5-4 Research and Development of Application-oriented Management Platform

MASUDA Hisanori, SUGANUMA Takuo, KEENI Glenn Mansfield, SHIBATA Yoshitaka, KINOSHITA Tetsuo, and SONE Hideaki

This article summarizes the research activities at Tohoku JGN II Research Center. The main theme of our Research Center is “Research and Development of Application-oriented Management Platform”. It consists of three sub themes: (i) Development of network traffic measurements/analysis for ultra high speed and large scale network, (ii) Development of application-oriented management and security techniques, (iii) Development of flexible middleware technique. Network event detection is important for network management, where managers need to know what is happening in their local network. For example, security related incidents, network faults and so on. Our proposed method provides the useful event information, based on multiple traffic monitoring and log mining. We conducted an experiment and evaluated the proposed method using http traffic and logs. The result shows that the event information is enough for the network managers to recognize the contents of network event.

Keywords
Application-oriented, Event detection, Network management, Flexible network middleware

1 Outline of the Tohoku JGNⅡ Research Center

The Tohoku JGNⅡ Research Center (hereafter referred to as the “Tohoku RC”) is currently undertaking the development of an application-oriented management platform that can provide the network information required by an application accurately, upon demand, and with sufficient quality, with the goal of R&D of an Application-Oriented Management Platform (a sub-theme of the JGNⅡ Research and Development Project Theme IV: Research and Development of Platform Application Technologies).

The Tohoku RC has set three further sub-themes for R&D of an Application-Oriented Management Platform and has instituted one research group for each sub-theme. There are two advisors for the overall theme, and Professor Hideaki Sone of Tohoku University is a sub-leader overseeing projects at the Tohoku RC. A visiting researcher and an expert researcher are also involved in promoting research activities at the Tohoku RC.

The sub-themes are summarized as follows:

(1) Development of network traffic measurement/analysis technology for an ultrahigh-speed and large-scale network

Effective monitoring and management of the ultrahigh-speed and large-scale networks of today is growing difficult due to the dramatic increase in the number of devices and volumes of data involved. The group for this theme is pursuing R&D of detection and analysis technology for network events based on measurement and analysis of network traffic[1]-[5].

(2) Development of an application-oriented

management and security technology

This group is carrying out research on a method for extraction of application control information from the observed network information, and on methods for measuring, consolidating, and efficiently collecting the characteristics of communication at an application-level in order to establish network observation technology for a single application unit. Further, the group will conduct research on intelligent operation and management technologies for high-quality, highly efficient networks, taking into consideration application characteristics and user activity information, and on development of methods of assuring equivalent distribution of resources between various applications and of controlling and optimization the bandwidth over the entire network. Research is also underway to develop service maintenance technology to provide defense against network attacks[6]-[13].

(3) Development of flexible network middleware technologies

This group is undertaking R&D on network middleware technology that can respond flexibly to demands from users and applications and to network environments and characteristics, with the goal of realizing a knowledge-based network based on the "flexible network" concept. The main focus of R&D of flexible network middleware (FNM) is currently placed on the development of a mechanism for dynamic construction and reconstruction by agent-based middleware components using domain knowledge[14]. Furthermore, we have adopted Midfield System based on the transcoding function in order to establish a flexible multimedia communications service function that will provide the quality of service (QoS) required for various changes in the characteristics of network resources[15]-[17].

In addition to the above sub-themes, the Tohoku RC is actively soliciting requests for support in regional events and offers for collaboration in a range of local projects. This collaboration is exemplified in joint research with regional organizations in the development of an application for intra- and inter-regional broadcasting and remote education systems. The following sections detail the research for each sub-theme.

2 Network traffic measurement/analysis technology for an ultrahigh-speed and large-scale network

2.1 Event detection method

2.1.1 Summary

In recent years, active research has been focused on techniques for detecting abnormal changes in traffic through so-called "anomaly detection" applied to actual network management. However, methods to date have relied on evaluation measures that identify anomalies based on only two states—the presence or absence of an anomaly—and thus were incapable of providing detailed information on the actual event upon detection. As a result, individual network administrators were forced to investigate such events as part of actual network management. To resolve this problem, this sub-theme group has proposed a system that will automatically prepare a summary of the anomalous event by linking the results of traffic anomaly detection with log information.

2.1.2 Network event detection

In this paper, a "network event" is defined as one event (among all of the events occurring within the domain managed by an administrator) that he or she recognizes to be of significance in terms of network management. Some examples include linkdowns caused by switch malfunctions or cable breaks, unauthorized access from an external source (such as DoS attacks and portscans), unauthorized use of P2P file transfer software, excessive resource consumption (such as the domination of bandwidth by worms), and bursts in traffic accompanying the release of software. Administrators investigate and determine the contents of such events after detection and apply emergency measures when necessary. Administrators also conduct more detailed investigations of the events in question to aid in long-

term management strategies; these investigations inevitably require extensive knowledge and experience, and the workloads placed on the administrators are thus immense. This study aims to relieve this administrative burden through automation of the work involved.

2.1.3 Event summation system[4] [5]

This study proposes a scheme to supplement the lack of event information under existing anomaly-detection techniques, through automatic summation of an event by combining log information with event detection. Existing methods report only on the results of anomaly detection with the message that an anomaly has been detected in traffic characteristics, while under the present scheme, the relevant report also includes more useful information on the type of event detected. Figure 1 shows an outline of the proposed system. First, traffic is input to an anomaly-detection module, and determination of normal/abnormal conditions are made in real time. The volume of calculations is small at this level, and a traffic-event detection model based on an anomaly detection method using frequency analysis is under consideration for use in the real-time detection algorithm. Here the high-frequency components are first extracted from the traffic data series using a fourth-order Butterworth high-pass filter. The deviation score method is then applied to the extracted components to detect the anomaly. Concurrently with this procedure, a continuous log is kept on the application and system logger, and events occurring within the log are analyzed, with similar events clustered for future use. The event summation module analyzes information from both the anomaly-detection module and the log file. When an "anomaly detected" judgment is input to the event summation module, the module searches through all related logs near the time of the event and prepares a summary of the event by selecting the necessary information and conveying this data to the administrator. The details of the algorithm are given elsewhere [4] [5].

2.1.4 Experiment and evaluation

To verify the feasibility and effects of the proposed scheme, actual traffic data and application logs were obtained from the network for an experimental run. This experiment was aimed at anomaly detection in http traffic and mining of the http server application log. The LAN was connected to the external network via a single router unit, with http servers operating on two host units (A and B) constituting the LAN. The target logs for mining consisted of the access and error logs for each unit. The left-hand plot in Fig. 2 shows the change in traffic with time for the traffic data used for anomaly detection observed at the router, with total traffic sampled for one week in units of five-minute periods. The right-hand plot in Fig. 2 shows the deviation scores of the high-frequency components extracted by the high-pass filter. The results of analysis revealed that the error logs for Host A showed massive incidences of the errors "segmentation fault", "file does not exist", and "script not found or

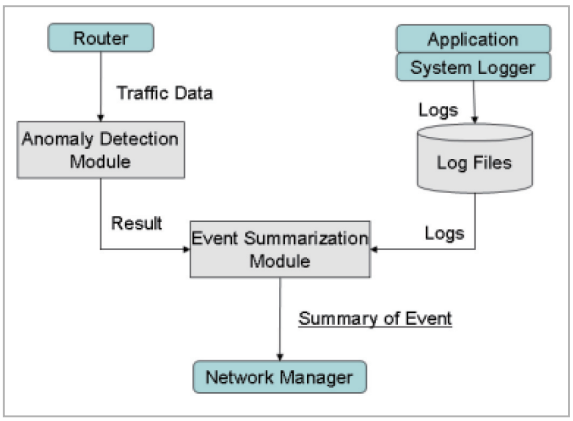

Fig.1 Scheme of event-detection system

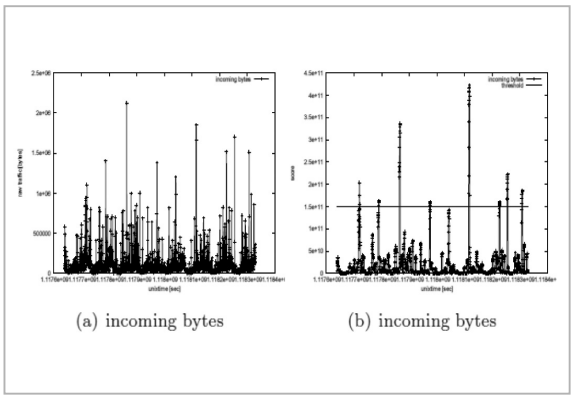

Fig.2 Http traffic and corresponding deviation score

unable to state", all within a short period of time. The access logs of Hosts A and B revealed that large volumes of requests had been sent from a specific server, and this information was judged as significant by the module. The event was then summarized based on this judgment. The information supplied in the corresponding report is both necessary and sufficient for the administrator to understand the contents of the event with ease, and we thus concluded that this scheme can effectively relieve the administrator of the workload involved in searching through logs on his or her own.

2.2 Event detection and management system

(1) Event detection

Network traffic monitoring is an important element of network management and security. Network monitoring should not be the end goal, but rather should serve as a means for analyzing and understanding exactly what is taking place on the network. Observation results obtained from monitoring can reveal the effects of network anomaly events, errors in operation, and security problems, among others. In addition, these results can also be used to predict the quality of service (QoS) or to estimate required bandwidth.

With this project, the authors are working to develop an event model for monitoring traffic data on the JGNⅡ network. The details of this event model are given in Section **2.1**. Further, we are currently developing a group of analysis tools that will support data analysis both online and offline, so that we may provide an effective evaluation of the model under study.

This group of tools will be used to detect target events on the network. The detected events will then be classified according to cause (for example, access concentrations due to a surge in ticket reservations on the web, increases in traffic due to security problems, or traffic anomalies associated with failures) and subsequently investigated. Ultimately, our aim is to provide network event information for users ranging from network administrators to the general user.

(2) Basic tool group

The network monitoring described in (1) above involves complex configurations. The five tools below have been developed to date to facilitate these configurations and to enable efficient overall monitoring.

(a) "Switch monitor configuration system" to simplify setup of the network monitoring system: This tool enables efficient setup of the monitoring system by the network administrator.

(b) "Piped NetGrapher" for visualization of traffic: This tool enables the visualization of traffic data generated by an application and allows online traffic observation.

(c) "Summary Traffic Data Module" summarizing statistical information: This tool outputs statistical information in CSV format and enables statistical analysis using standard visualization tools.

(d) "Traffic Tracker Bar Graph (TTBG) system" to track specific traffic on a Layer-2 network: This tool allows for tracking of the port-based traffic source for switches.

(e) "Event Detection and Management System" to define and detect events both online and offline: details for this tool are given in (3) below.

(3) Event detection and management system (Fig. 3)

Normal network monitoring routines focus mainly on events. In the absence of detected events, the network administrator is unlikely to check the massive volumes of traffic data, which will usually be archived, backed-up on offline media, or discarded without detailed analysis. Present monitoring systems lack the ability to detect a specific target event, and so administrators are left with two choices—either to search through the massive volumes of traffic data or to abandon the effort altogether. In this study, events are assessed in terms of long-term changes based on statisti-

cal analysis. In many cases, administrators are interested in a specific event (e.g., micro-events such as file transfers, web-page transfers, and mail transfers). The administrator may also be interested in macro-events, such as sessions between two points involving multiple micro-events or data streaming. Network problems may also be viewed as events. In these cases, traffic may suddenly decrease, leading to a dramatic change in RTT. The aim of this study is to develop a mechanism to detect various types of events automatically and to report outbreaks of these events to the administrator. The present application detects events based on the given rules, with a resultant event report that allows the administrator to visualize the associated traffic information graph directly (Figs. 4–6).

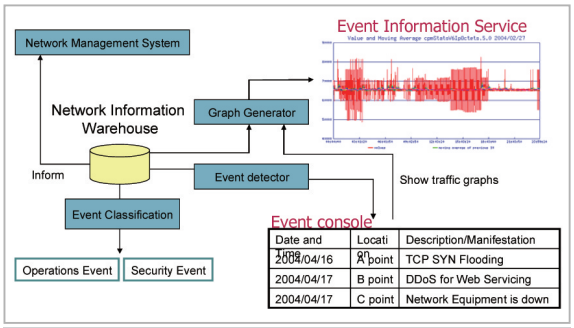

Fig.3 *Scheme of event detection and management system*

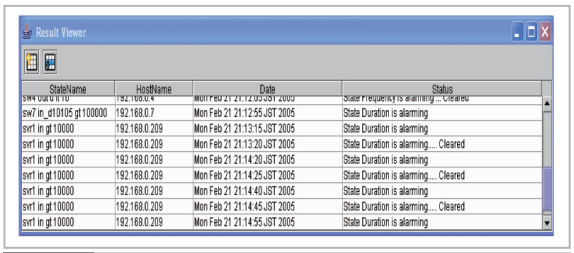

Fig.4 *Display of alarm list*

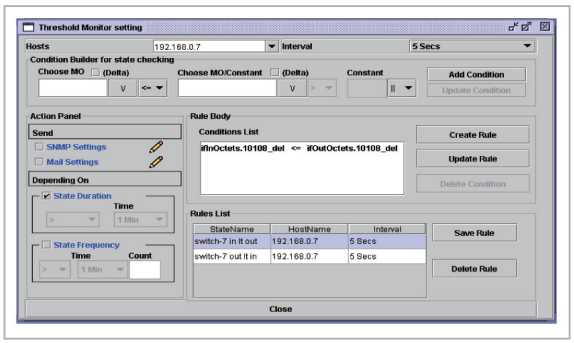

Fig.5 *Rule definition by U/I*

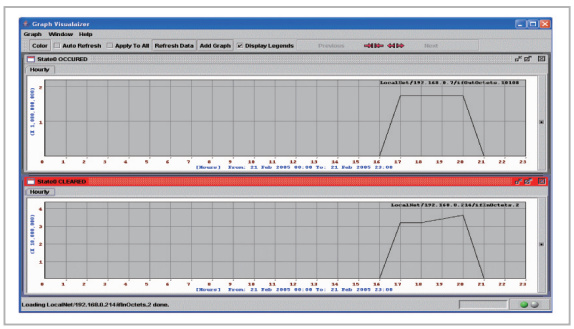

Fig.6 *Traffic graph of target event*

3 Application-oriented management platform and middleware technology

3.1 Application-oriented management platform and security technology

3.1.1 Management assist technology based on integration of management information

The video-distribution system based on network-operation intelligence is under development as a network management technology for a multipoint mutual video-distribution network (Fig. 7)[6]. The system is a relay-and-distribution splitter with a protocol conversion function to enable video distribution between multiple points, and is expected to improve efficiency of bandwidth usage over the entire distribution network. The operation-and-statistical information integration system is for collection and handling of observation data of network and application status (Fig. 8)[7]. The system integrates information on both operation and statistical information along the time axis, and performs continuous and quantitative measurements for each layer[8]. Field experiments for these developed technologies are conducted though numerous video-distribution events as part of the "Experiment for an Inter-regional Broadband Content-Distribution Backbone" and "CATV Content-Distribution Experiment" projects on the JGNⅡ testbed network[9]. Practical experiments[12] are also underway to assess an on-demand distributed

file system as an effective operation technique of a large-volume distributed distribution system[10][11].

3.1.2 Application development with regional cooperation

Along with the practical experiments using JGNⅡ described above, establishment of an end-user environment for the use of distributed images is also undergoing development as an application in collaboration with regional organizations. Intra- and inter-regional applications are carried out in the broadcasting activities and remote education[13].

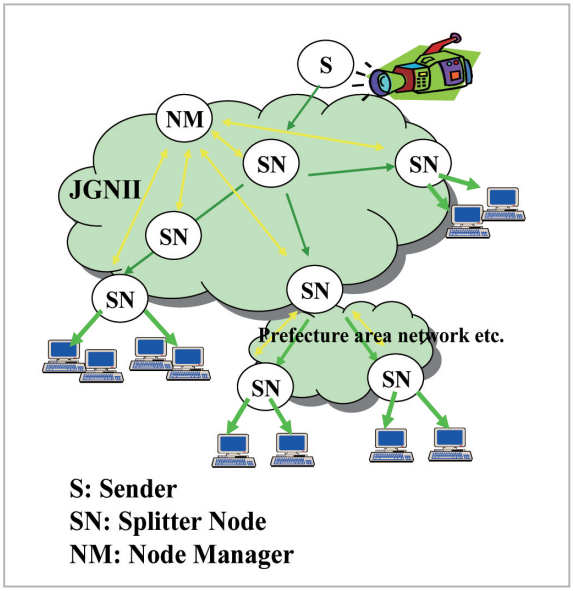

Fig.7 *Multipoint image-distribution network*

3.2 Flexible network middleware technology

3.2.1 One-to-many and many-to-many communication mechanism

To study one-to-many or many-to-many communication mechanisms for an agent-based middleware architecture, we investigated a method of constructing an application-layer multicast (ALM) tree in a total-connection overlay network and examined an agent-oriented design for specific middleware components. Under existing ALM methods, a simple overlay network with a relatively small number of branches (i.e., several branches) which correspond to the number of direct connections established between nodes, as shown in the left-hand side of Fig. 9, is established in order to reduce the computational load during the construction of the tree. The drawback of the restriction on the number of branches is that in many cases this leads to the construction of inefficient trees. We therefore examined a method for calculating a multicast tree of a total-connection overlay network that did not limit a number of candidate branches at the outset[14]. For instance, nodes B–F are first grouped based on the delay from transmitting node A, as shown in the right-hand side of Fig. 9. Each group is arranged in levels (Lv) of increasing order, from groups with small delays to those with large delays. A pro-

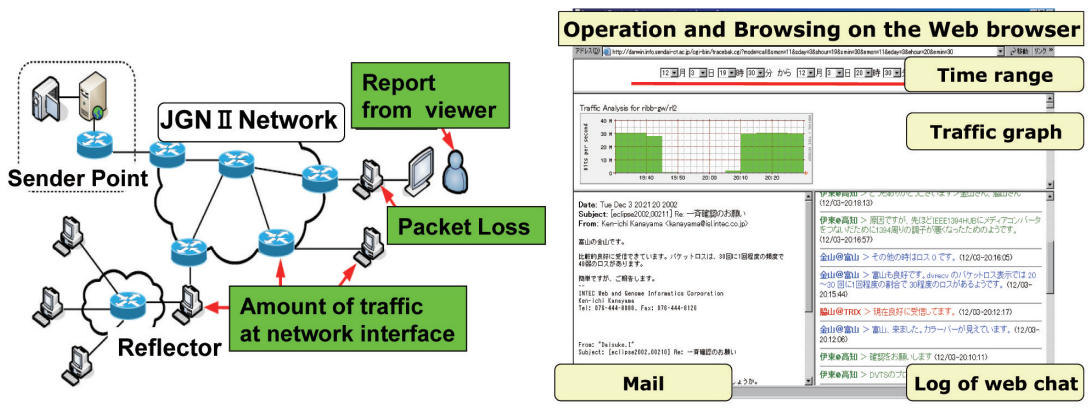

Fig.8 *Management and statistic information-integration system: System configuration (left) and example screen image (right)*

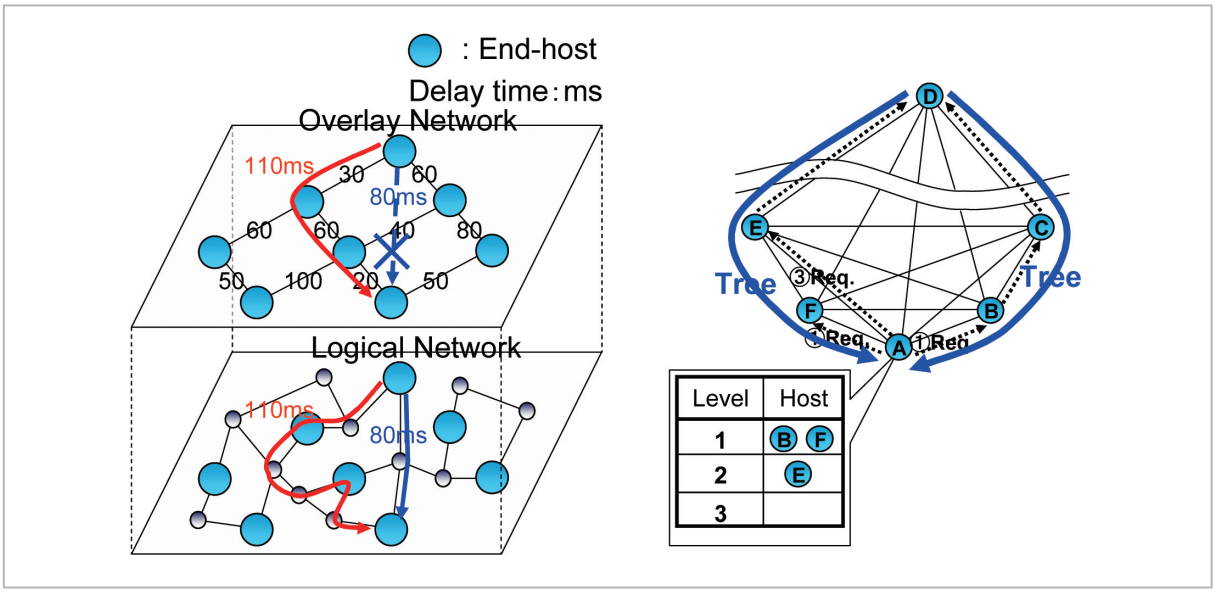

Fig.9 *Existing method of ALM tree construction (left) and the total-connection method proposed by the authors (right)*

visional calculation is made for a tree taking the nodes in the group with a low delay Lv as candidates for connection. When the required delay conditions are not satisfied, calculations proceed to include as candidates the nodes in the group on the next Lv. In this way, a tree satisfying the required delay conditions will eventually be found insofar as a solution is possible.

Further, we examined an agent-oriented design proposed to put the above method into practice. As a result, we were able to come up with the four agent-based middleware components shown in Fig. 10: (1) an Application Controller, (2) a Data Info Holder, (3) a Main Controller, and (4) a Communicator. In the future, we will construct a prototype system based on these results and evaluate the proposed method.

3.2.2 MidField system

In various network and interconnected computing resource environments, more flexible multimedia communication service functionality is required to respond to the temporal change in available resources and quality of service (QoS) requirement for transmitted media. To realize this service function, we have now introduced MidField, which is a middleware system based on a transcoding

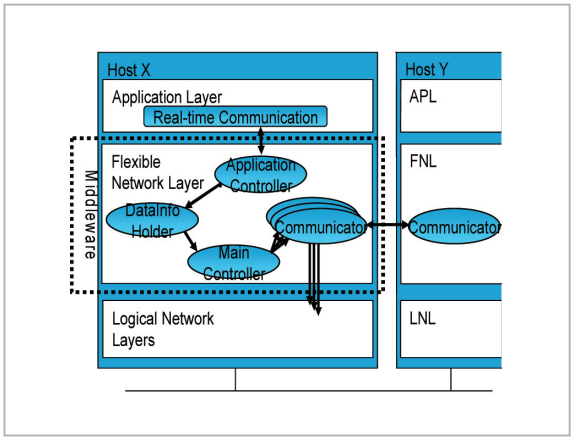

Fig.10 *Middleware component design*

function[15]-[17].

As can be seen in Fig. 11, the MidField System consists of a three-layer and four-plane structure on top of the transport layer, and provides flexible multimedia communication functions to applications. The Stream Plane carries out multimedia streaming transmission functions including media synchronization, data conversion, and flow control. The Session Plane performs session managements on end-to-end intercommunication, the System Plane is in charge of resource management, and the Event Process Plane performs event processing within the system.

The MidField System enables both multi-

cast and unicast transfer functions for a wide variety of media streams—from high quality DV format videos to low quality MPEG4 format videos—according to available bandwidth and load conditions corresponding to the computing resources on both sender and receiver sides by using dynamic media conversion and transcoding functions in response to user's demands for service, as can be seen in Fig.12.

Currently, in addition to DV format videos and high definition video, an HDV (1080 × 1440) format video transfer system featuring not only the standard one-directional camera, but also an omni-directional camera with a special 360° viewing lens, is currently under development to guarantee transmitted video quality for various applications such as tele-conference and tele-observation systems. Performance and functional evaluations of the system are also planned.

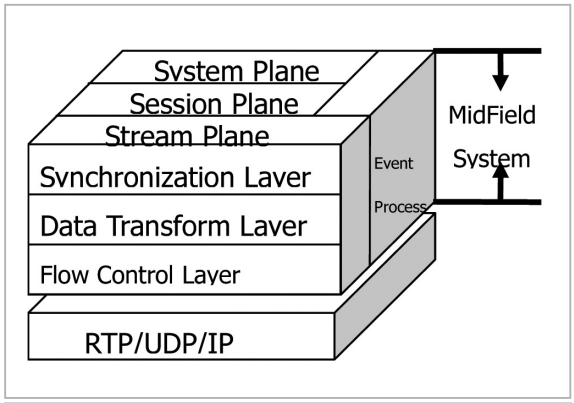

Fig.11 *Architecture of the Midfield System*

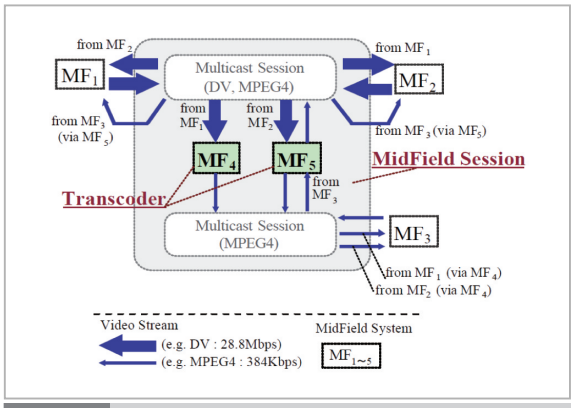

Fig.12 *Midfield transcoding function*

4 Conclusions

This paper summarized the research and development efforts underway at the Tohoku JGNⅡ Research Center. The Center is currently pursuing the three sub-themes described above, and studies to date have produced results essentially according to the original schedule. In the future, we will link the efforts among the three sub-themes with the aim of expanding the overall scope of our research.

References

1 Zhang Ding Hui, Kazuhide Koide, Gen Kitagata, Glenn Mansfield Keeni and Norio Shiratori, "Detection of Network Events using Digital Signal Processing Techniques", IEICE Technical Report, IN2004-66, pp.37-41, September, 2004.

2 Katsuhisa Abe, Glenn Mansfield Keeni and Norio Shiratori, "Network Traffic Analysis on the basis of RTT measurements", IEICE Technical Report, MoMuC2004-92, pp.27-32, January, 2005.

3 Zhang Ding Hui, Kazuhide Koide, Gen Kitagata, Glenn Mansfield Keeni and Norio Shiratori, "Detection of Network Events based on Digital Filtering", IPSJ SIG Technical Reports, 2005-DPS-122, pp.271-276, March, 2005.

4 Masahiro Nagao, Gen Kitagata, Takuo Suganuma and Norio Shiratori, "Automatic Event Interpretation based on Traffic Analysis using Difference Filter and Log Mining", IPSJ SIG Technical Reports, 2005-DPS-123, pp.19-24, June, 2005.

5 Masahiro Nagao, Gen Kitagata, Takuo Suganuma and Norio Shiratori, “Automatic Network Event Summarization based on Combination of Traffic Anomaly Detection and Log Mining”, IEICE Technical Report, IN2005-70, pp.55-60, September, 2005.
6 Kenichi Sakurai and Hironori Kanno, “Design and Implementation of a DV/IP Splitter System”, 2005 Tohoku-Section Joint Convention Record of Institutes of Electrical and Information Engineers, 1E-10, August, 2005.
7 Go Naraoka, Yasuyuki Aizawa, Erika Tsuruta and Shunichiro Wakiyama, “Development of an integrated information system of network operation and statistics which aimed at the support of video delivery experiments”, ITRC Technical Report, C-6, January, 2005.
8 Erika Tsuruta, Yasuyuki Aizawa and Shunichiro Wakiyama, “Improvement of usability in an integrated information system for video delivery network”, 2005 Tohoku-Section Joint Convention Record of Institutes of Electrical and Information Engineers, 1E-08, August, 2005.
9 Shunichiro Wakiyama, Hironori Kanno and Hideaki Sone, “Outline of experiments at Tohoku JGN2 research center for inter-regional broadband contents distribution”, ITRC Technical Report No.36, September, 2005.
10 Hironoi Kanno, Hideaki Sone and Yoshiaki Nemoto, “Modeling of the Traffic in On-demand NetNews Delivery System and Its Evaluation of Response Time”, IPSJ Journal, Vol.44, No.3, pp.535-543, March., 2003.
11 Hironori Kanno and Hideaki Sone, “A Study of Directory Information Management Method in On-demand Delivery System”, ITRC Technical Report No.26, February, 2004.
12 Satoshi Nounin, Hironori Kanno and Hideaki Sone, “Information management and server selection of a distributed delivery system”, Joint Seminar of Core University Program and JSPS 163rd Committee on NGI, Daejon , A23-1, November, 2004.
13 Shunnichiro Wakiyama, Hironori Kannno, Yuichi Hayashi, Go Naraoka, Masatomo Nishikibe and Hideaki Sone, “Construction and operation of video delivery network at "JGN2 promotion forum 2004 in Tohoku" ”, 2004 Tohoku-Section Joint Convention Record of Institutes of Electrical and Information Engineers, 1F-4, August, 2004.
14 Daisuke Hasegawa, Gen Kitagata, Takuo Suganuma, Tetsuo Kinoshita and Norio Shiratori, “An Application Level Multicast Tree Construction Scheme for Multi-User Communications”, ITRC Technical Report No.37, A-3, October, 2005.
15 Koji Hashimoto and Yoshitaka Shibata, “Mobile Agent-Based Adaptive Multimedia Communication”, “INTELLIGENT VIRTUAL WORLD Technologies and Applications in Distributed Virtual Environment”, World Scientific Publishing Co. Pte. Ltd., ISBN:981-238-618-1, pp.179-190, 2004.
16 Koji Hashimoto and Yoshitaka Shibata, “A Middleware for Intercommunication Adapted to User's Communication Environments”, IPSJ Journal, Vol.46, No.2, pp.403-417, February, 2005.
17 Yuya Maita, Koji Hashimoto and Yoshitaka Shibata, “A New TV Conference System with Flexible Middleware for Omni-directional Camera,” Proc. on DEXA2005 Workshop, NBiS, pp.84-88, August, 2005.

MASUDA Hisanori

Expert Researcher, Tohoku JGNII Research Center, Collaborative Research Management Department

Human-Computer Interaction

***KEENI Glenn Mansfield**, Ph.D.*

Guest Researcher, Tohoku JGNII Research Center, Collaborative Research Management Department

Network Operation, Management, Security

***KINOSHITA Tetsuo**, Dr. Eng.*

Guest Researcher, Tohoku JGNII Research Center, Collaborative Research Management Department

Knowledge Engineering, Agent Engineering

***SUGANUMA Takuo**, Dr. Eng.*

Guest Researcher, Tohoku JGNII Research Center, Collaborative Research Management Department

Multimedia Communication System

***SHIBATA Yoshitaka**, Ph.D.*

Guest Researcher, Tohoku JGNII Research Center, Collaborative Research Management Department

Computer Networks, Human Interface, KANSEI Information Processing

***SONE Hideaki**, Dr. Eng.*

Expert Researcher, Tohoku JGNII Research Center, Collaborative Research Management Department (Professor, Tohoku University)

Computer Network Engineering