2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

웹 기반 RMON 에이전트 시스템 설계 및 구현

이경남*, 김명균*, 김진수**
*울산대학교 컴퓨터 정보통신공학부
**건국대학교 컴퓨터과학전공
e-mail : mkkim@mail.ulsan.ac.kr

Design and Implementation of a Web-based RMON Agent System

Kyung-Nam Lee*, Myung-Kyun Kim*, Jin-Su Kim**
* School of Computer Engineering and Information Technology, University of Ulsan
**Dept. of Computer Science, Konkuk Univ.

요 약

본 논문에서는 네트워크 계층 및 어플리케이션 계층의 트래픽 분석을 수행할 수 있는 RMON2 MIB를 이용하여 LAN 세크먼트의 트래픽을 분석하는 웹 기반 RMON 에이전트 시스템을 설계하고 구현하고자 한다. 구현된 RMON 에이전트 시스템은 제어기능 설정 모듈과 패킷 수집 모듈 그리고 패킷 분석 모듈로 구성된다. 제어기능 설정 모듈은 관리자가 RMON 에이전트가 수행할 제어기능과 제어 인자들을 설정하는 기능을 수행한다. 패킷 수집 모듈은 네트워크상의 패킷을 수집하고 패킷 분석 모듈은 설정된 제어 기능에 따라 수집된 패킷으로부터 필요한 정보를 얻어 RMON MIB 에 따라 설계된 데이터베이스에 저장한다. 본 RMON 에이전트 시스템은 웹 인터페이스를 사용하여 관리자가 인터넷을 통해 제어기능 설정 및 모니터링할 수 있게 함으로써 대규모 네트워크에서 많은 RMON 에이전트 시스템들의 관리를 용이하게 할 수 있으며, PC 상에서 순수한 소프트웨어만으로 구현되었으므로 고가의 RMON 장비 없이 효율적인 네트워크 관리를 수행할 수 있다.

1. 서론

오늘날 정보화가 급속히 진행되면서 네트워크 사용이 일반화 되고, 각 기업이 인터넷/인트라넷의 열풍 속에서 많은 부분의 업무를 네트워크에 의존하고 있다. 인터넷의 성장과 함께 그 응용 프로그램의 사용이 증가하고 있으며, 네트워크가 대형화, 복잡화 되고 이를 이용한 업무처리가 증가하면서 네트워크상에 많은 트래픽을 유발하게 되고 이로 인한 여러 장애 요인을 발생시키고 있다. 이는 자연히 네트워크 관리의 중요성을 부각시키게 되었고 효율적인 네트워크 관리를 위한 여러 가지 노력들이 진행되고 있다.

현재 네트워크 관리를 위해서 관리자(Manager)와 에이전트(Agent)사이에 정보를 주고 받기 위한 표준 프로토콜로는 SNMP, CMIP 등이 있으며, 관리되어야 할 특정한 정보, 자원을 객체라 하고, 이런 객체들을 모아놓은 집합체를 MIB(Management Information Base)라 하여 계속 새로운 항목들이 정의되어 추가되고 있다.

기존의 네트워크 관리 장비들은 관리되고자 하는 장비마다 SNMP 에이전트가 데몬 프로세스로 동작하고 있어야 하며 이 SNMP 데몬은 관리자의 요구에 따라 자신이 관리하고 있는 MIB 의 관리 객체의 값을 읽어오거나, 변경하는 기능을 수행했었다. 이러한 방식은 주기적인 폴링을 요구하는 번거로운 작업이었으며 네트워크 트래픽을 증가시키는 요인이 되었다. RMON 이 등장하면서 망 관리자는 에이전트를 주기적으로 폴링할 필요가 없어졌으며, 하나의 서브네트워크에 오직 하나만의 RMON 에이전트가 동작하고 있으면 서브네트워크상에 존재하는 모든 단말들의 통계 정보들을 모

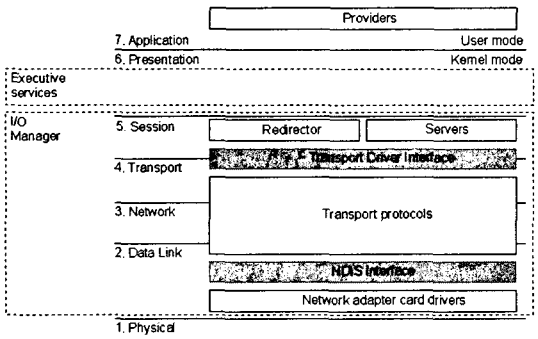
을 수 있으며, 이 외에도 부가가치가 높은 관리 정보를 제공함으로써 관리자의 부담을 상당히 덜어주게 되었다[1]. 그러나 이러한 RMON 에이전트가 탑재된 고가의 라우터나 허브 장비를 구비하는 것은 네트워크 관리자에게 관리 비용에 대한 부담을 안겨 준다.

본 논문에서 제안된 웹 기반 RMON 에이전트 시스템은 기존의 네트워크 관리 표준 프로토콜인 SNMP 대신 HTTP 를 통해 관리되고 정보 교환이 이루어지므로 관리자는 가상의 네트워크 어디에서나 웹 브라우저를 통해서 에이전트 시스템을 제어하고 네트워크 트래픽을 모니터링할 수 있다. 웹 브라우저로부터 관리자의 관리 요구를 받아 들이고 이에 해당하는 값을 관리자에게 제공하는 일은 자바 에플릿이 담당하며, 이는 에플릿이 자바 보안 모델을 따르며 HTTP 를 통해 쉽게 복사할 수 있는 루틴들의 확장 라이브러리를 가지고 있어 네트워크 환경이나 분산환경에 적합하기 때문이다.

본 논문의 2 장에서는 본 시스템 구현을 위한 기반 기술에 대해서 살펴보고, 3 장에서는 본 논문에서 구현한 RMON 에이전트 시스템의 구조, RMON 과 관련된 MIB 항목을 살펴 보았다. 4 장에서는 본 논문에서 구현된 시스템을 실제 LAN 세그먼트상에서 실행한 결과를 보여 본 시스템의 타당성을 검토해 보았다. 끝으로 5 장에서는 이 논문의 기대 효과와 추후 연구과제의 제시로 끝을 맺는다.

2. 네트워크 패킷 수집 기술

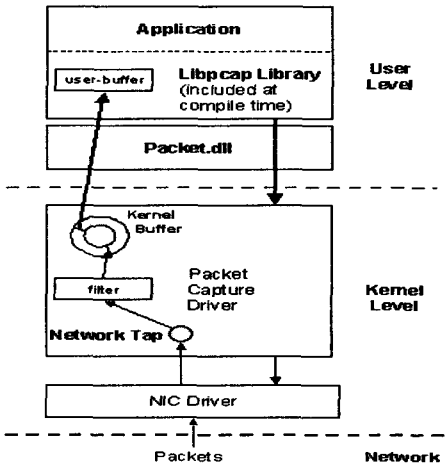
네트워크 상의 모든 패킷들을 수집하여 이를 분석하고 하는 정보를 추출하기 위해서는 직접 NIC(Network Interface Controller)에 접근 할 수 있어야 하는데, Windows OS 환경에서는 NDIS(Network Device Interface Specification)을 통해 NIC 에 직접 접근할 수 있다. NDIS 는 현재와 같이 한 개 이상의 프로토콜 사용이 필요할 뿐 아니라 한 컴퓨터가 여러 개의 네트워크 어댑터 카드를 사용할 경우에 다중 프로토콜을 사용할 수 있는 다중 카드 드라이버 어댑터 역할을 한다.



(그림 1) Windows NT 네트워킹 모델

(그림 1)은 Windows NT 에서의 네트워킹 모델을 보여 주는데, NDIS 는 트랜스포트 프로토콜과 네트워크 어댑터 카드 드라이버 사이에 인터페이스 역할을 하여 하나의 네트워크 어댑터 카드 드라이버가 각각의 프로토콜에 대한 특별한 코드 없이 여러 개의 프로토콜을 지원할 수 있는 것이다.

(그림 2)는 본 논문에서 패킷 수집을 위해서 사용된 가상 드라이버의 구조를 나타내는데, WIN32 어플리케이션과 네트워크 카드 드라이버 사이에 인터페이스 역할을 하며, 패킷 수집과 관련된 라이브러리(Libpcap.lib)를 제공하고 있어 PC 기반에서 네트워크 모니터링 툴을 구현하는데 매우 유용하다[2].



(그림 2) 가상 드라이버 구조

3. RMON 에이전트 시스템 설계

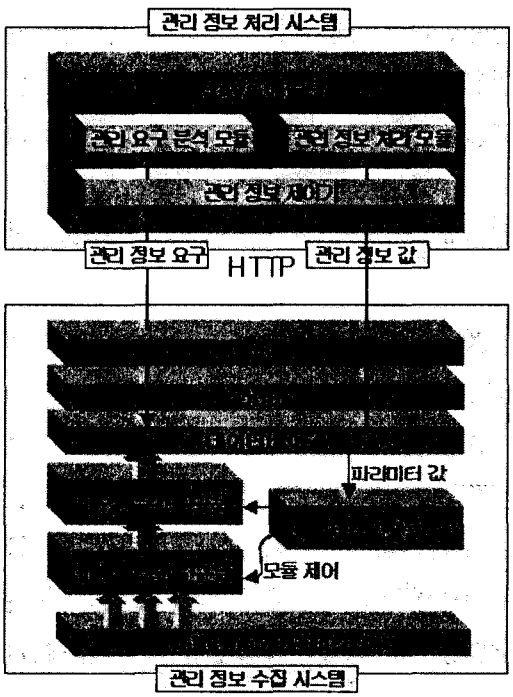
3.1 시스템 전체 구조

(그림 3)에서 보듯이, 전체 시스템은 관리 정보 수집 시스템과 관리 정보 처리 시스템으로 구성된다. 관리 정보 수집 시스템은 관리 항목에 대한 정보를 수집하여 데이터베이스에 저장하는 역할을 한다. 관리 정보 처리 시스템은 자바 에플릿으로 구현되었으며 웹 브라우저로부터 관리자의 관리 요구를 받아 들여 RMON 에이전트의 기능을 제어하고 관리자에게 관리 정보를 제공하는 인터페이스 역할을 한다.

3.2 관리 정보 처리 시스템 구조

관리자에게 관리 정보를 제공하기 위한 에플릿으로서, 관리 요구 분석기, 관리 정보 제이기, 분석 결과 출력기로 구성된다. 에플릿은 현재 RMON 에이전트 시스템이 관리하고 있는 항목들을 라디오 버튼, 콤보 박스등의 인터페이스로 제공하며, RMON 에이전트의 기능을 설정하고 관리 정보를 얻기 위해 관리자에게 친숙한 인터페이스를 제공한다. 관리자는 관리 기능 설정에 의해서 분석된 항목에 대해서 관리 요구를 하게 되고 에플릿은 관리자의 요구를 분석하여 관리 정

보 제어기에 넘겨 준다. 관리 정보 제어기는 관리 요구 항목을 적절한 SQL 쿼리 문으로 변환하여 ODBC 를 통해 데이터베이스에 접근하여 원하는 관리 정보를 가져온다. 이렇게 가져온 정보는 분석 결과 출력기에서 그래프 등으로 관리자에게 네트워크 정보를 제공한다.



(그림 3) 전체 시스템 구성도

3.3 관리 정보 수집 시스템

관리 정보 수집 시스템은 패킷 수집 모듈, 패킷 분석 모듈, 데이터베이스, 제어 모듈로 구성이 된다. 패킷 수집 모듈에서 서브네트워크상의 모든 패킷을 수집하기 위해서 가상 드라이버의 라이브러리를 이용해 네트워크 카드를 "promiscuous" 모드로 설정해 주는데, 이렇게 함으로써 네트워크 카드는 목적지 주소가 자신의 주소가 아니더라도 모든 패킷을 캡쳐하여 (그림 2)와 같이 가상 드라이버 내의 버퍼로 수집하게 된다. 이 수집된 패킷은 분석 모듈의 버퍼로 옮겨져 패킷 분석이 이루어진다.

패킷 수집에서 수집된 패킷들은 패킷 분석 모듈에서 분석을 통하여 RMOM MIB 별로 미리 정의 되어 있는 데이터 베이스에 그 결과 값이 저장되는데, 분석을 행하기 위한 RMON MIB 분석 항목은 다음과 같다.

① statistics 그룹

statistics 그룹에서는 서브네트워크 상의 기본적인 통계 정보를 갖는 항목들을 정의해 놓고 있다[1].

<표 1. statistics 분석 항목>

분석 항목	관련 MIB
이용율	etherStatsPkts, etherStatsOctets
패킷 크기 별 분포율	etherStatsPkts64Octets, etherStatsPkts65to127Octets, etherStatsPkts128to255Octets, etherStatsPkts256to511Octets, etherStatsPkts512to1023Octets, etherStatsPkts1024to1518Octets
패킷 유형 별 분포율	etherStatsBroadcastPkts, etherStatsMulticastPkts, etherStatsPkts

② protocolDist 그룹

각 프로토콜별로 유출입되는 패킷량과 옥텟량을 얻기 위한 항목들을 정의해 놓고 있다[1].

<표 2> protocolDist 분석 항목

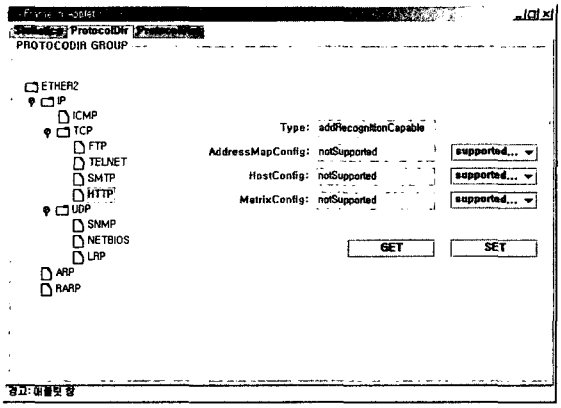
분석 항목	관련 MIB
유출입 패킷량	ProtocolDistControlIndex, ProtocolDirLocalIndex, ProtocolDistStatsPkts
유출입 옥텟량	ProtocolDistControlIndex, ProtocolDirLocalIndex, protocolDistStatsOctets

4. 실험 결과

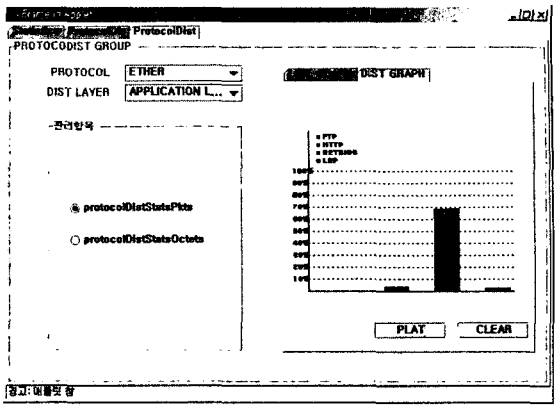
본 시스템은 본교의 서브네트워크에서 관리 분석을 실행했으며 RMON 에이전트 시스템의 OS 환경은 Windows NT 이며, 웹 서비스를 위한 HHTP 데몬은 Windows NT 에서 제공되는 IIS(Internet Information Server) 4.0 을 사용했다. 대상 네트워크 환경은 이더넷이다.

(그림 4)는 웹 브라우저로 본 시스템에 접근하여 얻은 애플릿이다. 현재 에이전트가 분석하고 있는 프로토콜에 대한 인자 값을 설정한다.

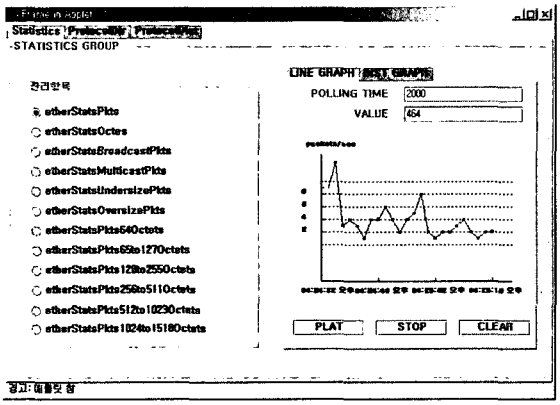
(그림 5)는 관리 항목에 대한 실시간 폴링 결과를 초당 패킷량으로 관리자에게 그래프로 제공되는 것을 보여준다.



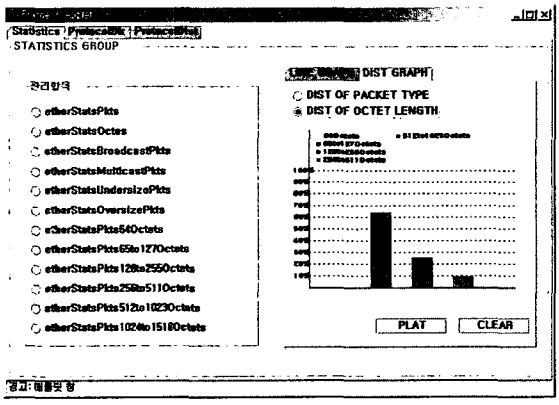
(그림 4) 에이전트의 관리 기능 설정



(그림 7) 어플리케이션 프로토콜별 패킷 비율



(그림 5) 분석 항목에 대한 실시간 폴링 결과



(그림 6) 패킷 크기별 비율

(그림 6)은 누적된 분석 결과로부터 패킷의 크기별 분포율을 그래프로 나타낸 결과이다.

(그림 7)은 현 네트워크에서 사용된 어플리케이션 레벨 프로토콜별로 사용된 패킷량의 비율을 보여준다. 본 네트워크에서는 NETBIOS 의 사용이 가장 많음을 알 수 있다.

5. 결론

본 논문에서는 네트워크 관리를 위하여 별도의 고가의 하드웨어 장비 없이, PC 상에서 순수 소프트웨어만으로도 네트워크 관리 시스템 구현이 가능함을 보였다. 이를 위하여 NIC 접근 기술에 대해서 기술하였으며, 본 시스템을 실제 서브네트워크상에서 관리 분석을 실행해 봄으로써 본 시스템의 타당성을 검증해 보았다. 특히 본 논문에서 기존의 네트워크 관리 프로토콜로 주로 사용된 SNMP 대신 HTTP 를 사용하여 RMON 에이전트 시스템을 설계함으로써 관리자가 네트워크상의 어디에서나 웹 브라우저만으로 쉽게 에이전트 시스템을 관리할 수 있으며, RMON 에이전트 시스템 설계자가 SNMP 데몬과 까다로운 MIB 규정을 따라야 하는 부담을 줄였다. 또한 웹 기반 네트워크 관리는 웹이 가지는 장점을 네트워크 관리에 적용할 수 있어 접근제어, 서버 인증, 자료 암호화등 많은 이점이 있다.

앞으로의 연구과제로는 HTTP 를 이용하여 네트워상에 존재하는 네트워크 에이전트 시스템들의 관리 정보들을 통합하기 위한 방법과 표준이 연구되어야 하겠다.

참고문헌

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

[2] WinDump: TCPdump for Windows http://www.ntop.org/

[3] Gilbert Held, "LAN Management with SNMP and RMON", Wiley Computer Publishing, 1996

[4] 김은성, "RMON2 MIB 을 이용한 네트워크 및 응용 서비스 분석 시스템의 설계 및 구현", 정보처리학술발표논문집, 제 6 권 제 2 호, 1999

[5] W. Richard Stevens, "TCP/IP Illustrated, Volume I", Addison Wesley, 1994

[6] David Perkins and Evan McGinnis, "Understanding SNMP MIBs", Prentice Hall. Inc, 1997