A Method on Multimedia Service Traffic Monitoring and Analysis[1]

Hun-Jeong Kang, Myung-Sup Kim, James Won-Ki Hong
Department of Computer Science and Engineering
POSTECH, Korea
{bluewind, mount, jwkhong}@postech.ac.kr

Abstract. The use of multimedia service applications is growing rapidly on the Internet. These applications are generating a huge volume of network traffic, which has a great impact on network performance and planning. For various purposes, obtaining information on multimedia service traffic is important. However, traditional analysis methods based on well-known ports cannot be used to analyze such traffic. Because the majority of multimedia service applications use dynamically allocated port numbers, the traditional methods misidentify multimedia service traffic as unknown traffic. This paper presents a method for monitoring and analyzing multimedia service traffic. Our method detects transport protocol and port numbers for dynamically created sessions during a control session. We then use such information to analyze traffic generated by the most popular multimedia service applications, namely Windows Media, RealMedia, Quicktime, SIP and H.323. We also present a system architecture that uses our method to monitor and analyze multimedia service traffic.

1. Introduction

The use of streaming media and multimedia conferencing applications is growing rapidly. Many Internet sites provide various rich media content of broadcast, movies, and music. We call the network traffic generated by the streaming media and multimedia conferencing applications as multimedia service traffic. This multimedia service traffic is becoming increasingly dominant in IP networks and is affecting the network performance and planning. Therefore, it is important to monitor and analyze multimedia service traffic for acquiring information about the network usage.

However, most existing traffic monitoring systems cannot be used to analyze multimedia service traffic. These systems use well-known port numbers for identifying applications [1]. Most multimedia service applications make use of port numbers that are not well-known but are dynamically allocated during set up sessions. As a result, traffic to transfer multimedia service data is misidentified as unknown traffic in these systems [2, 3].

This paper presents a method and a system architecture to monitor and analyze multimedia service traffic. We have developed a dynamic session analyzer which parses control protocols. This analyzer processes the payload of a packet associated with a control protocol and extracts information such as transport protocol and port numbers used for transferring multimedia service data. We then use this information

[1] This work was in part supported by the Electrical and Computer Engineering Division at POSTECH under the BK21 program of Ministry of Education and HY-SDR Research Center at Hanyang University under the ITRC program of Ministry of Information and Communication, Korea.

to analyze popular multimedia service traffic, namely Windows Media [4], RealMedia [5], Quicktime [6], SIP [7], and H.323 [8] traffic.

This paper is organized as follows. Section 2 provides an overview of several popular multimedia service protocols. Section 3 discusses related work on traffic monitoring and analysis. Section 4 presents our analysis method for multimedia service traffic. Section 5 describes the architecture of our multimedia service traffic monitoring and analysis. Finally, Section 6 summarizes our work and discusses possible future work.

2. Overview of Multimedia Service Protocols

This section describes backgrounds of multimedia service protocols and their characteristics. In streaming media service, we are aiming to most popular services: Windows Media Technology (WMT), RealMedia, and QuickTime. These services differ in their protocols, as illustrated in Table 1. In Internet multimedia service conferencing services, most applications are based on SIP (Session Initiation Protocol) or H.323. Table 2 describes protocols used in these applications.

streaming media service	control session protocol	data session protocol
RealMedia	RTSP	RDT
QuickTime	RTSP	RTP
WMT	MMS	MMST/MMSU

Table 1. Streaming Media Service Protocols

application	control session protocol	data session protocol
based on SIP	SIP	RTP
based on H.323	Q.931, H.245	RTP

Table 2. Multimedia Conferencing Protocols

During a multimedia service, two types of sessions are created between a client and a server: a **control session** and a **data session**. The control session is responsible for setting up connection and controlling navigation, such as play and pause. This session uses control protocols such as RTSP (Real Time Streaming Protocol) [9] and MMS (Microsoft Media Server) [4]. The data session sends the multimedia service contents to the client over the data session protocol, including RDT (RealNetworks Data Transfer) [5], RTP (Realtime Transfer Protocol) [10], and MMST/MMSU (MMS over TCP/UDP) [4]. We designate each packet related to the control session and data session as a control packet and a data packet, respectively.

Figure 1 illustrates a client/server interaction for a control and data transfer session. To begin, a control session is set up through a well-known port number. As described in Figure 1 (a), streaming media services (e.g., RealMedia, QuickTime) or applications based on SIP have one control session. On the other hand, H.323 applications have two control sessions: Q.931 [8] and H.245 [8] sessions. A control session creates a new data session by negotiating a transport protocol and port

numbers. Then the data session transfers multimedia data through the dynamically assigned transport protocol and port numbers. In this paper, we introduce a new term, **dynamic session,** that makes use of the transport protocol and port numbers that are dynamically negotiated by the control session, such as the data session and second control session in Figure 1 (b).

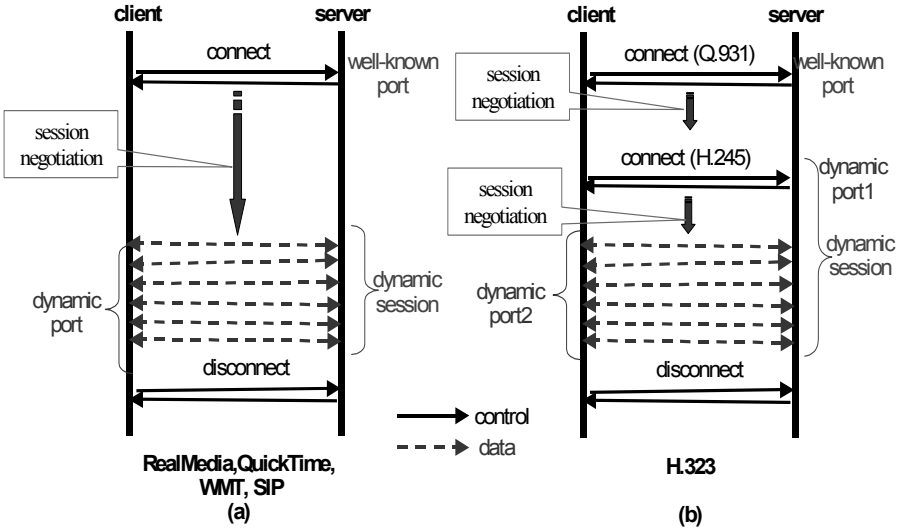

Figure 1. Multimedia Service Control and Data Session

When a control session negotiates about a dynamic session, the packet payload of the control session contains negotiation results such as a transport protocol and port numbers used in the dynamic session. By selecting and analyzing the control packet, we can discover information about the dynamical session, which is called the **dynamic session information** in this paper.

The use of dynamic sessions in multimedia services causes disadvantages in traffic monitoring, although the use benefits in delivering data. These services can send multimedia data efficiently by changing appropriate protocols for streaming and conferencing. On the other hand, new and not well-known port numbers appear after the session negotiation. Because of these unknown port numbers, the traffic used by dynamic session is misidentified as unknown traffic by most traffic monitoring systems that use well-known port numbers for identifying applications. That is the reason why we find dynamic session information and use it when determining multimedia service traffic.

3. Related Work

A flow represents a series of packets traveling between ‘‘interesting’’ end points. There are various definitions about the flow [13, 14, 15]. In this paper, we define a flow as a sequence of packets with the same 5-tuple: source IP address, destination IP address, source port, destination port, and protocol number. By aggregating related

packets into a flow, one can reduce system overhead to process data. Due to this compressibility, many systems, such as NG-MON [16], analyze traffic based on flows.

Flowscan [11] is also a flow-based traffic analysis system. Its monitoring target related to multimedia service is the traffic using RTSP. It uses a heuristic method as follows. The system records ongoing control sessions. When a flow is seen with an unknown port number on two hosts, it checks to verify whether an active control connection exists between the same hosts. If so, it assumes that the flow corresponds to a dynamic session. However, this analysis may provide inaccurate information. The reason is that traffic seen with an unknown port number may not be related to the active control connection that exists between two connected hosts. Further, some multimedia service data can be transferred from another source that does not participate in the active control connection. In this case, this heuristic method misidentifies the multimedia service traffic as unknown traffic, because no active control connection exists between these hosts that transfer multimedia service data.

mmdump [3] is a tool for monitoring multimedia traffic on the Internet. This tool is used to investigate the characteristics of multimedia service traffic over RTSP and H.232. The tool contains a parsing module for the RTSP and H.323 protocol. It parses the control messages to extract the dynamically assigned port numbers. The parsing module then dynamically changes a packet filter to allow packets associated with these ports to be captured. By changing the packet filter, this tool can capture only packets that contain listed port numbers, while reducing the resource requirements and capture overhead. However, it is also a burden to frequently compile and change the packet filter. In addition, this tool reveals the following problems. First, it does not analyze MMS [4] that is considered to be the most widely used streaming service in the world. Next, it does not consider IP-fragmentation. We observed that about 40~70% of WMT packets are fragmented during our tests. Similarly, some applications send large streams into the network, and these data are fragmented. The port number of these fragmented packets cannot be identified without reassembly. Because mmdump captures a packet by referencing only port numbers, it misses fragmented packets, even though they are multimedia service packets. Further, it may commit a false-rejecting error, where the real data packet is misidentified as not associated with the multimedia service session. Consider a streaming data packet that belongs to a data session but is not contained in the packet filter to be captured. Some data packets pass the probing point after deletion of port numbers from the filtering list. Then the packet may pass the probing point without being captured. In these cases, the analysis results of mmdump are not accurate.

4. An Analysis Method For Multimedia Service Traffic

4.1 Analysis Procedure

In this section, we present our proposed method for analyzing multimedia service traffic. Figure 2 is a flowchart to illustrate packets being captured and processed. The overall procedure consists of three major parts: flow generation, dynamic session analysis, and traffic analysis.

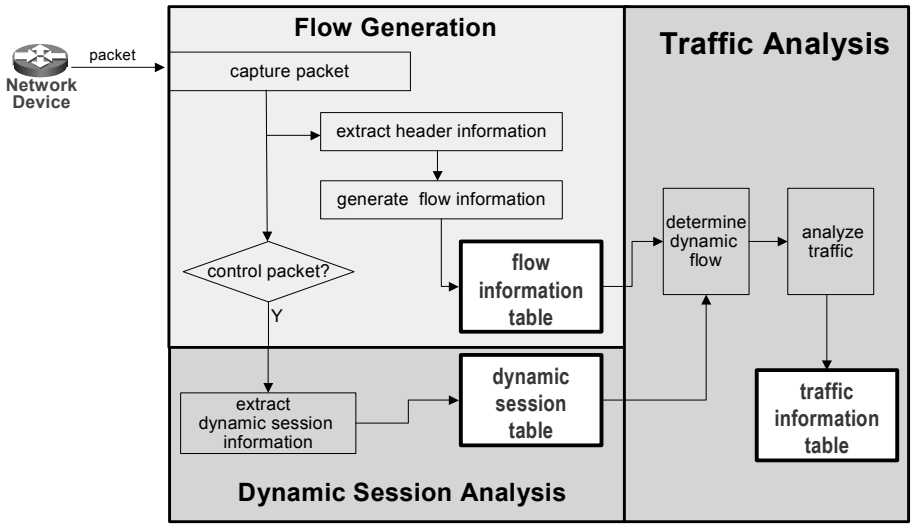

Figure 2. Flowchart for Multimedia Service Traffic Monitoring and Analysis

The flow generation part captures packets and analyzes their header. By collecting and aggregating related packets, this part generates flow information. Based on this flow information, the traffic analyzer generates various traffic information into the traffic information table. However, it is insufficient to identify dynamic session traffic with only a port number. The reason is that dynamic sessions do not use well-known ports. Therefore, we need dynamic session information to decide whether or not a flow with an unknown port number is related to multimedia service traffic. This information can be extracted in the dynamic session analysis part. When a packet is analyzed by the flow generation part, the control packet is sent to the dynamic session analysis part. Next, the packet is analyzed to determine whether or not it contains dynamic session information. In the following sections, we describe the dynamic session analysis part in detail.

4. 2 Dynamic Session Analysis

Figure 3 describes our algorithm to discover dynamic session information from the control packet. The dynamic session analyzer receives a control message, including packet header information, and a payload of the transport layer. First, the procedure determines if the FIN flag is set to identify it as a session disconnect request. If not, the module analyzes whether the packet contains dynamic session information. We can reduce the analysis overhead by selecting a packet, which is likely to contain dynamic session information. The payload of the selected packet is parsed according to each control protocol (line 6, 9, 11, 14, or 16). After parsing, the procedure confirms if the dynamic session information is discovered (line 17). If so, this information is stored into the dynamic session table that contains information on active dynamic sessions (line 19).

```
1  Procedure DynamicSessionAnalyzer ( Msg )
2   BEGIN
3    if FIN Flag in Msg is NOT set
4      then if protocol in Msg = RTSP
5           then if SourcePort in Msg = RTSP server port number
6                then result = ParseRTSP (payload of Msg ) ;
7           else if protocol in Msg = MMS
8                then if DestinationPort in Msg = MMS server port number
9                     then result = ParseMMS (payload of Msg ) ;
10               else if protocol in Msg =SIP
11                    then result = ParseSIP (payload of Msg ) ;
12                    else if protocol in Msg = Q.931
13                         then if SourcePort in Msg = Q.931 receiver port
14                              then result = ParseQ931 (payload of Msg ) ;
15                         else if protocol in Msg = H.245
16                              then result = ParseH245 (payload of Msg ) ;
17       if result= TRUE then
18         create new dynamic session information;
19         insert dynamic session information into dynamic session table;
20   else
21      delete session information from dynamic session table;
22  END
```

Figure 3. Multimedia service Traffic Analysis Algorithm

When a multimedia service is completed, information on the dynamic session must be removed. This information is usually deleted from the dynamic session table (line 21) when the TCP FIN flag is set to disconnect the control session. However, the FIN packet may never be captured because of such effects as packet losses or route changes [3]. In such cases, the information is removed from the table by selecting a session, which shows no activity for a certain period of time. Consequently, the traffic analysis module can identify the application of dynamic flows by referencing the dynamic session table.

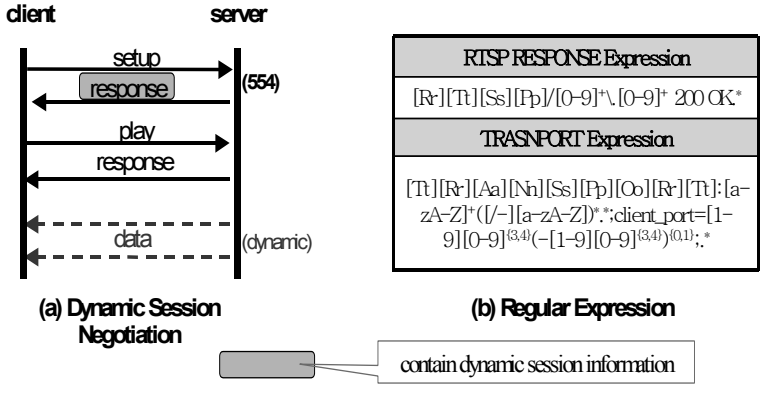

Figure 4. Dynamic Session Construction in RTSP

4.2.1 Analysis of RTSP

RealMedia and QuikTime applications use RTSP as control protocol. Figure 4 (a) illustrates messages of RTSP during negotiation of a dynamic session. A client sends a SETUP request to a server, along with the candidates for a data transfer protocol and port number (or a range of port numbers) to be used for receiving multimedia service data. Next, the SETUP response contains the protocol and port numbers chosen by the server. Accordingly, the procedure ascertains whether the source port of the packet is an RTSP server port (i.e., 554) (line 5 in Figure 3), and whether the packet from the server contains 'RTSP RESPONSE Expression' in Figure 4 (b). Then, the procedure parses the payload and searches for 'TRANSPORT Expression': "Transport:", ";client_port=", the number or range of numbers, and ";".

4.2.2 Analysis of MMS

MMS is a control protocol of Windows Media Technology (WMT). Although its specification is not publicly open, we have discovered by observing and analyzing packets that the client's request in MMS contains the transport protocol and port numbers used for transferring multimedia service data. Therefore, the destination port number is checked to verify that it is the MMS server port number (i.e., 1755) (line 8 in Figure 3) for the purpose of choosing the client request packet. Among the client request packets, the only SETUP packet, named for convenience in this paper, contains dynamic session information. Accordingly, the procedure verifies the client request packet contains 'SETUP Expression' as illustrated in Figure 5 (a). Even though we have not ascertained the specification of MMS, we can analyze by searching for 'TRANSPORT Expression': string of "MMS", 'URL-string format', "TCP" or "UDP," and the port number.

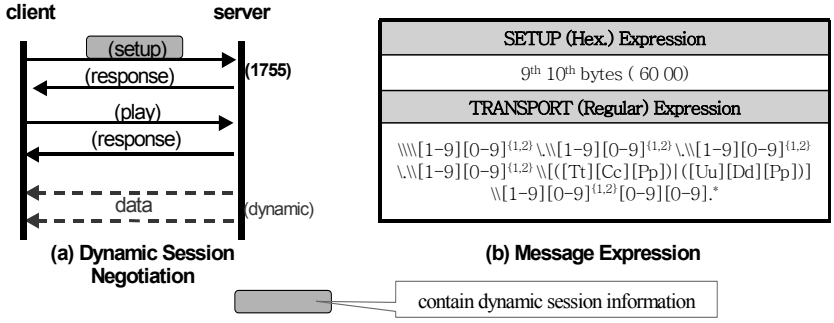

Figure 5. Dynamic Session Construction in MMS

4.2.3 Analysis of SIP

Figure 6 (a) illustrates messages of SIP during negotiation of a dynamic session. A client sends an INVITE request to a server, along with the port number that is used to for the client to receive multimedia service data. Then the server sends the RESPONSE packet that contains port number through which the server receives data from the client. For this reason, the procedure selects packets with 5060, SIP server

port (line 10 in Figure 3). Then, it verifies if they are invite or response message by matching the payload of the selected packet with 'INVITE Expression' or 'RESPONSE Expression' in Figure 6 (b). After selecting, the procedure extracts dynamic session information from a SDP (Session Description Protocol) [15] part of the payload. It finds 'MEDIA Expression', which consists of components, such as "M=", media type, port number, transport protocol, and payload type.

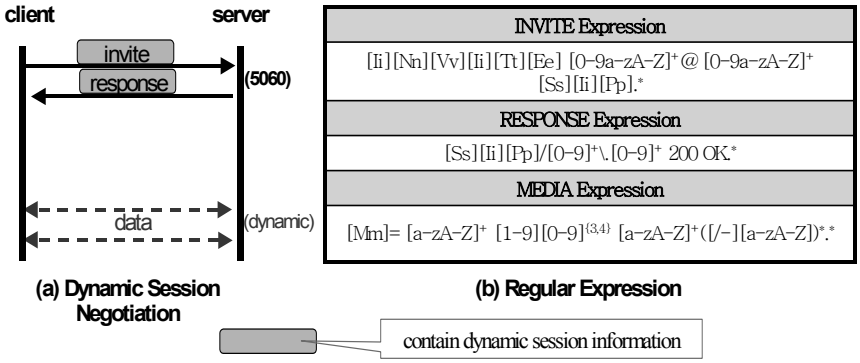

Figure 6. Dynamic Session Construction in SIP

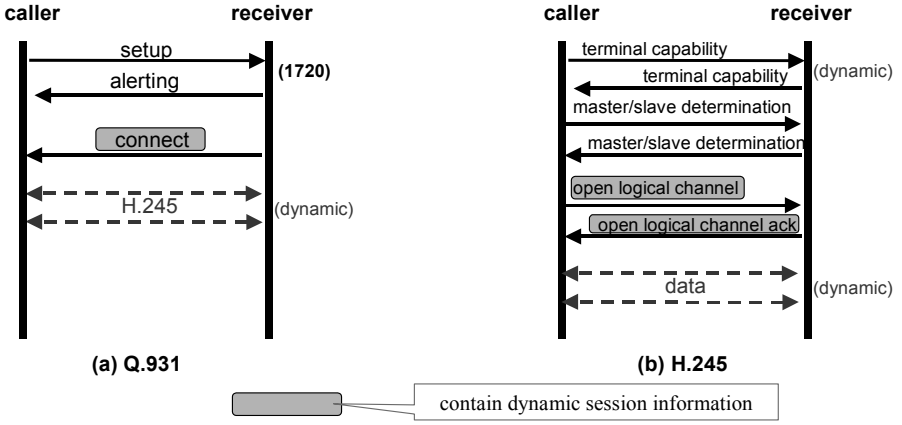

Figure 7. Dynamic Session Construction in H.323

4.2.4 Analysis of H.323

Services based on H.323 have two dynamic sessions, as illustrated in Figure 7 (a) and (b). First, Q.931 uses a well-known receiver port, 1720. Because the information about H.245 is contained in the connect message, the procedure checks if the source port is the receiver port (line 13 in Figure 3) and if it is a connect message. In the case of H.245, this session uses a port number that is dynamically allocated by a Q.931 session. Accordingly, we need to determine whether a captured packet is related to a

H.245 session by matching dynamic session information that generated by the Q.931 session (line 15 in Figure 3). Then the procedure selects an open logical channel or open logical channel ack packet in the H.245 session.

Contrary to the above text-based protocols of RTSP, MMS, and SIP, the procedure searches for the locations of port number in Q.931 and H.245 packets. In Q.931, the dynamic session analyzer extracts a dynamically assigned port number from a port in an User-User info Element information. It can discover the port number of H.245 in tsap Identifier of a forwardLogicalChannel, reverseLogical Channel, or network access parameter.

5. Architecture for Multimedia Traffic Monitoring and Analysis

We have developed a system for monitoring and analyzing multimedia service traffic. We have adopted the system architecture of **NG-MON** [16] and integrated the proposed method with NG-MON. As illustrated in Figure 8, traffic monitoring and analysis tasks are divided into several phases, which are serially interconnected using a pipelined architecture. One or more systems may be used in each phase to distribute and balance the processing load. Each phase performs its defined role in the manner of a pipelined system. This architecture can improve the overall performance and scalability, with each phase configured with a cluster architecture for load distribution. We have also defined a communication method between each pair of phases. Each phase can be replaced with more optimized modules as long as they provide and use the same interfaces. The divided architecture provides flexibility. By assigning tasks to each phase, this architecture enables us to easily append or remove modules for added work such as dynamic session analysis.

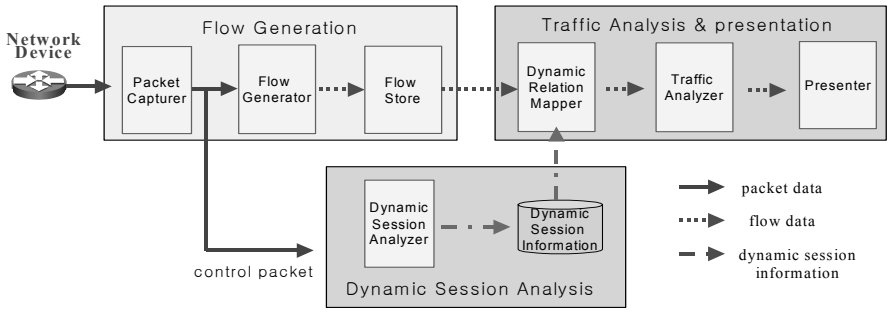

Figure 8. Multimedia Service Traffic Monitoring Architecture

5.1 Flow Generation

The flow generation module consists of a packet capturer, a flow generator, and a flow store. The packet capturer collects packets passing a probing point. Another function of the packet capturer is to extract information from the packet header and to send it to the flow generator. The format of the packet header information is also shown in Figure 9. The time stamp represents the time when the packet is captured.

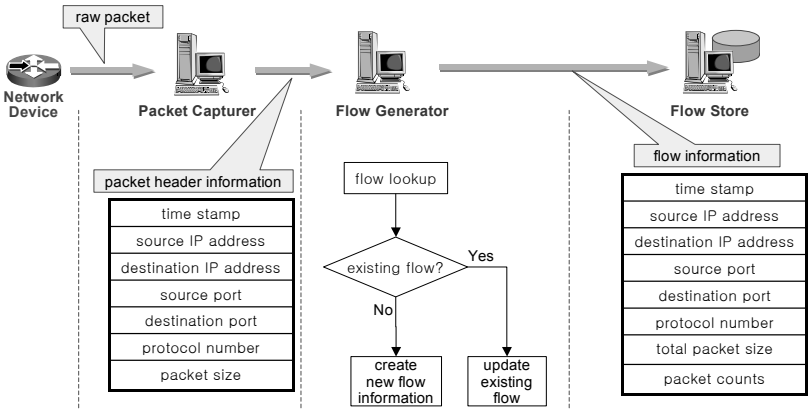

Figure 9. Flow Generation Module

The flow generator creates a flow by collecting a series of packets. Figure 9 illustrates the function and parameters of the flow generator. Whenever receiving packet header information, the flow generator looks up the flow table to search for an existing flow to which the packet belongs. If a matched flow exists, the packet is added to the flow by updating the flow information by increasing the count and total size of the packet. If not, a new flow is constructed from the packet header information. Next, the flow is inserted into the flow table. Flows in the table are periodically stored into a database. Here, the period can be configured according to the flow time-out in order to aggregate flow information during the predetermined time, such as one minute.

5.2 Dynamic Session Analysis

The dynamic session analysis module provides information for identifying multimedia service traffic. If a packet is determined to be a control packet, the packet capturer sends the packet to the dynamic session analyzer. By using the algorithm for streaming analysis described in Figure 3, the dynamic session analyzer discovers the information on the dynamic session. This information is stored into the dynamic session table and referenced by the relation mapper in the traffic analysis module.

dynamic IP address	dynamic port	transport protocol	
Control client address	control client port	control server address	control server port
session start time		session end time	

Figure 10. Dynamic Session Information

Figure 10 shows the format of the dynamic session information. In this format, the control server address and control server port are IP addresses and the port number of the server in the control session that created the dynamic session. Similarly, the control client address and control client port are the IP address and the port number of client in the control session. By making use of this information, the system is aware of the relationship between the control and dynamic sessions. The session start time is

the time when the dynamic session information is newly created, and the session end time is the time when the control session is disconnected. The session end time is set either when a TCP FIN flag of a control packet is set, or when no packet in the same session is captured during a predetermined threshold time. These time fields are used to determine whether a dynamic session is active or inactive.

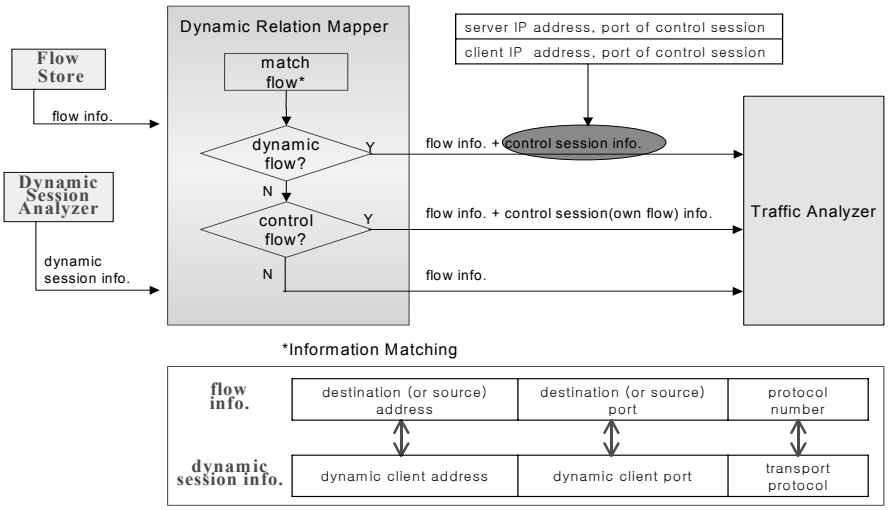

Figure 11. Dynamic Relation Mapping

5.3 Traffic Analysis

The dynamic relation mapper decides the relation between a dynamic flow and a control flow. This module identifies whether a flow with unknown port number is related to a dynamic session. As illustrated in Figure 11, this module matches flow information with dynamic session information. Tuples to be compared are as follows: destination (or source) IP address and dynamic client address, destination (or source) port and dynamic client port, and protocol number and transport protocol. If the compared tuples are equal, some fields are added to the flow information, such as the IP address and port number of the control session. By adding these fields, we can map the dynamic flow and the control flow that creates the dynamic flow. In the case of control flows, the control server and client information are filled up with its own IP address and port number. Otherwise, only flow information is sent to the traffic analyzer without an addition of fields.

The traffic analyzer performs an analysis of traffic by querying the flow data stored in the database. It can analyze multimedia service traffic at the session level. It is possible for a multimedia service to open several sessions. The traffic analyzer can discover and analyze sessions separately. In addition, it integrates the information of sessions which belong to the same multimedia service. For example, it can analyze the traffic volume exchanged in the control and data sessions related to the same multimedia service.

6. Conclusion and Future Work

In this paper, we presented a method and system architecture for monitoring and analyzing multimedia service traffic. This method analyzes control protocol messages and extracts information on dynamic sessions. The extracted information includes dynamically selected protocol and port numbers, which are used to determine whether or not the unknown traffic is multimedia traffic. This approach makes it practical to monitor previously unknown multimedia service traffic, as well as other services.

This method boosts the analysis of traffic from the packet level to the session level. It does not simply extract header information of a packet, but makes it possible to analyze traffic per session by acquiring session information. In addition, it overcomes the problems with existing approaches that use only well-known port numbers of TCP or UDP for identifying the application of traffic. By analyzing application messages, this method discovers the status of the application and raises the analysis application level.

We are currently integrating our multimedia service traffic analysis method with NG-MON. We plan to analyze the multimedia service traffic on our campus network and then use our system to monitor and analyze ISP networks in Korea. We are planning to extend the proposed analysis method to other types of traffic that creates and use dynamic sessions.

References

[1] Internet Assigned Numbers Authority, http://www.iana.org/.

[2] James W. Hong, Soon-Sun Kwon and Jae-Young Kim, "WebTrafMon: Web-based Internet/Intranet Network Traffic Monitoring and Analysis System," Computer Communications, Elsevier Science, Vol. 22, No. 14, Sept. 1999, pp. 1333-1342.

[3] Jacobus van der Merwe, *et. al*., "mmdump - A Tool for Monitoring Internet Multimedia Traffic," ACM Computer Communication Review, 30(4), October 2000.

[4] Microsoft, WMT, http://www.microsoft.com/windows/windowsmedia/default.asp.

[5] Real Networks, Real Media Technology, http://www.realnetworks.com/.

[6] Apple, QuickTime, http://www.apple.com/quicktime.

[7] M. Handley, H. Schulzrinne, E.Schooler, J. Rosenberg, "SIP: Session Initiation Protocol," RFC 2543, March 1999.

[8] ITU-T, "Recommendation H.323: Visual Telephone Systems and Equipment for Local Area Networks Which Provide a Non-guaranteed Quality of Service," 1996.

[9] H. Schulzrinne, A. Rao, and R. Lanphier, "Real Time Streaming Protocol (RTSP)," RFC 2336, April 1998.

[10] H. Schulzrinne, S. Casner, R. Frederick, V, and Jacobson, "RTP: A Transport Protocol for Real-Time Applications," RFC1889, January 1996.

[11] Dave Plonka, FlowScan, http://net.doit.wisc.edu/~plonka/FlowScan/.

[12] Siegfried Lifler, "Using Flows for Analysis and Measurement of Internet Traffic," Diploma Thesis, University of Stuttgart, 1997.

[13] J.Quittek, T. Zseby, B. Claise, K.C. Norsth, "IPFIX Requirements," Internet Draft, http://norseth.org/ietf/ipfix/draft-ietf-ipfix-architecture-00.txt.

[14] CAIDA, "Preliminary Measurement Spec for Internet Routers," http://www.caida.org/tools/measurement/measurementspec/.

[15] M. Handley, V. Jacobson, "SDP: Session Description Protocol," RFC 2327, April 1998.

[16] S. H. Han, M. S. Kim, H. T. Ju and J. W. Hong, "The Architecture of NG-MON: A Passive Network Monitoring System", DSOM 2002, Montreal, Oct., 2002, pp. 16-27.