IMPLEMENTATION OF TRAFFIC MEASUREMENT AND FILTERING OVER ACTIVE NETWORKS†

Li-Der Chou⋆ *Jui-Ming Chen* *Neng-Tsung Tsai*
Department of Computer Science and Information Engineering
National Central University
Chungli, Taoyuan, Taiwan, 32054 R.O.C.
Tel: +886-3-422-7151 ext. 4521, Fax: +886-3-422-2681
E-mail: cld@csie.ncu.edu.tw

ABSTRACT

As the growth of the traffic over Internet, network management becomes more important than before. Traffic measurement and filtering technology helps to manage the network to utilize the network bandwidth efficiently, and filter out improper information. Active network technology is a new approach to enable users' customized computations in network nodes. An architecture of the traffic measurement and filtering system is proposed and implemented in the paper based on Active Node Transfer System (ANTS), an active network execution environment developed by MIT. With the proposed system, the amount of the capsules can be measured precisely, and data transmitted over the network can to be filtered according to specific rules and purposes. Besides, a graphical user interface is also supported in the system.

Keywords: *active networks, ANTS, traffic filtering, traffic measurement*

1. INTRODUCTION

As the Internet traffic grows, traffic management becomes a key technology to manage the network resources not to be abused. Traffic measurement is able to collect the information for the status of the network, such as jitters, congestions, and possible crimes. With the information, the network management mechanism is able to adaptively control network. Traffic filtering helps to stop network crimes, prevent from improper information being transmitted and segregate a network failure. Moreover, congestion of the network can be eased.

NetXRay [1], a packet-spoofing program, can capture packets in the network and list detailed information of the traffic. However, only the packets in the same broadcasting segment can be captured. Multi Router Traffic Grapher (MRTG) [2] polls the MIBs of the network nodes periodically for the traffic statistics, by introducing another server. Traffic measurement mechanisms can be also implemented in network nodes to collect the detailed status of the traffic flowing through the nodes, to support further advanced network management.

Traffic filtering mechanisms can be implemented in network nodes or on an extra machine such as a firewall [3]. The former needs a cooperative system to control the filters among the network nodes, and the latter must prevent the extra machine from being the network bottleneck. In general, the filtering rules consist of protocols and addresses of sources and

† This research was supported by Ministry of Education of the Republic of China under grant 89-H-FA07-1-4.
⋆ The corresponding author

destinations. However, from the viewpoint of network managers, the packet content should be considered in the filtering rules.

The active network provides a platform for users to inject their own services into network nodes. Thus the flexibility and customizability of the networks is increased, and the pace of network services deployed can be accelerated. By using the active network technology, new protocols can be defined and deployed without wasting time for standardization, and new possibilities for network services are enabled by simple computation of network nodes.

In the paper, a traffic measurement and filtering system is implemented in active networks based on Active Node Transfer System (ANTS) [4] which is an active network execution environment developed by MIT. The implemented measurement and filtering programs can be deployed easily in any active nodes, and cooperate easily. For the part of filtering, filtering rules of the implemented system includes not only protocols and addresses but also contents. For the part of traffic measurement, the status of the whole network can be measured. Moreover, A graphic user interface is designed in the system for network managers to monitor the traffic of the whole active network and setup the filtering rules.

2. ACTIVE NETWORKS AND ANTS

The current research on active networks concentrates on two approaches [5]: programmable switches and capsules. For the programmable switch approach, network managers load authenticated programs into switches and routers. For the capsule approach, switches or routers are able to load programs dynamically from code servers or packet-like capsules so as to increase the flexibility of the networks.

The active networks have the following features.

1. New protocols and services can be deployed on the network dynamically and immediately without red tapes of standardization. Protocol designers do not have to take away a part of the network for a while to inject new services.
2. Active nodes can do simple computations, such as filtering or merging, to process part jobs of network servers. Thus, network servers can cooperate by scheduling their jobs on active nodes.
3. Information about packets or flows passed by can be stored in the active node to help the node to process the packets or flows passed by.

The active networks have been studied greatly in the literature. The ANTS system provides an environment to build and deploy dynamically network protocols in active networks [1]. The SwitchWare project proposed active packets, active extension and active router infrastructure to balance the flexibility and the safety of the active networks [6]. Smart packets for active networks focused on the network management using the active networking technology [7]. The Active Network Encapsulation Protocol (ANEP), an RFC draft, specifies a mechanism for transmission over different media or different link layers [8]. Active Network Overlay Network (ANON) describes a network architecture and protocol to interconnect execution environments using ANEP [9]. The active networking technology has been successfully applied to the cache routing [10] and the self-organizing wide-area network caches [11]. Active Networks Backbone (ABone) [12] is a DARPA-funded testbed to support the active networks research program. The ABone forms a virtual network infrastructure on which a growing set of active network components can be tested and experimentally deployed. Currently, six countries, US, Italy, France, Taiwan, Canada and Germany, participate in the

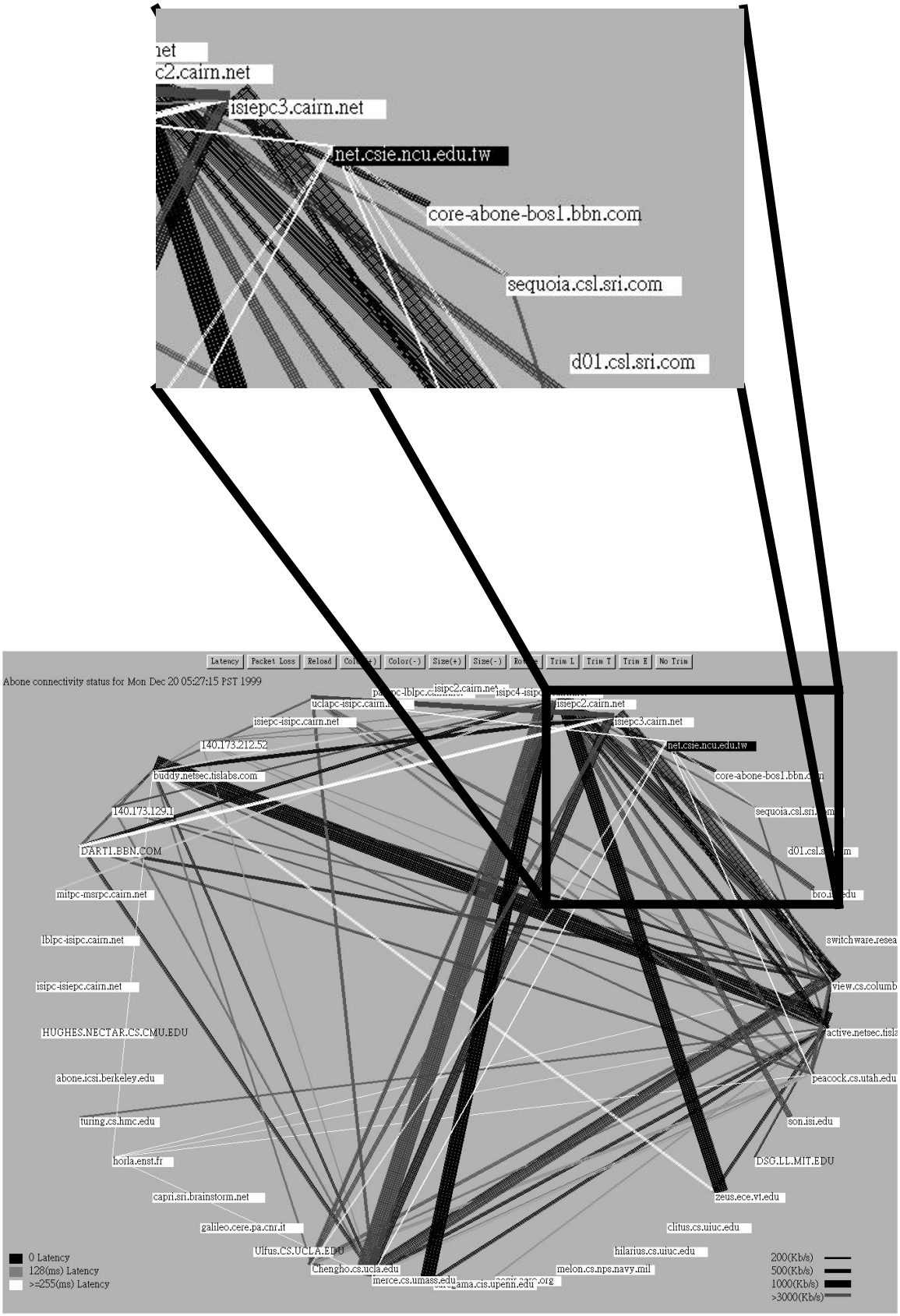


Fig. 1 The status of ABone, where net.csie.ncu.edu.tw is the first and the only ABone node in Asia.

ABone. Note that the active node located at National Central University in Taiwan is the first and the only ABone node in Asia, as shown in Fig. 1.

In the paper the traffic measurement and filtering system will be implemented on ANTS where ANTS is written in Java because of its supports for safety and mobility through bytecodes and its verification and the likely emergence of higher performance compilers and runtimes. New protocols can be automatically deployed at both intermediate nodes and end systems by using mobile code techniques, and expressed in a programming language-like model in terms of operations at nodes. For safety, flexibility and convenience of dynamic deployment of new protocols, some systems were also proposed to be implemented on ANTS, such as active network support for multicast applications in Spain [13].

3. ARCHITECTURE OF THE TRAFFIC MEASUREMENT AND FILTERING SYSTEM

The system is designed to focus on traffic measurement and traffic filtering according to the requirements of network managers. Thus the architecture of the system designed is also to be divided into these two subsystems. Figure 2 shows the architecture of the designed system. ANTS will remove the IP and UDP header of all the capsules passing through the active node, and then the ANTS header of the capsules will be removed by the unpack module. The capsules will then be sent to the measurement module to record the information needed, such as source, destination and protocol, in the measurement log. After measuring, the capsules are sent to the filtering module. First, the filtering module will do a 3-tuple filtering. The content of the capsule are retrieved here to do online content filtering according to the filtering rules retrieved in the filtering rules base. The filtering module will also

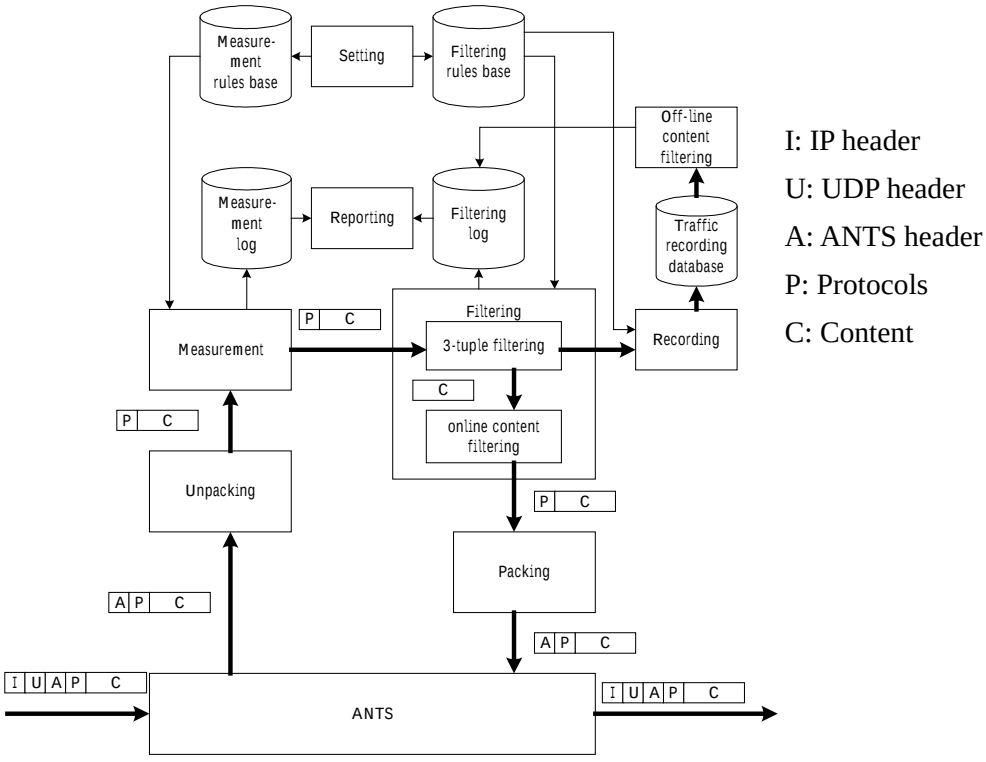
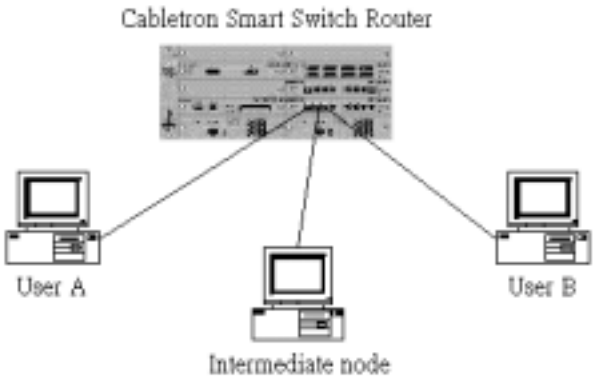
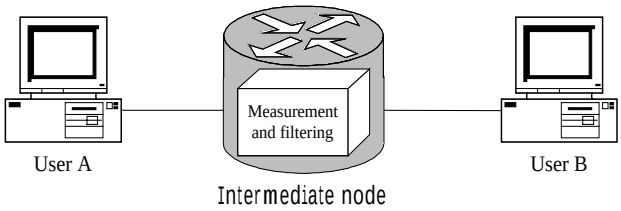


Fig. 2 The architecture of the proposed traffic measurement and filtering system.



(a) physical connection diagram



(b) logical connection diagram

Fig. 3 The experimental environment of the system.

record the information about the dropped capsules in the filtering log module. The content of the capsules can also be fully recorded by the recording module in the traffic-recording base for off-line content filtering if required. Also, the log of filtering will be recorded in the filtering log. The capsules not filtered out will be sent to the packing module to re-encapsulate to sent to ANTS. ANTS will forward the capsules out to the destination of the capsules. Network managers can use the setting module to set up the measurement and filtering rules separately to the measurement rules base and the filtering rules base, and the reporting module will make a report according to the setting of network managers.

4. IMPLEMENTATION

An experimental environment is set up to develop and test the designed traffic measurement and

Fig. 4 The 3-tuple measurement.

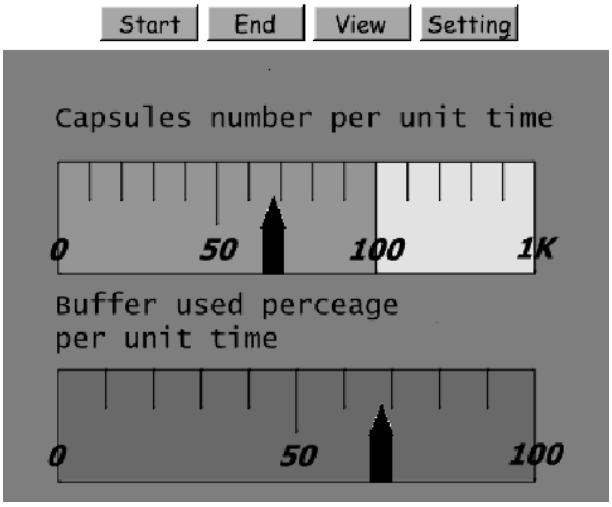


Fig. 5 Real-time traffic measurement.

filtering system. There are three active nodes built on PCs: one plays the role of intermediate node, and the

Table 1. The equipment of the experimental environment.

	CPU	Memory	OS
User A	Pentium II 233	64 MB	Windows 98
Intermediate node	AMD K6-200	32 MB	RedHat Linux 6.0
User B	Pentium II 233	64 MB	Windows 98

Fig. 6 Traffic flows measurement

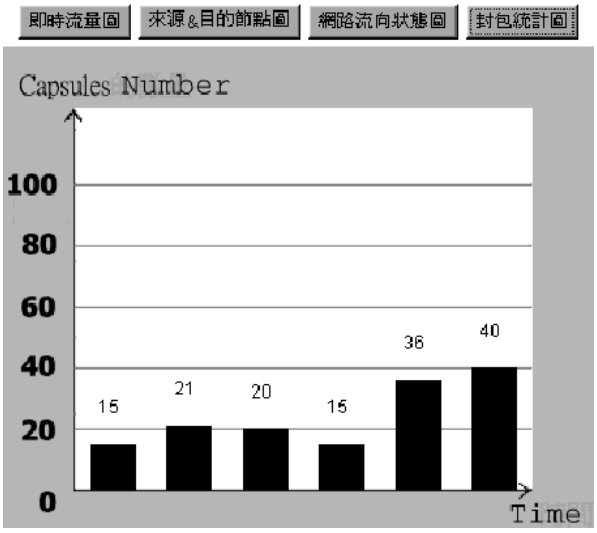


Fig. 7 The number of capsules.

other two are set to be end systems. The physical diagram is shown in Fig 3 (a), And the routing of the experimental system are simulated as Fig 3 (b). Details of the equipment for the PCs are given in Table 1. All of the three PCs are connected to a Cabletron Smart Switch Router SSR-8000 [14] with 100 Mbps Ethernet links. The designed architecture described in the previous section is implemented are deployed on all active nodes.

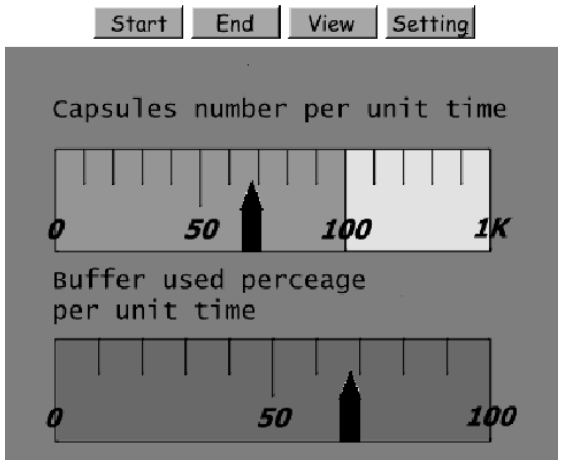


Fig. 8 The instant number of filtered capsules and the percentage of used buffer.

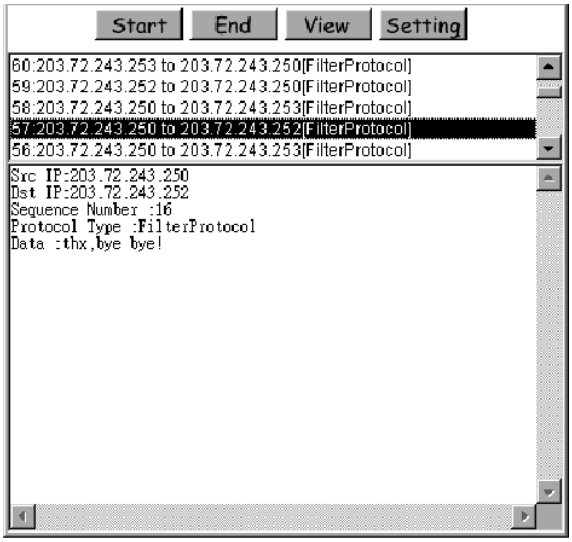


Fig. 9 The content of filtered capsules.

Functions of traffic measurement implemented are listed as follows.

1. The 3-tuple measurement: source, destination addresses and for all capsules, as shown in Fig. 4.
2. Real-time measurement.
   The transmission rate of capsules and the buffer utilization can be measured on line, as shown in Fig. 5.
3. Status of all existing traffic flowing through the intermediate node can be monitored and

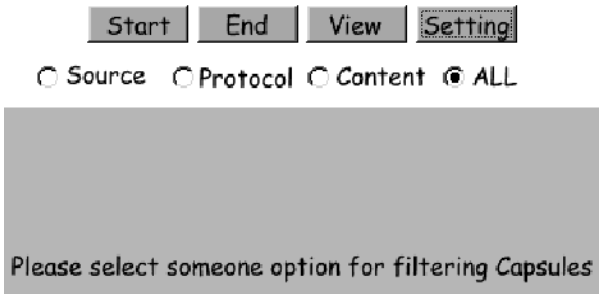


Fig. 10 The selection of filtering rules.

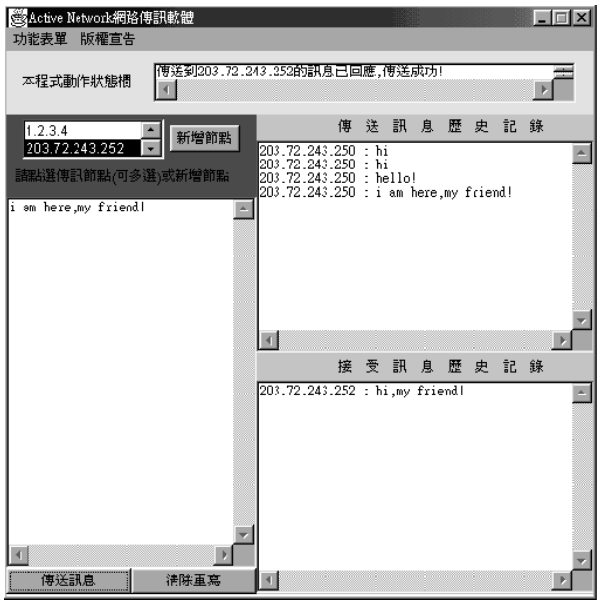


Fig. 11 The GUI interface for clients.

updated periodically, as shown in Fig. 6.

4. Statistics of capsules can be calculated, as shown in Fig. 7.

Functions of traffic filtering implemented are listed below:

1. The total number of filtered capsules and the current buffer utilization can be calculated, as shown in Fig. 8.
2. The content of capsules can be filtered out and listed, as shown in Fig. 9.
3. The traffic with specified words can be filtered out by checking the capsule payloads, and these capsules will be dropped.
4. All capsules can be filtered and banished according to the 3 tuples: source address, destination address and protocols.

Fig. 10 shows four ways for filtering: source filtering, protocol filtering, content filtering and all filtering. By simple setups, the system can filter out any capsules. Figure 11 shows the GUI interface in the end user side, where the program sends capsules with user-specified content.

5. CONCLUSIONS

In this paper, a traffic measurement and filtering system over active networks is designed and implemented on ANTS. With the features for active networks, the system implemented can be deployed on or removed from active nodes without removing any part of the network and modifying the program. Besides, functions of real-time traffic measurement and content filtering are provided. In the near future, the implemented system in the paper will be deployed and tested on the ABone.

REFERENCE

[1] NetXRay, http://www.ngc.com.

[2] Multi Router Traffic Grapher, http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html.

[3] S. M. Bellovin and W. R. Cheswick, “Network firewalls,” *IEEE Communications Magazine*, vol. 32, iss. 9, pp. 50-57, Sept. 1994.

[4] D. Wetherall, J. Guttag and D. Tennenhouse, “ANTS: a toolkit for building and dynamically deploying network protocols,” *Proceedings of IEEE Open Architectures and Network Programming*, San Francisco, CA, USA, pp. 117- 129, Apr. 1998.

[5] D. Tennenhouse, D. Wetherall, “Towards an active network architecture,” *Proceedings of 1996 Multimedia Computing and Networking*, San Jose, CA, USA, http://www.tns.lcs.mit.edu/publications/ccr96.html, Jan. 1996.

[6] D. Alexander, W. Arbaugh, M. Hicks, P. Kakkar, A. Keromytisk, J. Moore, C. Gunter, S. Nettles and J. Smith, “The SwitchWare active network architecture,” *IEEE Network*, vol. 12, no. 3, pp. 29-36, May/June 1998.

[7] B. Schwartz, A. Jackson, W. Strayer, W. Zhou, R. Rockwell and C. Partridge, “Smart packets for active networks,” http://www.net-tech.bbn. com/smtpkts/smart. ps.gz, Jan. 1998.

[8] D. Scott Alexander, B. Braden, C. Gunter, A. Jackson, A. Keromytis, G. Minden and D. Wetherall, “Active Network Encapsulation Protocol (ANEP),” *Experimental RFC draft*, http://www.cis.upenn.edu/~switchware/ANEP/ docs/ ANEP.txt, July 1997.

[9] B. Braden, M. Hicks and C. Tschudin, “Active Network Overlay Network (ANON),” *Experimental RFC draft*, http://www.cis.upenn .edu/~switchware/ANEP/docs/anon-rfc.txt, Dec. 1997.

[10] U. Legedza and J. Guttag, “Using network level support to improve cache routing,” *Proceedings of the 3rd International WWW Caching Workshop*, Manchester, England, http://www.sds.lcs.mit.edu/publications/webca che98.html, June 1998.

[11] S. Bhattacharjee, K. Calvert and E. Zegura, “Self-Organizing Wide-Area Network Caches,” *Proceedings of IEEE INFOCOM '98*, San Francisco, CA, USA, vol.2, pp.600-608, Mar. 1998.

[12] M. Calderon, M. Sedano, A. Azcorra and C. Alonsa, “Active network support for multicast applications,” *IEEE Network*, vol. 12, iss. 3, pp. 46-52, May 1998.

[13] S. Berson, B. Braden and L. Ricciulli, “Introduction to the ABone,” http://www.csl .sri.com/activate/index.html, Dec. 1999.

[14] Cabletron systems, http://www.cabletron.com