# Network 모니터링을 위한 자동 노드 인식 기법

손민호*, 정인환
한성대학교 컴퓨터공학과
{kylie*, ihjung}@hansung.ac.kr

# A Network Monitoring System with Automatic Node Identification

Minho Son*, In-hwan Jung
School of Computer Engineering, Hansung University

요 약

ARP는 IP 네트워크 상에서 IP 주소를 물리적 네트워크 주소로 대응시키기 위해 사용되는 프로토콜이다. 네트워크에서 데이터를 전송할 때는 컴퓨터간의 물리적 주소를 이용하여 전송하는데 이 물리적 주소는 각각의 랜카드마다 고유하게 갖는 값으로 네트워크에서는 실제로 데이터를 전달할 때 네트워크 카드가 가진 물리적 주소를 이용하여 전달 하지만 소프트웨어 차원에서는 IP 주소라는 것을 사용한다. ARP 프로토콜은 IP 주소를 실질적인 네트워크 어댑터의 물리적 주소와 연관시킬 때 사용되는 것이다. 본 논문에서는 ARP 동보 패킷을 이용한 네트워크 감시 대상 노드들의 정보를 자동적으로 구축하는 기능을 갖는 네트워크 모니터링 시스템을 설계하고 구현한다. 본 네트워크 모니터링 시스템은 ARP 동보 패킷을 분석하여 네트워크 감시 대상 노드들을 인식하고 NETBIOS 모듈을 이용한 노드 이름 확인과 Ping 모듈을 이용한 노드 상태 및 정보를 표시하며 주기적인 업데이트를 통해 노드 정보를 표시하는 기능을 갖는다.

## 1. 서 론

일반적인 네트워크 모니터링 시스템은 모니터링 할 대상인 네트워크 노드들의 IP주소를 목록으로 가지고 있으면서 지속적으로 노드들에 대한 네트워크 사용을 모니터링 한다. 네트워크 모니터링 시스템에서 감시 대상 노드들에 대한 정보는 관리자가 수동으로 입력하는 것이 일반적이다. 이 경우 관리자는 네트워크의 전체 노드들에 대한 정보를 가지고 있어야 한다. 따라서 네트워크의 상황 변화에 실시간으로 대처할 수 없는 문제점이 발생된다. 이러한 문제점을 해결하는 방법으로 ARP 동보 패킷을 이용한다. ARP 동보 패킷은 이더넷에서 네트워크 노드들이 네트워크에 패킷을 전송하기 위해서는 필수적으로 선행되어야 하는 패킷이며, 이 패킷에는 해당 노드의 이더넷 주소와 IP 주소가 담겨있다. 또한 ARP 동보 패킷은 공유 허브(shared hub) 뿐만 아니라 스위칭 허브(switching hub)를 통해서도 모든 노드들에게 전달되므로 모니터링 시스템이 동작하는 PC에서도 해당 ARP 패킷을 수신할 수 있다. 따라서 ARP 동보 패킷을 이용하면 네트워크에 연결되어 있으면서 네트워크 활동이 있는 모든 노드들을 인식할 수 있다.

본 논문에서 제안하는 네트워크 모니터링 시스템은 ARP 동보 패킷을 실시간으로 수집하여 노드의 IP 주소를 인식하고 해당 노드의 정보를 얻는 자동 노드 인식 및 정보 표시 기능을 갖는 네트워크 모니터링 시스템을 설계하고 구현한다. 또한 제안된 네트워크 모니터링 시스템은 노드 정보를 실시간으로 표시하고 주기적으로 노드 정보를 업데이트 하는 기능을 가지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안된 네트워크 모니터링 시스템의 설계 및 구현에 대해 기술하고 3장에서는 네트워크 모니터링 시스템에 대한 실험 및 성능평가에 대해 기술한다. 마지막으로 결론 및 향후 연구 과제는 4장에서 기술한다.

## 2. 설계 및 구현

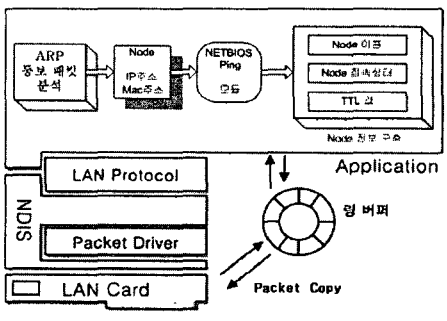


그림 1 프로그램 구성도

본 논문에서 구현된 네트워크 모니터링 시스템은 그림 1과 같이 패킷 드라이버(Packet Driver)[1]와 응용 프로그램으로 구성으로 되어 있다. 연구 개발한 대상은 응용 프로그램 부분이며 ARP 동보 패킷을 실시간으로 수집하여 ARP 패킷 헤더를 분석하

고 네트워크 노드들을 인식한다. 인식된 노드들에 대해서 해당 노드 정보를 표시하고 주기적으로 노드 정보를 업데이트 한다. 응용 프로그램의 흐름도는 그림 2와 같다.

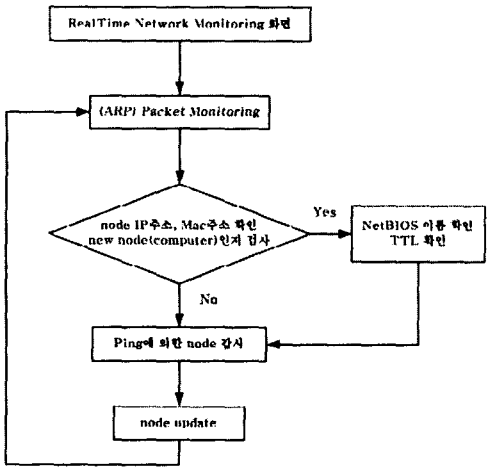


그림 2 프로그램 흐름도

2.1 응용 프로그램(Application)

네트워크 모니터링 시스템은 자신의 노드를 기준으로 네트워크 상에서 전송되는 ARP 동보 패킷을 실시간으로 수집하고 분석한다. 새로운 노드가 인식되면 자동적으로 노드 정보 목록에 추가되고, 주기적으로 노드 정보를 갱신한다. 본 논문에서 제안하고 구현한 내용을 기술하면 다음과 같다.

2.1.1 ARP 패킷 수집 및 분석 기능

응용 프로그램에서는 패킷 드라이버에서 전달된 패킷 중에 ARP 패킷만 수집한다. 수집된 ARP 헤더 정보를 분석하여 ARP_INFO 구조체에 저장한다. ARP_INFO 구조체는 ARP 헤더 정보를 나타내는 구조로서 노드를 인식하는데 필요한 정보만 저장하여 사용되는 구조체이다. 그림 4는 ARP 헤더 정보를 저장한 ARP_INFO 구조체의 내용이다.

```
struct ARP_INFO
{
    static int ArpCount;

    UCHAR ArpOperation[2];
    UCHAR SenderMac[6];
    UCHAR SenderIPAddr[4];
    UCHAR DestMac[6];
    UCHAR DestIPAddr[4];
}
```

그림 4 ARP 정보 구조체

2.1.2 노드 정보 표시 기능

노드 정보 표시 기능은 새로운 노드가 인식되면 자동적으로 노드 정보를 표시하는 기능이다. 노드 정보를 표시하기 위해 노드의 이름을 확인하는 Nbtstat 프로그램과 노드의 상태 정보 및 TTL값을 확인하는 Ping 프로그램을 응용 프로그램의 모듈로 추가하여 응용 프로그램 안에서 Nbtstat와 Ping 기능을 사용할 수 있도록 하였다. 노드 이름은 NetBIOS[2][3] 프로토콜을 이용하여 구현된 NETBIOS 모듈을 통하여 각 노드들의 실제 사용되는 이름을 추출하고, 노드의 상태 정보는 ICMP[4] 프로토콜을 이용하여 구현된 Ping 모듈을 통해 확인된 정보를 각각 다른색의 아이콘으로 표시함으로써 쉽게 노드 상태를 판단할 수 있다. 즉, 녹색은 네트워크에 접속된 상태이고, 회색은 네트워크에 접속되어 있지 않은 상태로 표시하였다. 또한, Ping 모듈을 통하여 추출된 TTL값을 각 노드별로 표시하여 자신의 노드를 기준으로 동일 서브넷의 노드인지 판단할 수 있다.

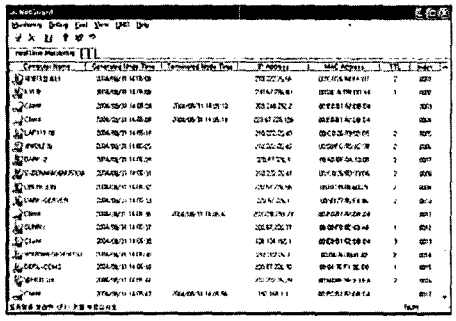

그림 5 프로그램 실행 화면

그림 5에서 보듯이 제안된 네트워크 모니터링 시스템이 관리하는 노드들의 정보에는 노드 이름, 노드 감지 시간(Node Generated Time), 노드 감지 종료 시간(Node Terminated Time), IP 주소, MAC 주소 및 TTL 값 등의 정보로 구성된다.

## 3. 실험 및 평가

네트워크에 연결된 전체 노드들에 대해서 네트워크 모니터링 시스템이 자동적으로 정보를 구축하는데 걸리는 시간을 측정하여 성능을 평가한다.

3.1 실험 방법

실험 환경은 6개의 스위칭 허브로 연결된 local 네트워크에 있는 130대 노드들을 대상으로 하며, 각 노드들은 네트워크 활동이 있는 상태이다. 본 논문에서 구현된 네트워크 모니터링 시스템을 임의의 하나의 노드에 설치하여 130대의 노드들에 대해서 자동적으로 정보를 구축하는데 걸리는 시간을 측정하였다.

3.2 실험 결과 및 분석

대상 네트워크에 대해 자동적으로 정보 구축하는데 걸리는 시간 측정을 테스트한 결과는 그림 6과 같다. Local 네트워크에 속해 있는 노드들은 네트워크 활동 상태이기 때문에 패킷이 발생하지만 특정 노드가 다른 노드에 대한 정보를 요청할 때 ARP 패킷이 발생되므로 ARP 동보 패킷을 이용한 130대 노드들의 정보를 구축하기 위해서는 모든 노드들이 한번이라도 통신을 해야 하므로 본 실험에서는 약 2100초가 소요되었다.

만약 노드들이 사용자에 의해 네트워크 활동이 더 활발해 진다면 local 네트워크에 대한 정보를 수집하는데 소요되는 시간은 기존의 실험 결과보다 현격하게 줄어들 것이라고 판단된다.

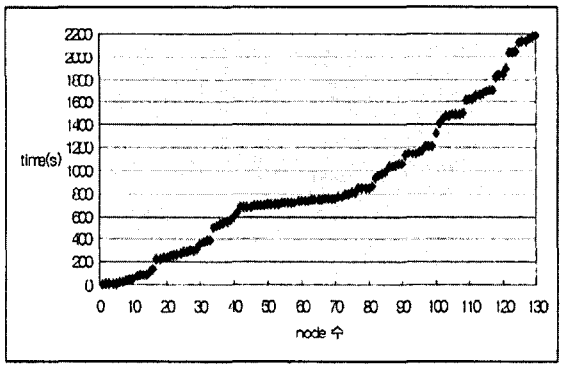


그림 6 노드 정보 구축 시간 분석 결과

## 4. 결론 및 향후 연구

본 논문에서는 ARP 동보 패킷을 실시간으로 수집 및 분석하여 자동 정보 구축 기능을 갖는 네트워크 모니터링 시스템을 설계 및 구현하였다. 구현된 네트워크 모니터링 시스템은 네트워크로 연결되어 있는 노드들의 정보를 자동적으로 구축함으로써 네트워크 진단을 위한 추가적인 비용이 줄어든다.

향후 연구는 네트워크 모니터링 기능의 보완 및 사용자 인터페이스의 개선과 무선 LAN을 대상으로 WinCE 기반 PDA용 네트워크 모니터링 시스템을 개발하는 것이다.

참고 문헌

[1] F. Risso and L. Degioanni, "An Architecture for High Performance Network Analysis", Proceedings of the Sixth IEEE Symposium on Computers and Communications, pp. 686 - 693, 2001.

[2] IETF, Internet Control Message Protocol, RFC 792

[3] IETF, Protocol standard for a NetBIOS service on a TCP/UDP transport: Concept and methods, RFC 1001

[4] IETF, Protocol standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications, RFC 1002