Traffic Identification for Dependable VoIP

KITAMURA Tsutomu, SHIZUNO Takayuki, OKABE Toshiya, TANI Hideaki

Abstract

The Voice over Internet Protocol (VoIP), which is expected to function as a substitute for the Public Switched Telephone Network (PSTN) is required to be highly dependable. To provide a dependable VoIP service, it is necessary to apply traffic controls such as rate control and filtering by accurately identifying the legitimate VoIP traffic from the prohibited traffic. NEC has developed a traffic identification technology that analyzes the packet exchange patterns as the key to traffic control without being dependent on the port numbers and signatures. When this technology is applied to a traffic control system, a dependable VoIP service can be implemented by traffic control based on the accurate identification of any Peer-to-Peer applications traffic that deteriorates the quality of the VoIP traffic.

Keywords

dependable, VoIP (Voice over IP), traffic identification

1. Introduction

In order to provide a dependable voice communication service, it is necessary to apply traffic controls such as rate control and filtering by accurately identifying legitimate VoIP traffic from prohibited traffic. This paper introduces a traffic identification technology that analyzes the packet exchange patterns as the key to controlling the traffic without being dependent on the port numbers and signatures.

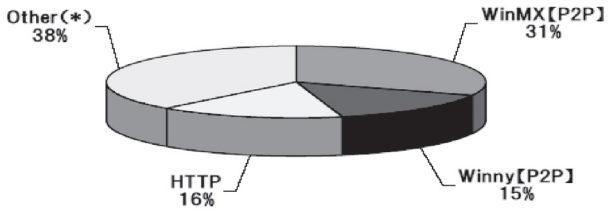
2. Issues for the Realization of a Dependable VoIP Service

A dependable VoIP service cannot be implemented unless there is a stable delivery of the voice traffic. However, the Peer-to-Peer applications that have recently been disseminating, have generated a large amount of traffic occupying the network resources and causing problems such as significant delays and loss of voice traffic. For instance, the Peer-to-Peer traffic as of February 2003 occupies about 46% of the total traffic and exerts an important influence as shown in **Fig. 1**[1].

Network administrators maintain the quality of voice communication by installing traffic control systems such as a traffic shaper or firewall at the entrance and exit ports of their networks. These traffic control systems identify the traffic type depending on the addresses of the packets flowing into the network, the port numbers used by them and the application-specific bit patterns (signatures) observed in them. Quality assurance is thus offered to the VoIP traffic and effective filtering of other traffic, including bandwidth limiting is applied.

However, in the case of Peer-to-Peer traffic, there is no convention on port number use because it consists of direct communications between hosts, and the packet data contents (payloads) are usually encrypted. As a result, port number or signature dependent traffic identification as described above is incapable of accurate traffic control when Peer-to-Peer traffic is in question.

At NEC, we have developed a traffic identification technology as a solution to the present problem that analyzes packet exchange patterns independently from the port numbers and signatures. When this technology is applied to a traffic control system, a dependable VoIP service becomes possible by implementing the appropriate traffic controls based on an accurate identification of any traffic of Peer-to-Peer applications that tends to deteriorate the quality of the VoIP traffic.



(*) Also expected to include Peer-to-Peer traffic partially.

Fig. 1 Share of Peer-to-Peer traffic in traffic of ISP[1].

3. Traffic Identification Technology for VoIP Quality Management

3.1 Application Identification Based on Packet Exchange Patterns

Communications between applications running on different hosts are usually accompanied by packet flows such as; 1) exchange of signaling control messages for establishing a session between hosts, and; 2) exchange of media data including voices, images and data using the established session.

The signaling for establishing a session is performed using a packet exchange pattern that is specific to each application such as HTTP (web accessing), FTP (file transfer), SIP (VoIP) and Winny (Peer-to-Peer file sharing) applications. On the other hand, in the case of media data transfer after session establishment, the amount and frequency of packet exchanges are characterized by differences in the data contents such as file, voice and image.

Traditional traffic identification technology identified applications based on the port numbers in packet headers or signatures of payloads, but identification was not always accurate because these attributes could be altered or concealed by applications. The new identification technology that we have developed detects elements that cannot be concealed by applications, such as the packet size and packet arrival interval, and enables accurate traffic identification when these are applied to the signaling messages or the packet exchange patterns in media data transfer. In the following sections, we describe the traffic identification technology that analyzes two kinds of non-concealable packet exchange patterns[2, 3].

3.2 Analysis of Packet Exchange Patterns

Here, we define a group pf packets, the five elements of which (source address, destination address, source port, destination port and protocol type) are identified as "flow," and a group of packets that are exchanged interactively between two hosts using their individual port that are identified as "interaction."

Fig. 2 shows the application identification procedure of a traffic control system. Firstly, the received packets are isolated per flow or per interaction (1, 2), and then the characteristics of the flow and interaction are analyzed (3, 4). Finally, the application is identified based on a pattern matching (5). If the characteristics of flow or interaction do not match any of the reference patterns, the application is regarded as an unknown application and its pattern is added to the reference pattern.

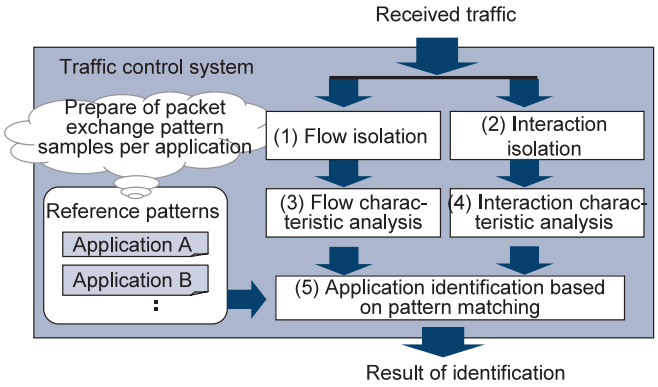


Fig. 2 Packet exchange pattern analyses.

In the flow characteristic analysis (3) and interaction characteristic analysis (4) shown in Fig. 2, each analysis extracts the characteristics of the received flow behavior or those of the received interaction behavior. In the following sections, we examine the results of measurements of the characteristics of flow behavior and also those of interaction behavior that depends on applications.

3.3 Characteristics Analysis of Flow Behavior

Fig. 3 and **Fig. 4** show the results of measurements of differences in the voice flow characteristics of some VoIP applications (Skype 2.0, Netmeeting 3.0, SIPphone). The characteristics of voice flow behavior vary mainly depending on the voice codecs and packet parameters (such as the bit rate and voice packet send interval) used. Skype 2.0 uses a variable-rate voice codec that controls the packet size and bit rate dynamically. Netmeeting 3.0 uses multiple voice codecs, SIPphone uses a single voice codec, but their voice communications mostly use fixed packet sizes and fixed bit rates.

As shown in Fig. 3, the packet size and arrival interval of Skype vary over a wide range according to the dynamic rate control. The figure also shows that those of Netmeeting 3.0 and SIPphone are distributed around specific values that are determined according to the set voice codecs and packet parameters.

The average packet size in Fig. 4, is obtained by measuring the packet size at one second intervals for 60 seconds and shows that the packet size varies widely with Skype but that it is fixed with Netmeeting 3.0 and SIPphone. With Netmeeting 3.0, three kinds of packet sizes are observed only when the voice codec is SBC and the bit rate is 12kbps.

The flow behavior measurement results in Figs. 3 and 4 can

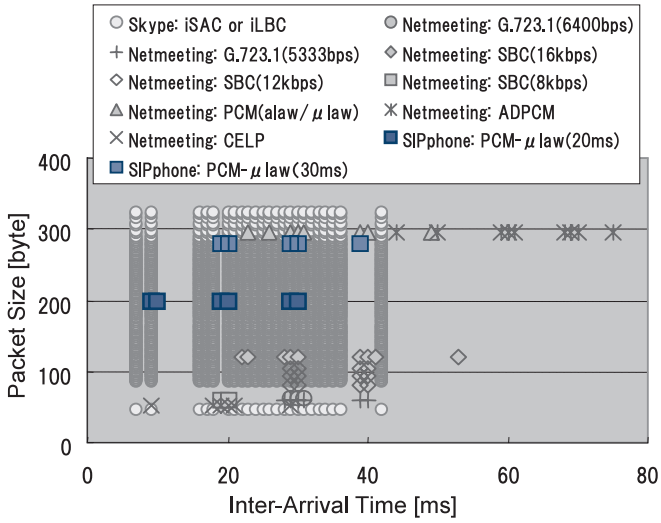


Fig. 3 Results of packet sizes and arrival interval measurements.

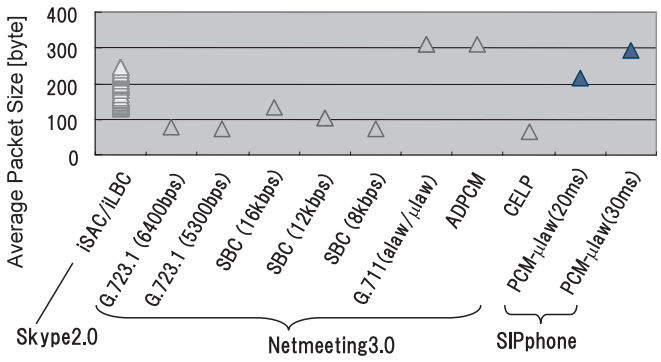


Fig. 4 Results of packet size measurement.

also be utilized to extract the characteristics of the individual application flow, and the characteristics obtained with each application are used as reference patterns. To improve the traffic identification accuracy, it is necessary to prepare reference patterns by measuring the traffic until the data quantity required for learning the reference patterns.

3.4 Characteristics Analysis of Interaction Behavior

The characteristics of interaction behavior vary depending on the signaling protocols used by the applications. **Fig. 5, Fig. 6** and **Fig. 7** show the results of measurements of the interaction characteristics of SIPphone, Netmeeting 3.0 and Skype 2.0 in the same way as in the previous section. SIPphone uses the SIP as the signaling protocol, while Netmeeting 3.0 uses the H.323 and Skype 2.0 uses an original Peer-to-Peer signaling protocol.

Fig. 5 is a representation of the relationship between the packet arrival order and packet size of a server-client interaction using SIPphone. This result was obtained by measuring actual interactions for a total of 5 events. The appearance patterns shown in Fig. 5 allow us to observe the characteristics of the SIP signaling protocol shown in **Fig. 8**.

Since the packet size in the SIP message varies according to the SIP URI (Uniform Resource Identifier) that contains the source/destination address and the presence/absence of the SIP

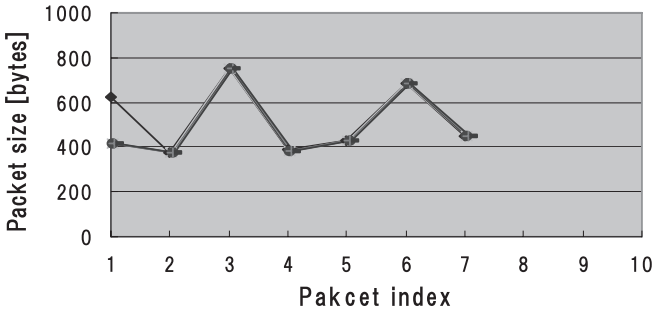


Fig. 5 Packet size appearance pattern of SIPphone.

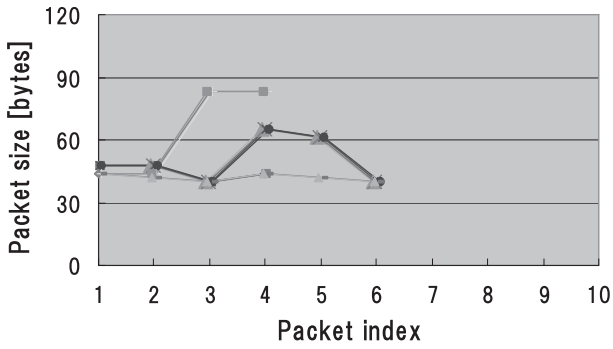


Fig. 6 Packet size appearance pattern of Netmeeting 3.0.

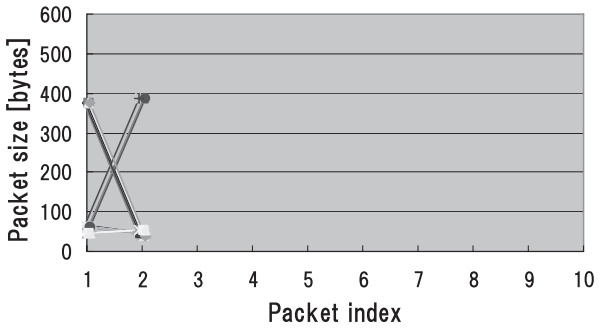


Fig. 7 Packet size appearance pattern of Skype 2.0.

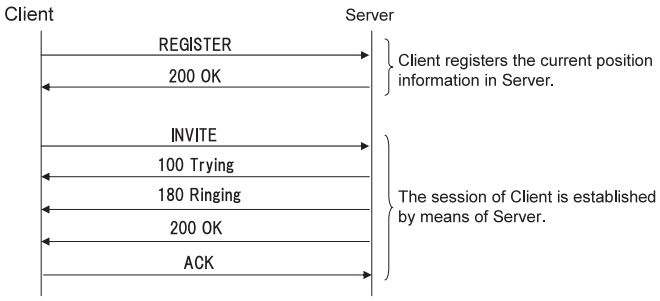


Fig. 8 Signaling protocol using SIP (Session Initiation Protocol).

extension header, it is necessary to consider their tolerance values when preparing the reference patterns.

Fig. 6 shows the results of measurements of the packet size appearance pattern between the hosts holding a voice communication using Netmeeting 3.0. The appearance patterns shown in this figure are observed in any of the measured sessions and can be regarded as representing the characteristics of the call control protocols of Netmeeting 3.0 such as the H.225 (Q.931) and H.245. Fig. 7 shows the results of measurements of the packet size appearance patterns observed in voice communications using Skype 2.0 of a host with multiple destination hosts. The appearance patterns that are observed in any of the measured sessions in this figure represent the characteristics of the original Peer-to-Peer signaling protocol of Skype 2.0.

Since a Peer-to-Peer application such as Skype 2.0 always establishes communications links with multiple hosts, it is regarded that the identification accuracy can be improved by analyzing the interaction behavior on a per-host basis.

As shown in the above examples, interaction characteristics vary depending on the signaling protocols. This phenomenon can be used to extract the characteristics of each application, prepare reference patterns and identify the applications by applying the pattern matching to the flow into the network.

4. Conclusion

In the above, we described a traffic identification technology based on an analysis of application traffic characteristics. This technology makes it possible to realize more dependable traffic controls by identifying traffic based on multiple characteristics including flow and interactive behavior as well as that based on the concealed information in packet headers such as port numbers and signatures. In the future, we will conduct research into the practical implementation of this technology with the aim of providing dependable VoIP services.

References

1) Okada and Kawahara, “A Consideration on Traffic Characteristic Analysis of IP Network,” the Institute of Electronics, Information and Communication Engineers, journal of IEICE NS2003-5, April 2003.
2) Kitamura, et al., “A Technique of Application Identification Based on Flow Behavior Analysis,” the Institute of Electronics, Information and Communication Engineers, Journal of IEICE NS2005-136, December 2005.
3) Kitamura, et al., “Proposal of a Traffic Identification Technique Based on Packet Type Transition,” the Institute of Electronics, Information and Communication Engineers, Proc. IEICE Gen. Conf. ‘06, March 2006.

Authors' Profiles

KITAMURA Tsutomu
Reseacher,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

SHIZUNO Takayuki
Reseacher,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

OKABE Toshiya
Assistant Manager,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation

TANI Hideaki
Senior Manager,
System Platforms Research Laboratories,
Central Research Laboratories,
NEC Corporation