Traffic Analysis on a Domain Name System Server. SMTP Access Generates Many Name-Resolving Packets to a Greater Extent than Does POP3 Access

Yasuo Musashi,* Ryuichi Matsuba,* and Kenichi Sugitani

Center for Multimedia and Information Technologies, Kumamoto University, Kumamoto 860-8555 Japan, E-mail: musashi@cc.kumamoto-u.ac.jp

Table of Contents

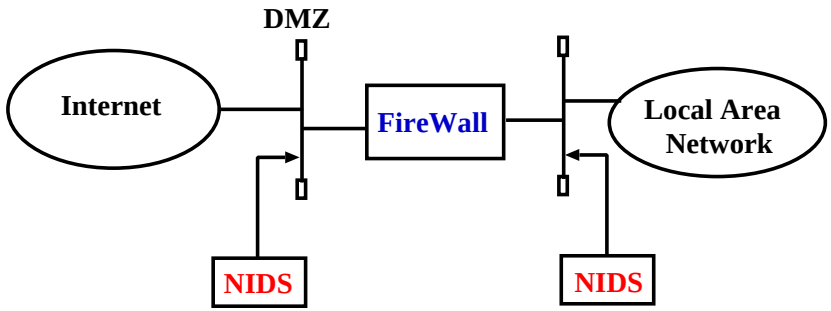
Domain Name System and Intrusion Detection System

The most important network services on the Internet.

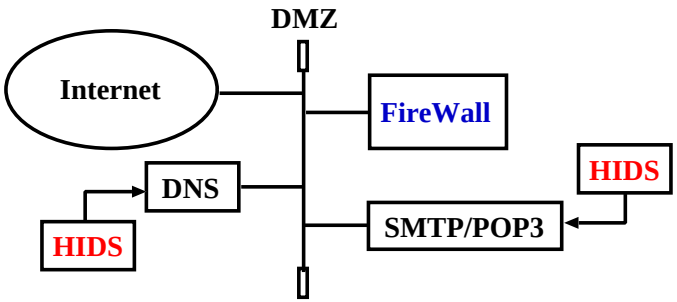
SMTP/POP3(Mail),FTP,HTTP,...

We need to protect the DNS server, firmly.

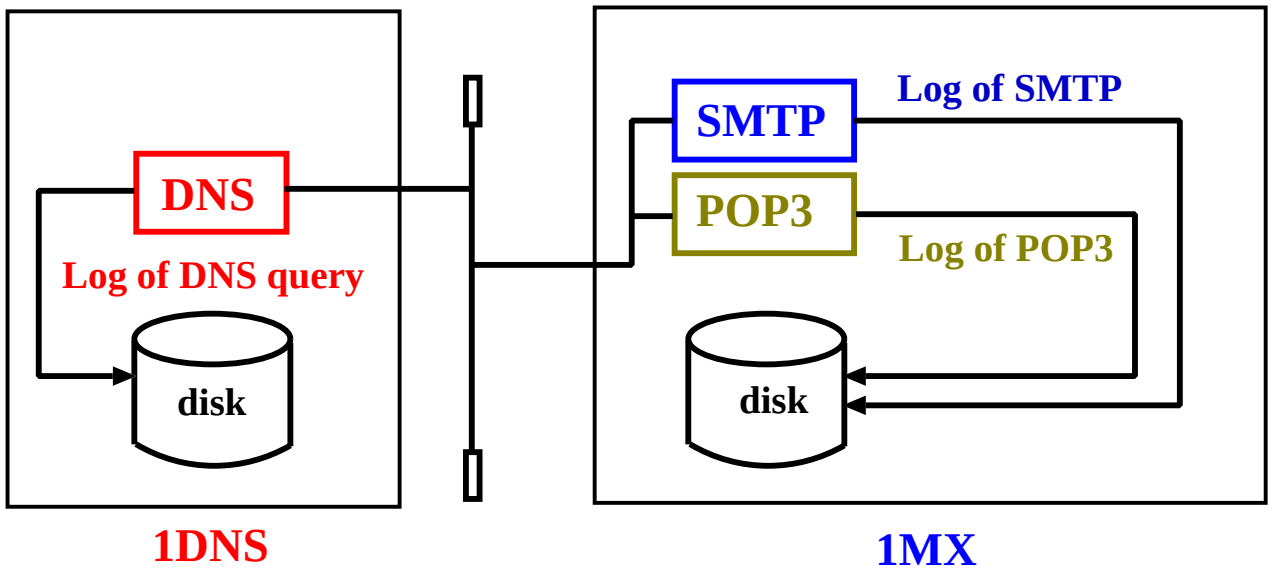
(A) Network Based Intrusion Detection System



(B) Host Based Intrusion Detection System



This Work



(1) Statistical investigation on traffic of the DNS query packets between the DNS server (1DNS) and the E-mail server (1MX).

(2) How are the DNS query packets generated by the SMTP and POP3 accesses?

(3) Cache effects of the DNS query.

Computations: Normal Equation 1

$$D_{\mathrm{q}} = R_{\mathrm{SMTP}} + R_{\mathrm{POP3}} + R_{\mathrm{FTP}} + \cdots \tag{1}$$

$$R_i = m_i N_i \tag{2}$$

D_{q} = the DNS query access between the 1DNS and 1MX.

R_i = the access numbers from the DNS clients.

i = a network protocol, such as SMTP, POP3, FTP, ...

N_i = the access counts of a network application,

m_i = a linear coefficient.

$R_{\mathrm{SMTP}} + R_{\mathrm{POP3}} \gg R_{\mathrm{FTP}} + \cdots$(1MX)

$$D_{\mathrm{q}} = m_{\mathrm{SMTP}} N_{\mathrm{SMTP}} + m_{\mathrm{POP3}} N_{\mathrm{POP3}} \tag{3}$$

Computations: Normal Equation 2

$$\boldsymbol{A}_{\mathbf{SMTP,POP3}}\ \boldsymbol{x}_{\mathbf{SMTP,POP3}} = \boldsymbol{d}_{\mathbf{SMTP,POP3}} \tag{4}$$

$$\boldsymbol{A}_{\mathbf{SMTP,POP3}} = \begin{bmatrix} \sum_{j=1}^{n} \boldsymbol{N}^{\mathbf{2}}_{\mathbf{SMTP},j} & \sum_{j=1}^{n} \boldsymbol{N}_{\mathbf{SMTP},j}\boldsymbol{N}_{\mathbf{POP3},j} \\ \sum_{j=1}^{n} \boldsymbol{N}_{\mathbf{SMTP},j}\boldsymbol{N}_{\mathbf{POP3},j} & \sum_{j=1}^{n} \boldsymbol{N}^{\mathbf{2}}_{\mathbf{POP3},j} \end{bmatrix}$$

$$(\boldsymbol{j} = \mathbf{1, 2, 3, \cdots, }\boldsymbol{n}\mathbf{;\ days})$$

$$\boldsymbol{x}_{\mathbf{SMTP,POP3}} = (\boldsymbol{m}_{\mathbf{SMTP}}, \boldsymbol{m}_{\mathbf{POP3}})^{t}$$

$$\boldsymbol{d}_{\mathbf{SMTP,POP3}} = (\sum_{j=1}^{n} \boldsymbol{N}_{\mathbf{SMTP},j}\boldsymbol{D}_{\mathbf{q},j},\ \sum_{j=1}^{n} \boldsymbol{N}_{\mathbf{POP3},j}\boldsymbol{D}_{\mathbf{q},j})^{t}$$

Used Server Daemon Programs and Estimation of Traffic

Used server daemon programs

- **1DNS: The DNS server and the DNS packet recorder.**
  BIND-9.1.3 and iplog-1.2
- **1MX:The SMTP and POP3 servers.**
  ISC sendmail-8.9.3 and Qualcomm qpopper-4.0

Estimation of Traffic

(1) D_q**:**

```
% grep domain /var/log/messages.1 | wc
```

(2) N_{SMTP}**:**

```
% grep "sendmail" /var/log/syslog.0 | wc
```

(3) N_{POP3}**:**

```
% grep "poppe\[" syslog.0 | wc
```

Observed data of N_{SMTP}, N_{POP3}, and D_{q} (day^{-1}).

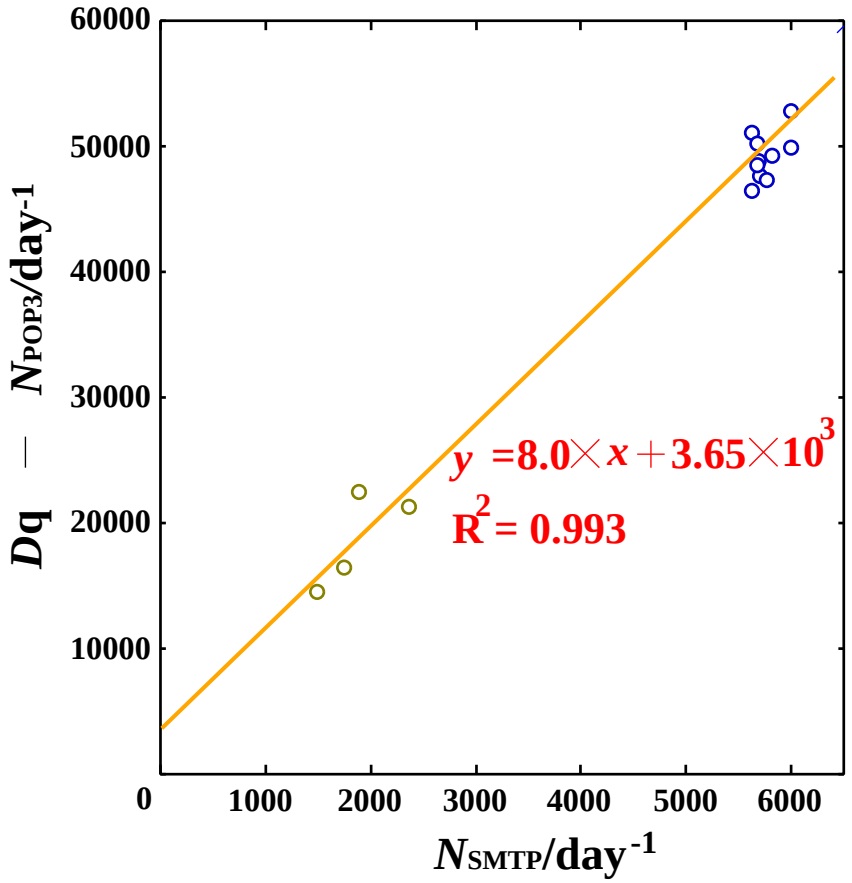
j	N_{SMTP}	N_{POP3}	D_{q}
2002/02/11	1878	4480	26845
02/13	6010	17701	70327
02/14	5647	17663	68574
02/15	5744	16469	65849
02/17	1487	4004	18370
02/18	5973	16959	67262
02/19	5594	16118	62489
02/20	5666	17178	66718
02/21	5701	15851	63614
02/23	2363	6451	27540
02/24	1749	3814	20199
02/25	5731	16020	63626
02/26	5675	17688	68612

$$\boldsymbol{A}_{\mathrm{SMTP,POP3}} = \begin{bmatrix} 3.120 \times 10^8 & 9.084 \times 10^8 \\ 9.084 \times 10^8 & 2.652 \times 10^9 \end{bmatrix}, \quad \boldsymbol{d}_{\mathrm{SMTP,POP3}} = (3.612 \times 10^9, 1.052 \times 10^{10})^t,$$

$$\boldsymbol{x}_{\mathrm{SMTP,POP3}} = (8.6, 1.0)^t$$

$$\boldsymbol{D}_{\mathrm{q}} = 8.6\boldsymbol{N}_{\mathrm{SMTP}} + \boldsymbol{N}_{\mathrm{POP3}}$$

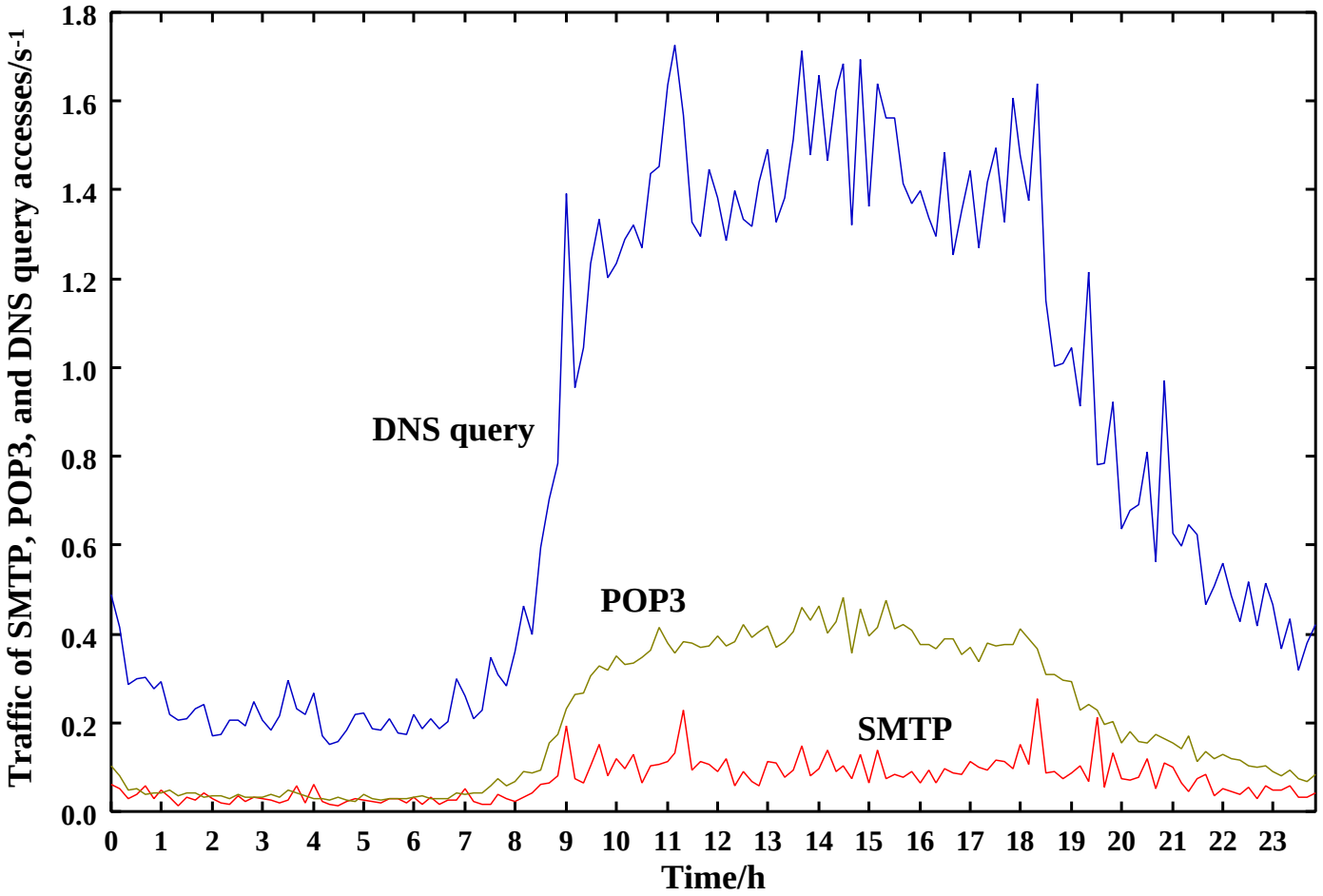
$D_q - N_{POP3}$ versus N_{SMTP} plot



$m_{SMTP} = 8 \sim 9$ and $m_{POP3} = 1$

The SMTP access generates the DNS query, rather than that of the POP3 access.

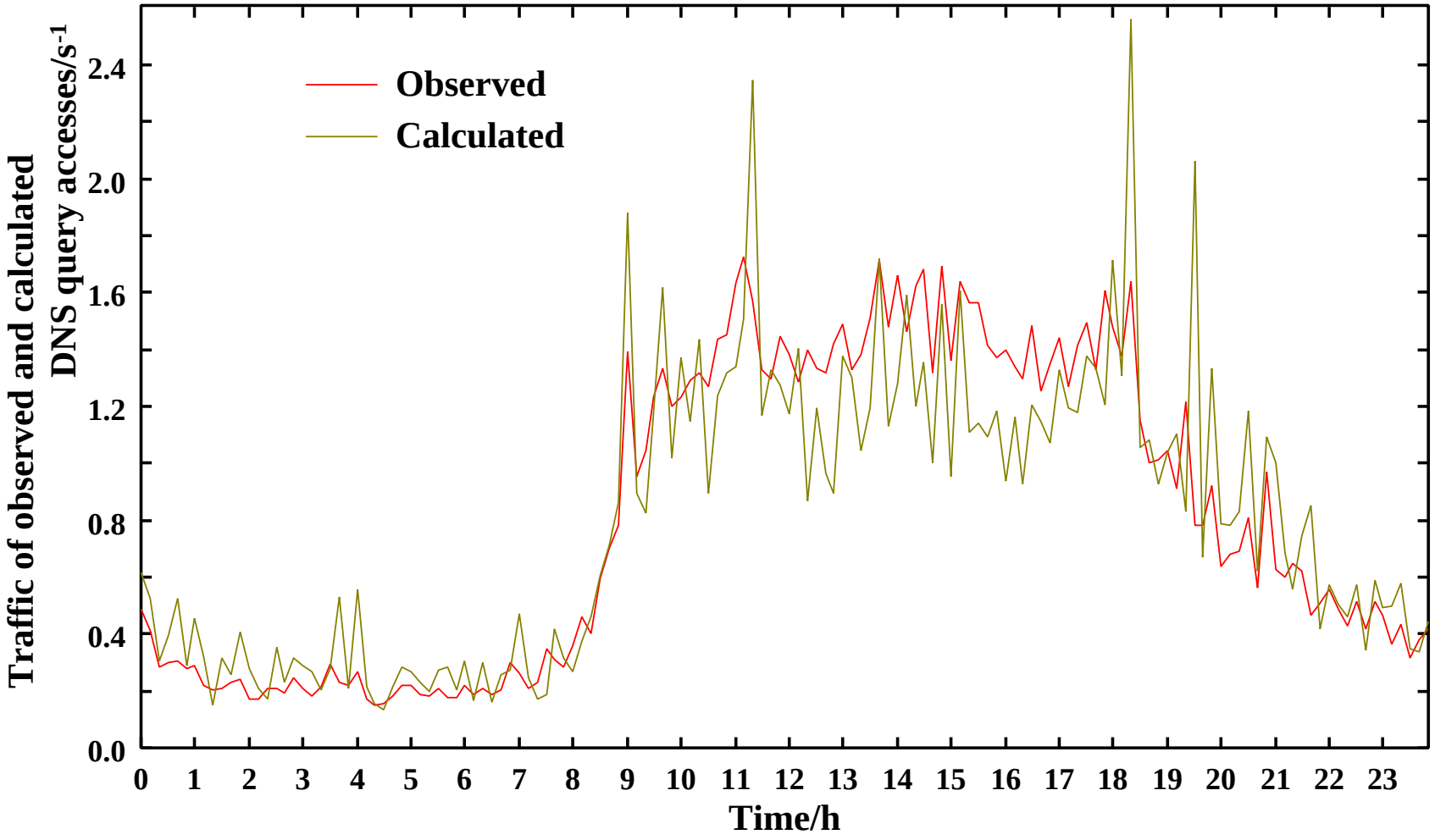
Traffic of SMTP, POP3, and DNS query in 2002/02/13



(1) There are three peaks.

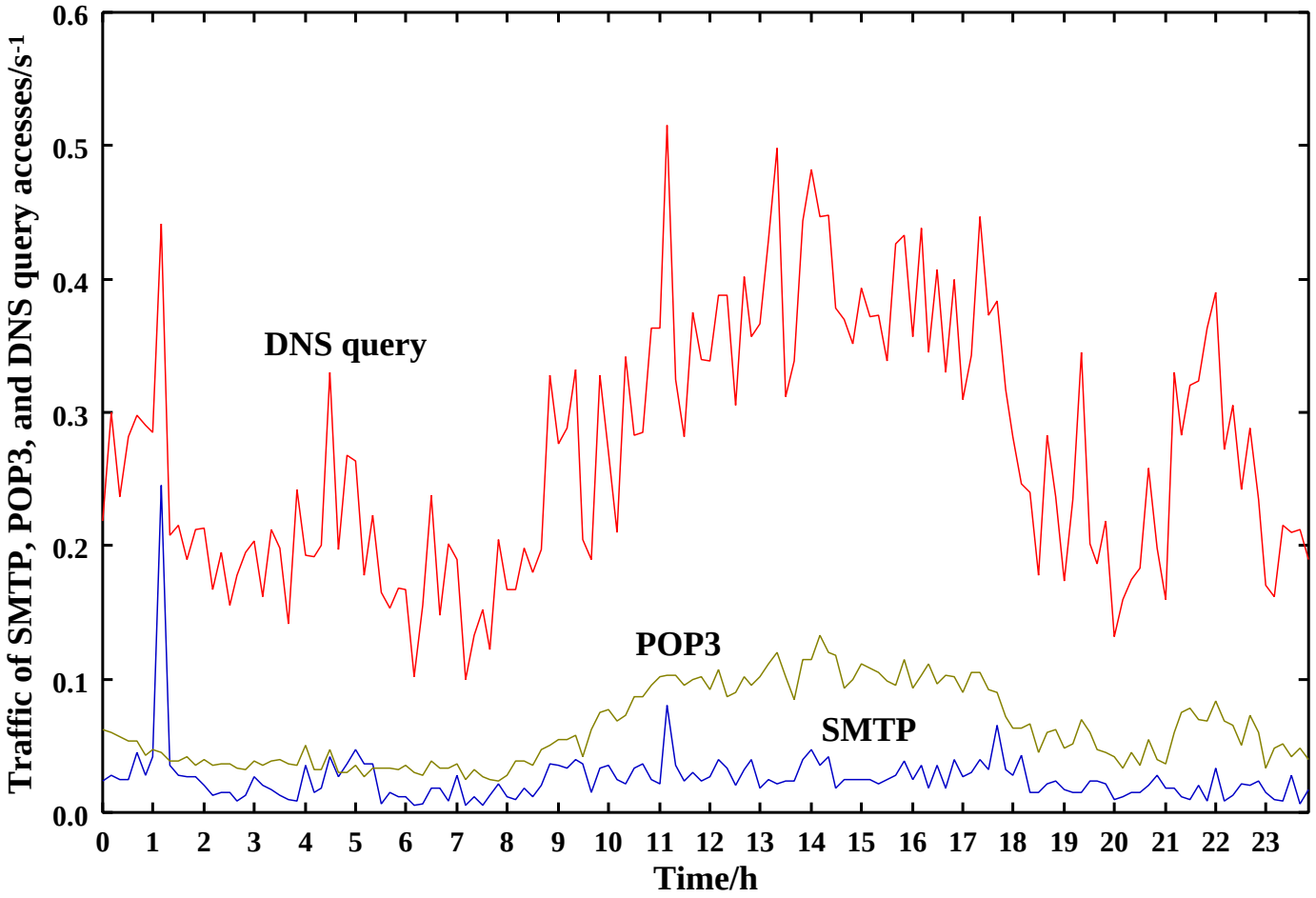
(2) The DNS traffic resembles well the SMTP one.

Observed and calculated DNS traffic in 2002/02/13



The calculated curve resembles well the observed one.

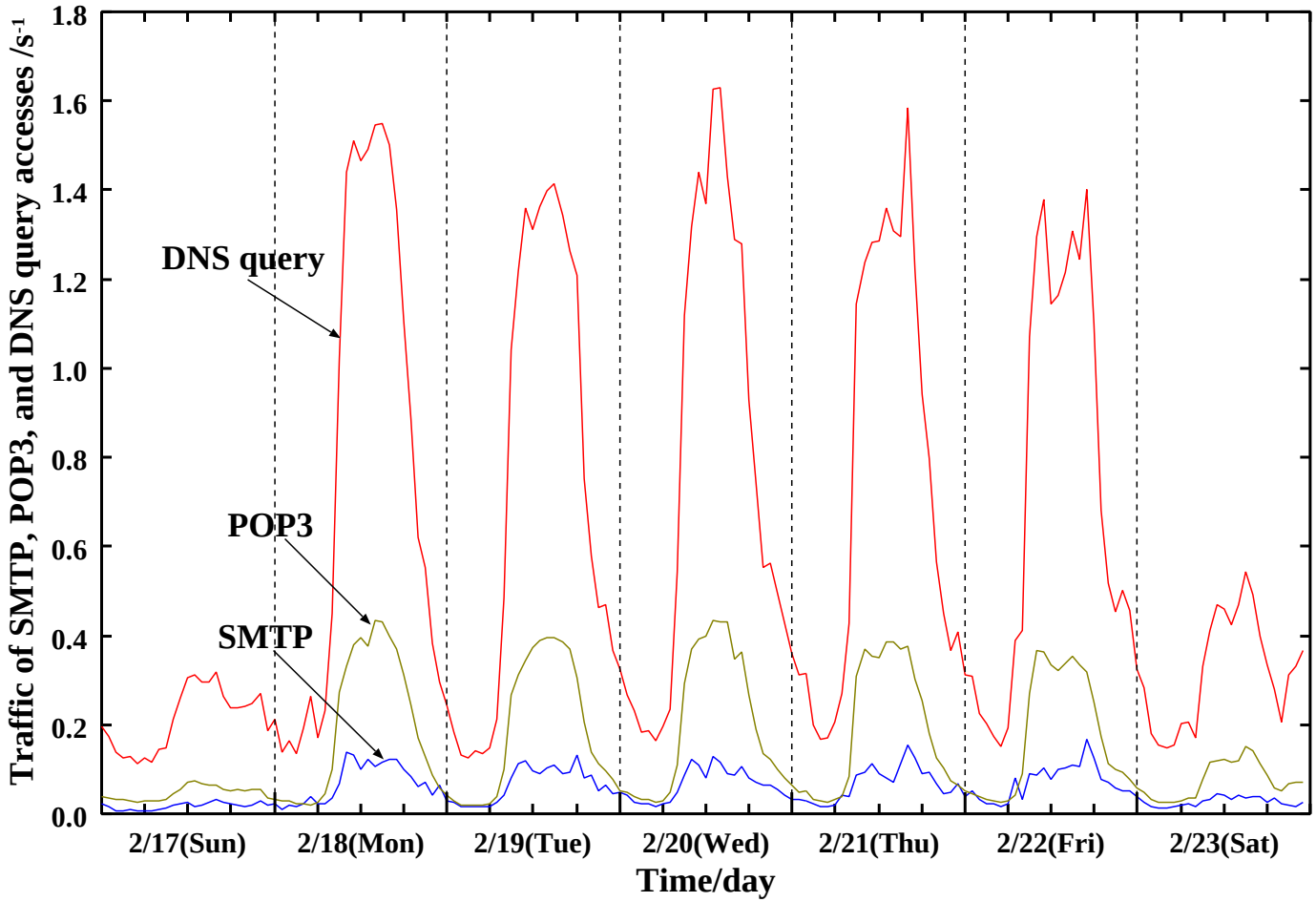
Traffic of SMTP, POP3, and DNS query in 2002/02/16



(1) The DNS traffic resembles well the SMTP one.

(2) The peak of the early morning maybe network trouble?

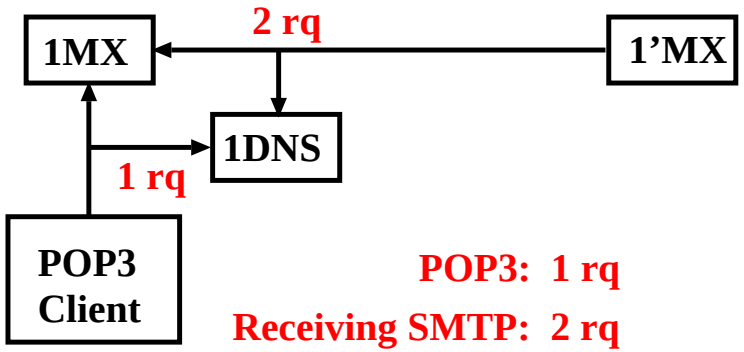
Traffic of Weekday and Holiday



All traffic in weekday is larger than that in holiday.

Why is m_{SMTP} 8.6?

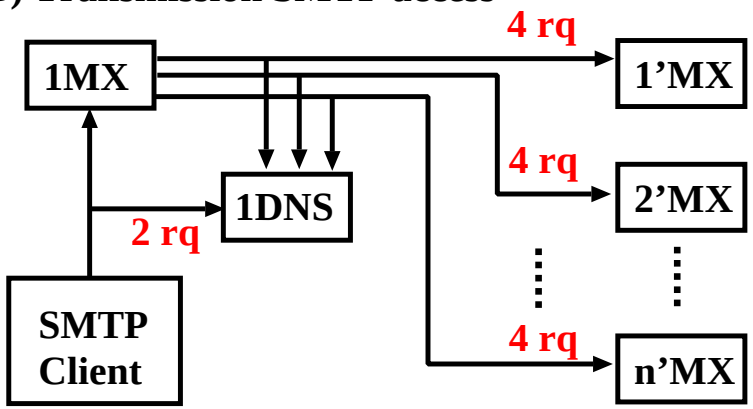
(A) POP3 access and Receiving SMTP access



POP3: 1 rq

Receiving SMTP: 2 rq

(B) Transmission SMTP access



Transmission SMTP : 2 + 4n rq

1 rq = 1 request of DNS query packet

DNS query accesses by a SMTP access

$$\boldsymbol{R}_{\mathbf{POP3}} = \boldsymbol{N}_{\mathbf{POP3}} \tag{5}$$

Receiving SMTP access

$$\boldsymbol{R}^{\mathbf{rec}}_{\mathbf{SMTP}} = \mathbf{2}\boldsymbol{N}^{\mathbf{rec}}_{\mathbf{SMTP}} \tag{6}$$

Transmitting SMTP access

$$\boldsymbol{R}^{\mathbf{tr}}_{\mathbf{SMTP}} = (\mathbf{2} + \mathbf{4}\boldsymbol{n})\boldsymbol{N}^{\mathbf{tr}}_{\mathbf{SMTP}} \tag{7}$$

DNS vs SMTP/POP3

$$R_{\mathrm{SMTP}} = R^{\mathrm{rec}}_{\mathrm{SMTP}} + R^{\mathrm{tr}}_{\mathrm{SMTP}} \tag{8}$$

$$q = \frac{N^{\mathrm{rec}}_{\mathrm{SMTP}}}{N^{\mathrm{rec}}_{\mathrm{SMTP}} + N^{\mathrm{tr}}_{\mathrm{SMTP}}} \tag{9}$$

$$\begin{aligned} m_{\mathrm{SMTP}} N_{\mathrm{SMTP}} &= 2qN_{\mathrm{SMTP}} + (1-q)(2+4n)N_{\mathrm{SMTP}} \quad (N_{\mathrm{SMTP}} > 0) \\ m_{\mathrm{SMTP}} &= 2q + (1-q)(2+4n) \\ &= 2 + 4n(1-q) \end{aligned} \tag{10}$$

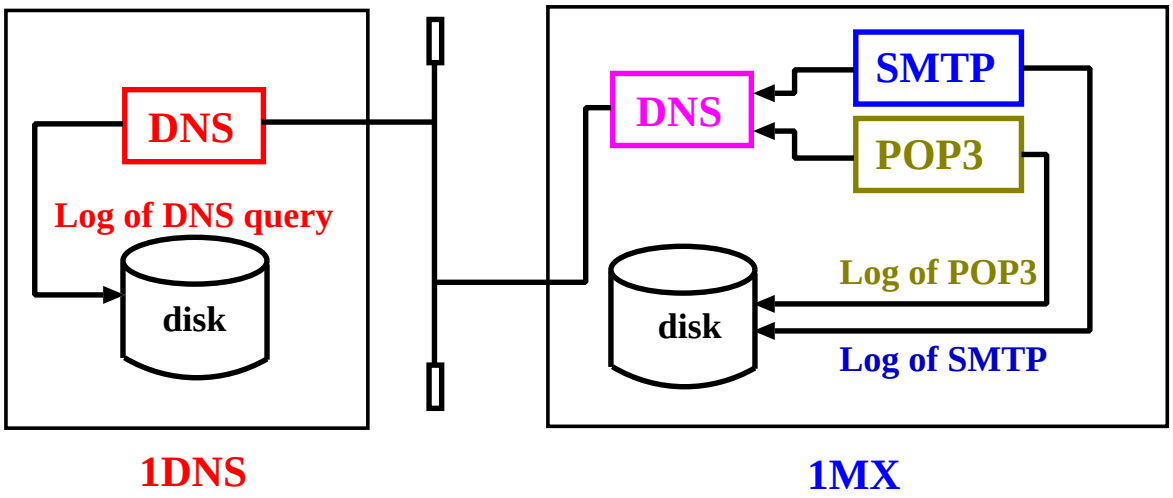
$$D_{\mathrm{q}} = (2 + 4n(1-q))N_{\mathrm{SMTP}} + N_{\mathrm{POP3}} \tag{11}$$

If $q = 0.50 \sim 0.75$ and $m_{\mathrm{SMTP}} = 8.6$; $n = 3.3 \sim 6.6$.

The user of 1MX sends to at least $3 \sim 7$ persons by one E-mailing.

Cache Effects on DNS traffic from E-mail servers

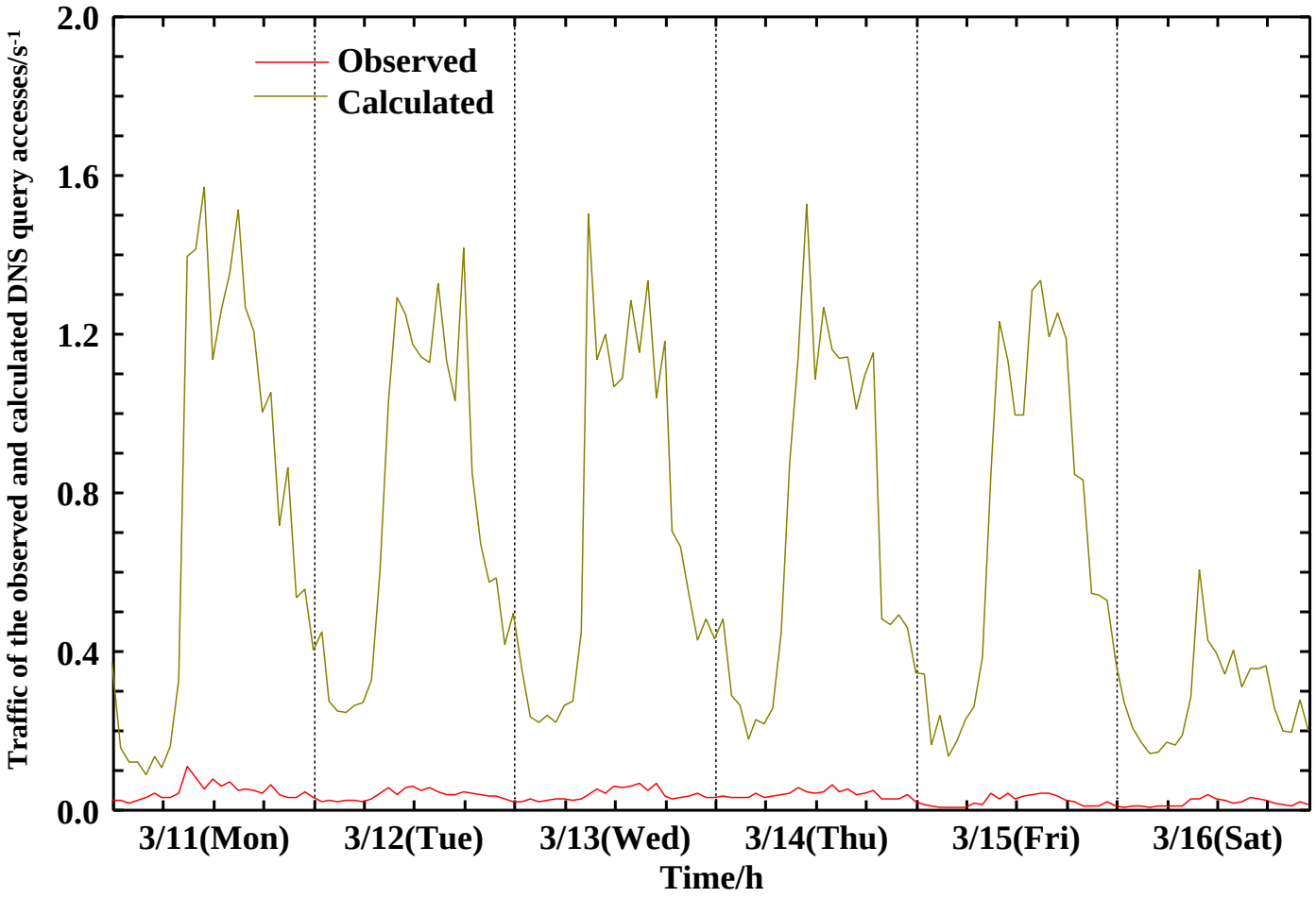
We present the DNS cache effects of the DNS query access between 1DNS and 1MX with the equation ($D_q = 8.6N_{SMTP} + N_{POP3}$).



Used server daemon programs

- 1DNS: The DNS server and the DNS packet recorder.
  BIND-9.1.3 and iplog-1.2
- 1MX:The SMTP and POP3 servers.
  ISC sendmail-8.9.3 and Qualcomm qpopper-4.0

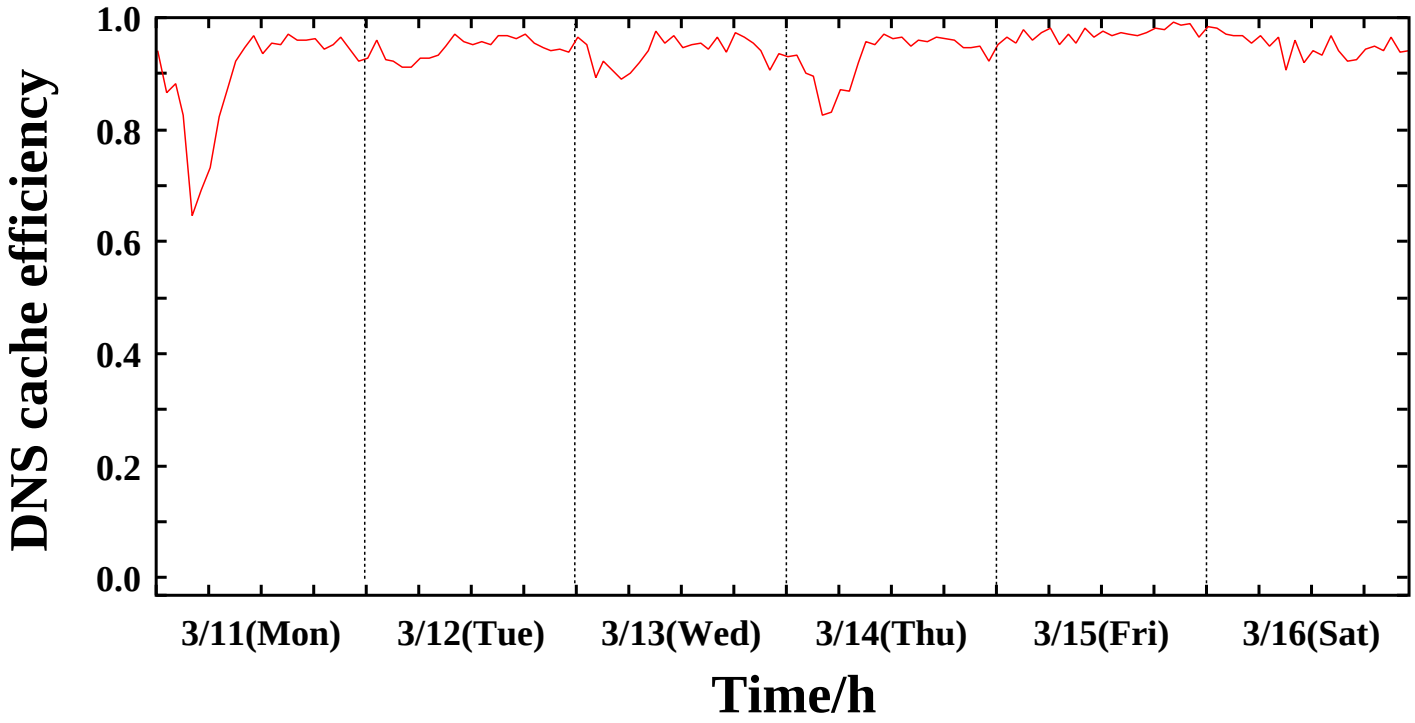
Observed and calculated DNS traffics in 20020311-0316



The observed traffic is considerably much smaller than the calculated one.

Estimated Cache Efficiency of DNS traffic

$$\mathrm{DCE} = 1 - \frac{D_{\mathrm{q}}^{\mathrm{obs}}}{D_{\mathrm{q}}^{\mathrm{calc}}} \tag{12}$$



The DNS cache for SMTP/POP3 services is considerably effective.

Conclusions

(1) The total number of DNS packets, D_q, are represented as

$$D_q = m_{SMTP} N_{SMTP} + m_{POP3} N_{POP3}$$

where N_{SMTP} and N_{POP3} represent the number of the SMTP access and that of the POP3 access, respectively. The linear coefficients m_{SMTP} and m_{POP3} are calculated to be 8.0-8.6 and 1.0.

(2)
$$m_{SMTP} = 2 + 4n(1 - q)$$

where q is a mail-receiving rate and n is a number of different domain hosts.

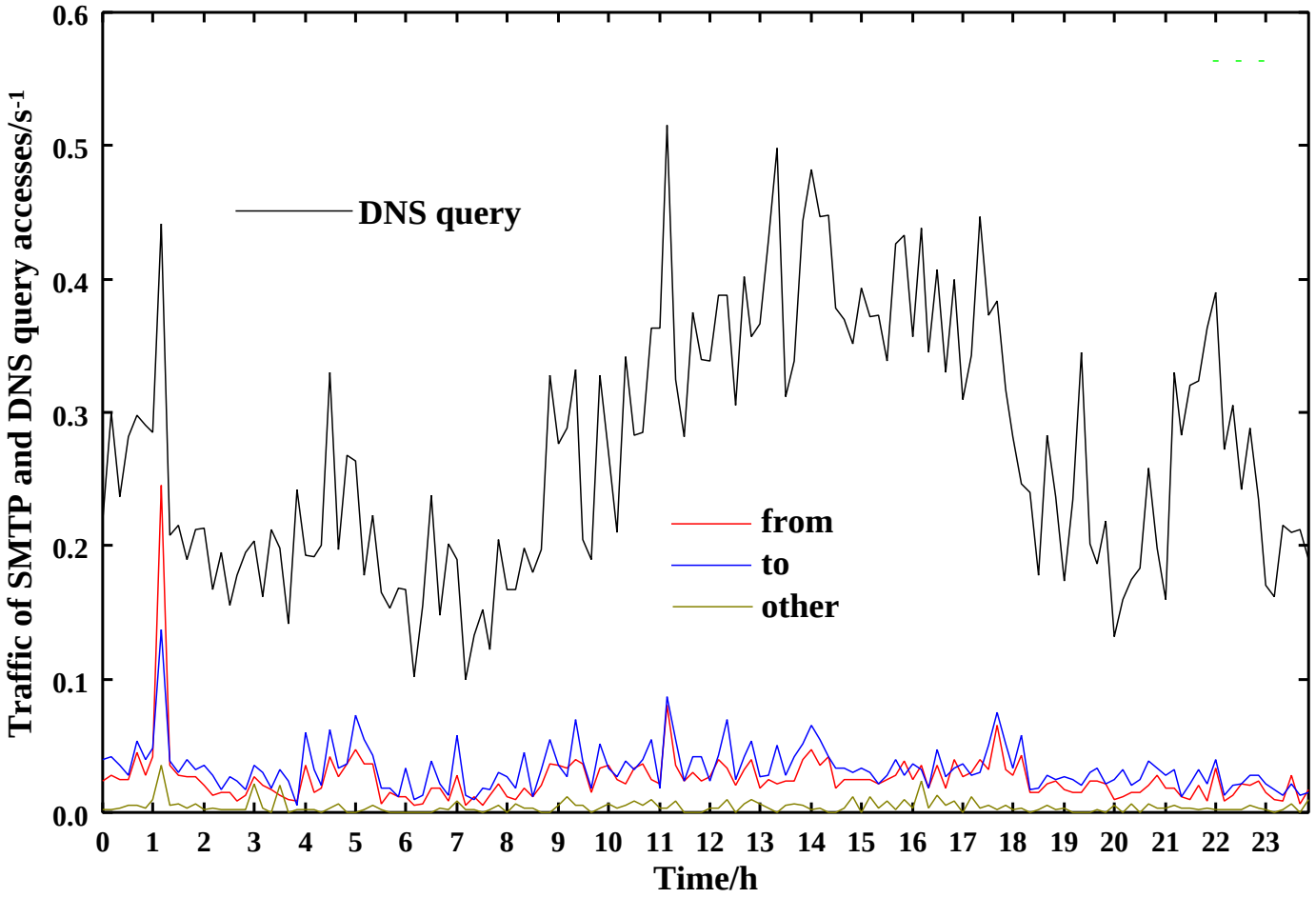
(3) The DNS cache sufficiently affects on the traffic between the DNS server and the E-mail server, and the cache efficiency is about 0.85-0.99. The DNS cache on the E-mail server reduces the traffic between the DNS server and the E-mail server, drastically.

The DNS cache should be applied to the E-mail server.

Acknowledgement

All the calculations were carried out with AMD Athlon, Intel Pentium III, and Sun Microsystems Ultra-Sparc machines in our center.

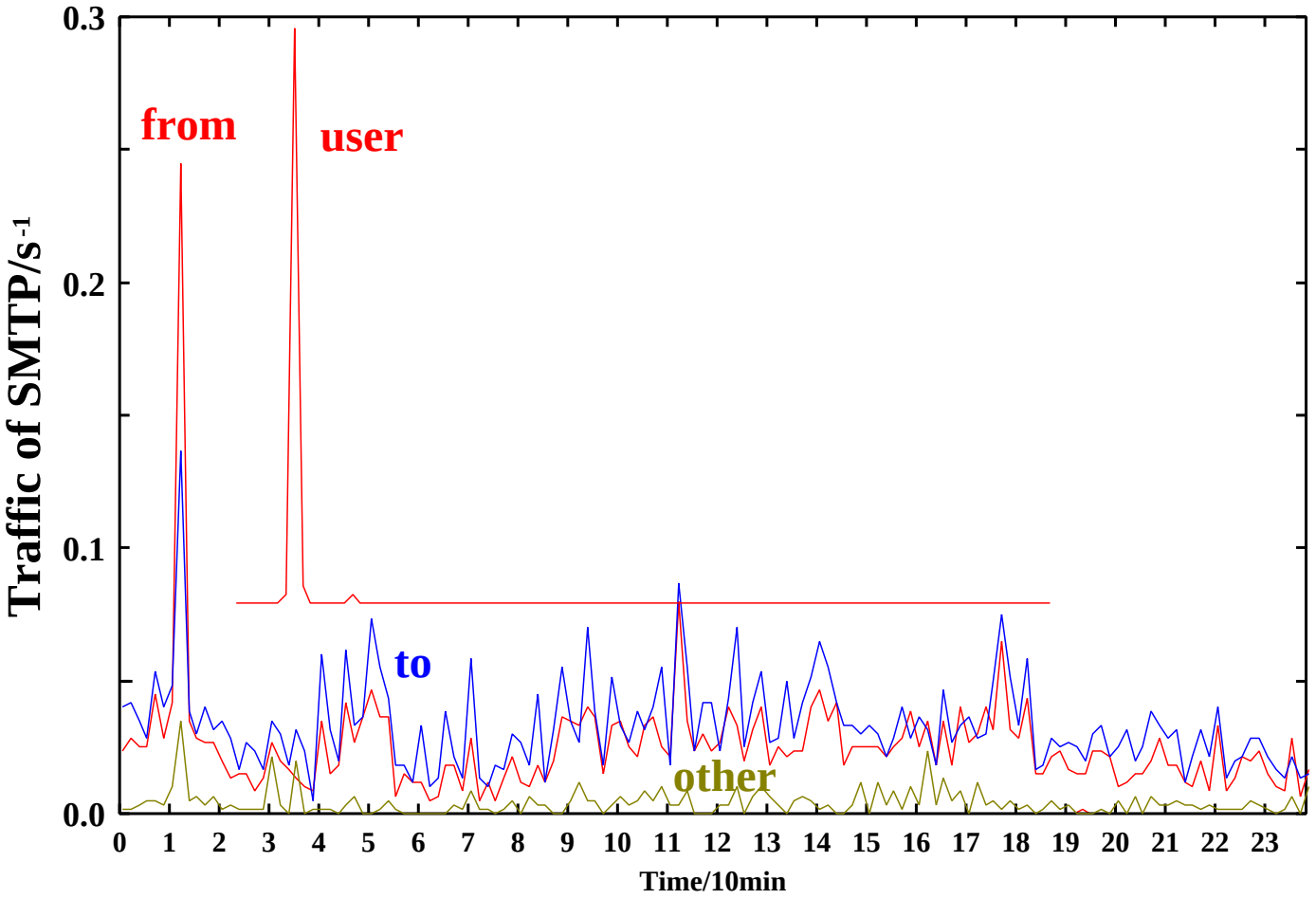
Traffic of SMTP(from,to, and others) in 2002/02/16



(1) $N_{\text{from}} > N_{\text{to}} > N_{\text{others}}$.

(2) Many SMTP sessions and several nslook-up failures.

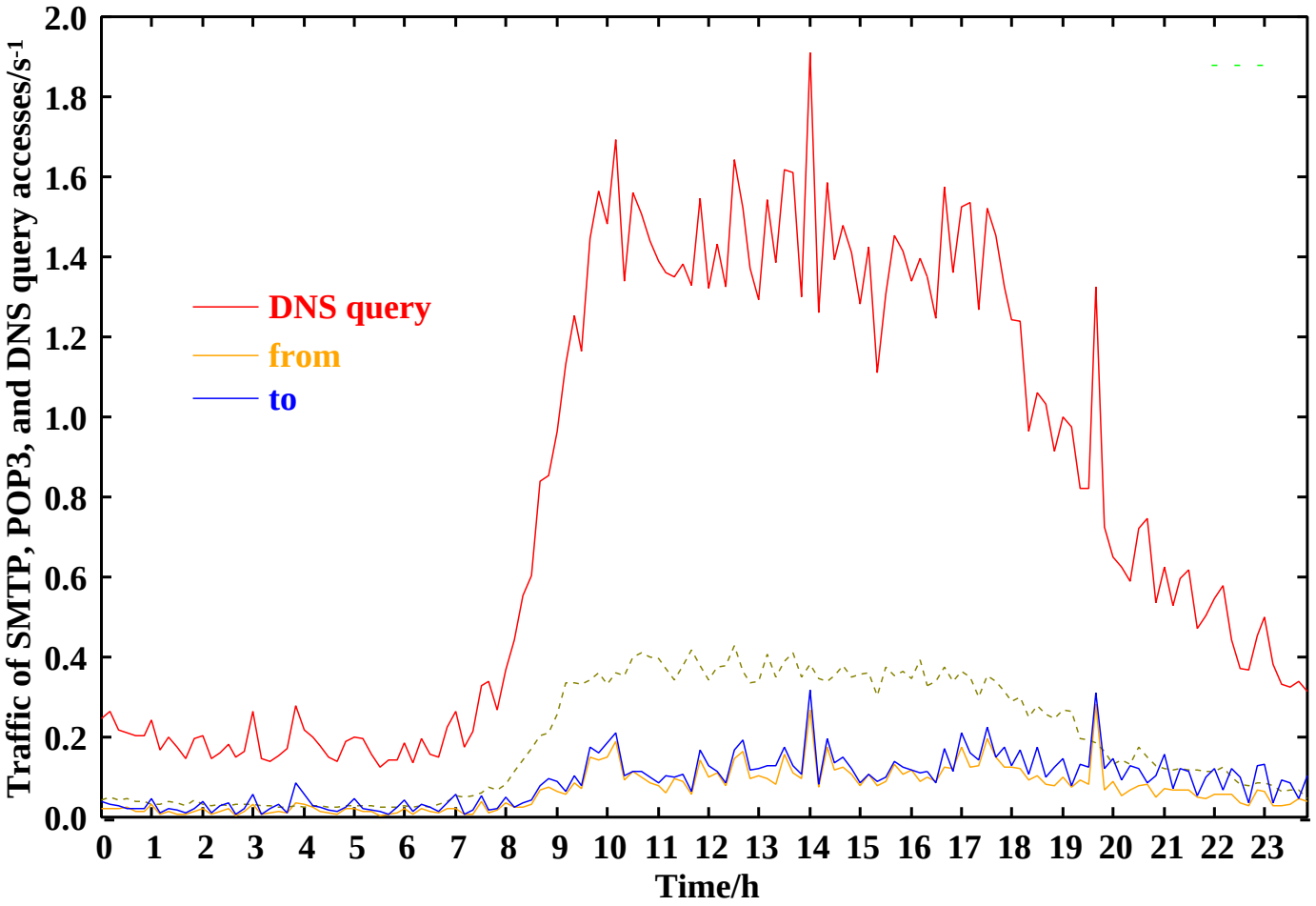
Traffic of SMTP(from,to, user and others) in the peak



(1) $N_{\text{user}} \sim N_{\text{from}}$

(2) Is the user cracked?

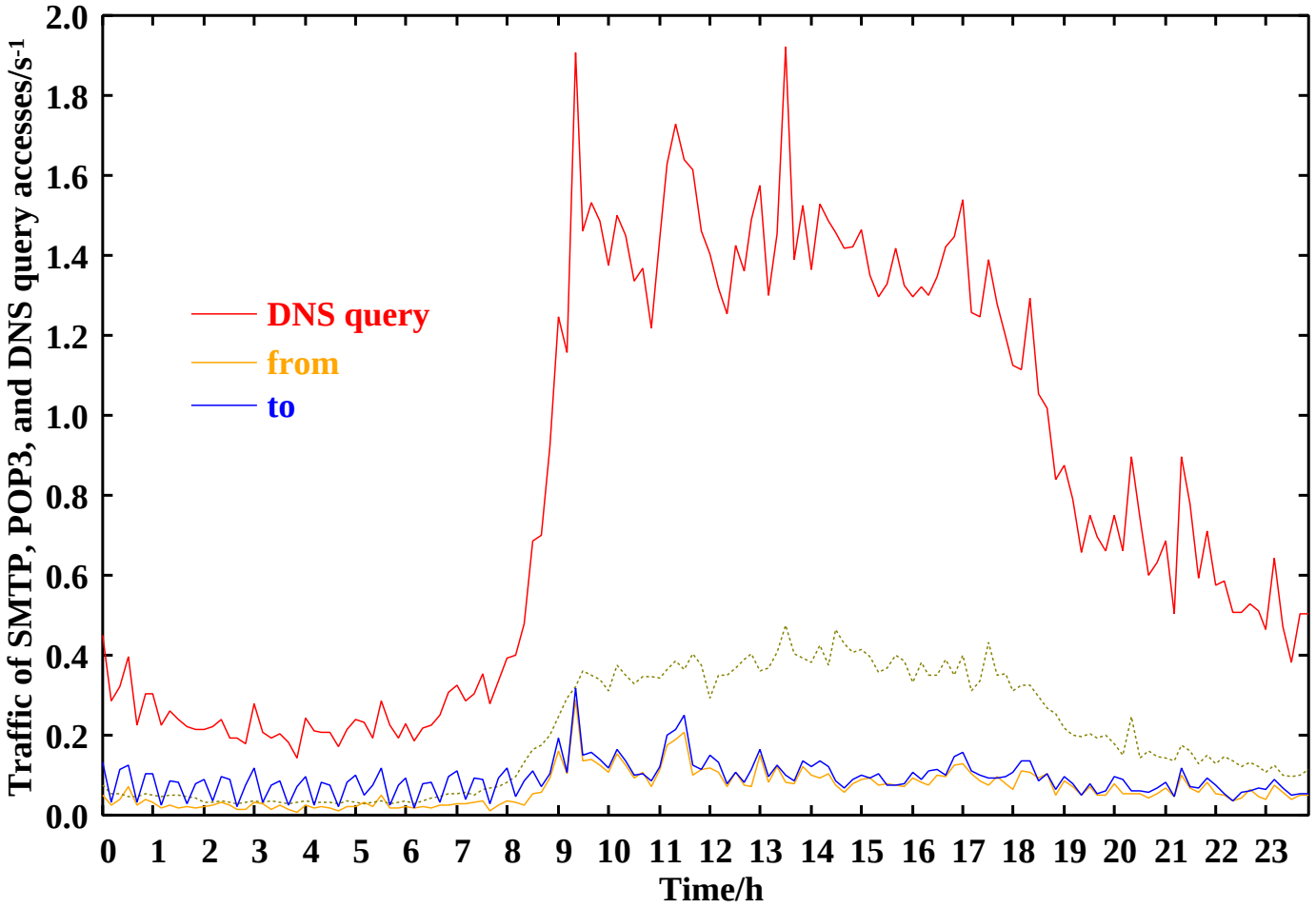
Traffic of DNS and SMTP at 2002/07/15



(1) The curve of N_{to} is rippled in the midnight hours.

(2) In the morning, the MMI-worm, Frethem.K, was detected.

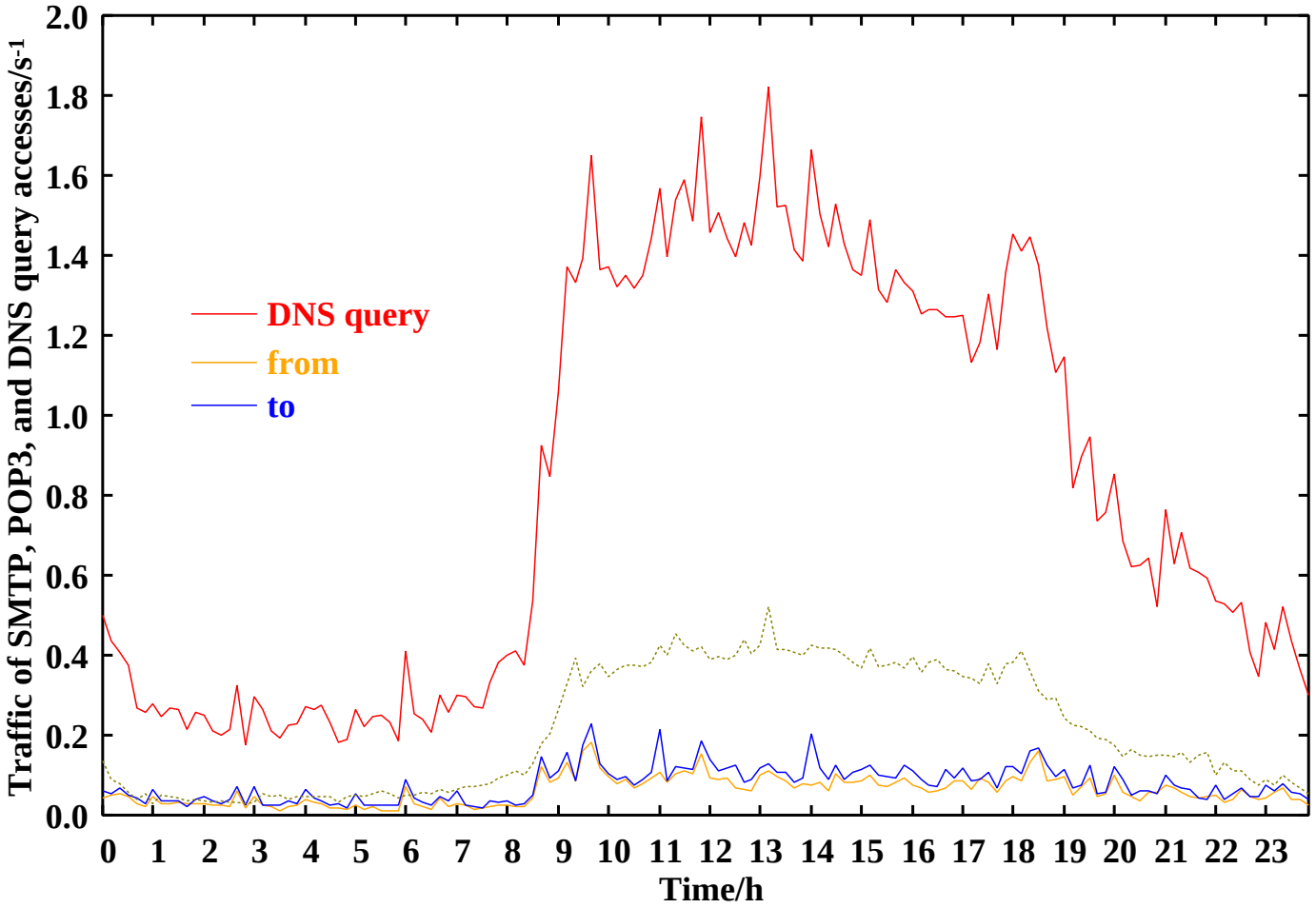
Traffic of DNS and SMTP at 2002/07/16



(1) The curve of N_{to} is rippled in the early morning.

(2) Frethem.K was spread by the internet.

Traffic of DNS and SMTP at 2002/07/17



(1) The curve of N_{to} is normal in the early morning.

(2) Frethem.K was disappeared from 1MX.