SPECIAL FEATURES OF TCP/IP NETWORK TRAFFIC AND PROBLEMS OF THE PROGRAM MONITORING

(1)Radi ROMANSKY

(1)Department of Computer Systems, Technical University – Sofia
e-mail address: rrom@tu-sofia.bg
Bulgaria

Abstract: The effective organization of distributed information environment requires actual information about system workload, type of informational flows and specific features of the distributed processes and resources. The program monitoring is a suitable method for obtaining experimental measures for analysis system parameters of distributed information servicing. The paper systematizes the types and special features of TCP/IP traffic and proposes a methodological scheme for organization and planning of program monitoring.

Key words: network traffic, monitoring, program tools, experiment organization

1. INTRODUCTION

The support and management of the resources in a network environment needs actual information about system workload, type of the flows and processes efficiency [1, 2, 3]. The process of defining these characteristics is an important phase for each research project in information technologies area. The used methods and tools for investigation and evaluation of performance indexes (of the system resources, of the information processes, etc,) should be based on the means of emulation or simulation or on the base of the measurement in a distributed medium [4, 5, 6], including TCP/IP based network [7, 8, 9]. The choice of concrete approach for investigation is determined by the specific of the research problem [10, 11, 12].

NetBIOS is the network interface developed by IBM for Windows based applications. This interface is known as NetBT (NetBIOS-over-TCP/IP) and realizes processes for network traffic supporting. The paper systematizes the different types of TCP/IP traffic and their special features. Some methodological problems concerning program monitoring organization and experiments planning are presented.

2. CLASSIFICATION AND SPECIAL FEATURES OF TCP/IP NETWORK TRAFFIC

The network traffic is very varied and it has stochastic nature. The traffic types form two different categories – functional (transaction) traffic and background traffic. A classification of different traffic types that forms the full network traffic is proposed below. Their special features concerning the problems of monitoring, registration and analysis are generalized.

- ARP traffic – usually this traffic is background type and has relatively small size for a separately station, but it increases geometrically with the number increasing of the stations (mainly the number of servers machines). This traffic is not a problem for slow network connections.

- ICMP traffic – the level of this traffic is relatively low at a normal work of the information infrastructure. It connects with auxiliary activities as a prophylactic and network diagnostic. It can be investigated at fixed cases only.

- DHCP traffic – it gives a possibility for automatic configuration of TCP/IP based clients and its usage causes background traffic in the network. The volume of this traffic increases linear on the base of the number increasing of connected stations and its analysing is very rare.

- DNS traffic – this traffic is not typical of Windows NT based network environments. It is possible mainly for access to Intranet or Internet sites. In this reason the DNS traffic should be a factor at the loading of slow DNS connections.

- WINS traffic – this traffic or NetBIOS Name Service (NBNS) in general is very important for Windows NT based environments, because Windows NT depends strongly on the NetBIOS.It is connected to the names exchange and its volume is relatively small, but it depends on the number of NetBIOS services in each station. It is possible to influence on slow WAN connections and it must to be investigated and analysed.

- Computer Browse traffic – the corresponding service gives a possibility to organize a list of the active stations in the network and it is a broadcasting service. The service ideology includes a machine named Master Browser putting in each broadcasting segment. These machines support a main list of all machines in your segment. Each machine with a Server service will announce periodically for your presence in the network and this will make traffic of background type.

- File sessions traffic – this is basic functional traffic for Windows based networks. The file sessions in Windows environments are realized using the SMB (Server Message Block) protocol based on the NetBIOS interface. The SMB session establishing is preceded of establishing a NetBIOS session and establishing a TCP session (at the TCP/IP version of transportation).The SMB traffic is very large for Windows based networks and it may be dangerous for slow connections – this fact requires its precise analysis.

- Traffic by the Directory Replicator service – in general this is file traffic and it is connected to communication between export server and import stations. If the replicated directory has a big size this traffic should be very dangerous for local network and it must be precisely investigated and analysed.

- Traffic form directory services – it is built mainly of file session traffic (SMB traffic). It is dangerous for slow network connections and it is necessary to search a compromise at contact to the sites without BDC.

- Traffic from Internet/Intranet browsing – this traffic is typically functional because of the specific of HTTP protocol and it is generated at the user access to Web site. The size of this traffic depends on the number of the objects included in Web page and the user work.

- E-mail traffic – this traffic (by SMTP and POP3 protocols) is functional type and its size depends on the messages size between users. This traffic could load seriously the long connections and needs attentive analysis.

- Microsoft NetMeeting traffic – this traffic is generated at audio/video connections and common utilization of applications. The application generates both functional and background traffic. The functional traffic should be large at the high quality audio/video connections and this enforce its analysis.

- ICQ Group Ware traffic – ICQ is an application for common work optimized for slow Internet connections. It generates relatively low traffic size of both functional and background types. The functional traffic is mainly small. The background traffic is defined of periodically client access to the ICQ server.
- Traffic of printing – the access to the network printers generates traffic between the printer server and work station in the network segment. Usually is used a queue for requests into the print server, but this strategy increases the traffic because of duplication of print requests. The printing process analogically of file sessions should generate big background traffic.

3. BASIC PROBLEMS OF THE PROGRAM MONITORING

The program monitoring of network traffic is a suitable means for investigation and analysis its characteristics. The *main problems* of monitoring organization and planning that could be decided are listed below.

- The network traffic volume into the work-loaded segments should be sizable. In different Ethernet segments (10 Mbps, 100 Mbps, Gigabit Ethernet) the network traffic volume could reach to the maximum value. The memory selection for traffic storage buffer is very difficult problem because this buffer for network frames must be organized into the memory. If the buffer is on the hard disk the time for frame processing will be very large and some frames will be missed out.
- Another problem of the network traffic program monitoring is the choice of point for measurement. The network analysers can work effectively if the network interface is switched on in the regime of all frames catching. This requirement brings to the full network traffic catching, but into the local segment (between two routers). The segment forming by a bridge using causes another problem for monitoring because the bridge isolates the traffic from the not concerned ports.
- Next problem of the program monitoring is the choice of suitable traffic types for measurement. In some of the cases is necessary to monitor concrete network protocols and services, in other cases – to monitor the full network traffic between two or more network machines. It is very important to decide correctly this problem that is connected to the problems of traffic filtering during the catching in the network.
- Choice of method for carry out of the monitoring – some different methods for traffic monitoring exist and each of them has a specific level of usability and special features for concrete application. The main methods are listed below:

a) Method for segment work-load monitoring. – relatively simple method connected to measurement of physical segment work-load of the network. A concentrator or special unit should be used. This method is not suitable for monitoring of relation work of two or more segments and for traffic evaluation

b) Method for monitoring of service and objects – more of the network operating systems has tools for elementary evaluation of the traffic, for example Server Manager (Windows NT), Computer Management (Windows 2000), Monitor (Novell Netware), Show Users (Cisco IOS). Unfortunately these tools are oriented to the concrete server and concrete services of the operating system, but not to the network work. They do not permit highest granularity (for example a sequence of file operations) and an analysis on the network or transport level of the OSI model.

c) Monitoring of full network traffic – this is a means for quality-quantity evaluation of network traffic generated for each service and each network protocol. It could be used for a local network or WAN environment. The results from the monitoring permit to characterise the frequency and volume of the traffic, relatively and absolute work-load generated by monitored services and protocols in the network. All frames are accessible in the end of each monitoring phase that permits to trace the traffic. A defect of this method is the forming of frame buffer in the time. Different program tools called protocol analysers are used for monitoring of full traffic.

d) Monitoring with statistically processed results – it permits to monitor the full network traffic, but the obtained results are statistical, for example as traffic types, assessments for the communicated machines without details of the real frames, etc. This method is very suitable for a long time monitoring. Usually the statistical results are accessible not only in the end but during the different phases of the experiments.

- The utilization of tools for visualization of the monitoring results is very important problem at the traffic analysis. In more of the cases the tools for packets catching and analysis don’t offer possibilities for results exporting to a popular format for digital presentation and visualization.

- Utilization of the monitoring results for traffic optimization – the network traffic optimization is a consequence of the registration process and analysis. It is connected to the reconfiguration of the different network infrastructures defined by OSI model. The main goals of the optimization could be as follows:

a) to decrease the size of the network traffic (work-load decreasing) by elimination of redundant traffic;

b) to decrease the time of answer in network medium that is connected with defining the minimal route in a complex topology. This goal is applicable usually for applications with critical time requirements, for example, applications based on the technology Voice-Over-IP (VoIP);

c) to increase the traffic capacity of the network environment – this optimization could be made for network applications with high needs of resources.

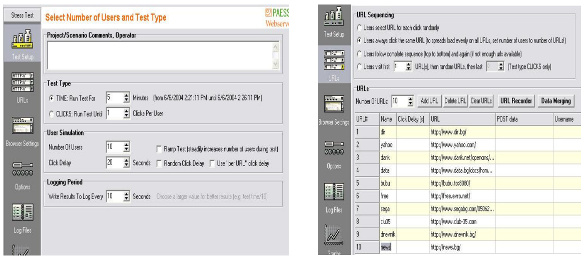
Two *basic approaches* for network traffic monitoring should be defined:

1. Monitoring of the details for each or more part of frames passed through the network medium – this approach permits inspection of each passed frame or filtering using special criteria. This method is very suitable for decision of different network problems

2. Monitoring of statistical processed results for the network segments workload and investigation of the distribution of the network protocols and services under segments. The method is suitable for optimization based on long time monitoring of the network segment parameters.

The monitoring of network traffic should be made using different system or application *tools* for measurement, registration and analysis. Some of them are listed below:

- *Webserver Stress Tool* – HTTP client-server application for testing designed for precise results in the server. It gives information for reasons for performance decreasing. The server performance should be tested at a normal and high workload. The program simulates independent users accessed to the set of sites. Each user is simulated by a thread with own session information and it generates URLs independently from other users (fig. 1). Webserver Stress Tool for Windows can test different type servers (static pages, JSPs/ASPs, CGIs) and gives the results about performance, loading and carry out “stress” tests (fig. 2).



Select Number of Users and Test Type

Project/Scenario Comments, Operator

Test Type
● TIME: Run Test For 5 Minutes (from 6/6/2004 2:21:11 PM until 6/6/2004 2:26:11 PM)
○ CLICKS: Run Test Until 1 Clicks Per User

User Simulation
Number Of Users 10 □ Ramp Test (steadily increases number of users during test)
Click Delay 20 Seconds □ Random Click Delay □ Use "per URL" click delay

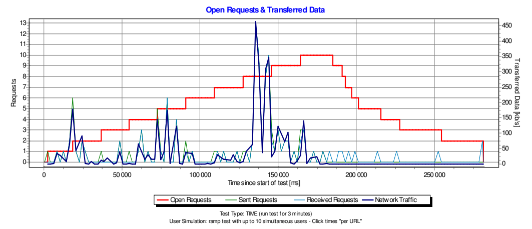
Logging Period
Write Results To Log Every 10 Seconds Choose a larger value for better results (e.g. test time/10)

URL Sequencing
○ Users select URL for each click randomly
● Users always click the same URL (to spreads load evenly on all URLs, set number of users to number of URLs!)
○ Users follow complete sequence (top to bottom) and again (if not enough urls available)
○ Users visit first 1 URL(s), then random URLs, then last 0 (Test type CLICKS only)

URLs
Number Of URLs: 10 Add URL Delete URL Clear URLs URL Recorder Data Merging

URL#	Name	Click Delay [s]	URL	POST data	Username
1	dir		http://www.dir.bg/		
2	yahoo		http://www.yahoo.com/		
3	darik		http://www.darik.net/opencms/...		
4	data		http://www.data.bg/docs/hom...		
5	bubu		http://bubu.to:8080/		
6	free		http://free.evro.net/		
7	sega		http://www.segabg.com/05062...		
8	clu35		http://www.club-35.com		
9	dnevnik		http://www.dnevnik.bg/		
10	news		http://news.bg/		

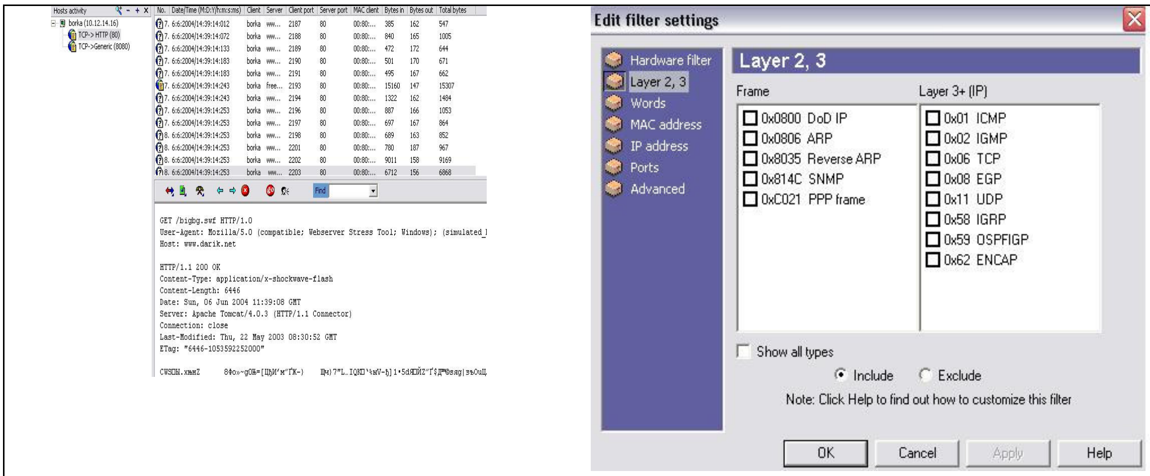
Figure 1. Defining of the URLs count and names



Test Type: TIME (run test for 3 minutes)
User Simulation: ramp test with up to 10 simultaneous users - Click times "per URL"

Figure 2. Statistic for requests and transferred data obtained by "stress" test

- *Iris* – this is a software product for management of network traffic. It has graphical user interface for observation of input and output network traffic and permits to investigate each session and its owner by measured data. Iris permits to trace the sequence of packets in a session. The formed HTTP session is decoded and the web page is visualised as a result. By this way Iris shows not only the packet that defines the session, but the content of data sent in this session (fig. 3a). It is possible to observe the input and output connections for concrete machine that should be realized by filtering (fig. 3b). The filters should be made based on HW level, protocol level, keywords, MAC addresses, IP addresses, port of the sender or of the receiver, size of the package, etc. The program gives different statistical estimations



No.	Date/Time (M:D:Y/h:m:s:ms)	Client	Server	Client port	Server port	MAC client	Bytes in	Bytes out	Total bytes
7.	6:6:2004/14:39:14:012	borka	ww...	2187	80	00:80:...	385	162	547
7.	6:6:2004/14:39:14:072	borka	ww...	2188	80	00:80:...	840	165	1005
7.	6:6:2004/14:39:14:133	borka	ww...	2189	80	00:80:...	472	172	644
7.	6:6:2004/14:39:14:183	borka	ww...	2190	80	00:80:...	501	170	671
7.	6:6:2004/14:39:14:183	borka	ww...	2191	80	00:80:...	495	167	662
7.	6:6:2004/14:39:14:243	borka	free...	2193	80	00:80:...	15160	147	15307
7.	6:6:2004/14:39:14:243	borka	ww...	2194	80	00:80:...	1322	162	1484
7.	6:6:2004/14:39:14:253	borka	ww...	2196	80	00:80:...	887	166	1053
7.	6:6:2004/14:39:14:253	borka	ww...	2197	80	00:80:...	697	167	864
8.	6:6:2004/14:39:14:253	borka	ww...	2198	80	00:80:...	689	163	852
8.	6:6:2004/14:39:14:253	borka	ww...	2201	80	00:80:...	780	187	967
8.	6:6:2004/14:39:14:253	borka	ww...	2202	80	00:80:...	9011	158	9169
8.	6:6:2004/14:39:14:253	borka	ww...	2203	80	00:80:...	6712	156	6868

```
GET /bigbg.swf HTTP/1.0
User-Agent: Mozilla/5.0 (compatible; Webserver Stress Tool; Windows); (simulated_
Host: www.darik.net

HTTP/1.1 200 OK
Content-Type: application/x-shockwave-flash
Content-Length: 6446
Date: Sun, 06 Jun 2004 11:39:08 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Connection: close
Last-Modified: Thu, 22 May 2003 08:30:52 GMT
ETag: "6446-1053592252000"

CWS□Ы.xњнZ      8Фо»~gOЊ=[ЦђИ'м"ЃЖ-)     Щч)7"L…IQK□'%ыV-ђ]1•5dЯ□ЙZ"Ѓ$Д™©sяg|зъOuЦ
```

Layer 2, 3

Frame
- ☐ 0x0800 DoD IP
- ☐ 0x0806 ARP
- ☐ 0x8035 Reverse ARP
- ☐ 0x814C SNMP
- ☐ 0xC021 PPP frame

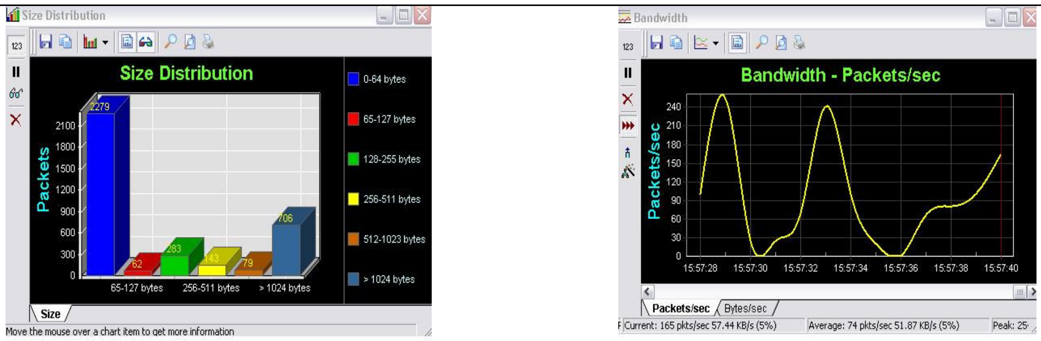
Layer 3+ (IP)
- ☐ 0x01 ICMP
- ☐ 0x02 IGMP
- ☐ 0x06 TCP
- ☐ 0x08 EGP
- ☐ 0x11 UDP
- ☐ 0x58 IGRP
- ☐ 0x59 OSPFIGP
- ☐ 0x62 ENCAP

☐ Show all types

● Include ○ Exclude

Note: Click Help to find out how to customize this filter

Figure 3. A session defining and filters using

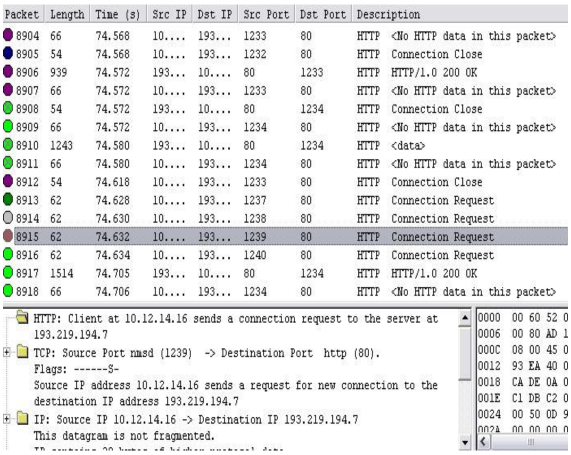


Move the mouse over a chart item to get more information

Current: 165 pkts/sec 57.44 KB/s (5%) Average: 74 pkts/sec 51.87 KB/s (5%) Peak: 25

Figure 4. Network statistic

about protocols parameters, size distribution, bandwidth, etc. (fig. 4)



Packet	Length	Time (s)	Src IP	Dst IP	Src Port	Dst Port	Description
8904	66	74.568	10....	193...	1233	80	HTTP <No HTTP data in this packet>
8905	54	74.568	10....	193...	1232	80	HTTP Connection Close
8906	939	74.572	193...	10....	80	1233	HTTP HTTP/1.0 200 OK
8907	66	74.572	10....	193...	1233	80	HTTP <No HTTP data in this packet>
8908	54	74.572	193...	10....	80	1234	HTTP Connection Close
8909	66	74.572	10....	193...	1234	80	HTTP <No HTTP data in this packet>
8910	1243	74.580	193...	10....	80	1234	HTTP <data>
8911	66	74.580	10....	193...	1234	80	HTTP <No HTTP data in this packet>
8912	54	74.618	10....	193...	1233	80	HTTP Connection Close
8913	62	74.628	10....	193...	1237	80	HTTP Connection Request
8914	62	74.630	10....	193...	1238	80	HTTP Connection Request
8915	62	74.632	10....	193...	1239	80	HTTP Connection Request
8916	62	74.634	10....	193...	1240	80	HTTP Connection Request
8917	1514	74.705	193...	10....	80	1234	HTTP HTTP/1.0 200 OK
8918	66	74.706	10....	193...	1234	80	HTTP <No HTTP data in this packet>

```
HTTP: Client at 10.12.14.16 sends a connection request to the server at
193.219.194.7
TCP: Source Port nmsd (1239)  -> Destination Port  http (80).
Flags: ------S-
Source IP address 10.12.14.16 sends a request for new connection to the
destination IP address 193.219.194.7
IP: Source IP 10.12.14.16 -> Destination IP 193.219.194.7
This datagram is not fragmented.
```

```
0000  00 60 52 0
0006  00 80 AD 1
000C  08 00 45 0
0012  93 EA 40 0
0018  CA DE 0A 0
001E  C1 DB C2 0
0024  00 50 0D 9
002A  00 00 00 0
```

Figure 5. Main form of the Distinct Network Monitor

- *Distinct Network Monitor* – this is a program for packets catching and analysis of the network protocols. It presents the complex relationships of the protocols by natural language and defines correct by the errors (fig. 5). It registers the measured data and analyses the modules and after that shows an actual picture for reality in the investigated network segment. A module for statistics is integrated into this program.

- *Microsoft Performance Monitor* – this is a standard instrument of the Windows NT system that permits observation of the parameters of different internal for Windows NT and external objects.
- *Microsoft Network Monitor* – this monitor is a typical network analyser. The basic version is included in the operating system Windows NT as a component for observation and analysis. The full version is a component of the Microsoft Systems Management Server. The difference between two versions is in the functionality. This monitor is a program showed the content of the catch packages. It uses the driver Network Monitor Agent (standard system component) for realization of its functions.
- *LANAlyzer* – this program is power instrument of Novell and should be used for long time observation of the network traffic.

4. CONCLUSION

The investigation of the processes in a distributed environment is very important for making an optimization of topology, relationships and all network structures for session management. In this reason the analysis of network traffic permits to obtain actual assessments for stochastic parameters of the communication between users and servers in a network medium. There are two basic methods for realisation of the investigation – modelling and monitoring.

The modelling should be used at the network infrastructure organization and defining an optimal topology for communications. There are different program tools for designing suitable models for description of network objects and processes. The realization of different experiments based on these models will permit to evaluate alternative structures or topologies, condition for the communications organization, level of workload, etc.

The monitoring is very suitable means for direct measurement of characteristics of the active computer processes and evaluation of work parameters of the computer components. In the case of network traffic analysis this method is more appropriate because it allows to obtain real measures for investigated stochastic parameters as traffic size, packets distribution, bandwidth, requests servicing, access time, etc. The measured values should be used for an evaluation of the information servicing parameters and to define the limitations of the network infrastructure on the information processes and access to de distributed resources. The contemporary program monitoring tools are very functional and give rich statistical assessments for precise analysis and evaluation.

REFERENCES

[1] Dong-Hyung Heo, Sang-Wook Chung, Gil-Haeng Lee. The effects of management traffic on the local call processing performance of ATM switches using network models and Jackson's theorem. ETRI Journal (Information, Telecommunication & Electronics), 2003, vol. 25, No 1, pp. 34-40.

[2] Korres, G.N., P. Katsikas. Real-time monitoring of network topology through analog measurements. Power Tech Proceedings, 2001 IEEE Porto, 10-13 Sept. 2001, vol. 3, 6 pp.

[3] Kun-Chan Lan, J. Heidemann. Rapid model parametrization from traffic measurements. ACM Trans. on Modeling and Computer Simulation (TOMACS), July 2002, vol. 12, No 3, pp. 201-209.

[4] Downie, J.D., D. J. Tebben. Performance monitoring of optical networks with synchronous and asynchronous sampling. Optical Fiber Communication Conference and Exhibition, 2001, vol. 3, pp. WDD50-1 - WDD50-3.

[5] Ji, C., A. Elwalid. Measurement-based network monitoring: missing data formulation and scalability analysis. Proceedings of the IEEE International Symposium on Information Theory, 25-30 June 2000, p. 78.

[6] Korres, G.N., G. C. Contaxis. External system monitoring based on a reduced state estimation model. Power Tech Proceedings, 2001 IEEE Porto, 10-13 Sept. 2001, vol. 3, 6 pp.

[7] Hung-Kai Shiu, Yi-Hao Chang, Ting-Chao Hou, Cheng-Shong Wu. Performance analysis of TCP over wireless link with dedicated buffers and link level error control. Proc. of the 2001 IEEE International Conference on Communications (ICC 2001), 11-14 June 2001, vol. 10, pp. 3211-3216.

[8] Li, L., M. Thottan, B. Yao, S. Paul. Distributed network monitoring with bounded link utilization in IP networks. Proc. of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), 30 March-3 April 2003, vol. 2, pp. 1189-1198.

[9] van der Merwe, J., R. Caceres, Y. Chu, C. Screenan. A tool for monitoring Internet multimedia traffic. ACM SIGCOMM Computer Communication Review, Oct. 2000, vol. 30, No 5, pp. 48-59.

[10] Fabre, E., V. Pigourier. Monitoring distributed systems with distributed algorithms. Proceedings of the 41st IEEE Conference on Decision and Control, 10-13 Dec. 2002, vol. 1, pp. 411-416.

[11] Liang Xu, Xuemin Shen, J. W. Mark. Performance analysis of rate adaptation scheme for data traffic in DS-CDMA systems. Proc. of the International Conference on Dependable Systems and Networks, 23-26 June 2002, pp. 957-666.

[12] Thurm, B., H. B. Wiltfang. Link-based performance monitoring of ATM networks. Proceedings of the 25th Annual IEEE Conference on Local Computer Networks (LCN 2000), 8-10 Nov. 2000, pp. 604-613.