무선랜 트래픽 분석을 위한 측정 시스템의 설계와 구현*

**김해용, **최낙중, **백승민, **최양희, ***이고운, ***김성만, ***정한욱
**서울대학교 컴퓨터공학부, ***KT 컨버전스 연구소
** {hykim, fomula, smbaek, yhchoi} @mmlab.snu.ac.kr
*** {barney, sungmann, hanuk} @kt.co.kr

Design and Implementation for Measurement System to Analyze Wireless LAN Traffic*

**Haeyong Kim, **Nakjung Choi, **Sungmin Baek, **Yanghee Choi,
***Gowoon Lee, ***Sungmann Kim, ***Hanwook Jung
**School of Computer Science and Engineering, Seoul National University
***Conversions Laboratory, KT

요 약

노트북과 PDA 사용자의 증가로 인해 무선랜 사용률 역시 크게 증가하였다. 이러한 변화에 따라 KT에서는 가정이나 공공 지역에서 무선랜 접속이 가능하도록 *NESPOT* 서비스를 시행하고 있다. 하지만 점점 증가하는 트래픽의 양으로 인해 네트워크 관리자는 사용자 그룹과 장소에 따른 이용 패턴 및 무선랜 트래픽 특성을 분석하고 병목현상, 과부하등의 문제점을 파악하여 네트워크를 최적화 할 수 있어야 한다. 본 논문에서는 이를 위한 백본 라우터, AP, 단말에서의 측정 시스템 설계와 구현에 대한 주제를 다룬다. 이러한 측정 시스템을 통한 분석을 통해 사용자 그룹과 장소에 따른 최적의 AP의 위치 및 개수를 선택할 수도 있고, 망 장애 발생에 대한 모니터링도 가능하다.

1. 서 론

초고속 인터넷 망의 보급이 확산되면서 관공서, 기업뿐만 아니라 대부분의 가정에서도 인터넷이 이용 가능하게 되었다. 최근에는 노트북과 PDA 보급의 확산으로 무선랜을 통해 인터넷을 이용하려는 사용자가 급속히 증가하였다. KT는 이러한 사용자들의 요구에 맞추어 *NESPOT* 서비스를 2002년부터 시행하였다. *NESPOT*은 IEEE 802.11b 기술에 기반한 무선랜 서비스로써 가정이나 공항, 터미널, 학교 등의 공공장소에서 무선 인터넷을 이용할 수 있도록 하는 서비스이다 [1]. KT의 *NESPOT* 서비스는 가정과 사람이 많은 공공 장소뿐만 아니라 2004년 9월에는 연구 환경 조성과 U-Campus 시범 구축을 위해 서울대학교에 1500여 개의 AP를 설치, *NESPOT* 망을 구축하여 서울대학교내 어디에서든지 무선 인터넷을 이용할 수 있도록 하였다.

NESPOT 서비스의 이용자가 증가하여 트래픽이 증가하게 되면서 네트워크 관리자는 보다 나은 서비스 제공을 위하여 사용자 그룹과 사용 장소에 따른 *NESPOT* 서비스 이용 패턴 및 무선랜 트래픽 특성을 분석하고 병목현상, 과부하등의 문제점을 파악하여 네트워크를 최적화 할 수 있어야 한다. 이를 위해 네트워크 트래픽의 모니터링과 분석을 위한 측정 시스템 구축의 필요성이 대두되었다.

본 논문에서는 무선랜의 트래픽 특성을 분석하기 위한 측정 시스템의 설계와 구현에 대한 내용을 소개한다. 그림 1은 서울대학교 내의 *NESPOT* 트래픽 분석을 위한 시스템으로써 백본 라우터, AP, 사용자 단말, 인증 서버로부터 네트워크 관련 정보를 획득하는 구조를 단순화시켜 나타낸 그림이다. 백본 라우터에서는 TCPDUMP와 NetFlow 데이터를 이용하고 AP에서는 SNMP를, 단말에서는 TIS (Terminal Information System)을 이용하여 정보를 수집한다. 인증 서버에 기록되는 로그 데이터도 무선랜 트래픽 분석에 있어서 중요한 자료이다.

본 논문의 2장에서는 기존의 무선랜 트래픽 측정과 관련된 연구에 대하여 알아보고, 3장에서는 백본 라우터의 트래픽 측정 시스템의 구조에 대하여 상세히 살펴본다. 4장에서는 그밖에 AP,단말 및 인증서버의 트래픽 측정 시스템 구조에 대해 알아보고 마지막으로 5장에서는 결론을 내린다.

* 본 논문은 2004년도 KT, 두뇌한국21, 국가지정연구실 프로젝트 지원을 받아서 수행되었음.

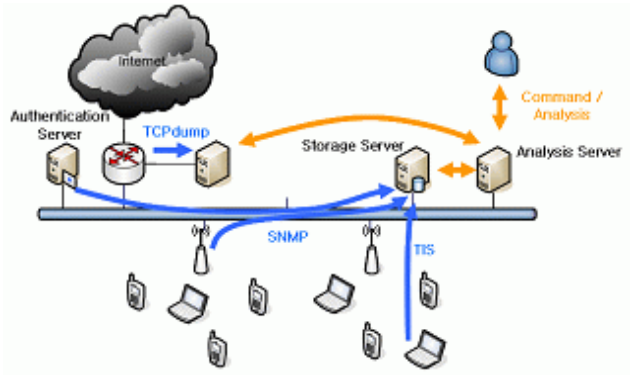

그림 1. 트래픽 분석을 위한 측정 시스템 구조

2. 관련 연구

무선랜 트래픽에 대해서는 이전에도 많은 연구가 있었다. Tang과 Baker는 1992년에 TCPDUMP를 이용해 8대의 노트북 사용자의 트래픽을 측정하였다. 그들은 유선과 무선의 액세스 채널의 교환 회수와 이에 따른 패킷의 지연 시간에 대한 특성을 얻고자 하였다 [2]. 1999년에 그들은 Metricom Ricochet 네트워크의 사용자의 이용 특성에 대해 연구하였다. 이 연구에서 그들은 네트워크의 상태와 이용자의 이동성에 초점을 맞춰 측정 결과의 분석을 시도했다 [3]. 2000년에는 스탠포드 대학교에서 72명의 무선랜 사용자들을 대상으로 하여 이용 특성을 분석하였고 [4], Balachandran외 3명은 SIGCOMM 학회가 열리는 2.5일 동안 학회에 참석한 195명의 무선랜 사용자를 대상으로 무선랜 이용자의 네트워크 이용 패턴과 무선랜 트래픽 특성의 분석을 시도하였다 [5].

이와 같은 연구로부터 알려진 무선랜의 특성은 다음과 같다. 각 AP에 발생하는 트래픽 부하는 AP에 접속중인 사용자의 수와 관계가 없으며 최대 트래픽 부하의 발생은 특정한 단 한 명의 사용자에 의해 발생한다. 다운로드와 업로드의 트래픽의 양은 거의 차이를 보이지 않는다. 웹서핑, 채팅으로 인해 발생하는 트래픽이 대부분이다. 이와 같은 특성 이외의 정량적인 연구 결과 대부분은 측정이 이루어진 지역에 따라 매우 다른 편차를 보이고 있다.

3. 백본 라우터의 트래픽 측정

3.1 트래픽 측정 툴

무선랜의 트래픽을 분석하기 위해 NetFlow[6], Flow-tools[7], FlowScan[8], TCPDUMP[9]를 사용한다. NetFlow는 네트워크의 통계 정보 수집과 QoS 정보 제공을 위하여 Cisco에서 만든 메시지 형식으로 트래픽의 모니터링과 계량화, 서비스와 사용자 모니터링, 네트워크 분석과 계획, 보안 분석 등이 주요한 기능이다. NetFlow 데이터는 Cisco 뿐만 아니라 이외의 많은 밴더들이 생산하는 라우터 혹은 스위치에서 모니터링 및 분석 기능으로 제공 되고 있다. NetFlow는 여러 개의 버전이 존재하는데 이중 버전 5를 이용한다. NetFlow V5 PDU (Packet Data Unit)은 24바이트의 헤더와 한 개 이상의 48바이트의 Flow Record로 이루어진다.

Flow-tools는 라우터나 스위치로부터 받은 NetFlow data와 관련된 작업을 할 수 있는 툴로써, 여러 개의 유용한 응용 프로그램들 포함하고 있다. flow-capture를 통해 NetFlow 데이터를 압축, 저장하고 flow-cat, flow-filter, flow-stat등을 통하여 원하는 기간 혹은 특정 IP address, 특정 application (port) 등에 대하여 여러 가지 통계 값을 얻을 수 있다.

Flow-tools가 트래픽 분석과 관련된 툴인 반면, FlowScan은 모니터링과 관련된 툴이다. 2000년 3월에 Wisconsin-Madison 대학의 Dave Plonka에 의해 발표된 Flowscan은 NetFlow 데이터를 읽어 들여 Round Robin Database (RRD)를 생성한다. 이 데이터는 주기적으로 계속 업데이트가 되며, 여러 가지의 리포트 형식을 통하여 웹에서 모니터링이 가능하다.

3.2 측정 서버의 설계

백본 라우터에서는 설정을 통하여 NetFlow 데이터를 특정 주소로 udp형식으로 보내는 것이 가능하다. 측정 서버가 NetFlow 데이터를 백본 라우터로부터 받으면 flow-capture[7]가 주기적으로 이 데이터를 저장한다. 트래픽 측정과 모니터링은 이렇게 저장된 NetFlow 데이터를 가공하여 이루어진다. 만약 백본 라우터가 NetFlow를 지원하지 않는다면, 측정 지점의 링크를 분할기(splitter)로 나누거나 측정 지점에서 포트 미러링을 통해 측정 서버에서 트래픽을 덤프 받을 수 있도록 하고, 이 트래픽을 NetFlow 형식으로 변환하는 방법을 활용한다. TCPDUMP도 함께 이용하여 라우터를 통과하는 모든 트래픽을 캡쳐하여 가공되지 않은 데이터를 저장해 둠으로써, 이후 추가적인 데이터 분석이 가능하도록 한다. 그림 2는 포트 미러링을 사용하는 경우의 측정 시스템 구조이다.

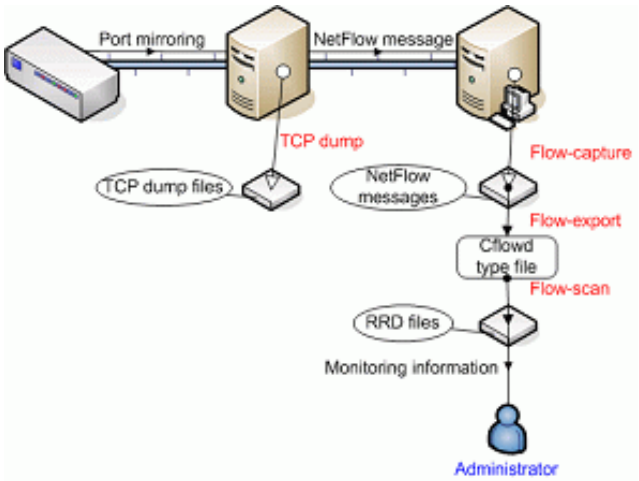

그림 2. 백본 라우터의 트래픽 측정 시스템 구조

NetFlow데이터는 모니터링을 위해 flow-exort[7]에 의해 cflowd[10]형식의 파일로 변환된다. 이것은 스크립트를 사용하여 주기적으로 자동으로 실행되도록 한다. FlowScan은 이렇게 변환된 cflowd 형식의 파일을 읽고 트래픽 모니터링을 위해 Round Robin Database (RRD)[11]를 생성한

다. 트래픽 모니터링은 바이트, 패킷, 플로우 별로 나누어 가능하며 각각의 경우에 프로토콜들(tcp, udp, icmp, etc.)의 사용정도와 응용프로그램들의 사용 정도를 알 수 있다. 또한 총 트래픽에 관한 통계 자료와 사용량이 가장 많은 사용자의 리스트를 보는 것도 가능하다. 이러한 모니터링은 편의를 위해 웹을 통해 어디서든지 가능하도록 되어있다. 그림 3은 일주일간의 시간에 따른 초당 패킷의 수를 응용 프로그램 별로 나타낸 그래프이다.

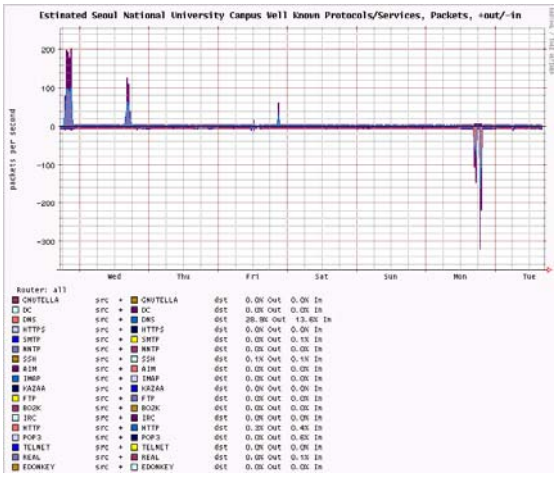

그림 3. 시간에 따른 각 응용프로그램의 초당 패킷 수

저장된 NetFlow 메시지는 또한 flow-cat, flow-print, flow-stat 등의 Flow-tools 내부의 프로그램을 이용하여 트래픽 분석에도 이용된다. 이로부터 바이트, 패킷, 플로우별 평균 트래픽 양과 총 트래픽 양을 알 수 있고 패킷 사이즈 혹은 플로우당 패킷수 등의 분산에 대해서도 조사가 가능하다. 그림 4는 flow-stat을 이용해 1일간의 트래픽의 간략한 통계 정보를 얻어낸 것이다.

```
#  --- ---- ---- Report Information --- --- ---
#
# mode:                 streaming
# capture start:        Sat Sep 18 00:00:01 2004
# capture end:          Sun Sep 19 00:00:00 2004
# capture period:       86399 seconds
# compress:             off
# byte order:           little
# stream version:       3
# export version:       5
# lost flows:           668
# corrupt packets:      0
# capture flows:        326596
#
Total Flows                     : 326596
Total Octets                    : 160818237
Total Packets                   : 892890
Total Time (1/1000 secs) (flows): 1028225667
Duration of data  (realtime)    : 86372
Duration of data (1/1000 secs)  : 86518119
Average flow time (1/1000 secs) : 5597.0000
Average packet size (octets)    : 180.0000
Average flow size (octets)      : 492.0000
Average packets per flow        : 2.0000
Average flows / second (flow)   : 3.7749
Average flows / second (real)   : 3.7813
Average Kbits / second (flow)   : 14.8703
Average Kbits / second (real)   : 14.8954


IP packet size distribution:
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .094 .740 .011 .004 .005 .020 .098 .007 .005 .001 .002 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .004 .000 .000 .000 .000 .000 .000 .000 .000 .000

Packets per flow distribution:
     1    2    4    8   12   16   20   24   28   32   36   40   44   48   52
   .839 .038 .051 .022 .017 .010 .003 .002 .001 .003 .003 .001 .002 .000 .004

    60  100  200  300  400  500  600  700  800  900 >900
   .001 .002 .001 .000 .000 .000 .000 .000 .000 .000 .000

Octets per flow distribution:
    32   64  128  256  512 1280 2048 2816 3584 4352 5120 5888 6656 7424 8192
   .000 .037 .719 .141 .023 .037 .020 .011 .005 .001 .002 .001 .000 .001 .000

  8960 9728 10496 11264 12032 12800 13568 14336 15104 15872 >15872
   .000 .000  .000  .000  .000  .000  .000  .000  .000  .000  .002

Flow time distribution:
    10    50   100   200   500  1000  2000  3000  4000  5000  6000  7000  8000  9000 10000
   .856 .001 .000 .001 .000 .003 .014 .016 .006 .002 .002 .001 .003 .011  .016
```

그림 4. 트래픽의 통계 정보

4. AP, 단말 및 인증 서버의 트래픽 정보

4.1 AP

서울대학교 내에 배포되는 AP의 경우 SNMP 기능을 지원하고 있다. 특정 AP를 실시간으로 모니터링하고 추후 데이터 분석을 위한 자료로서 SNMP 정보를 수집하는 시스템을 구축하였다. 정보 수집 프로그램은 net-snmp 라이브러리를 사용하여 구현하였고 [12] 일정한 주기로 SNMP bulk get 명령어를 사용하여 해당 AP의 SNMP 정보를 수집하고 이 정보를 RRD에 저장한다. 이 때 제공되는 SNMP 정보는 크게 RFC에서 정의되는 공인 MIB 정보와 KT 측에서 추가로 제공하는 사설 MIB 정보로 나눌 수 있다. 공인 MIB 정보는 인터페이스 정보(IF-MIB), IP 정보(IP-MIB), UDP 정보(UDP_MIB), TCP 정보(TCP-MIB)로 세분화되어 저장되고, 사설 MIB 정보는 현재 AP 접속자 수 등의 추가적인 관리 정보를 포함하고 있다.

AP들은 웹을 통하여 등록이 가능하며, 각각 AP의 저장된 정보는 실시간으로 모니터링 하거나 원하는 구간을 지정하여 해당 구간의 통계 정보가 확인이 가능하다. 실시간 정보는 웹 인터페이스를 통하여 1분 간격으로 갱신되어 유선, 무선 인터페이스에 대하여 송수신 데이터 양, 송수신 에러율, 프로토콜별(IP, UDP, TCP) 송수신 패킷 수 등에 대한 그래프를 제공한다. 통계 정보의 경우는 저장된 모든 데이터에 대하여 질의를 통한 지정 구간에서의 측정 결과를 그래프로 확인할 수 있는 인터페이스를 제공하고 있다. 그림 5는 실시간 모니터링 시스템의 예로써 송수신 에러율을 보여준다.

그림 5. 실시간 모니터링 시스템

4.2 단말

네트워크의 인프라에서 얻을 수 없는 단말에 관련된 정보를 분석하기 위해서는 서울대학교 내의 *NESPOT* 서비스 사용자의 단말에 정보 획득을 위한 프로그램을 설치하고, 측정 서버 프로그램과의 통신을 통하여 추가 정보를 획득한다. TIS (Terminal Information System)는 단말이 현재 접속 가능한 AP와 각 AP의 MAC 주소와 그 신호 세기, 전송 실패한 프레임 수, 재전송 횟수, RTS 실패 횟수, FCS (Frame Check Sequence) 오류 횟수 등의 정보 획득을 위해 개발된 시스템이다.

TIS 클라이언트는 *NESPOT* 서비스를 사용하는 Microsoft Window XP 환경의 단말에서 동작하며, IEEE 802.11b 관련 정보를 TIS 서버로 전송한다. 이때, IEEE 802.11b 관련 정보(접속 AP, 접속 가능 AP, 전송 실패 수, 재전송 수 등)를 얻기 위해서 NDIS (Network Driver Interface Specification)을 사용한다 [13]. 또한 ACPI (Advanced Configuration and Power Interface)를 이용

하여 이동 단말의 파워 관련 정보를 획득한다 [14]. 그림 6은 TIS의 전체 구조를 보여준다.

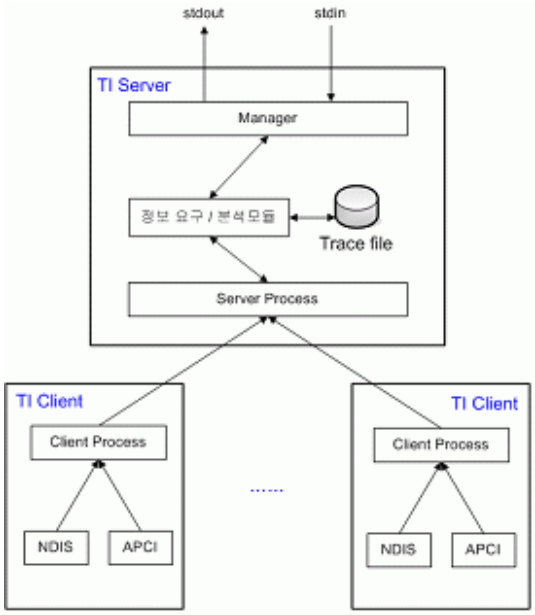

그림 6. TIS 전체 구조도

4.3 인증 서버

*NESPOT*은 상업 서비스 이므로 인증이 필수적이다. 인증 서버는 사용자의 ID와 password를 확인한 후에 AP를 통해 사용자에게 IP를 할당해 주어 *NESPOT* 서비스를 이용할 수 있게 한다. 인증 서버는 이러한 인증 과정에 대한 로그를 모두 기록하고 있기 때문에 이러한 인증 정보는 무선랜 사용자의 사용 패턴을 분석하는 데에 큰 도움이 된다. 인증 로그에는 사용자의 ID와 할당받은 IP주소, MAC주소 등이 기록되므로 사용자의 위치나 이동성, 각 사용자의 선호하는 응용 프로그램 및 평균적인 접속 시간등에 대한 정보가 TCPDUMP를 통해 얻어진 데이터와의 연동을 통하여 얻어질 수 있다.

5. 결 론

본 논문에서는 무선랜 트래픽의 특성과 서비스 사용 패턴을 분석하기 위한 시스템의 구축에 대해서 설명하였다. 트래픽에 대한 정보를 저장하여 추후에 분석하는 것 뿐만 아니라 실시간으로 트래픽을 모니터링 하는 것 또한 가능하다. 이러한 구현은 특히 웹 인터페이스 방식을 통하여 이루어져, 관리자가 어디서든지 쉽게 Network의 상태를 파악할 수 있도록 하였다.

무선랜 사용자의 서비스 이용 패턴과 트래픽 특성을 분석하여 AP의 위치 및 개수를 지역별 수요에 적합하게 설치할 수 있고, AP 별로 최대동시 사용자 집중도의 시간별 날짜별 추이 분석을 통해 통신망 재구성 필요성 판단의 자료로 이용할 수 있다. 또한, 서비스별 트래픽 증감 추이 변화분석을 통해 최적의 엔지니어링을 할 수 있고, 유선망과 무선망의 용량의 밸런스 조절이 가능하다. 망 장애 발생에 대해 모니터링하여 유형별 모델을 정립할 수 있을 것이다.

이러한 시스템은 서울대학교에 구축된 KT *NESPOT* 서비스에 대하여 가능한 부분에 대하여 실제로 적용되어 활용될 것이다. KT는 무선랜을 통한 인터넷 서비스 뿐만 아니라, SWING이라는 CDMA와 무선랜을 동시에 가입하여 편리한 인터페이스를 이용하여 인터넷을 사용할 수 있는 서비스를 제공하고 있다. 따라서 많은 PDA 사용자들이 *NESPOT* 서비스를 사용할 것으로 예상하고 있으며, 이를 위해 TIS 시스템을 PDA에서도 동작할 수 있도록 확장할 예정이다. 서울대학교 내의 트래픽 측정은 사용자가 무선랜과 CDMA 서비스를 이용할 때 네트워크 트래픽 특성이나 서로 다른 네트워크 인터페이스 간의 핸드오프에 대한 연구를 수행할 수 있을 것으로 판단된다.

6. 참고 문헌

[1] KT *NESPOT*, http://www.nespots.com
[2] K. Lai, M. Roussopoulos, D. Tang, X. Zhao, and M. Baker, "Experiences with a mobile testbed," Worldwide Computing and its Applications in LNCS, 1998.
[3] D. Tang and M, Baker, "Analysis of a metropolitan-area wireless network," Wireless Networks, Mar-May 2002.
[4] D. Tang and M. Baker, "Analysis of a local-are wireless network," Mobicom2000, Aug. 2000.
[5] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan, "Characterizing user behavior and network performance in a public wireless LAN," In SIGMETRICS Conf., Jun. 2002.
[6] NetFlow, http://www.cisco.com/warp/public/732/Tech/nmp/netflow
[7] Flow-tools, http://www.splintered.net/sw/flow-tools
[8] FlowScan, http://www.caida.org/tools/utilities/flowscan
[9] TCPDUMP, http://www.tcpdump.org
[10] cflowd, http://www.caida.org/tools/measurement/cflowd
[11] RRDtool, http://people.ee.ethz.ch/~oetiker/webtools/rrdtool
[12] net-snmp web page, http://www.net-snmp.org.
[13] NDIS Developer's Reference, http://www.ndis.com.
[14] Microsoft, http://www.microsoft.com/whdc/system/pnppwr/powermgmt/default.mspx.