



MOT: Memory Online Tracing of Web Information System

Yun Mao, Kang Chen,

DS. Wang, WM. Zheng, XT. Deng

High Performance Computing Institute

Computer Science & Technology Dept.

Tsinghua University

Beijing 100084, P.R. China

maoyun00@mails.tsinghua.edu.cn



Presentation Outline

- **Introduction**
- **Related Work**
- **Design and Implementation**
- **Applications**
- **Experimental Results**
- **Conclusions**



Introduction



Why care about Web?

- **Web applications become dominant**
 - ~ 72% flows, ~ 55% packets, ~ 56% bytes
- **Web is undergoing changes**
 - HTTP 1.0 -> HTTP 1.1, multimedia
- **Web is based on other protocols**
 - TCP, DNS
- **How to understand Web?**
 - Measure, then analyze



How to measure?

- **From log-files of Web servers**
 - Specific, not representative
- **From users running modified browsers**
 - Lack enough volunteers
- **From log-files of Web proxies**
 - Bottleneck, level of detail in logs is low
- **From log-files of packet sniffing**
 - rich, transparent, passive, complicated



Advantages of passive sniffing

- Provides all useful information
- Does not affect the Internet performance
- Remains transparent to end users



Why Complicated?

- **Network bandwidth is increasing**
 - CPU, network adapters, disk I/O
- **TCP reconstruction**
 - Packet loss, retransmission, IP fragmentation
- **HTTP reconstruction**
 - Persistent connections, pipeline
 - incompatible client/servers
 - Inaccurate Content-Length
 - Non-80 port service



MOT features

- Parse the packets in memory, reduce the unnecessary I/O operation.
- Do not save HTTP contents, prevents some potential privacy problem.
- Event-driven architecture, scalable and suitable for highly concurrent applications



Related Work



Related Work

- HTTPDump, (Virginia Tech University)
- BLT(Bi-Layer Trace), AT&T Research Lab
- Olympics data analysis, IBM
- HTTP tracing based on ISPE, UC Berkeley



Design and Implementation



Feasibility(1)

- **Not all Internet traffic is Web data**
 - Non-TCP packets(UDP, ICMP, IGMP)
 - Well-known port number(23 for telnet)
- **Adopt Linux Socket Filter to pre-filter these useless packets in the kernel space**



Feasibility(2)

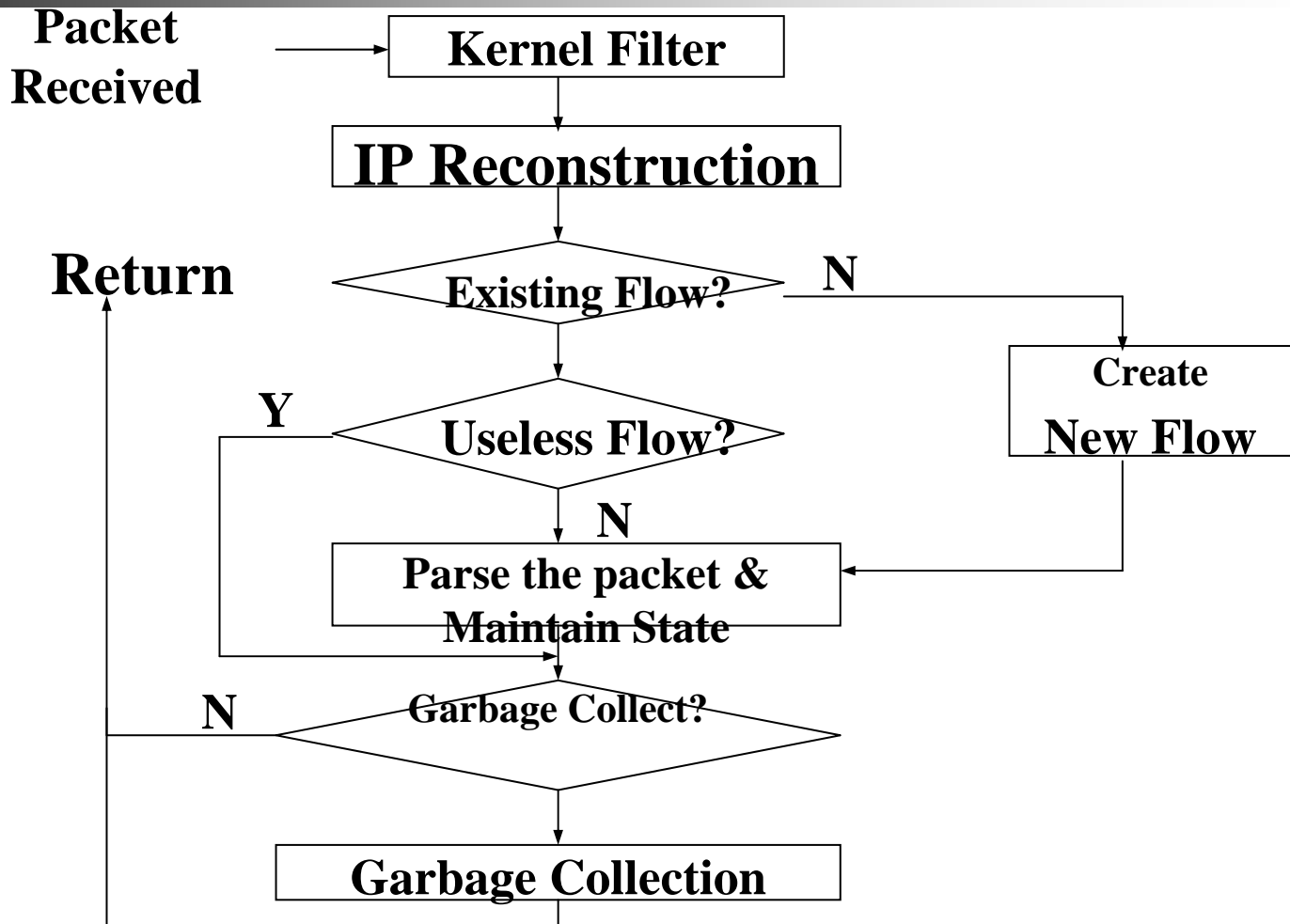
- Protocol headers need not to save
- Web traffic can be easily identified from their first 200 bytes(RFC2616)
- The tracing system cares only about HTTP headers



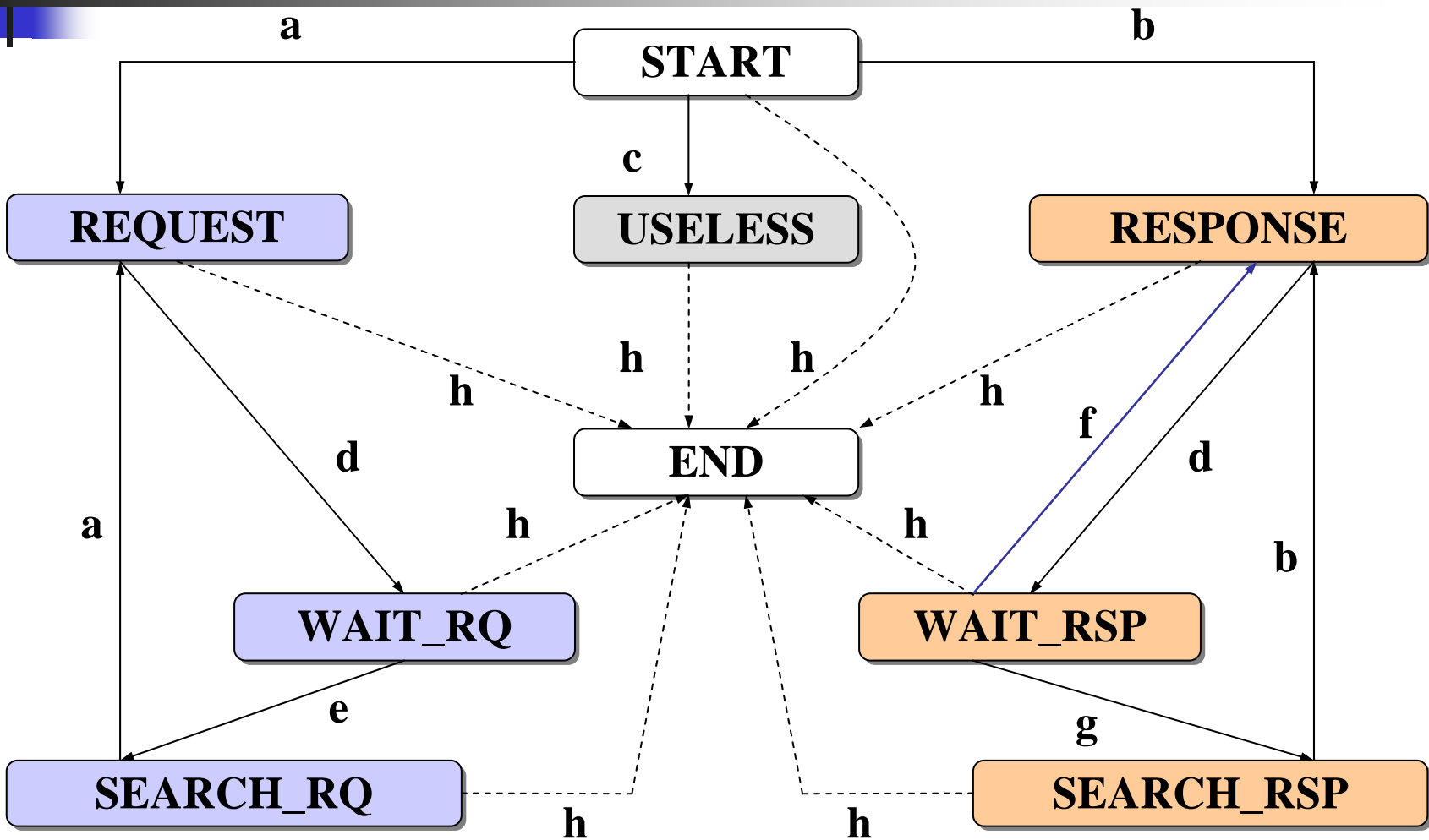
Reconstruction in Memory

- **Not all the Internet traffic is Web data**
 - Non-TCP: UDP, ICMP, ..
 - Well-known ports: 20,21 FTP, 25 SMTP, ..
 - Kernel filter
- **Protocol headers**
- **Only HTTP headers, no contents**
- **Disk I/O is reduced!**

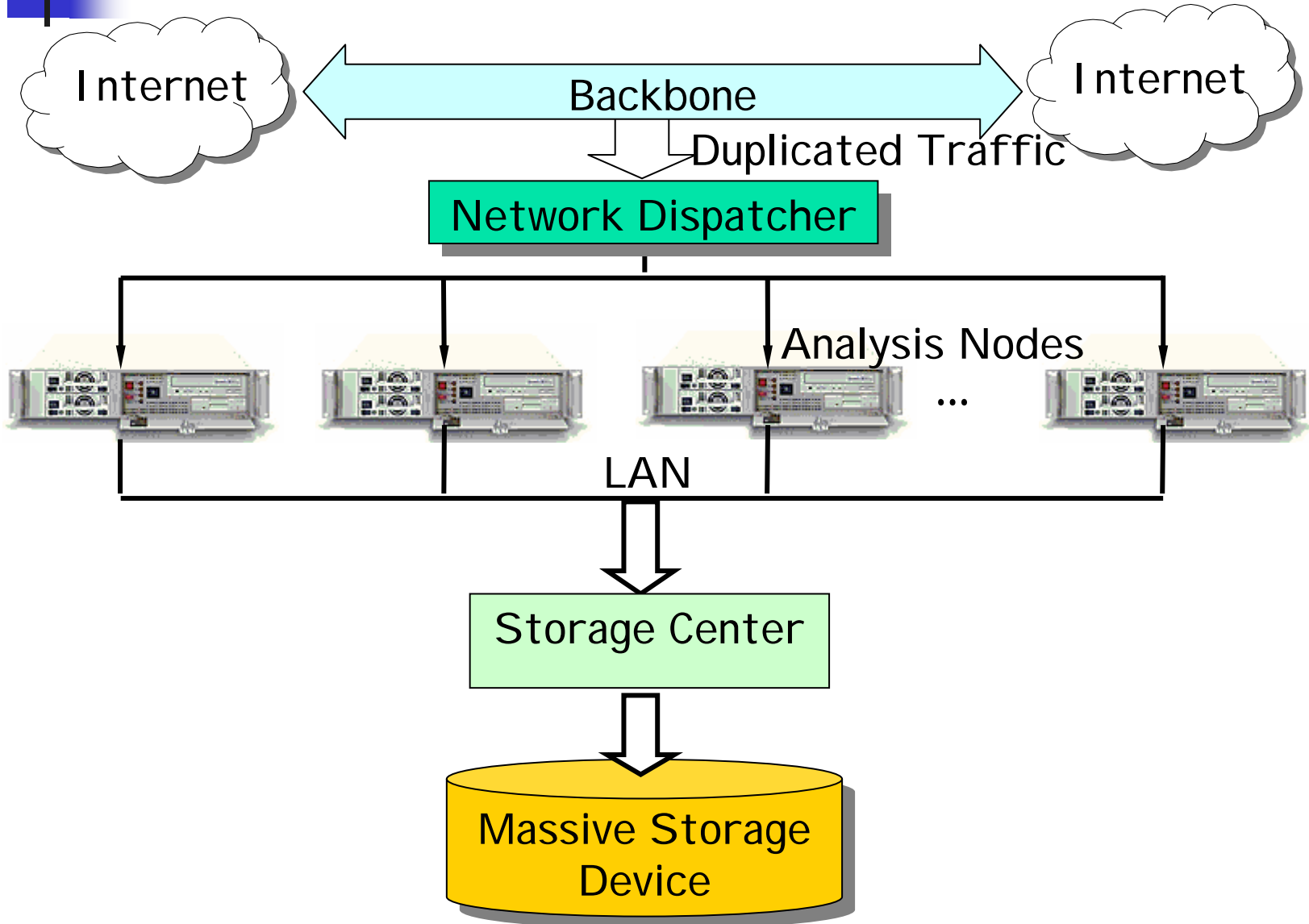
Function flow chart



State Transition Diagram



Cluster-based Architecture





Applications



Applications

- How does the access rate vary in different time scales?
- What is the page size distribution?
- Which web is the most popular one in any given month?
- What is the ratio of multimedia content data to all Web data?



Applications(advanced)

- Web change analysis
- Link analysis
- Geographical distribution
- Protocol performance evaluation



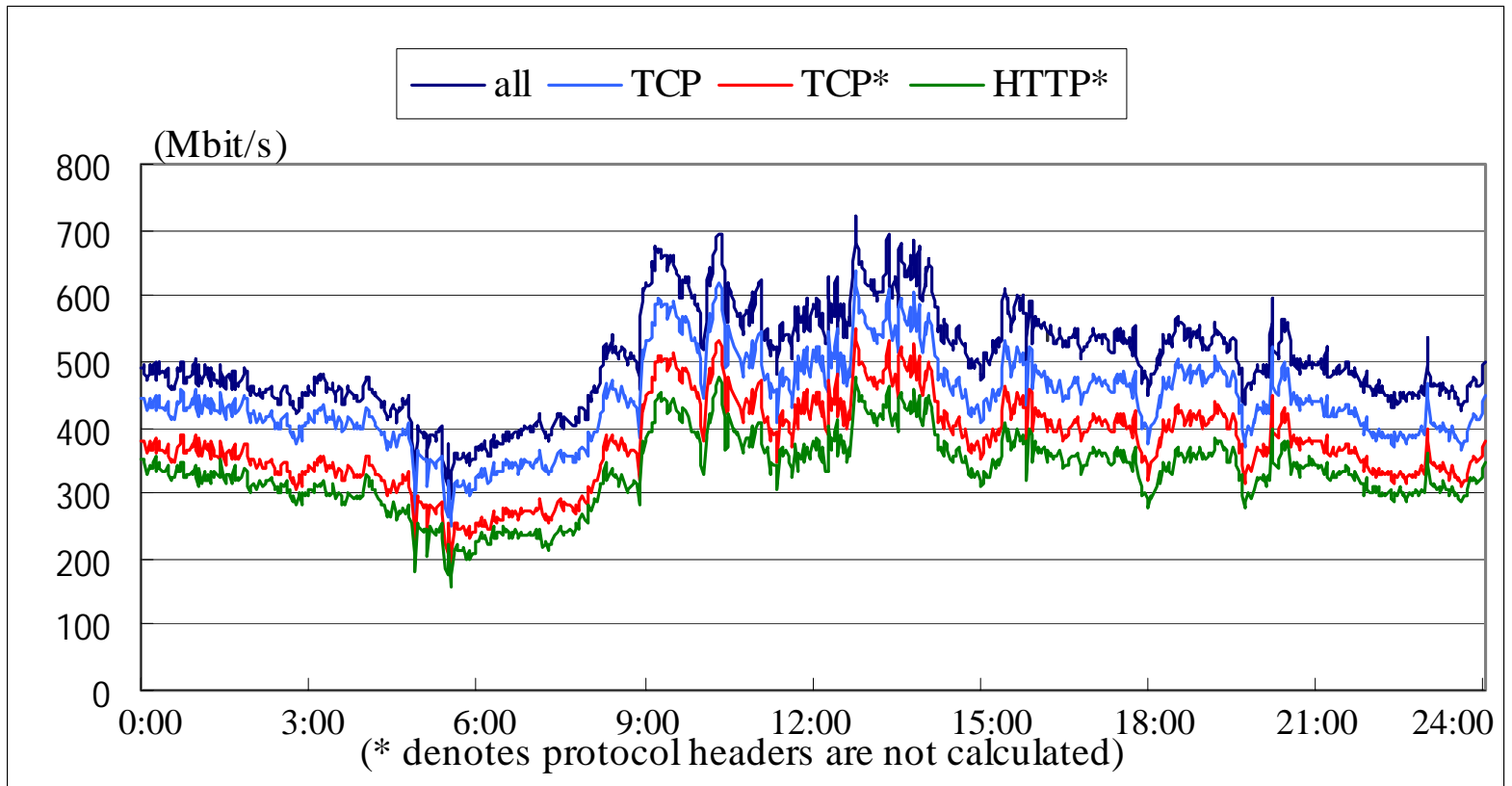
Experimental Results



Single Node Testing

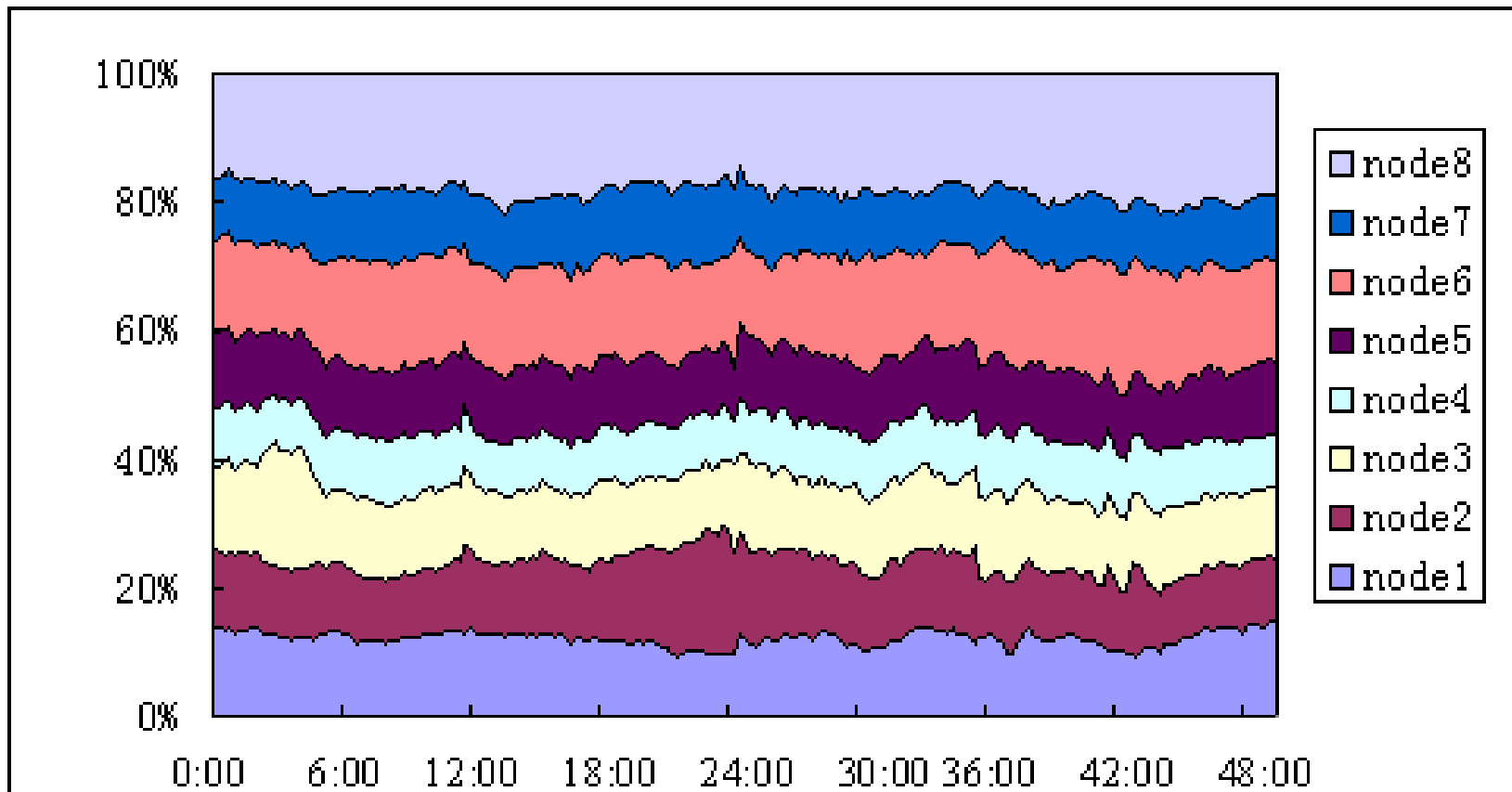
Page Size (Bytes)	Concurrent Connections	Bandwidth (Mbps)	Requests Generated	Requests Caught	Accuracy
6519	100	33.1	2,000,000	2,000,000	100.0%
6519	600	43.9	6,000,000	6,000,000	100.0%
6519	2000	50.2	2,000,000	1,992,136	99.61%
6519	4000	55.8	4,000,000	3,613,871	90.34%
18156	100	67.2	2,000,000	2,000,000	100.0%
18156	600	86.5	6,000,000	6,000,000	100.0%
18156	2000	88.6	2,000,000	1,999,204	99.96%
18156	4000	91.1	4,000,000	3,824,178	95.60%

Preliminary Results



Traffic Composition of Common Protocols in Bit-Rate Over 24-hour

Preliminary Results (cont'd)

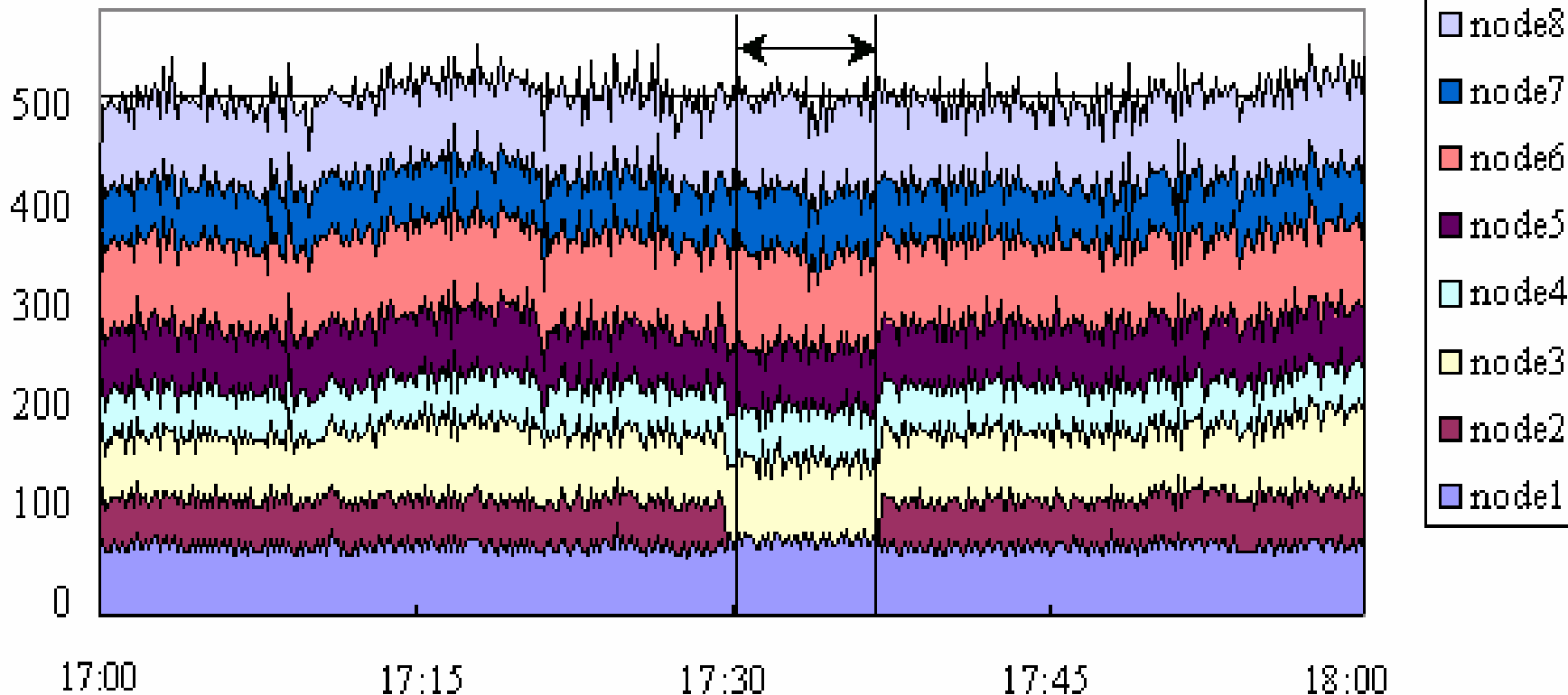


Bit Rate in Each Analysis Node During 2 Consecutive Days

Preliminary Results (cont'd)

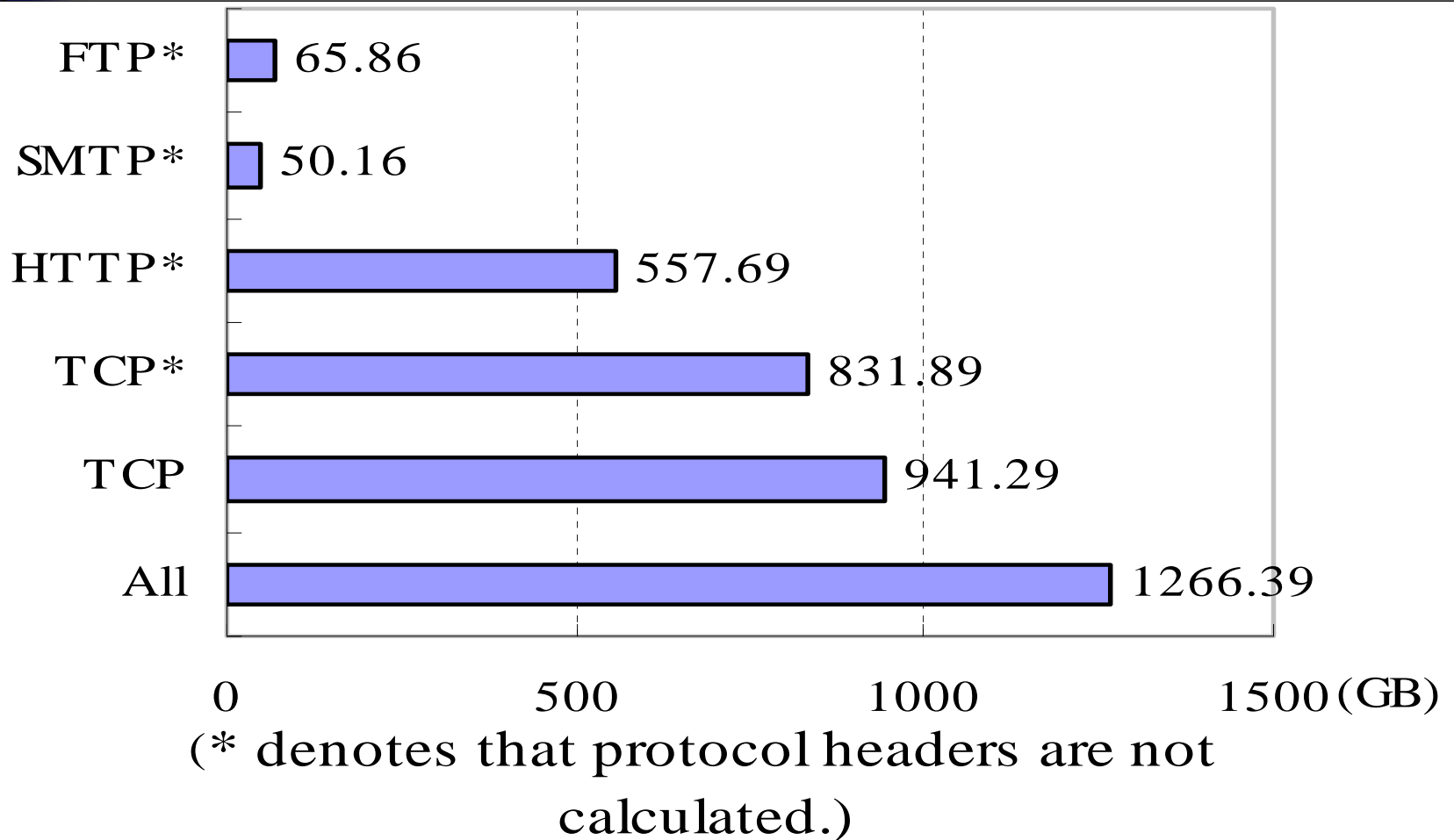
Fault Injection in Node 2

(Mbit/s)



Traffic Distribution in Bit-rate During 1-hour Period

Byte Volume Distribution





Conclusions



Summary & Conclusion

- **Processing in Memory**
 - Reduce disk I/O -> high performance
 - Flow reconstruction, parsing and logging is incorporated
 - Maintain per-flow state to extract and record related information
 - Extract header information to save time and memory
- **Cluster-based Solution**
- **A useful measurement system**
 - Link analysis, Web change analysis, performance evaluation (bi-layer)

