Statistical Traffic Identification Method Based on Flow-Level Behavior for Fair VoIP service

April 3, 2006

Toshiya Okabe

<t-okabe@bx.jp.nec.com>

Application identification

Traffic control is necessary for Edge routers, SBCs and various GWs

- to give priority to emergency call, priority call, pay-tv service.
- to screen malicious traffic.
- to rate-control bulk data traffic like P2P file transfer, Web traffic etc.

Traffic control

- Traffic identification <- here our target.
- Traffic manipulation

An possible threat:

Without accurate identification, malicious traffic might pretend to be an priority call to be prioritized.

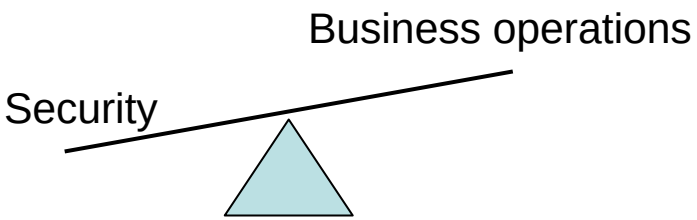
Differences between carrier network and enterprise network.

Enterprise network:

The purpose of a business network is to smoothly carry out business operations.

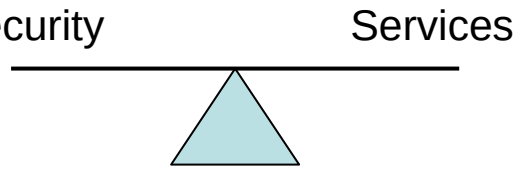
It’s possible to secure an enterprise network by

- Education
- Company regulation
- Packet inspection



Carrier network:

The purpose of a carrier network is to provide stable services to all subscribers, under CONFIDENTIALITY.



Carrier network

- Various users

Some of them are good users but not all.

You need higher security but you can not expect that users have knowledge on various threats and devices.

- Regulations

There are regulations which restrict carrier's operation but not user's activity in many cases.

- Confidentiality

Peeping into packets is not appropriate. You should not wiretap packets under the daily operation.

Approaches to application identification

Host behavior approach

Packet inspection

Traffic-behavior approach

- Flow-level behavior
- Transaction-level behavior

Host behavior approach

A method to infer an application from relationship between hosts.

Example:

Client-server application: one server communicates a lot of clients and in most cases the port number is static.

P2P application: a peer communicates various peers simultaneously and uses different ports.

The method is suited for detecting P2P application.

You need to monitor many terminals for a long time to identify an application.

Packet inspection

A method to detect an application from a header or payload pattern of a single packet.

Its easy to detect but easy to spoof.

You cannot trust port number. There are a lot of applications using 80 and 8080 to traverse firewalls.

Several applications encrypt payloads.

It needs to keep signature files up-to-date.

Traffic-behavior approach - Flow-level behavior

A method to identify an application from statistical information such as inter-arrival time, duration of the flow, average packet size.

The method is suited for voice and video stream.

- statistically stable
- relatively long duration (more than 10s)

The method is not suited for signaling protocols and bulk data.

Traffic-behavior approach - Transaction-level behavior

A method to infer an application from the transition of attributes of each packet such as packet size and its flow direction.

ex.) SIP registration & call setup sequence

1. REGISTER	419byte up
2. 200 OK	370byte down
3. INVITE	253byte up
4. 100 Trying	385byte down
5. 180 Ringing	429byte down
6. 200 OK	685byte down
7. ACK	448byte up

This approach is suited for signaling protocols

- which are relatively short-lived and
- which the attributes vary packet by packet. (not like VoIP media traffic)

VoIP traffic identification method

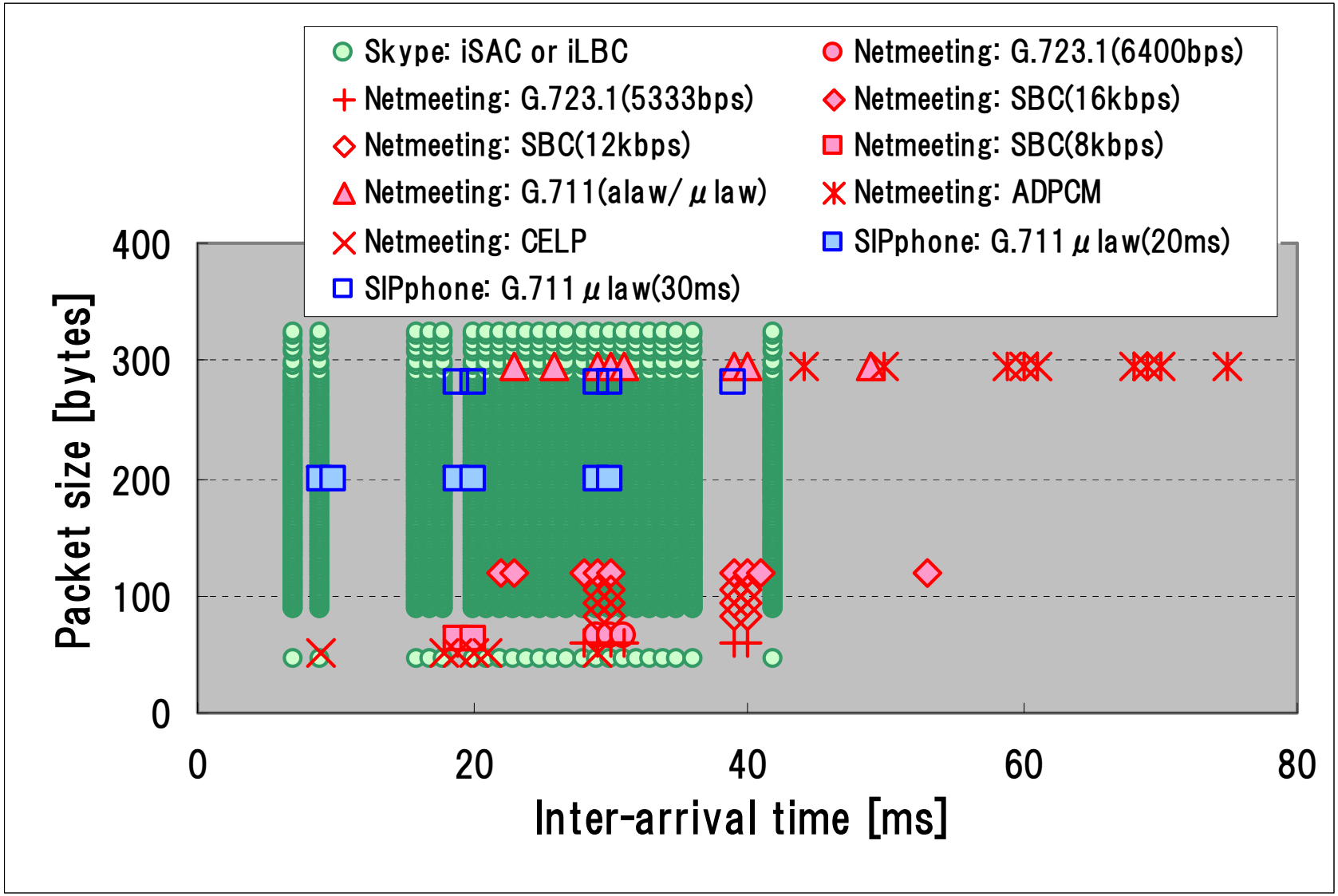
We chose flow-level behavior and transaction-level behavior approach.

Because the methods can

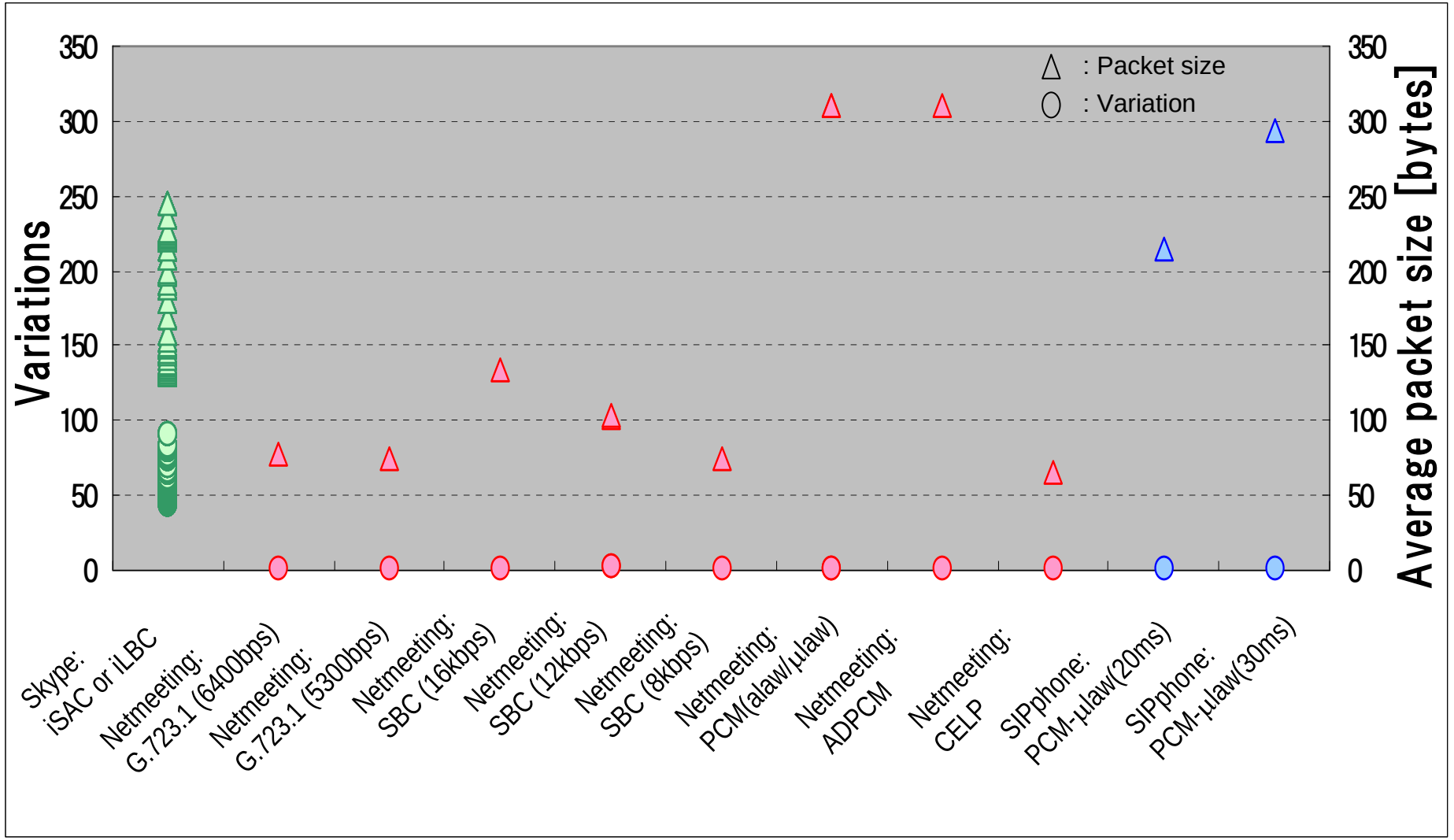
- keep confidentiality of user packets.
- identify VoIP media traffic.
  -> Flow level behavior approach
- identify signaling traffic.
  -> Transaction level behavior approach

To verify these approaches we measured several application traffic.

Flow-level behavior (1)

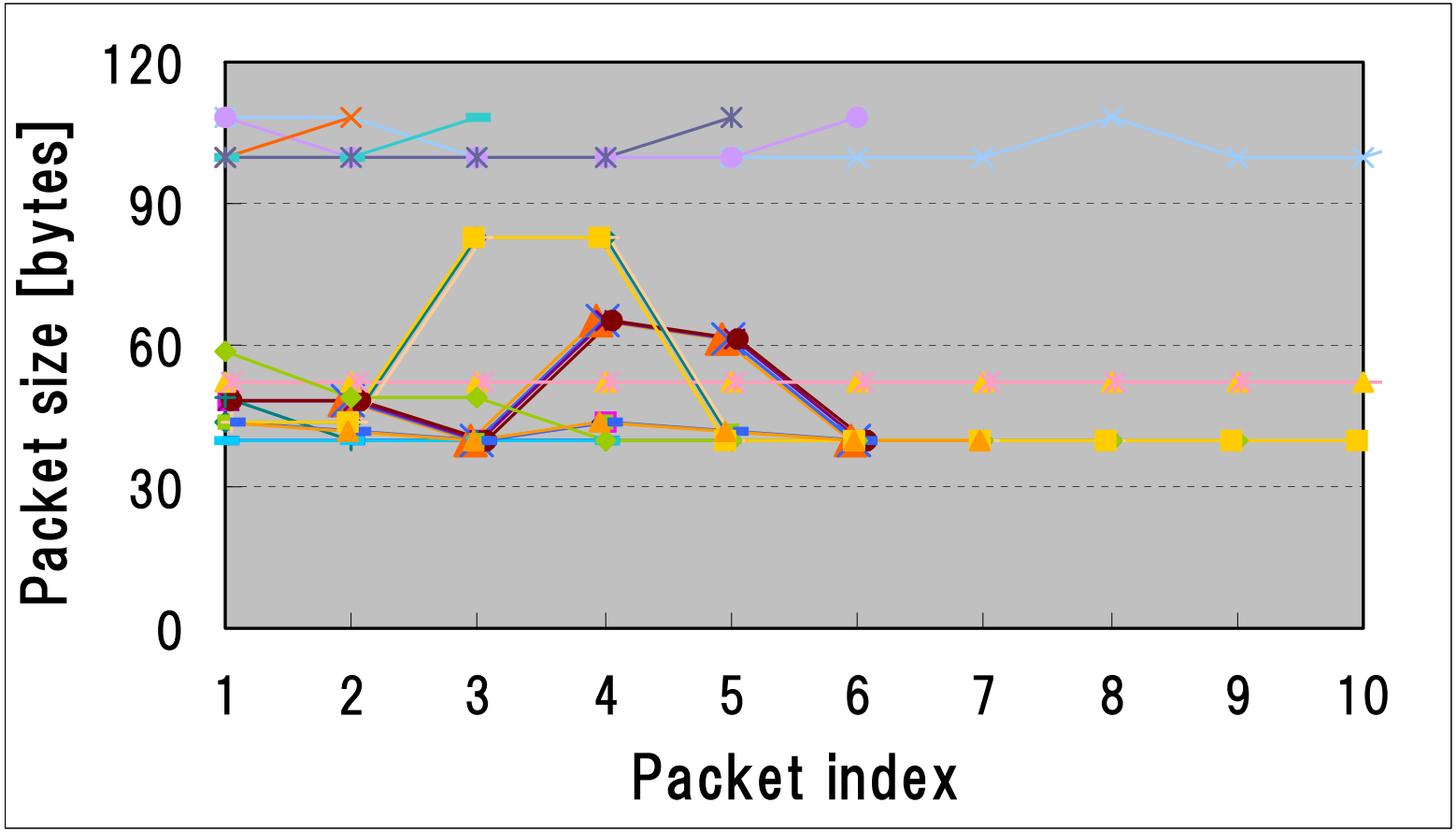


Flow-level behavior (2)



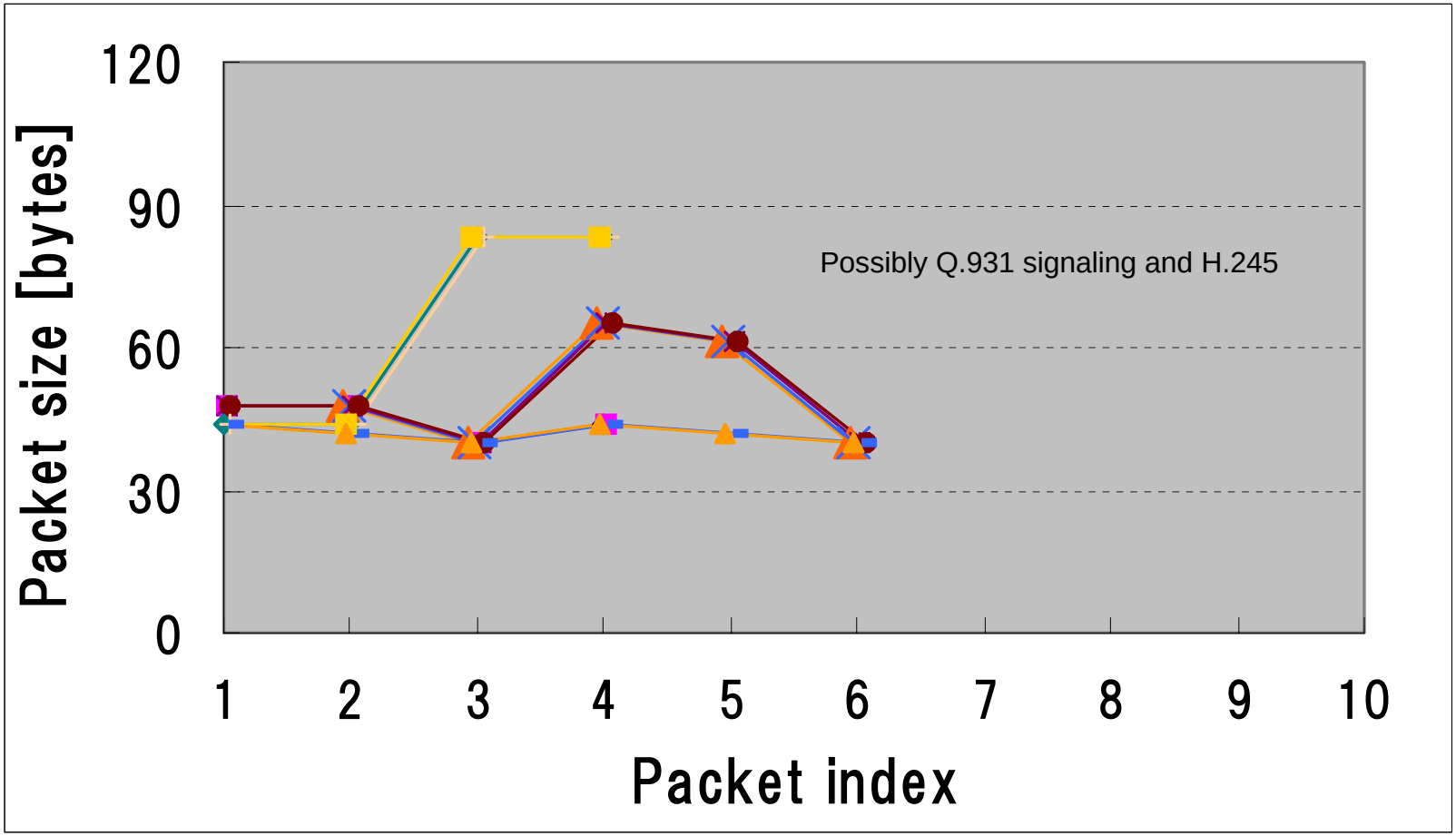
Transaction-level behavior

Netmeeting 3.0 call setup (10 s * 5 time trials)



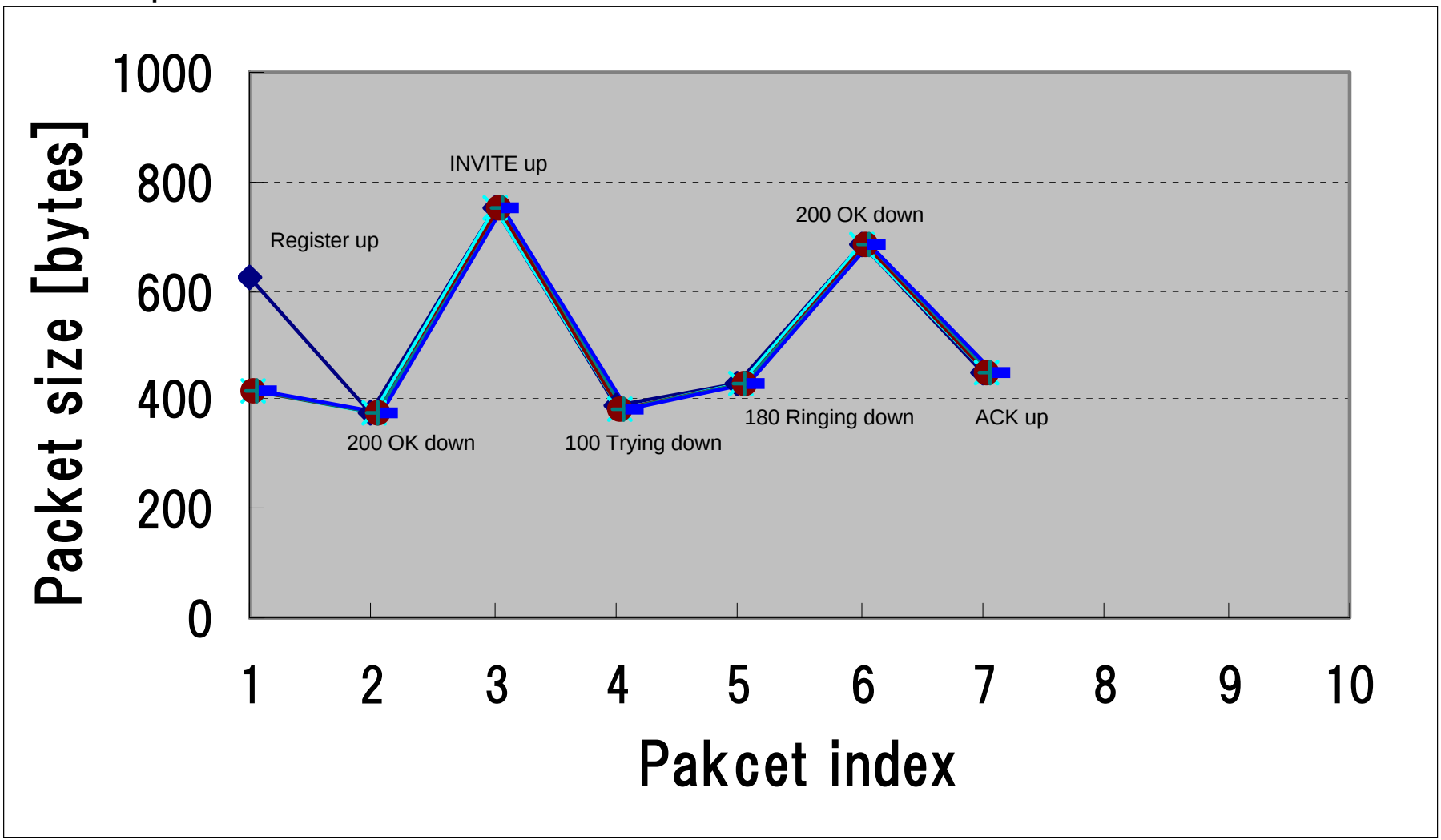
Transaction-level behavior

Netmeeting 3.0 call setup (transactions included in ALL trials)



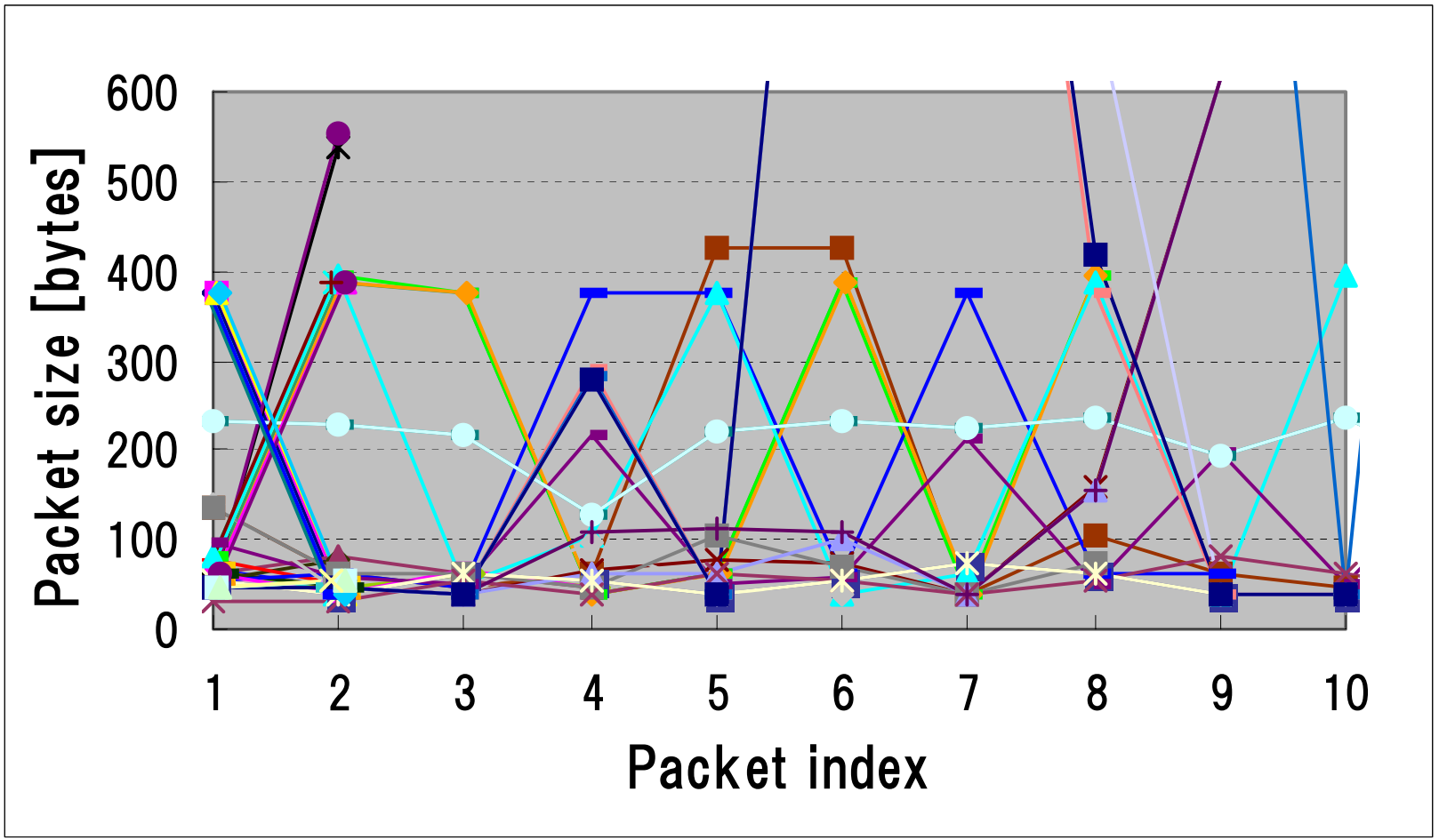
Transaction-level behavior

SIP phone



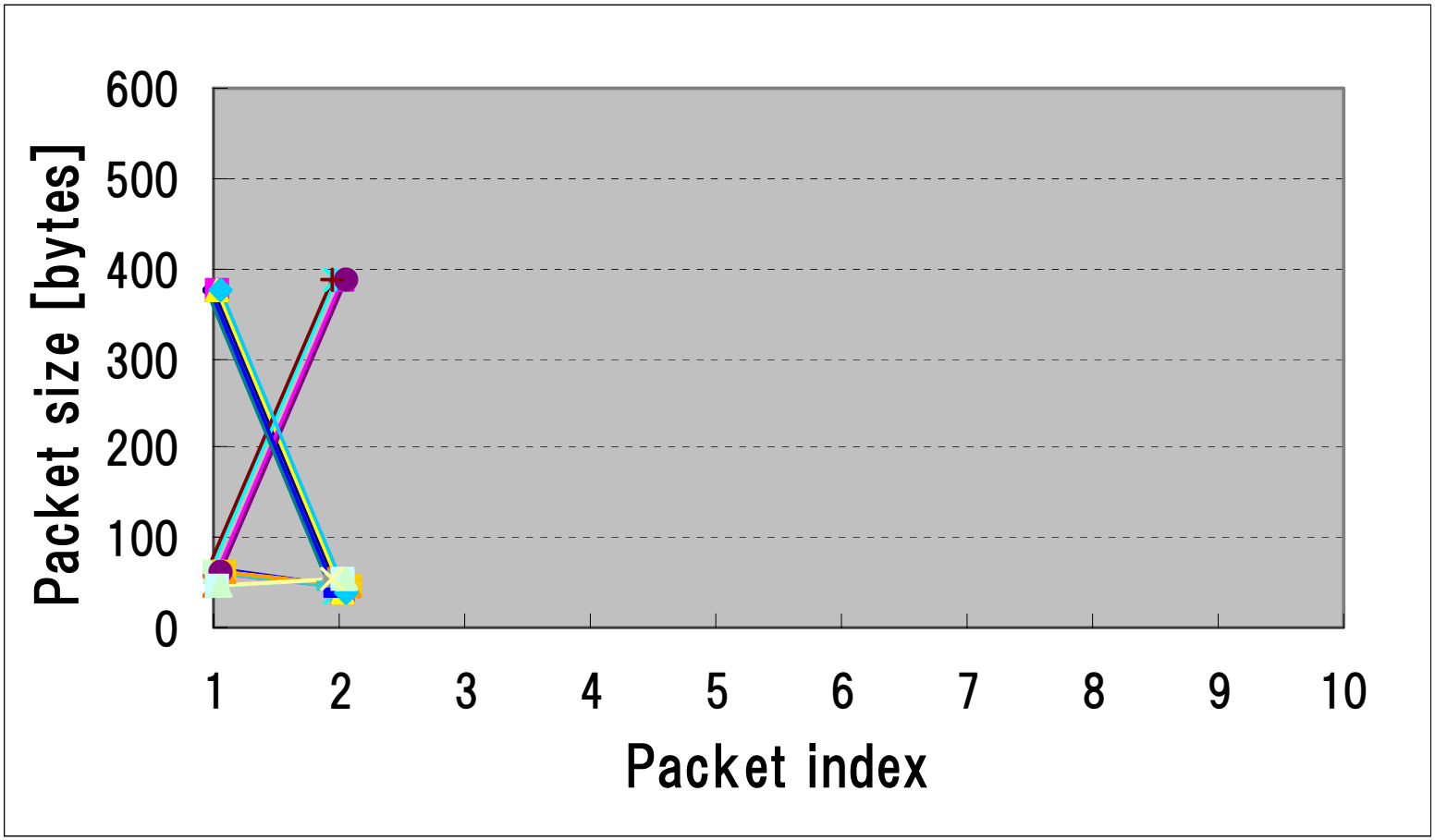
Transaction-level behavior

Skype 2.0 call setup (10 s * 5 time trials)



Transaction-level behavior

Skype 2.0 call setup (transactions included in ALL trials)



Host behavior approach seems better than Transaction-level behavior approach.

Conclusion

We are expecting

Transaction-level is suited for VoIP media.

Flow-level is suited for VoIP signaling.

And Host-level is suited P2P application.

We are planning to execute evaluation of the two methods using actual traffic data of network to achieve

- high accuracy,
- high responsiveness and
- high performance (low CPU-load and memory usage)