(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 April 2010 (08.04.2010)

PCT

(10) International Publication Number
WO 2010/037308 A1

(51) International Patent Classification:
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/CN2009/073852

(22) International Filing Date:
10 September 2009 (10.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/101,522 30 September 2008 (30.09.2008) US

(71) Applicant *(for all designated States except US)*: THE CHINESE UNIVERSITY OF HONG KONG [CN/CN]; Shatin, N.T., Hong Kong (CN).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: SHI, Xingang [CN/CN]; Room 725A, Ho Sin Hang Engineering Building, CUHK, Shatin, N.T., Hong Kong (CN). CHIU, Dah-Ming [US/CN]; Department of Information Engineering, CUHK, Shatin, N.T., Hong Kong (CN).

(74) Agent: INSIGHT INTELLECTUAL PROPERTY LIMITED; 19 A, 19B, Tower A, InDo Building, No. 48A Zhichun Road, Haidian District, Beijing 100098 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) **Title**: SYSTEMS AND METHODS FOR DETERMINING TOP SPREADERS

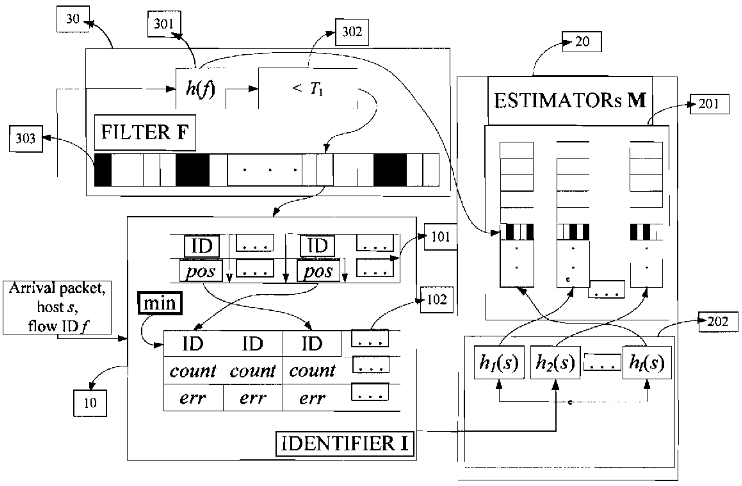


Fig. 5

(57) **Abstract**: Disclosed are a method and a system for determining top spreaders in high speed network. The method may comprise: sampling a plurality of packets from the plurality of hosts during an interval of time; determining a difference between a count and a count error for each host based on the sampled packets; ranking the hosts based on the determined difference to identify a first set of hosts that are top in the ranked hosts; and selecting a second set of hosts from the first set of hosts as the top spreaders.

WO 2010/037308 A1

Published:

— *with international search report (Art. 21(3))*

SYSTEMS AND METHODS FOR DETERMINING TOP SPREADERS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of US provisional Application No. 61/101,522 filed on September 30, 2008, of which the contents are incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Technical Field

[0002] The disclosure of the application is related to systems and methods for determining top spreaders in high speed networks.

2. Related Prior Art

[0003] Efficiently and accurately identifying hosts that are spreading the largest amount of flows during an interval of time, so called *top spreaders*, is very important for managing a network and studying host behaviors on application level, ranging from detecting DDoS attack, worm propagation, peer-to-peer hot spots and flash crowds. No previous work has been able to efficiently and accurately identify the top spreaders at very high link speed, for example, 10 to 40 Gbps.

[0004] There has been a lot of work on measurement of traffic statistics for network management, security, and better understanding of internet and its evolvement. The size distribution and matrices of the flows may help network provisioning and traffic engineering. Finding flows that have a large number of packets is useful in billing and accounting. It has also been shown that flow level communication patterns may further reveal application level behaviors of each host.

[0005] To tell whether a host is a top spreader, it always needs to test if a flow count of the host is above a threshold according to one known method in the art. However, it's difficult to fix such a threshold. Even if the threshold can be fixed, there will be either too many or too few top spreaders. For most situations, it should be more interested in only a few top spreaders and their accurate flow numbers. However, no previous work has been able to accurately identify top spreaders on very high speed links in a large network, for example, under the speed of 10 to 40 Gbps, where the total host number is around hundred of thousands and the total flow number is around several millions, which happen on ISP backbone links.

SUMMARY OF THE INVENTION

[0006] The present invention application aims to propose a system and method to not only accurately identify the top spreaders, but also accurately estimate their spreading out cardinality, that is, the flow number of each identified top spreader.

[0007] In an aspect, there is disclosed a method for determining top spreaders from a plurality of hosts, comprising:

an identifier configured to receive a plurality of packets from the hosts during an interval of time and comprising:

a difference determination unit configured to determine a difference between a count and a count error for each host based on the received packets; and

an identifying unit configured to rank the hosts based on the determined difference to identify a first set of hosts in the ranked hosts; and

an estimator configured to select a second set of hosts from the first set of hosts as the top spreaders.

[0008] In other aspect, there is disclosed a method for determining top spreaders from a plurality of hosts, comprising:

sampling a plurality of packets from the hosts during an interval of time;

determining a difference between a count and a count error for each of the hosts based on the sampled packets;

ranking the hosts based on the determined difference to identify a first set of hosts in the ranked hosts; and

selecting a second set of hosts from the first set of hosts as the top spreaders.

[0009] According to the invention, it can work on the highest speed link that is 40Gbps. It can handle millions of flows and hundreds of thousands of hosts with very limited memory, for example, only 700KB memory is needed for 8M flows and 200K hosts. There is almost no error on the identified top 20 spreaders, and the relative error of the estimated flow numbers of these top spreaders are typically around 3%, and much smaller for more skewed data.

No previous work can get such high efficiency and accuracy. The method is very easy to implement by modest hardware support and efficiently provides very accurate information to help these applications on very high speed large networks.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Fig. 1 is a block diagram schematically illustrating a system for determining top spreaders according to one embodiment of the application;

[0011] Fig. 2 is a block diagram schematically illustrating the structure of the identifier of the system as shown in Fig.1;

[0012] Fig. 3 is a block diagram schematically illustrating the structure of the estimator of the system as shown in Fig.1;

[0013] Fig. 4 is a block diagram schematically illustrating the structure of the filter of the system as shown in Fig.1;

[0014] Fig. 5 is a system block diagram schematically illustrating the architecture with data structures for the system as shown in Fig.1, wherein some units therein are omitted for the purpose of clarity;

[0015] Fig. 6 is a flow diagram schematically illustrating a processing of computing the final flow number for host s.

[0016] Fig. 7 is a flow diagram schematically illustrating the algorithm of adjusting the flow number for host s ; and

[0017] Fig. 8 is a flow diagram schematically illustrating a processing for determining top spreaders according to one embodiment of the application.

DETAILED DESCRIPTION OF THE INVENTION

[0018] Hereinafter, a detailed description of embodiments in the present application will be given with reference to the appended drawings.

[0019] As shown in Fig.1, a system 1000 for determining top spreaders from a plurality of hosts in high speed network comprises an identifier 10 and an estimator 20.

[0020] The identifier 10 operates to receive packets from data flows of c hosts in the network in a period of time, where c is the number of the hosts. The identification information for the hosts and data flows, i.e. host ID and flow ID, may be defined by any combination of fields in packet header, for example, IP address, port, protocol, and TCP flags. In one embodiment of the application, source address s is used as host ID, and the flow ID is represented by the 5-tuple f =<srcIP, destIP, srcPort, destPort, proto>. Those skilled in the art should understand that the invention should not be limited thereto, other fields in the packet header should be used to represent the host ID and flow ID, respectively.

[0021] The identifier 10 comprises a hash table 101, a min-heap 102, a counting unit 103, a difference determination unit 104, an identifying unit 105 and an updating unit 106.

[0022] As shown in Fig.2, a key of a node in the hash table 101 is host ID, and a value of a node in the hash table 101 is a corresponding position of the node in the min-heap 102. Each node in the min-heap 102 has three fields, a host ID, a count, and a count error. At the beginning of the period of time, all the fields regarding the count and count error in the heap 102 are set to be zero.

[0023] For each arrival packet with a host ID s and a flow ID f, the counting unit 103 operates to check, through the hash table 101, if s is now counted by identifier 10, that is, to check whether s exists in the hash table 101 as a key.

[0024] If s exists in the hash table 101, the difference determination unit 104 operates to calculate the flow number M_s for the host with ID s by the following equation:

$$M_s = count_s - err_s \qquad 1)$$

[0025] And then, the identifying unit 105 operates to determine whether M_s is above an estimating threshold T_2. Typically, the estimating threshold T_2 may be set as a small integer number, e.g. 2-5. If it is, the identifying unit 105 determines that the host with the M_s may be a potential super spreader, after which an updating command will be sent by the identifying unit 105 to the estimator 20 to carry out an updating processing, which will be discussed hereinafter.

[0026] At the end of the intended measurement period, all the hosts with the flow number being above T_2 are ranked by the identifying unit 105 according to the calculated flow numbers in a descending or ascending order. The top-$2k$ hosts in the ranked hosts are identified as potential top spreaders, where k is an integer. Although theoretically, k can be selected from 1 to the total number of hosts, here it only considers the situation where k is a small constant number, e.g. 10 or 20, when the network management and security is concerned.

[0027] As shown in Fig. 2, the identifier 10 is also configured with an updating unit 106 for updating the hash table 101 and the heap 102, which will be discussed hereinafter.

[0028] The estimator 20 is used to select top-k hosts from the top-$2k$ potential top spreader identified by identifier 10.

[0029] The estimator 20 includes a first counter 201 configured with $w \times n$ counting units (n columns, each column has w counting units), with each counting unit represented by for example, 5 bits.

[0030] As shown in Fig. 3, besides the first counter 201, the estimator 20 also includes a first selecting unit 202, an estimating unit 203, a first determining unit 204, a first adjusting unit 205, a second adjusting unit 206, a second determining unit 207, a second selecting unit 208 and an updating unit 209. The updating unit 209 is used to updating the first counter 201.

[0031] The processing for estimating the flow number for the host s with the units 201-208 will be firstly discussed in reference to Fig.6 as below, and the updating processing of the updating unit will be discussed latter.

[0032] Referring to Fig. 6, in step S601, for the host with ID s, the first selecting unit 202 operates to select corresponding l columns of the counting units from the first counter 201 based on the ID s. In the embodiment, for the purpose of illustration, three columns of the counting units are selected (i.e., l=3).

[0033] As is shown in Fig.5, the first selecting unit 202 is configured with l calculating units. Different calculating units may use different hash functions which can compute for example, 32 bits hash results, and each calculating unit is configured to use a hash function to select a column of counting units from the first counter 201 by the following equation.

$$column_s = h_i(s) \qquad \text{for } i = 1 \text{ to } l \qquad 2)$$

Where $column_s$ represents the selected column of the counting unit where an input parameter is the host ID s.

[0034] In step S602, the estimating unit 203 operates to select a minimal one from the selected three columns ($\mathbf{M}_{h1}(s)[i]$, $\mathbf{M}_{h2}(s)[i]$ and $\mathbf{M}_{h3}(s)[i]$) in the same level as the estimation counter by the following equation,

$$M_s[i] = \min(\mathbf{M}_{h1(s)}[i], \mathbf{M}_{h2(s)}[i], \mathbf{M}_{h3(s)}[i]) \qquad \text{for } i = 1 \text{ to } w \qquad 3)$$

[0035] In step S603, the estimating unit 203 operates to estimate the flow number Ms, for example, by the following equation,

$$M_s=\alpha_w \times w^2 \times (\sum_{i=1}^{w} 2^{-Ms[i]})^{-1} \quad \text{for } i = 1 \text{ to } w \qquad 4)$$

[0036] where α_w represents a bias correction parameter. For example, the value of α_w may be approximated by 0.72134 as proposed by P. Flajolet etc. in "Hyperloglog: The analysis of a near-optimal cardinality estimation algorithm", In Proc. of the 2007 International Conference on Analysis of Algorithms (AofA'07), June 2007. In step S604, the first determining unit 204 operates to determine whether the estimated number Ms is less than, for example, 2.5w, wherein w is the number of counting units in each column in the first counter 201. If it is the case, the first adjusting unit 205 operates to adjust Ms using an algorithm as illustrated in Fig.7 which will be discussed as below. Otherwise, M_s needs no adjustment.

[0037] As shown in Fig.7, in step S6041, the first adjusting unit 205 operates to translate $M_{h1(s)}[i]$, $M_{h2(s)}[i]$, $M_{h3(s)}[i]$ into 3 bitmaps B_1, B_2, B_3 by the following equation:

$B_k[i]=0$, if $M_{hk(s)}[i]=0$;

$B_k[i]=1$, else for $i = 1$ to w 5)

[0038] In step S6042, set B_4=(B_1 or B_2), B_5=(B_1 or B_3), B_6=(B_2 or B_3), B7=(B_1 or B_2 or B_3). And then in step S6043, the first adjusting unit 205 operates to count empty bits in B_1~B_7 as E_1~E_7, and then in step S6044 determine whether E1~E7 > 0. If it is the case, the first adjusting unit 205 adjusts the number M_s by the following rule in step S6045.

$$M_s = m(ln(\tfrac{m}{E_1}) + ln(\tfrac{m}{E_2}) + ln(\tfrac{m}{E_3}) - ln(\tfrac{m}{E_4}) - ln(\tfrac{m}{E_5}) - ln(\tfrac{m}{E_6}) + ln(\tfrac{m}{E_7})) \qquad 6)$$

[0039] Returning to Fig. 6, in step S605, the second adjusting unit 206 operates to further add a adjust value $1/r \times T_2$ to the adjusted flow number M_s, where r is the flow sampling rate.

[0040] Then in step S606, the second determining unit 207 operates to determine whether the adjusted number M_s is less than another threshold $2w/r$.

[0041] Next, the second selecting unit 208 selects the flow number of s based on the determination and outputs the top-k hosts with the largest flow numbers as the top spreaders. Specifically, in the case that the adjusted number Ms is less than 2w/r, the Ms is determined as the flow number of s in step S607; otherwise, the difference $count_s$-err_s is used as the flow number of s in step S608.

[0042] Referring to Fig. 1 again, the system 100 further comprises a filter 30 configured to sample packets from data flows of hosts in the network in the period of time, and for each sampled packet it provides a flow number increment to update the identifier 10. As shown in Fig. 4, the filter 30 is configured with a sampling unit 301, a determining unit 302 and a filtering unit 303.

[0043] The sampling unit 301 operates to sample the arrival packets and to calculate a value of V_f based on the flow ID f by the following equation:

$$V_f = h(f) \qquad 7)$$

Where $h()$ is a uniform hash function that may calculate, for example, a hash result of 32 bits.

[0044] An array F of m bits is arranged in the filtering unit 303. At the beginning of the sampling, all bits of the array are set to be zero.

[0045] The determining unit 302 operates to determine whether the calculated V_f is less than a predetermined sampling threshold T_1. If yes, this packet is sampled, and then filter 30 checks F[V_f]. If F[V_f]=0, then it operates to set F[V_f]=1, and send an updating command with a increment value to the identifier 10 to carry out an updating processing, which will be discussed as below. Specifically, if the number of empty bits in the array F in the filtering unit 303 is e, then the increment value should be m/e.

[0046] Hereinafter, the updating processing for the identifier 10 and estimator 20 will be discussed, respectively.

<u>1. Processing for updating the identifier 10</u>

[0047] In the embodiment, the processing for updating the identifier 10 may use any known top-k element methods, for example, the Space-Saving algorithm proposed by Metwally, 2006. Specifically, it is supposed that the increment value is m/e for the host s, then the updating unit 106 operates to add m/e to the count of s in the heap 102 if s is in the table 101; or find the key s_{min} which has the minimal *count* value $count_{min}$ in the min-heap 102, set the corresponding *err* value in the min-heap 102 to be $count_{min}$, increase $count_{min}$ by m/e, replace the ID s_{min} in the min-heap 102 with s, and replace the node corresponding to s_{min} in the hash table 101 by a new node corresponding to s.

<u>2. Processing for updating the estimator 20</u>

[0048] When the identifying unit 103 in the identifier 10 determines that M_s is higher than the estimating threshold T_2, the updating unit 209 in the estimator 20 operates to select three calculating units in the first selecting units 202, represented as $\mathbf{M}_{h1(s)}$, $\mathbf{M}_{h2(s)}$ and $\mathbf{M}_{h3(s)}$, and set counter $\mathbf{M}_{hi(s)}[V_f]=\max(\mathbf{M}_{hi(s)}[V_f], \rho(V_f))$, where $\rho(h(f))$ is the position of the leftmost 1 in binary presentation of V_f.

[0049] Hereinafter, a processing 2000 for determining top spreaders from a plurality of hosts will be discussed in reference to Fig. 8.

[0050] At step S801, a plurality of packets from the plurality of hosts during an interval of time is sampled, for example, with the filter 30, and the estimator 20 is updated as discussed above. At step S802, a difference between a count and a count error for each host is determined based on each sampled packet. At step S803, the hosts are ranked based on the determined difference so as to identify the top-$2k$ hosts in the ranked hosts. At step S804, top-k hosts is selected from the top-$2k$ hosts as the top spreaders, which is illustrated in Fig. 6 and the detailed discussion thereof is omitted.

[0051] The above disclosed system 1000 may be implemented by software, hardware, firmware and any combination thereof. The processing 2000 may be carried out for example by the system 1000. On the case that the system 1000 is implemented by software, the parameters may be chosen as: $m=2^{23}$, $w=256$, $n=1000$ and $c=1000$, then it costs around 700KB memory, and may be installed in high speed memory such as SRAM.

[0052] In addition, since the identifier 10 is configured with a min-heap 102, it needs at most 2log$c$ memory operations to update a count in the heap 102. When $c=1000$, this value is 20, so it may use a flow sampling rate of 1/16 such that less than 2 memory operations are needed on average, and can handle 40Gbps by SRAM. To handle extreme situations when flows come in burst and flow sampling select continuous flows, a small buffer can be used to temporarily save update information.

[0053] Moreover, the inventors have conducted experiments on various data, including synthetic data and real traffic traces. There is almost no error on identified top spreaders, the relative error of estimated flow number is typically less than 3%, and is much smaller for more skewed data. The maximum flow number we are dealing with is 8M, the maximum number of hosts is 200K, and the memory cost is at most 700KB.

[0054] The present application is not limited to the embodiments mentioned above. Other embodiments obtained by the skilled in the art according to the technical solutions in the present application should be within the scope of the technical innovation of the present application.

CLAIMS

1. A system for determining top spreaders from a plurality of hosts, comprising:

an identifier configured to receive a plurality of packets from the hosts during an interval of time and comprising:

a difference determination unit configured to determine a difference between a count and a count error for each host based on the received packets; and

an identifying unit configured to rank the hosts based on the determined difference to identify a first set of hosts in the ranked hosts; and

an estimator configured to select a second set of hosts from the first set of hosts as the top spreaders.

2. A system of claim 1, wherein the identifier further comprises:

a counting unit configured to count the received packets so as to obtain the count and the count error.

3. A system of claim 1, wherein the count and the count error are arranged in a min-heap in the identifier.

4. A system of claim 1, wherein the estimator further comprises:

a first counter (201) configured with a plurality of counting units;

a first selecting unit (202) configured to select at least one counting unit from the plurality of counting units;

an estimating unit (203) configured to select the minimal one counting unit from said at least one counting unit to estimate a flow number for each of the second set of hosts; and

a second selecting unit (208) configured to select the second set of hosts based on the estimated flow number.

5. A system of claim 4, wherein the estimator further comprises a first determining unit (204) and a first adjusting unit (205),

wherein the first determining unit (204) is configured to determine whether the estimated flow number is less than a first predetermined threshold; and if it is the case, the first adjusting unit (205) operates to adjust the estimated flow number.

6. A system of claim 4, wherein the estimator further comprises:

a second adjusting unit (206) configured to further adjust the adjusted flow number by a predetermined rule; and

wherein the second selecting unit (208) is further configured to select the second set of hosts based on the adjusted flow number.

7. A system of claim 6, wherein the predetermined rule is such that the second adjusting unit (206) add a adjust value to the adjusted flow number, where the adjust value is associated with a sampling rate of the system.

8. A system of claim 6, wherein the second selecting unit (208) is configured to select the second set of hosts with the adjusted flow number by following rule:

determining the flow number adjusted by the second adjusting unit (206) as a final flow number, if the adjusted flow number adjusted by the second adjusting unit (206) is less than a second predetermined threshold; where the second threshold is associated with the pluralities of counting units and a sampling rate of the system; otherwise,

determining said difference as a final flow number; and

selecting the second set of hosts with the largest final flow numbers.

9. A system of claim 1, further comprising:

a filter configured to determine a first packet of a flow consisting of a plurality of packets from the hosts so as to determine the interval of time.

10. A system of claim 9, wherein the filter is further configured to determine whether to update the identifier; and

wherein the identifier further comprises:

a heap configured to maintain information of each of the packets; and

an updating unit configured to update the information based on the determination of the filter.

11. A system of claim 4, wherein the estimator further comprises:

an updating unit configured to update the counting units.

12. A method for determining top spreaders from a plurality of hosts, comprising:

sampling a plurality of packets from the hosts during an interval of time;

determining a difference between a count and a count error for each of the hosts based on the sampled packets;

ranking the hosts based on the determined difference to identify a first set of hosts in the ranked hosts; and

selecting a second set of hosts from the first set of hosts as the top spreaders.

13. A method of claim 12, wherein the selecting further comprises:

calculating a flow number of each of the first set of hosts;

ranking the first set of hosts by the calculated flow numbers; and

selecting at least one host from the ranked hosts as the top spreaders.

14. A method of claim 13, wherein the calculating further comprises:

estimating the flow number for each of the first set of hosts;

adjusting the estimated flow number, if the estimated flow number is less than a first predetermined value;

determining the adjusted flow number as the flow number if the adjusted number is less than a second predetermined value; or

determining the difference as the flow number if the adjusted number is equal to or larger than the second predetermined value.

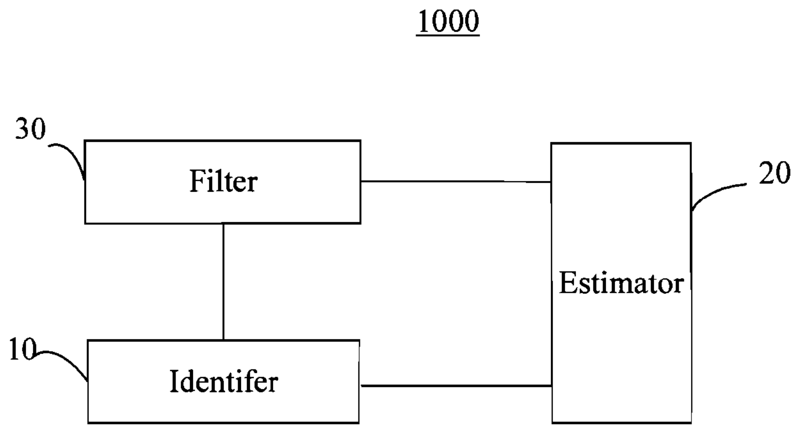

1000
30
Filter
20
Estimator
10
Identifer

Fig.1

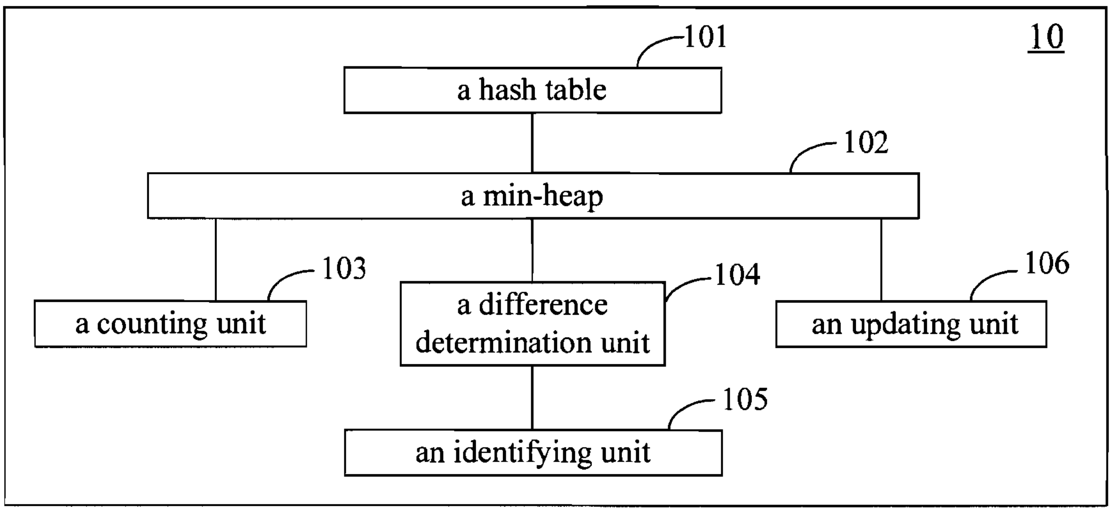

101
10
a hash table
102
a min-heap
103
a counting unit
104
a difference determination unit
106
an updating unit
105
an identifying unit

Fig. 2

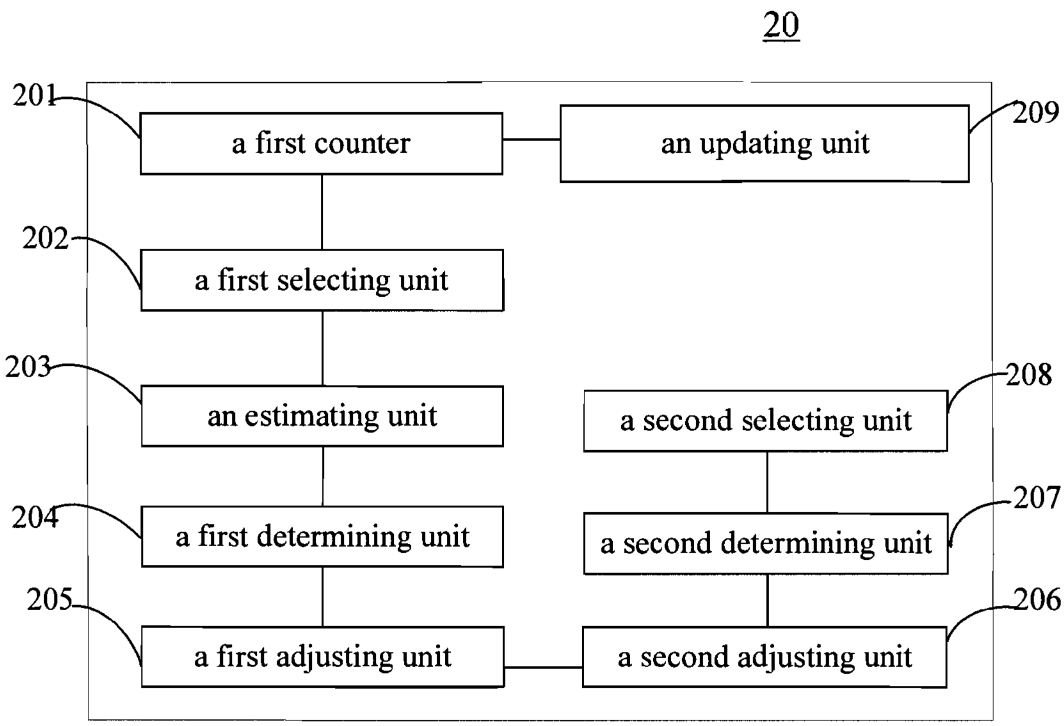

20
201
a first counter
an updating unit
209
202
a first selecting unit
203
an estimating unit
a second selecting unit
208
204
a first determining unit
a second determining unit
207
205
a first adjusting unit
a second adjusting unit
206

Fig. 3

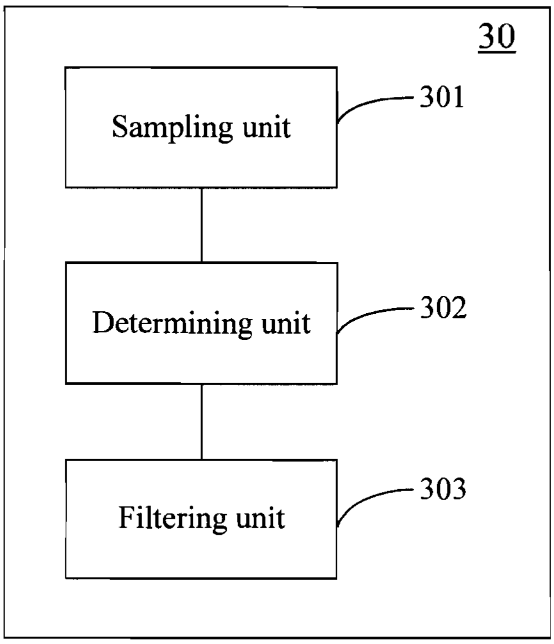

30
Sampling unit
301
Determining unit
302
Filtering unit
303

Fig.4

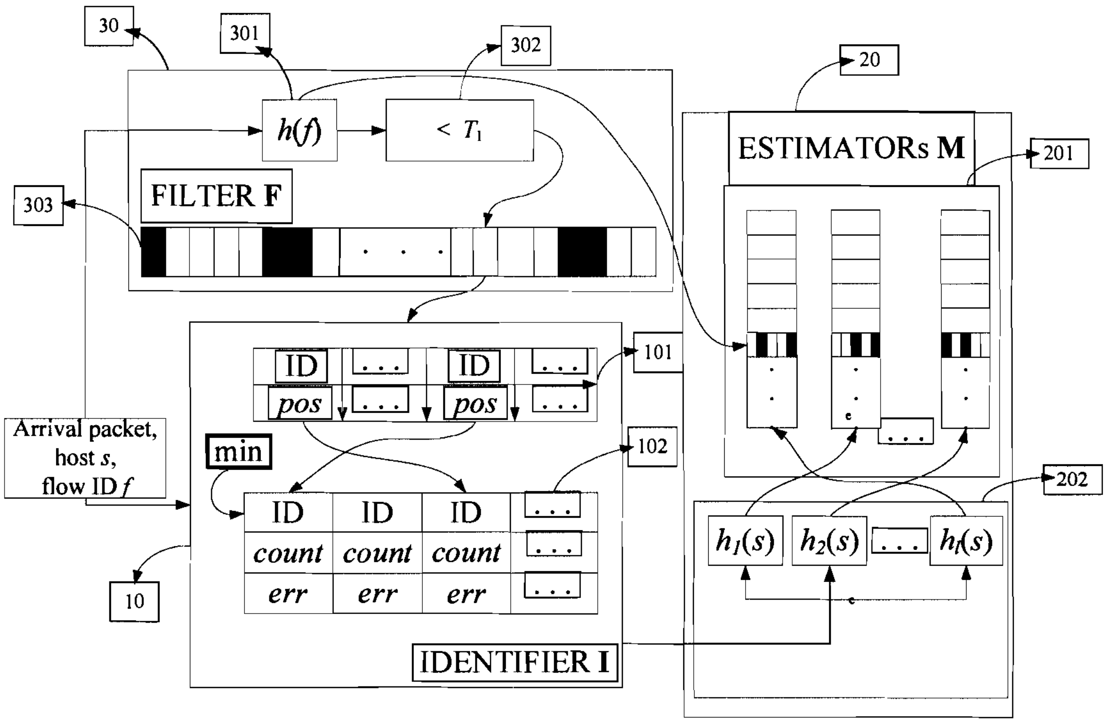
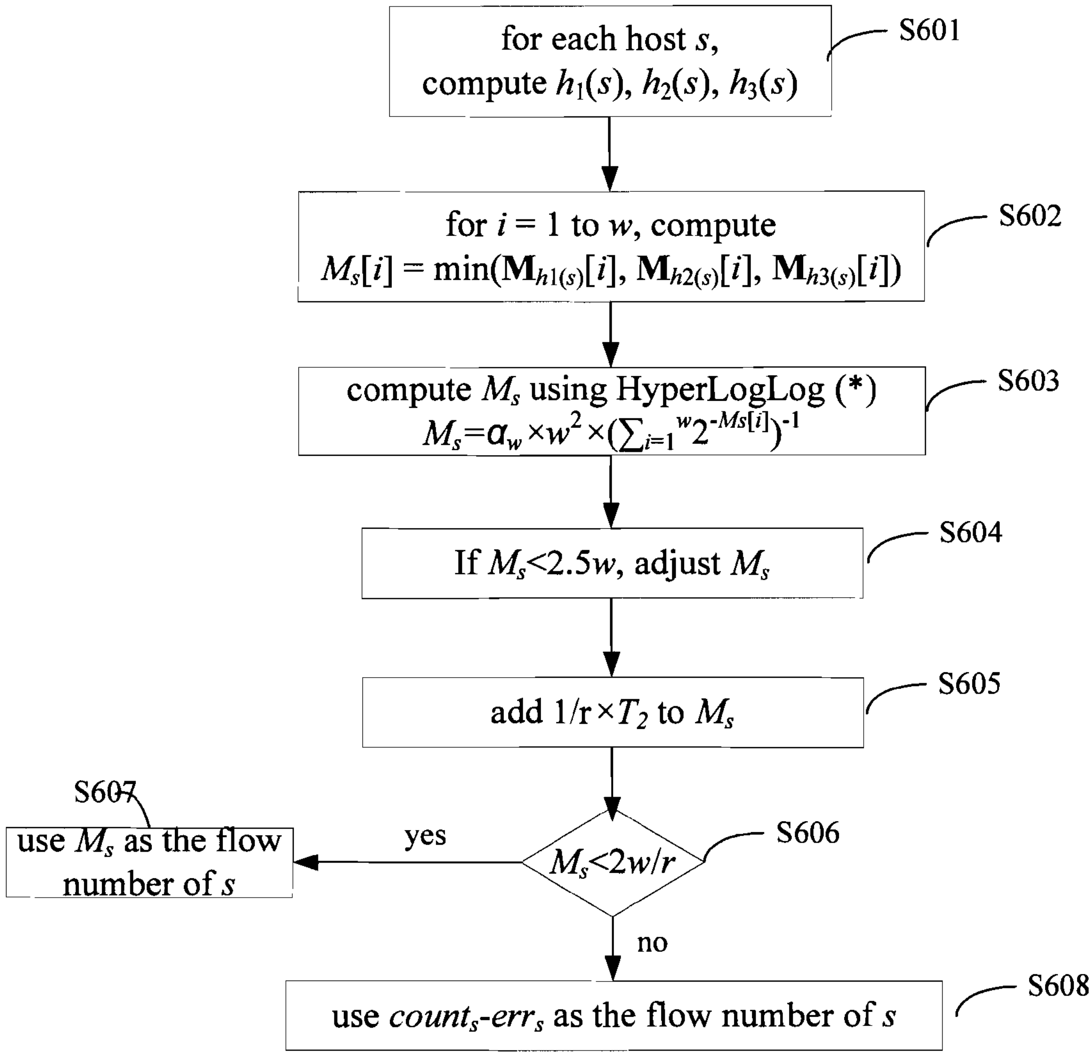

30
301
302
20
h(f)
< T1
ESTIMATORs M
201
FILTER F
303
ID
ID
101
pos
pos
Arrival packet, host s, flow ID f
min
102
202
ID
ID
ID
count
count
count
err
err
err
h1(s)
h2(s)
ht(s)
10
IDENTIFIER I

Fig. 5



(*)HyperLogLog algorithm [1] is a cardinality estimation algorithm proposed by P. Flajolet, 2007.

Fig. 6

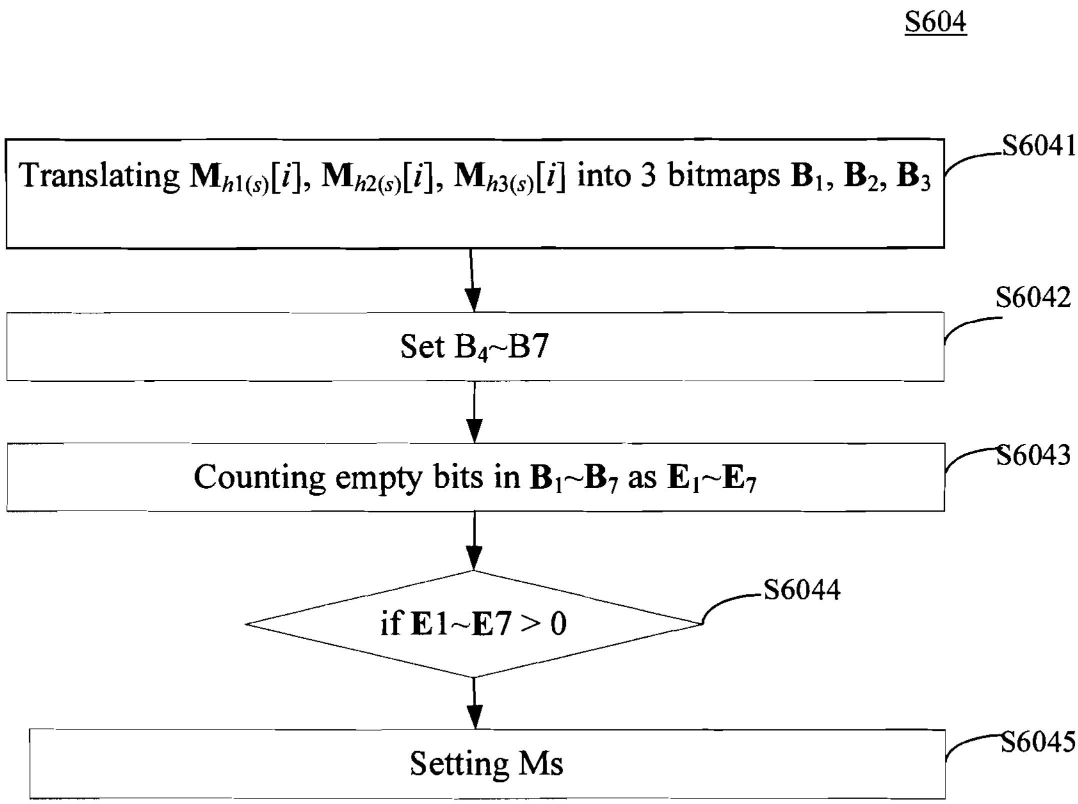

S604
Translating $\mathbf{M}_{h1(s)}[i]$, $\mathbf{M}_{h2(s)}[i]$, $\mathbf{M}_{h3(s)}[i]$ into 3 bitmaps $\mathbf{B}_1$, $\mathbf{B}_2$, $\mathbf{B}_3$
S6041
Set B_4~B7
S6042
Counting empty bits in $\mathbf{B}_1$~$\mathbf{B}_7$ as $\mathbf{E}_1$~$\mathbf{E}_7$
S6043
if **E**1~**E**7 > 0
S6044
Setting Ms
S6045

Fig. 7

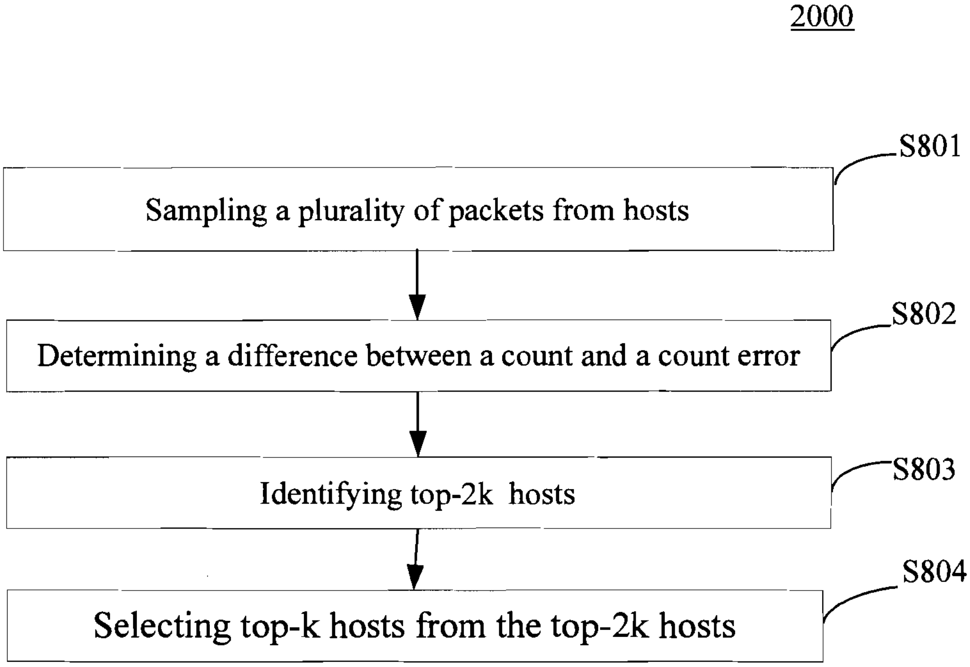

2000
S801
Sampling a plurality of packets from hosts
S802
Determining a difference between a count and a count error
S803
Identifying top-2k hosts
S804
Selecting top-k hosts from the top-2k hosts

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2009/073852

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/24(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L H04Q H04W G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT, CNKI: spread+, host?, flow?, stream?, traffic?, packet?, message?, interval?, time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1822548A (UNIV NANJING POSTS & TELECOM) 23 Aug. 2006(23.08.2006) the whole document	1-14
A	CN101309179A (QIMINGXINGCHEN INFORMATION TECHNOLOGY CO) 19 Nov. 2008(19.11.2008) the whole document	1-14
A	US20080273461A1 (IBM CORP) 06 Nov. 2008(06.11.2008) the whole document	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&”document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 Dec. 2009(08.12.2009)	**24 Dec. 2009 (24.12.2009)**

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
LIU Bin
Telephone No. (86-10)62411275

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2009/073852

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1822548A	23.08.2006	CN100364281C	23.01.2008
CN101309179A	19.11.2008	None	
US20080273461A1	06.11.2008	CN1842055A	04.10.2006