Analysis of Campus Users' Pattern in *NESPOT* Wireless LANs

Nakjung Choi, Yongsub Nam, Yongho Seok, Yanghee Choi
School of Computer Science and Engineering
Seoul National University, Seoul, Korea
Email: {fomula, ysnam, yhseok, yhchoi}@mmlab.snu.ac.kr

Sungmann Kim, Hanwook Jung
Convergence Laboratory
Korea Telecommunication, Seoul, Korea
Email: {sungmann, hanuk}@kt.co.kr

***Abstract*— Korea Telecommunication and Seoul National University initiated a joint project as an effort of collaboration for building U-Campus early this year. As a part, our project aims to develop a measurement infra system and measure wireless traffic in *SNU NESPOT Zone*. Currently, *SNU NESPOT Zone* is successfully built, so the registered users are able to use the Internet anywhere in Seoul National University.**

In this paper, we first introduce how to implement a *NESPOT Zone* Monitoring and Managing System (NMMS) in campus-wide wireless networks. This infra consists of two main parts: a data collection and a real-time monitoring system. Then, we really measured wireless traffic in *SNU NESPOT Zone* and analyzed measured data on the basis of both user IDs and MAC addresses. From measured results, we would derive a *resident* type and a *migratory* type as user mobility patterns.

***Index Terms*— Campus Wireless LAN; NESPOT Zone; Usage Pattern; User Mobility**

I. Introduction

As networking trends move toward ubiquitous computing, it is expected that a user be able to connect to the Internet anywhere, at any time and through any kind of device. Diverse access network technologies were introduced for the purpose of providing ubiquitous networking but a wireless LAN (WLAN) was the most successful one among these technologies, due to the inexpensive and easy installation. In such a situation that WLANs are increasingly common, a clear understanding of usage pattern and user mobility in WLANs is critical to build and manage in more efficient ways.

In the past, there have been several studies related to this topic in various environments. Wireless traffic measurements were conducted in such from a small area as conferences [2] and university campuses [3] in the pioneer days to a large area as corporate networks [4] and metropolitan networks [5] recently. Besides, the [6] analyzed access and mobility of wireless PDA users, and an analysis of wireless information locality and association patterns in a campus was performed in [7]. However, so far, analyzing wireless traffic and users' pattern of *commercial* wireless networks has not been conducted.

Korea Telecommunication (KT), the largest telecommunication and Internet service provider in Korea, has recently started providing particular type of high-speed Internet access called *NESPOT* on university and corporate campuses as well as in public places such as hotels, cafes and subway stations [1]. The subscribers to the *NESPOT* service are able to access to the Internet on ID/PW authentication or MAC authentication with any device such as a laptop or a PDA supporting WiFi (802.11b) networks in about 9,000 hotspots. As a part of the collaboration, KT is building the *NESPOT Zone* in SNU (U-Campus) and a joint project was initiated for the efficient deployment and management.

As a part, our project has two goals. First, we develop and deploy a *NESPOT Zone* Monitoring and Managing System (NMMS) for an efficient management. NMMS consists of two main parts: a core module collecting measured data and a real-time monitoring module. This system aims to detect and correct the network miss-configuration easily and quickly in the *NESPOT Zone*. Second, we measure and analyze the network traffic in *SNU NESPOT Zone*. By analyzing the service usage pattern of campus *NESPOT* users, the network manager is able to re-arrange the number and the position of *NESPOT* access points depending on the users' demand. The analysis such as the change tendency of network traffic per each service protocol and the maximum number of transient users per each access point according to date and time enables a network administrator to optimize traffic engineering, including network re-construction and capacity balance between the wired and wireless networks.

The rest of this paper is organized as follows. In section II, we provide a brief overview of the trace methodologies used in the implementation of NMMS. An analysis of measured data are presented in section III, and we conclude our work in section IV.

II. Methodologies

The measurement techniques in *NESOPT Zone* Monitoring and Management System includes dumping network traffic in the backbone networks, periodically collecting SNMP data from access points, getting logs from an authentication server and periodically collecting the terminal-specific data from some mobile terminals. The architecture of NMMS is depicted in Fig. 1.

This work was supported in part by the Brain Korea 21 project of Ministry of Education, in part by the National Research Laboratory project of Ministry of Science and Technology, and in part by Korea Telecommunication, 2005, Korea.

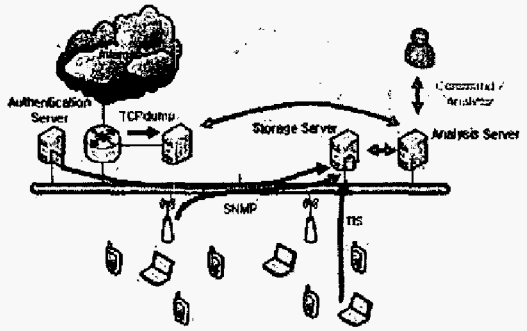


Fig. 1. The architecture of NMMS

A. Periodic Collection from Mobile Terminals

For the deeper understanding of user of terminal mobility, we also develop an application called Terminal Information System (TIS), operating on Microsoft Windows XP. TIS measures data available only in mobile terminals such as the list of available/associated access point(s), the number of failed/retransmitted frames, the received signal strength and the power status of its battery and periodically uploads the measured data to a storage server in the wired network. The flexible remote configuration of TIS on each mobile terminal is available on the web interface of an analyzing server.

TIS protocol enables a TIS server and TIS clients to communicate. Based on UDP, TIS clients send ALIVE messages periodically to a TIS server so that they would inform that they are using *NESPOT* services. A TIS server can maintain states of mobile terminals using *NESPOT* services and access points with which mobile terminals associate. Entries for mobile terminals that haven't sent ALIVE message for the pre-defined period in a TIS server are deleted because the entries are considered not using *NESPOT* service. A simple scenario of a TIS protocol is depicted in Fig. 2.

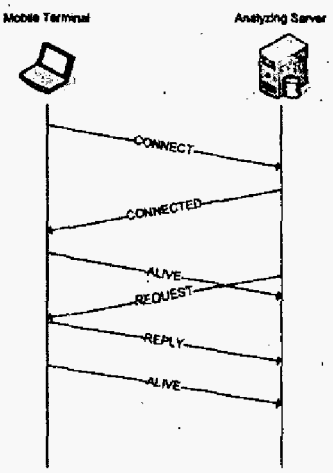


Fig. 2. Example of message flow

When a mobile terminal moves to another place and re-associates with new access point, a TIS client sends CONNECT message again. Therefore, a TIS server would have two entries for an identical mobile terminal. However, the previous entry will be deleted soon because the time to get a last ALIVE message of the previous entry is not updated.

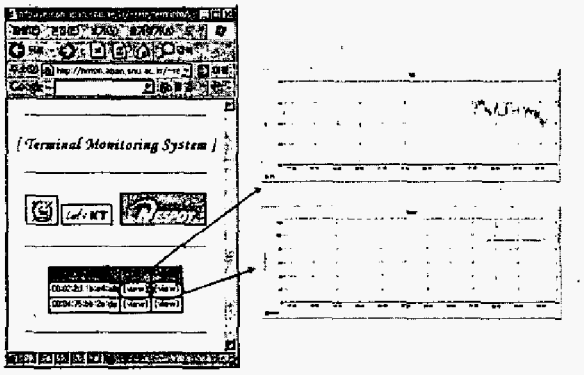


Fig. 3. SNR and Remaining Power of mobile terminals

Fig. 3 shows a real-time terminal monitoring system on a storage and analysis server. Although various terminal-specific information can be gathered, SNR and remaining power are being collected currently.

B. Periodic Collection from Access Points using SNMP

The current access points for *NESPOT* service support Simple Network Management Protocol (SNMP). A SNMP agent in a *NESPOT* access point provides public MIBs defined in RFCs and private MIBs additionally offered by KT. Private MIBs include additional information such as the number of the authenticated/unauthenticated users associated to an access point. A real-time monitoring system is placed to monitor and manage specific access points for traffic analysis. A data-collecting application is built on the system by using NET-SNMP library and stores the collected data to RRD (Fig. 4).

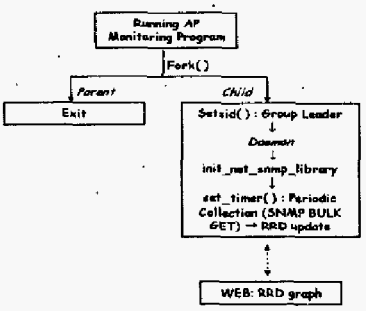


Fig. 4. Algorithm for a data-collecting application

The stored SNMP data in RRD is used to monitor and analyze the network traffic through specific access points during the pre-defined period. The graphes related to the

transmitted/received data volume, error rate and number of packets of each transport protocol are available on the web interface and renewed every a minute.

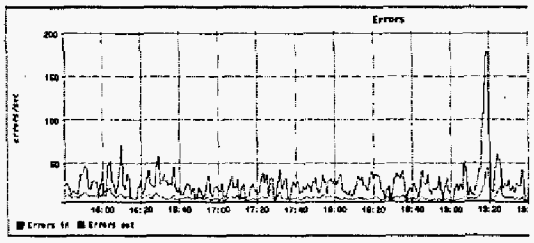


Fig. 5. Error rate of incoming and outgoing traffic

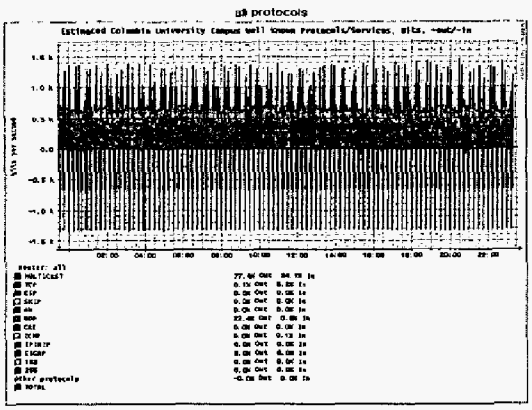


Fig. 6. Network traffic of all protocols

C. Traffic Dump in Backbone Networks

Raw data of *NESPOT* traffic is dumped and analyzed in a storage and analysis server. For this purpose, TCPDUMP, NetFlow, Flow-tools and FlowScan are utilized in each processing stage. TCPDUMP is used in saving and printing out the information in packet headers on a configured network interface, and NetFlow developed by CISCO formats the measured data. Then, Flow-tools consists of several tools to handle and to analyze NetFlow-formatted data and FlowScan is a web interface for a real-time monitoring.

For the traffic measurement, backbone router should send NetFlow data to a storage and analysis server using UDP. When a storage and analysis server receives NetFlow data from a switch or a router, Flow-capture as a part of Flow-tools stores NetFlow data periodically. Tracing *NESPOT* traffic is accomplished by processing the stored NetFlow data. In this process, Flow-cat, flow-print, flow-stat and other applications in Flow-tools are utilized. They report traffic statistics on a network related to the total number and the mean of incoming and outgoing flows, packets, bytes, and the distribution of packet size and the number of packets in a flow during a certain period. Raw dump data of all traffics to pass through a switch or a router is also used for the additional detailed post-analysis.

For a real-time monitoring, the stored NetFlow data are converted to cflowd type by flow-export as a part of Flow-tools periodically. Then, FlowScan reads cflowd files and creates Round Robin Database for traffic monitoring. Each subnet of a specific IP range can be monitored separately. Graphes related to the total number of incoming or outgoing flows, packets, and bytes during a certain period can be shown in web by processing stored RRD. The traffic monitoring also shows the usage pattern of protocols and applications, total traffic statistics, and a list of top ranked users.

D. Logs from an Authentication Server

As *NESPOT* is a commercial service, an authentication process is essential. A *NESPOT* user can connect to the Internet after an authentication server successfully authenticates the id and the password of the user. All logs of authentication information such as the user's id, the mobile terminal's MAC address and IP address of the associated access point are recorded in an authentication server. Currently, the L2 handoff is not supported in the roaming among NESPOT access points, so a roaming mobile node should re-authenticate itself after associating a new access point. Therefore, analyzing the logs in an authentication server are very useful to grasp user mobility in terms of the number of handoffs. Besides, combined with other measured results, it is possible to analyze the pattern of wireless traffic depending on a user and a mobile terminal.

III. Measurement

A. Environment

The measurement has been conducted in SNU NESPOT Zone for two weeks from Oct. 4, 2004 to Oct. 17, 2004. About 1,900 access points were deployed in the 76 buildings out of 150 ones. Currently, there are more than 3,000 subscribers and the number of subscribers is being increased.

The measured data was collected from several terminals, several access points, an entire network dump, and an authentication server. A storage and analysis system utilizes SNMP or developed protocols for the communication with access points, terminals, or an authentication server. Although we measured and analyzed data on the basis of a registered user ID and a MAC address of the wireless LAN card of a terminal, we applied a hash function to both an user ID and a MAC address for privacy assurance and we had no mapping table to identify user names or any other private information.

We analyze the statistics such as access frequency, connection time, and an amount of used data, so derive the traffic characteristics and an user movement pattern. During the duration, 540 users connected to the SNU NESPOT Zone on the basis of user IDs, and 558 users on the basis of MAC addresses. A total amount of used data was about 260(GB).

B. Analysis

Fig. 7 shows the number of users with respect to access frequency. Both an ID-based curve and a MAC-based one

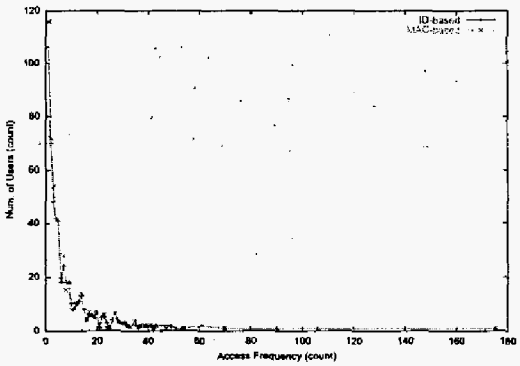


Fig. 7. Num. of Users wrt. Access Frequency

display similar distribution, which means that most users use a single terminal (e.g., laptop or PDA) to connect to SNU NESPOT Zone. Only 3(%) users use more than one terminal. As seen in Fig 7, most users attempted to connect SNU NESPOT Zone less than 40 times and a quarter of every user connected just once, reflecting the occasional and bursty access pattern. The user with the maximum access count connected 117 times, the average access count for top 1(%) users is around 100 times, 52 times for top 5(%) users, 40 times for top 10(%), and 15 times for top 50(%) users, compared to 9 times for every user. This result implies that many users used SNU NESPOT Zone only occasionally, while a few users used extensively.

Fig. 8 displays the distributions of access frequency and connection duration with respect to user IDs, in which user IDs are sorted by their access count and connection time in a descending order. As seen in Fig. 8(a), the curve declines more gently than one in Fig. 8(b), which means a user maintains a session for some even period in comparison with the access frequency. In other words, a single session can contain several handoffs, which increase access frequency because handoffed users should be re-authenticated in current SNU NESPOT Zone. Therefore, the access frequency is dependent on the movement which can cause handoffs. An average connection duration for top 1(%) users was about 360,000(s), 225,000(s) for top 5(%) users, 166,000(s) for top 10(%) users, and 55,000(s) for top 50(%) users, compared to 29,000(s) for every user. These results also implicate the occasional and bursty usage. Considering both results, we can assume that the session of each user lasted 53 minutes on average, which is rather a long duration.

Fig. 9 shows an amount of used data with respect to user IDs, in which user IDs are also sorted by an mount of used data in a descending order, ranged from 0 to 1,800 (MB). Most users tend to use less than a few megabytes, which was equal to the minimum amount to SNU NESPOT Zone. An average data amount for top 1(%) users was about 15,571 (MB), 6,530 (MB) for top 5(%) users, 3,900 (MB) for top 10(%) users, and 940 (MB) for 50(%) users, compared to 470 (MB) for every user.

Fig. 10(a) illustrates the number of distinct access points to which top 10 users ranked by an amount of used data connected, and user IDs which was chosen arbitrarily indicates each user. Fig. 10(b) shows the number of associations with access points for top 10 users. The user IDs in both graphes represent the same users. These graphes reveal two types of user mobility pattern: a *resident* type and a *migratory* type. A *resident* type means that such a user as user ID 2 spends most of time in a few specific areas, so has the small number of distinct access points connected and a number of associations with access points. The other type, *migratory* type means that such a user as user ID 1 moves around place to place and connects to a quite few access points in various areas.

As a whole, above figures show less typical distributions other than a heavy-tailed distribution. In this measurement, a user group was not large and matured enough to analyze and generalize measured data due to the immature state of SNU NESPOT Zone in the campus. However, most users connected to the AP just a few times and few who accessed many times, reflecting the occasional and bursty usage pattern. Users could be classified into two groups, say, a *resident* type and a *migratory* type, by the number of associations and access points which they connected to, representing the user mobility pattern.

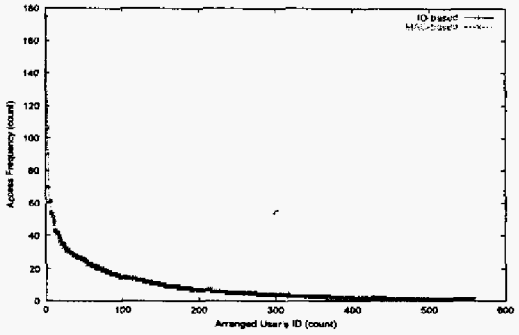
IV. Conclusion

We presented how to implement a measurement infra and measure wireless network traffic in *SNU NESPOT Zone* with several measuring skills. While the implementation of measurement system is focused on in this paper, a brief campus-wide trace-based study was performed in an effort to understand patterns of users' activity in commercial wireless networks. By analyzing the pattern of users' usage and traffic, we derived two types of user mobility pattern: a *resident* type and a *migratory* type. We expect that service providers be able to provide better services and exploit the analyzed results in deploying similar wireless networks in the future.

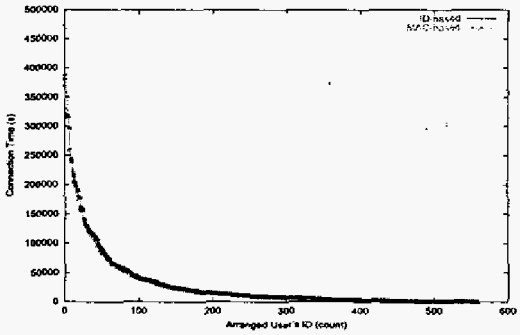
KT is selling *NESPOT Swing* phones which are dual-interfaced for a combined service of the wide-area CDMA network and WLAN. A user subscribed to the *NESPOT Swing* service can enjoy the Internet access using either the *NESPOT* service in *NESPOT Zones* or the CDMA2000 1x EV-DO service. Currently, there are a number of *NESPOT Swing* subscribers in *SNU NESPOT Zone*. Further research may include traffic measurement in such a CDMA2000 network and comparison of the measured data in such different networks.

References

[1] KT NESPOT, "http://www.nespot.com"
[2] Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl, and P. Venkat Rangan, "Characterizing user behavior and network performance in a public wireless LAN," in Proceedings of the 2002 ACM SIGMETRICS international conference on Measurement and modeling of computer systems, Marina Del Rey, California, June 2002.
[3] Ron Hutchins and Ellen W. Zegura, "Measurements From a Campus Wireless Network," College of Computing, Georgia Institute of Technology, ICC 2002

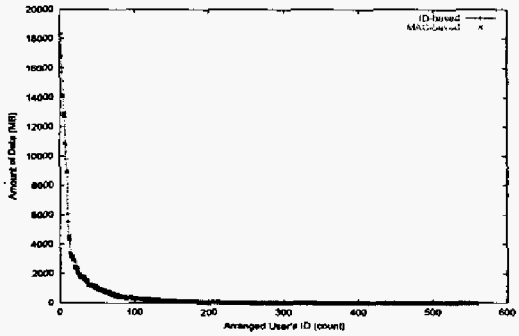


(a) Access Frequency wrt. User's ID

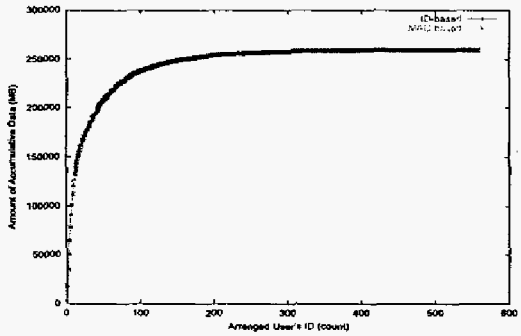


(b) Connection Time wrt. User's ID

Fig. 8. Access Analysis wrt. User's ID

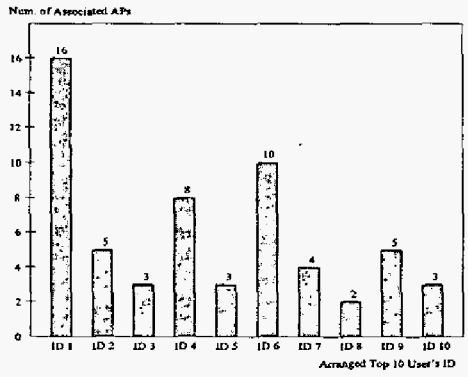


(a) Amount of Data wrt. User's ID

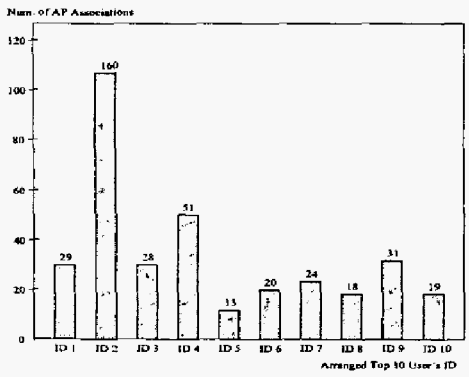


(b) Amount of Accumulative Data wrt. User's ID

Fig. 9. Data Analysis wrt. User's ID



(a) Num. of Associated APs of Top 10 Users



(b) Num. of Association of Top 10 Users

Fig. 10. Analysis wrt. Associated APs

[4] Magdalena Balazinska and Paul Castro, "Characterizing Mobility and Network Usage in a Corporate Wireless Local-Area Network," In ACM MobiSys, 2003.
[5] Diane Tang and Mary Baker, "Analysis of a metropolitan-area wireless network," In Mobile Computing and Networking, pages 13-23, 1999.
[6] Marvin McNett and Geoffrey M. Voelker, "Access and Mobility of Wireless PDA Users," 2003.
[7] Francisco Chinchilla, Mark Lindsey, and Maria Papadopouli, "Analysis of Wireless Information Locality and Association Patterns in a Campus," IEEE Infocom 2004, Hong Kong, March 2004.
[8] David Schwab and Rick Bunt, "Characterizing the Use of a Campus Wireless Network," IEEE Infocom 2004, March 2004.