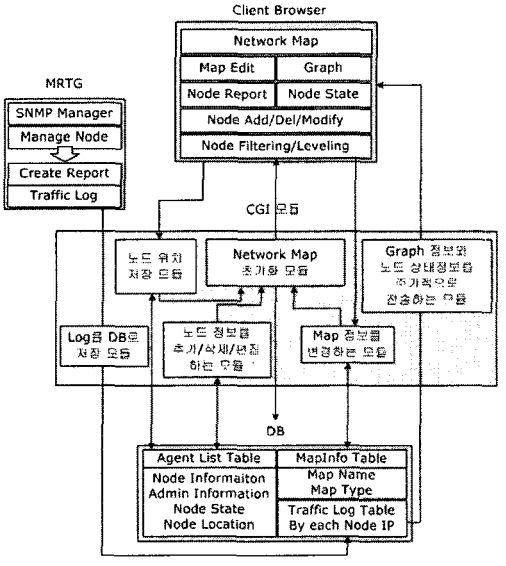

그림 5. Weather map 시스템 구성
Fig. 5. The architecture of weather map system

(그림 5)는 Weather Map 시스템의 모듈간 구성을 자세히 나타내고 있고 Weather Map 시스템의 주요 동작은 다음과 같다.

관리자가 설정한 일정한 주기에 따라서 관리자의 특별한 요청이 없이도 측정 DB에 접근하여 상태정보를 관리 콘솔의 Map Viewer로 전송한다.

SNMP 에이전트를 통해서 SNMP 매니저가 수집한 트래픽 로그 정보를 일정한 시간 주기에 따라 값을 읽어 측정 DB에 저장한다.

관리자가 관리 노드에 대한 추가, 삭제, 정보 수정, 노드 이동 정보 삽입 등의 요청이 있으면 관리자 콘솔의 Map Viewer로부터 관련정보를 받아서 처리하고 결과를 전송한다.

관리자가 Weather Map을 변경하고자 요청 시에 파일 정보를 전송받아 처리하고 결과를 전송한다.

IV. 결론

오늘 날의 네트워크 인프라는 과거와 비교하여 볼 때 규모가 엄청나게 커졌으며 하루하루가 다르게 빠른 속도로 커지고 있다. 이러한 상황에서 네트워크 관리의 중요성은 날이 갈수록 커지고 있다. 네트워크는 고정된 자원이기는 하나 그 활용 정도는 유동적이다. 본 논문에서는 네트워크 상태를 실시간으로 관찰할 수 있는 네트워크 Weather Report 프레임워크를 제안하였다.

본 논문은 전체 네트워크의 유동적인 상황 변화를 즉각 관리자에게 알리고, 네트워크 데이터를 축적하여 차후 네트워크 운영의 효율성을 높이고 이상 상황을 예방하는데 목적이 있다. 본 연구 내용의 결과는 특정 네트워크의 일반적인 상태를 표시할 수 있게 해주며 SNMP 에이전트를 통해서 수집된 관리 노드의 트래픽 정보는 관리 서버에서 모여서 관리자에게 보다 편리하고 보기 쉽게 제공이 된다. 장기간의 데이터가 축적되면 네트워크 트래픽이 몰리는 시점을 예측할 수 있고, 특정 구간 네트워크의 평균 대역폭 활용정도를 파악할 수가 있게 되어 부족한 경우 네트워크 장비를 신설하거나 회선을 증설하는 등의 상황에 따르는 대처를 가능하게 할 수 있다.

참고문헌

[1] Lazarus Vekiarides, David Finkel, NETCAP:A Tool for the Capacity Planning of Ethernet LANs , Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 1998. Proceedings. Sixth International Symposium on , 1998 , pp. 198-203

[2]. Sanjay K.Jha, Bruce R.Howarth, Capacity Planning of LAN Using Network Management , Local Computer Networks, 1994. Proceedings., 19th Conference on , 1994 , pp. 425-430

[3]. K.M.Khalil, J.C.Hand, M.Mariswamy, Analysis and Traffic Characterization of A Wide Area Network , Communications, 1993. ICC '93 Geneva. Technical Program, Conference Record, IEEE International Conference on Volume: 3 , 1993 , pp. 1829-1835 vol.3

[4]. Jerkins, J. L, ; Wang, J. L., A close look at traffic measurements from packet networks, Global Telecommunications Conference, 1998. GLOBECOM 1998. The Bridge to Global Integration. IEEE, Vol.4, pp. 2405-2411, 1998.

[5]. Heidemann, J., Obraczka, K., Touch, J., Modeling the performance of HTTP over several transport protocols, Networking, IEEE/ACM Transactions on, Vol.5, Issue : 5, pp. 616-630, Oct. 1997.

[6]. Crovella, M. E., Bestavros, A., Self-similarity in World Wide Web traffic : evidence and possible causes, Networking, IEEE/ACM Transactions on, Vol.5, Issue : 6, pp. 835-846, Dec. 1997.

[7]. Su, C. L., Lu, C. N., Lin, M. C., Wide area network performance study of a distribution management system, Transmission and Distribution Conference, 1999 IEEE, Vol.1, pp. 136-141, 1999.

[8]. Sedayao, J., World Wide Web network traffic patterns, Compcon 95. Technologies for the Information Superhighway, Digest of Papers., pp. 8-12, 1995.

[9]. 노경택, "TCP/IP 공격에 대한 보안 방법 연구", 한국컴퓨터정보학회, 제10권 제5호, pp217-225, 2005. 11.

[10]. 이홍규, "IPv6 기반 자동화된 공격 대응 도구", 한국컴퓨터정보학회, 제10권 제3호, pp217-257, 2005. 7.

[11]. Xin-You Zhang; Cheng-Zhong Li; Qing-Gui Hu, The network management design integrated with the intrusion detection system, Machine Learning and Cybernetics, 2004. Vol. 1, 26-29 Aug. 2004, pp. 257-262

[12]. Jae-Kyu Chun; Ki-Yong Cho; Seok-Hyung Cho; Young-Woo Lee; Young-Il Kim, Network management based on PC communication platform with SNMP and mobile agents, Distributed Computing Systems Workshops, 2002. July 2002, pp. 222-227

저 자 소 개

강 현 중

1980년 2월 성균관대대학교 수학교육학과 졸업
1986년 2월 연세대학교 대학원 전자계산학과 석사
1996년 2월 성균관대학교 대학원 정보공학과 박사
1979년 11월~1982년 2월 한국과학기술연구소(KIST)연구원
1982년 3월~1989년 2월 한화종합금융(주) 전산팀장
1989년 3월~현재 서일대학 인터넷정보전공 교수
〈관심분야〉 데이터통신, 프로그래밍언어

남 흥 우

2002년 2월 경희대학교 컴퓨터공학과 졸업
2005년 2월 고려대학교 대학원 컴퓨터학과 석사
2005년 9월~현재 고려대학교 대학원 전자.컴퓨터학과 박사과정
2005년 3월~현재 서일대학 정보통신과 시간강사

〈관심분야〉 센서네트워크, RFID