

학내 NESPOT 이용 특성 분석을 위한 측정 시스템 설계 및 구현

백승민*, 최낙중*, 김해용*, 최양희*, 이고운+, 김성만+, 정한옥+

*서울대학교 컴퓨터공학부
+KT 서비스 개발 연구소

Design and Implementation for Measurement System to Analyze Usage Pattern of Campus NESPOT Services

Sungmin Baek*, Haeyoung Kim*, Nakjung Choi*, Yanghee Choi*
Gwoon Lee+, Jaehwan Lee+, Hanwook Jung+

*School of Computer Science and Engineering, Seoul National University

+Service Development Laboratory, KT

Abstract - 서울대학교와 KT는 연구 환경 조성과 U-Campus 시범 구축을 위해서 산학협력 협약을 하고, 서울대학교에 NESPOT 시설을 구축하였다. 본 논문은 서울대학교 내의 NESPOT 이용자들의 NESPOT 서비스 이용 패턴 및 무선랜의 트래픽 특성을 분석하기 위한 시스템의 설계와 구현에 대한 내용을 다룬다. NESPOT 트래픽 특성을 분석하기 위한 시스템은 TCPDUMP를 이용하여 백본 라우터로부터 네트워크 전체에 대한 정보를 획득하고, SNMP (Simple Network management Protocol)을 통해 AP로부터 무선랜 관련 정보를 얻는다. 그리고, NESPOT 사용자의 단말에 관련된 보다 구체적인 정보를 얻기 위해서 TIS (Terminal Information System)을 개발하였다.

위한 귀중한 자료가 될 수 있을 것이다.

서울대학교 내의 NESPOT 존은 2004년 9월 중에 서비스를 개통할 예정이며, 본 논문은 서비스가 개통 되었을때, NESPOT 무선 인터넷 서비스를 사용하는 사용자의 이동 성향, 네트워크 트래픽 특성 등의 내용을 분석하기 위한 시스템의 설계에 대해 기술한다.

세계의 여러 연구 기관이 무선랜의 사용 특성에 대한 연구를 진행했다. 대표적인 사례로는 1992년, Tang 과 Baker의 무선랜 네트워크에 대한 연구로, 10일 동안 TCPDUMP를 이용해 8대의 노트북 사용자에 대한 연구이다. Tang과 Baker의 연구는 유선과 무선의 액세스 채널의 교환 횟수, 그리고 이에 따른 패킷의 지연시간에 대한 내용이었다 [2]. 그들은 또한, 1999년에 Metricom Ricochet 네트워크의 사용자의 이용 특성에 대해 연구했다. 이 연구에서 그들은 네트워크의 상태와 이용자의 이동성에 초점을 둔 분석을 시도했다 [3]. 그리고, 2000년에는 스탠포드 대학교 컴퓨터 과학과에서 72명의 무선랜 사용자들을 대상으로 네트워크 이용자의 이용 특성을 분석한 바 있다 [4]. Balachandran외 3명은 SIGCOMM 컨퍼런스가 열리는 2.5일 동안 컨퍼런스에 참석한 195명의 무선랜 사용자들을 대상으로, 무선랜 이용자의 네트워크 이용패턴과 무선랜 트래픽 특성의 분석을 시도했지만, 195명의 분석 대상자 모두가 컨퍼런스에 참석한 사람들로 비슷한 이용 양상을 보인다는 제한된 환경에서의 실험이었다 [5].

1. 서 론

KT는 2002년부터 IEEE 802.11b 기술에 기반한 무선랜 서비스인 NESPOT 서비스를 제공하고 있다. NESPOT은 기존에 KT의 DSL 기술 기반의 망 가입자의 가정에 무선랜 환경을 제공해 주는 형태의 서비스와 공공 장소에 NESPOT 존을 구축해 가입자들이 무선랜을 통해 인터넷에 접속할 수 있는 서비스를 제공한다 [1].

본 논문에서는 서울대학교 내 NESPOT 사용자의 이용 패턴을 분석하기 위해서 백본 라우터, 무선랜 AP, 이용자 단말의 세 가지 네트워크 구성 요소에 따라 이용자의 트래픽 특성 및 네트워크 이용 정보를 획득하기 위한 인프라를 구축했다.

NESPOT 서비스의 이용자가 증가하면서 네트워크의 유지, 관리에 관련된 문제들이 발생하기 시작했고, 실시간으로 네트워크를 모니터링 할 수 있는 시스템의 필요성이 대두되었다. 무선랜 사용자의 서비스 이용 패턴과 트래픽의 특성을 분석함으로써 보다 나은 서비스를 제공할 수 있을 것이며, 네트워크의 관리를

* 본 논문은 2004년도 KT와 두뇌한국21, 국가지정연구실 프로젝트 지원을 받아 수행되었음

본 논문 2장에서는 백본 라우터, 무선랜 AP, 이용자 단말의 네트워크 구성 요소로부터 정보를 획득하기 위한 인프라의 구성 요소에 대해서 설명한다. 3장에서는 단말의 정보를 획득하기 위한 시스템의 설계와 구현에 대해서 자세히 다룰 것이며, 4장에서는 차후 개선 사항 및 적용 방안에 대해서 설명한다.

2. 트래픽 특성 분석을 위한 인프라 구축

그림 1은 서울대학교 내의 NESPOT 트래픽 분석을 위한 시스템을 단순화한 구조이다. 백본 라우터, AP, 사용자 단말로부터 각각 TCPDUMP, SNMP, TIS를 이용해서 네트워크 관련 정보를 획득한다. 이외에도 인증 서버로부터 추가적인 정보를 획득 가능하다.

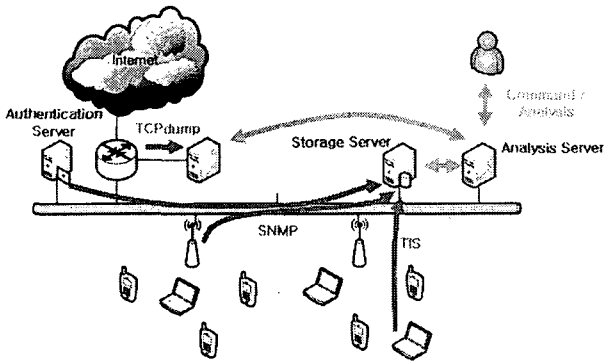


그림 1. NESPOT 사용 특성 분석을 위한 시스템 구조

2.1 백본 라우터 트래픽 분석

서울대학교 NESPOT 존의 트래픽을 분석하기 위해 TCPDUMP와 flow-tools, flowscan을 사용한다. 측정 지점으로부터 NETFLOW 메시지를 저장하고 이 정보를 이용하여 필요한 정보를 추출하여 저장하고 실시간 모니터링이 이루어지게 된다. 만약 라우터나 스위치에서 NETFLOW를 지원하지 않는다면, 측정 지점의 링크를 분할기(splitter)로 나누거나 측정 지점에서 포트 미러링을 통해 트래픽을 덤프 받을 수 있도록 하고, 이 트래픽을 NETFLOW 형식으로 변환하는 방법을 활용한다. 측정 서버에서 NETFLOW 메시지를 받게 되면, flow-tools의 flow-capture 프로그램을 이용하여 주기적으로 NETFLOW 메시지를 저장한다. 또한 TCPDUMP도 동시에 가공되지 않은(raw) 데이터를 저장해 둬으로써, 이후 추가적인 데이터 분석을 원하는 경우 언제든지 분석이 가능하도록 하였다.

저장된 NETFLOW 메시지는 모니터링을 위해 다시 flow-export 프로그램을 이용해 CFLOWD 파일 형식으로 변환하게 된다. 이 작업은 스크립트를 통해 NETFLOW 메시지가 기록될 때마다 CFLOWD 파일도 동시에 생성될 수 있도록 하였다. 이런 방법을 통하여 주기적으로 생성되는 CFLOWD 파일을 flowscan 프로그램으로 읽어 들여 RRD (Round Robin Database)를 작성하게 되고, RRD 파일을 이용하여 모니터링이 가능하다. 모니터링은 바이트, 패킷, 플로우 단위의 트래픽으로 구분하여 사용되는 프로토콜의 비율과 서비스(응용 프로그램), 총 트래픽 양 등에 대해 분석할 수 있으며, 또한 많은 트래픽을 야기하는 특정 주소도 알아낼 수 있다.

저장된 NETFLOW 메시지는 이후에 flow-tools의 flow-cat, flow-print, flow-stat 프로그램을 이용하여 분석이 가능하다. 총 플로우, 바이트, 패킷 수와 평균 값, 그리고 패킷 크기 혹은 개수에 따른 분포 등의 정보를 원하는 구간에 대해 조사할 수 있다. 그림 2는 포트 미러링을 사용하는 경우, 측정 시스템의 전체 구조를 보여준다.

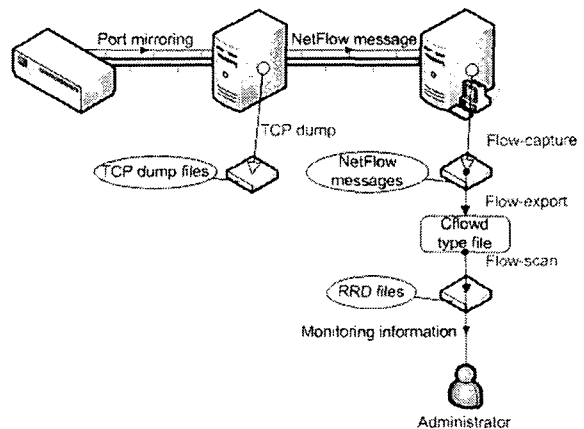


그림 2. 백본 라우터의 트래픽 측정

TCPDUMP로부터 저장된 메시지는 그 외의 다양한 분석에 활용할 수 있다. 예를 들어, 인증 서버에 저장된 정보를 이용할 수 있다면, 특정 시간에 특정 사용자의 MAC 주소와 사용 중인 IP 주소를 알 수 있고, 이것과 TCPDUMP로 저장된 메시지를 비교하여, 각 사용자의 이용 패턴의 분석이 가능하다.

2.2 AP로부터 정보획득

서울대학교 내에 배포되는 AP의 경우 SNMP 기능을 지원하고 있다. 특정 AP를 실시간으로 모니터링

하고 추후 데이터 분석을 위한 자료로서 SNMP 정보를 수집하는 시스템을 구축하였다. 정보 수집 프로그램은 net-snmp 라이브러리를 사용하여 구현하였고 [6] 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.

저장된 정보는 실시간으로 모니터링하거나 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 3은 실시간 모니터링 시스템의 예로써 송수신 에러율을 보여준다.

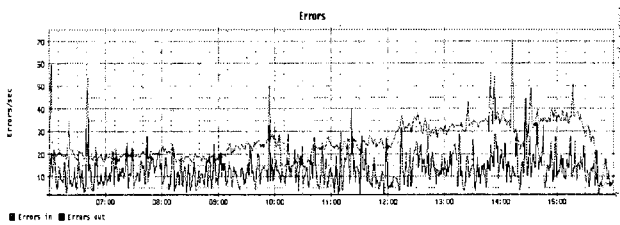


그림 3. 실시간 모니터링 시스템

2.3 단말의 정보 획득

네트워크의 인프라에서 얻을 수 없는 단말에 관련된 정보, 예를 들면, 각 단말의 현재 접속 가능한 AP, 배터리 정보, IEEE 802.11b 관련 정보와 같은 내용을 획득하고 분석하기 위해서 서울대학교 내의 NESPOT 서비스 사용자의 단말에 정보 획득을 위한 프로그램을 설치하고, 서버 프로그램과 통신을 통하여 분석을 위한 정보를 획득한다. TIS (Terminal Information System)는 개발한 단말의 정보 획득을 위한 시스템이며, TIS에 대한 자세한 내용은 3장에서 설명한다.

3. Terminal Information System 설계 / 구현

본 장에서는 2.3장에서 설명한 단말의 정보 획득을 위한 시스템에 대해서 보다 구체적으로 그 구조와 시스템이 사용하는 프로토콜, 구현상의 문제점에 대해서 살펴본다.

TIS의 목적은 네트워크 상의 라우터나 AP에서 획득할 수 없는 단말의 IEEE 802.11b 무선랜 관련정보를 획득하는 것이다. 해당 정보는 단말이 현재 접속 가능한 AP의 MAC 주소와 그 시그널 강도, 전송 실패한 프레임수, 재전송 횟수, RTS 실패 횟수, FCS (Frame Check Sequence) 오류 횟수 등이며 3.2 절에서 보다 자세히 설명할 것이다.

3.1 TIS 구조

TIS 클라이언트는 NESPOT 서비스를 사용하는 Microsoft WindowXP 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 [7]. 그리고, APCI (Advanced Configuration and Power Interface)를 이용해서 이동 단말의 파워 관련 정보를 획득한다 [8].

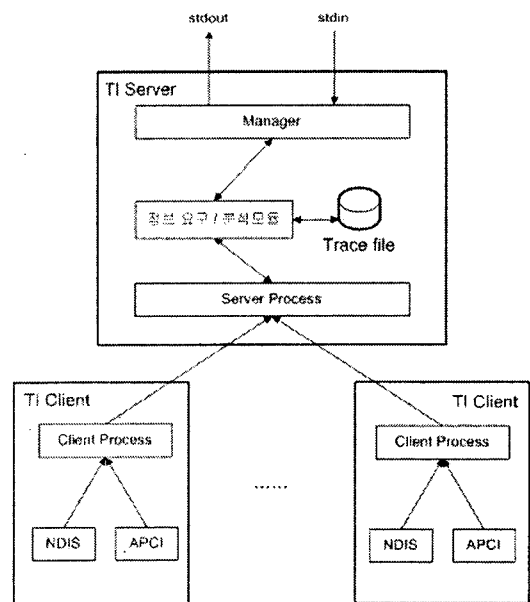


그림 4. TIS 전체 구조도

TIS 서버는 현재 서울대학교 내에서 NESPOT 서비스를 사용중인 단말의 정보를 유지하고 있으며, 이중 특정 단말에 원하는 정보를 요구할 수 있다. 단말로부터 전송된 정보는 차후에 단말 정보 분석을 위해 파일로 저장되며, 간략한 요약 정보가 관리자의 화면에 보여진다. 그림 4는 TIS의 전체 구조를 보여준다.

3.2 TIS 프로토콜

TIS 프로토콜은 단말의 IEEE 802.11b 정보와 배터리 관련 정보를 획득하기 위한 TIS 서버와 클라이언트 간의 메시지 타입을 정의한다. TIS는 UDP (User Datagram Protocol)를 전송 프로토콜로 사용한다. 그림 5는 클라이언트가 NESPOT AP를 통해서 인터넷에 접속했을때, TIS의 전형적인 동작 과정을 도식화 한 그림이다.

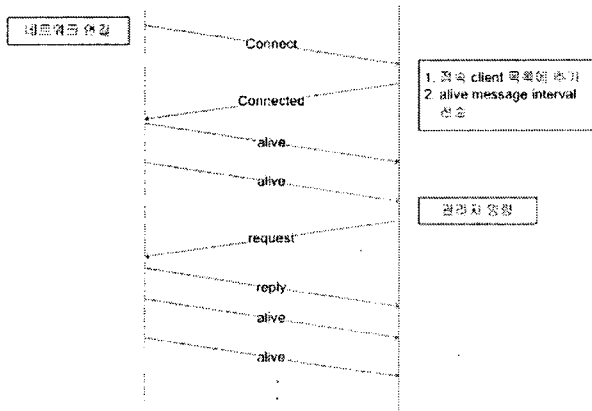


그림 5. TIS 클라이언트 / 서버 패킷 흐름도

이동 단말이 NESPOT 서비스에 접속하게 되면, 이동 단말은 TIS 서버에게 CONNECT 메시지를 전송하게 되고, TIS 서버는 이를 통해 해당 단말이 현재 NESPOT 서비스를 사용중임을 알 수 있다. 단말은 NESPOT 서비스를 사용중임을 지속적으로 알려주기 위해서 ALIVE 메시지를 TIS 서버에게 일정한 시간 간격으로 전송한다. 관리자는 TIS 서버가 관리하고 있는 NESPOT 서비스를 사용중인 단말 목록을 이용해서 해당 단말에게 REQUEST 메시지를 전송하고, REPLY 메시지를 통해 필요한 정보를 획득하게 된다.

그림 6과 표 1, 2는 TIS가 사용하는 메시지와 메시지를 나열한 것이다.

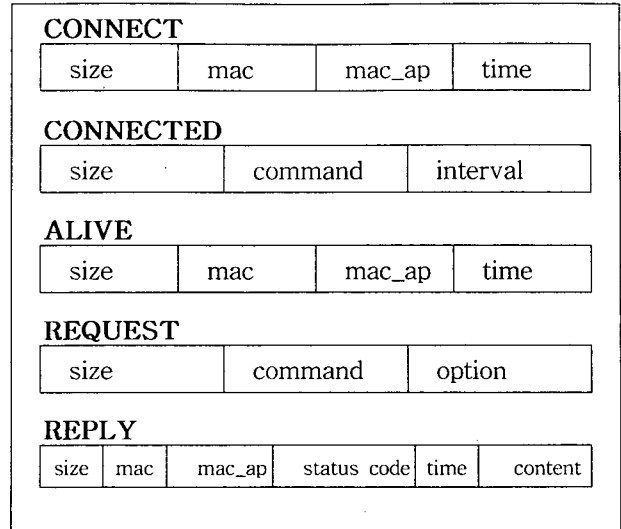


그림 6. TIS 메시지

표 1. TIS command 목록

command	설명	비고
AP	- 단말이 접속 가능한 AP의 MAC 주소, 시그널 강도	전송간격 명시
AP_STOP	- AP 정보 전송 중지	
POWER	- 배터리 관련정보 요구	일회성
802_11_STATE_ATE	- 전송한 fragment frame 수 - 전송한 multicast frame 수 - fail count - retry count - RTS 성공 count - RTS 실패 count - ACK 실패 count - FCS error count	일회성

표 2. TIS status code

STATUS CODE	설명
AP_OK	단말 주변 AP 정보
AP_CONTINUE	여러 메시지로 구분하여 AP 정보를 보내게 되는 경우
802_11_STATE_OK	IEEE 802.11 관련 정보
POWER	배터리 관련 정보 업로드
POWER_CONTINUE	여러 메시지로 구분하여 배터리 정보를 보내게 되는 경우
POWER_NO	배터리가 없는 클라이언트

3.3 TIS 구현

NESPOT 서비스 제공하는 AP는 모두 SSID (Server Set ID) 값을 'NESPOT'으로 갖는다. 이 SSID 값을 이용해서 현재 클라이언트가 NESPOT 서비스를 이용해 인터넷에 접속중이라는 것을 알 수 있다.

TIS 서버는 현재 NESPOT 서비스를 이용하고 있는 클라이언트의 목록을 유지해야 할 필요성이 있다. TIS는 클라이언트가 접속된 AP 별로 클라이언트에게 REQUSET 명령을 전송하기 때문에, 클라이언트가 접속하고 있는 AP 별로 클라이언트를 관리할 필요가 있다. 본 프로그램에서는 그림 7과 같이 클라이언트가 접속하고 있는 AP의 MAC 주소를 기준으로 해서 테이블을 만들고, 각 AP 해시 값에 따라 체인을 형성해 해당 AP에 접속한 클라이언트들을 관리한다. 클라이언트들의 목록은 클라이언트가 특정 시간 간격으로 전송하는 ALIVE 메시지를 통해 갱신되며, 특정 시간 동안 ALIVE 메시지를 전송하지 않는 클라이언트는 목록에서 삭제된다.

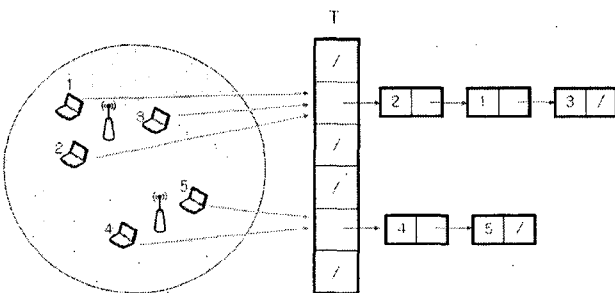


그림 7. 클라이언트 목록 관리

UDP는 비연결지향형 프로토콜이기 때문에, 특정 클라이언트가 장소를 이동해 다른 AP를 통해 인터넷에 접속되었을 경우, 다시 CONNECT, ALIVE 메시지를 전송함으로써 서버는 한 클라이언트에 대해 두 개의 목록을 가지게 될 수 있다. 하지만, 일정 시간이 지나게 되면 예전의 클라이언트 목록은 ALIVE 메시지를 통해 시간 정보가 갱신되지 않기 때문에 자연스럽게 목록에서 삭제되게 된다.

4. 결론 및 향후계획

본 논문에서는 서울대학교 NESPOT 존의 사용자 트래픽의 특성과 사용자의 NESPOT 서비스 사용 패턴을 분석하기 위한 시스템의 구축에 대해서 설명하였다. 앞으로 서울대학교에서 NESPOT 서비스가 시

작하게 되면, 개발한 시스템을 기반으로 실제 사용자들의 네트워크 트래픽의 특성을 분석할 것이다.

KT는 무선랜을 통한 인터넷 서비스 뿐만 아니라, Swing 이라는 CDMA과 무선랜을 동시에 가입하여 편리한 인터페이스를 이용해서 인터넷을 사용할 수 있는 서비스를 제공하고 있다. 현재 PDA 사용자들이 이 서비스를 주로 사용하고 있으며, TIS 시스템을 PDA에서도 동작하게 확장하여 사용자가 무선랜과 CDMA 서비스를 이용할 때의 네트워크 트래픽 특성이나, 서로 다른 네트워크 인터페이스 간의 핸드오프에 대한 연구를 수행 할 수 있을 것으로 판단된다.

(참 고 문 헌)

- [1] KT NESPOT, "<http://www.nesspots.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-area 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] net-snmp web page, "<http://www.net-snmp.org>".
- [7] NDIS Developer's Reference, "www.ndis.com".
- [8] Microsoft, "<http://www.microsoft.com/whdc/system/pnppwr/powermgmt/default.msp>".