(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 109 279 A1

# (12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
**14.10.2009 Bulletin 2009/42**

(51) Int Cl.:
***H04L 29/06*** *(2006.01)*

(21) Application number: **08154389.4**

(22) Date of filing: **11.04.2008**

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR**
Designated Extension States:
**AL BA MK RS**

(71) Applicant: **Deutsche Telekom AG**
**53113 Bonn (DE)**

(72) Inventors:
- **Roshandel, Mehran**
  **13591 Berlin (DE)**
- **Goldstein, Markus**
  **67655 Kaiserslautern (DE)**
- **Reif, Matthias**
  **67663 Kaiserslautern (DE)**
- **Stahl, Armin**
  **67663 Kaiserslautern (DE)**
- **Breue, Thomas**
  **67655 Kaiserslautern (DE)**

(74) Representative: **Vossius & Partner**
**Siebertstrasse 4**
**81675 München (DE)**

Remarks:
Amended claims in accordance with Rule 137(2) EPC.

## (54) Method and system for mitigation of distributed denial of service attacks using geographical source and time information

(57) The invention describes a method and system of protecting computer systems from attacks over a network to which the computer system is connected, the method comprising the steps of (a) establishing, during attack-free operation of the computer system, a regular request-time distribution for countries of origin of requests to the computer system; (b) monitoring current requests to the computer system; (c) determining the current amount of requests for the at least one country of origin; (d) during a detected attack comparing the current amount of requests for the at least one country of origin with the regular request-time distribution for at least one country of origin; and (e) restricting the number of requests from this country served by the computer system if it is determined as a result of step d) that the current amount of requests deviates from the expected amount according to the regular request-time distribution.

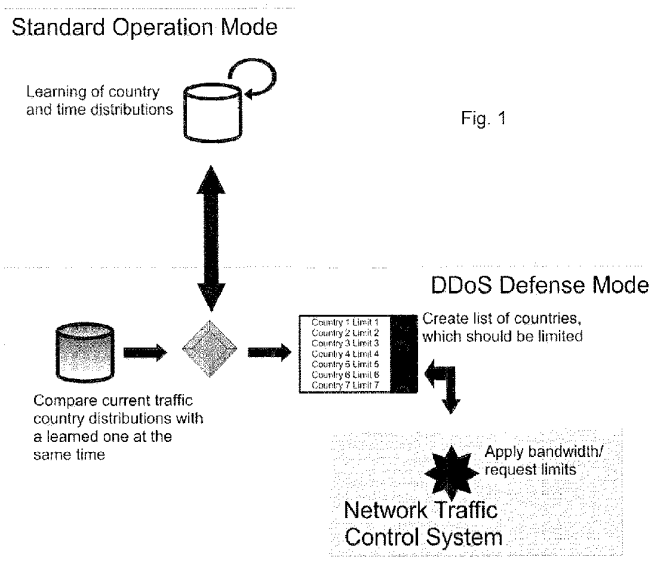


Fig. 1

EP 2 109 279 A1

## Description

### Field of the Invention

**[0001]** The invention generally relates to mitigation of Distributed Denial of Service (DDoS) attacks on public available Internet services. Examples of such services include websites, Internet telephony (VoIP), FTP server, DNS, etc.

### Background of the Invention

**[0002]** In the Internet, Distributed Denial of Service attacks (DDoS) have become a major threat today. Large scaled networks of infected PCs (bots or zombies) combine their bandwidth and computational power in order to overload a publicly available service and denial it for legal users. All public servers are basically vulnerable to DDoS attacks due to the open structure of the Internet. The bots are usually acquired automatically by hackers who use software tools to scan through the network, detecting vulnerabilities and exploiting the target machine.

**[0003]** The number of such DDoS incidents is steadily increasing. For example, the attacks against large e-commerce sites in February 2000 and the attacks against root DNS servers in 2003 and 2007 have drawn public attention to the problem of DDoS attacks. Today, mainly mid-sized websites are attacked by criminals in order to extort protection money from their owners without attracting too much public attention. Besides that, also Internet Service Providers (ISP) have to deal with the problem that DDoS traffic is contesting their link bandwidths.

**[0004]** The bot software also evolved alarmingly over time. Early tools like *TFN, Stacheldraht, Trinoo* or *Mstream* used unencrypted and hierarchically organized communication structure. Most of these tools used TCP-SYN, UDP or ICMP floods with possibly identifiable parameters. Since some of these attacks have successfully been mitigated, a new generation of bots arose. *SDBot, Agobot* or the very enhanced *Phatbot* are known representatives which use IRC as a robust and secure communication. These tools also contain methods for spreading themselves and have more sophisticated attack algorithms, which could be upgraded over the Internet. The attack traffic from those tools looks like legal traffic on the transport layer, which makes it nearly impossible to filter it effectively with standard firewalls.

**[0005]** Mitigating DDoS attacks at the origin or within the core of the Internet seems to be an impossible task due to the distributed and authorization-free nature of the IP based network. Approaches to achieve this objective typically rely on changing current internet protocols and are therefore not easily applicable. Ingress filtering as described in RFC 2827 (P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing," United States, 2000, available at: http://rfc.net/rfc2827,html.) also helps mitigating DDoS attacks with forged source IP addresses (IP spoofing) and should be applied by every ISP. Since ingress filtering only helps other ISPs on the Internet and not the one who is actually applying it, it took quite a long time until it was setup in many places. Furthermore, Savage et al. (S. Savage, D. Wetherall, A. R. Karlin, and T. Anderson, "Practical network support for IP traceback," in SIGCOMM, 2000, pp. 295-306) suggested IP Traceback to find the source of spoofed IP addresses by probabilistically marking packets. Nowadays, IP spoofing is not that common any more in DDoS attacks, except for the last octet of an IP address.

**[0006]** A known system to mitigate attacks is Radware's DefensePro with the APSolute operating system (http: //www.radware.com/ Products/ ApplicationNetworkSecurity/DefensePro.aspx). According to this system, the IP packets are examined for common striking features, for example identical packet sizes, source- and target ports etc. This system performs well in case of only a small number of attack sources, since attacker generate comparably high number of requests or in case of having identical attack packets.

**[0007]** Thus, today, there is a strong need to mitigate DDoS attacks near the target, which seems to be the only solution to the problem in the current internet infrastructure. The aim of such a protection system is to limit their destabilizing effect on the server through identifying malicious requests.

**[0008]** Thus, Distributed Denial of Service (DDoS) attacks are today the most destabilizing factor in the global Internet and there is a strong need for sophisticated solutions.

### Summary of the Invention

**[0009]** The invention starts out from the idea of monitoring the actual requests to a computer system and preventing overload situations on the basis of a request-time and country-distribution representing a normal situation. In more detail, for each country (i.e., country specific), a request-time distribution is calculated under normal operation (i.e., not experiencing attacks). Once a DDoS attack has been detected at a certain point in time, the expected percentage of requests from each country at that time is given and compared to the actual percentage of requests from each country to determine deviations from the regular distribution. In case a significant deviation is detected for one or more countries, the number of requests from these countries are accordingly restricted to prevent an overload of the system and guarantee normal operation for requests from other countries.

**[0010]** According to a first aspect, the invention provides a method of protecting a computer system from attacks over a network to which the computer system is connected, the method comprising the steps of: (a) establishing, during attack-free operation of the computer system, a regular request-time distribution for all countries of origin of requests to the computer system; (b) monitoring current requests to the computer system; (c)

determining the current amount of requests for all countries of origin; (d) during a detected attack comparing the current amount of requests for the countries of origin with the regular request-time distribution for at least one country of origin; and (e) restricting the number of requests from this country (e.g. traffic throttling) if it is determined as a result of step d) that the current amount of requests deviates significantly from the expected amount according to the regular request-time distribution.

**[0011]** The method preferably comprises the further step of setting a threshold for the significance of the deviation determined in step d) to differentiate between acceptable request amount deviations and request amounts to be restricted. This significance threshold can be defined by a certain deviation percentage or by more meaningful statistical methods like using a multiple of the variance over a couple of observed days.

**[0012]** According to a preferred embodiment of the invention, step e) comprises the step of restricting the number of requests from the at least one country. Preferably, the number of requests accepted in step e) correlates with the percentage of expected requests according to the regular country-time distribution for this time interval. Alternatively, step e) comprises limiting the bandwidth of the computer system available for the at least one country. Thus, certain requests or sender are not completely blocked. Rather, the number of accepted requests or the provided bandwidth for a particular sender is throttled, i.e. some requests are delayed or even denied. Technically, this corresponds to an artificial limitation of the bandwidth available for this particular sender by queuing or dropping IP packets, also known as bandwidth throttling, traffic shaping or policing.

**[0013]** According to one embodiment of the invention, the regular request-time-distribution for countries is established according to step a) by monitoring requests during a period of time and combining them for time or time intervals (preferable size of 15-120 minutes) of receipt of the requests and specific for each country. Alternatively, the regular request-time-distribution for at least one country is established by approximating a regular request-time-distribution from a comparable computer system with respect to user behaviour and time zone. This is advantageous if comparable computer systems are available because then no training or learning period is required. As a further alternative, the regular request-time-distribution for a country is established by extrapolating the request-time-distribution from a comparable country. This is advantageous if for a country there is not sufficient data, i.e. requests available to establish a reliable request-time distribution. It is encompassed by the invention that the different methods of establishing a request-time distribution for a plurality of countries are combined, i.e. that for individual countries alternative methods are used to obtain the distribution.

**[0014]** A request within the meaning of the invention is preferably an IP packet, an e-mail, a DNS request, a FTP download, a VoIP call, or a HTTP request.

**[0015]** It is a preferred feature of the invention that it also protects from attacks on an application level.

**[0016]** According to a second aspect, the invention provides a system for protecting computer systems from attacks over a network to which the computer system is connected, the system comprising: means for establishing, during attack-free operation of the computer system, a regular request-time distribution for countries of origin of requests to the computer system; means for monitoring current requests to the computer system; means for determining the current amount of requests for the at least one country of origin; means for comparing the current amount of requests for the at least one country of origin with the regular request-time distribution for countries of origin; and means for restricting the number of requests from these countries served by the computer system if it is determined as a result of step d) that the current amount of requests deviates from the expected amount according to the regular request-time distribution.

## Brief Description of the Drawings

**[0017]** Preferred embodiments of the invention are described in more detail below with reference to the attached drawings, which are by way of example only.

Fig. 1 shows a data flow diagram according to a preferred embodiment of the invention; and

Fig. 2 shows an example for a request-time distribution for various countries.

## Detailed Description

**[0018]** Fig. 1 shows a data flow diagram according to a preferred embodiment of the invention. As shown in Fig. 1, during normal use of the computer system, i.e. without experiencing any attack, the system undergoes a learning process to learn regular country and time distributions. Once an attack takes place, the current data traffic is monitored and the current distribution with respect to countries and time (day and time) is compared with the regular distribution. According to the preferred embodiment of Fig. 1. a restriction list is automatically determined for all countries having an excessively high number of request, so as to finally differentiate between acceptable requests and requests to be rejected.

**[0019]** According to the invention, certain requests or sender or countries are not completely blocked if they are determined as being abnormal. Rather, the number of accepted requests from a particular sender or country is reduced/restricted, i.e. some requests from a sender are accepted and some are rejected. This corresponds to an artificial limitation of the bandwidth available for this particular country. Thus, the number of request or packets to be rejected inversely correlates with number of expected request at the given time and for the given sender or country. For example, no requests or packets are

rejected from sender whose requests meet the, i.e. do not deviate from, the regular request-time-distribution. In contrast, a large number of request is rejected from countries send an unexpectedly high number of requests compared to the regular distribution for the given time and country. The overall number of requests to be rejected depends on the server load or the bandwidth of the computer system so that an overload is prevented.

**[0020]** Fig. 2 shows an example of a regular request-time-distribution for various countries. Due to the different time zones all around the world, the maxima and minima occur at different times. Fig. 2 shows only 10 selected countries for illustration, whereas the invention itself uses all available countries worldwide.

**[0021]** The invention will now be described by means of an example. During a DDoS attack at 5:00 am CEST an overload situation occurs. The computer system has a bandwidth of 1 Gbit/s. It is recognized that 99% of the requests come from a single European country. Assuming a request-time-distribution as shown in Fig. 2, at this time normally only around 3% of the requests originate from a single European country. Thus, according to the invention, the bandwidth for this particular country is limited to 30Mbit/s. Thus, the computer system is still fully available for all requests coming from other countries. User from this particular country (which are however only few anyway at this time) are likely not successful in accessing the requested computer system.

**[0022]** The present invention has now been described with reference to several embodiments thereof. It will be apparent to those skilled in the are that many changes can be made in the embodiments described without departing from the scope of the present invention. Thus the scope of the present invention should not be limited to the methods and systems described in this application, but only by methods and systems described by the language of the claims and the equivalents thereof.

## Claims

1. Method of protecting a computer system from attacks over a network to which the computer system is connected, the method comprising the steps of:

   a. establishing, during attack-free operation of the computer system, a regular request-time distribution for all countries of origin of requests to the computer system;
   b. monitoring current requests to the computer system;
   c. determining the current amount of requests for the at least one country of origin;
   d. comparing the current amount of requests for the at least one country of origin with the regular request-time distribution for at least one country of origin; and
   e. restricting the number of requests from this country served by the computer system if it is determined as a result of step d) that the current amount of requests deviates significantly from the expected amount according to the regular request-time distribution during a detected DDoS attack.

2. The method of any of the preceding claims, further comprising the step of setting a threshold for the deviation determined in step d) to differentiate between acceptable request amount deviations and request amounts to be restricted.

3. The method of any of any of the preceding claims, wherein step e) comprises the step of rejecting a number of requests from the at least one country.

4. The method of claim 3, wherein the number of requests accepted in step e) correlates with the percentage of expected requests according to the regular request-time distribution for this country.

5. The method of any of the preceding claims, wherein step e) comprises limiting the bandwidth of the computer system available for the at least one country.

6. The method of any of the preceding claims, wherein the regular request-time-distributions for countries are established by monitoring requests during a period of time and combining them for time or time intervals of receipt of the requests and specific for each country.

7. The method of any of the preceding claims, wherein the regular request-time-distribution for at least one country is established by approximating a normal request-time-distribution from a comparable computer system with respect to user and time zone.

8. The method of any of the preceding claims, wherein the normal request-time-distribution for a country is established by extrapolating the request-time-distribution from a comparable country.

9. The method of any of the preceding claims, wherein a request is an IP packet, an e-mail, a DNS request, a FTP download, a VoIP call, or a HTTP request.

10. The method of any of the preceding claims, wherein it protects from attacks on an application level.

11. System for protecting computer systems from attacks over a network to which the computer system is connected, the system comprising:

    means for establishing, during attack-free operation of the computer system, a regular request-time distribution for all countries of origin of re-

quests to the computer system;
means for monitoring current requests to the computer system;
means for determining the current amount of requests for countries of origin;
means for comparing the current amount of requests for the at least one country of origin with the regular request-time distribution for at least one country of origin during a detected DDoS attack; and
means for restricting the number of requests from this country served by the computer system if it is determined as a result of step d) that the current amount of requests deviates from the expected amount according to the regular request-time distribution.

**Amended claims in accordance with Rule 137(2) EPC.**

**1.** Method of protecting a computer system from attacks over a network to which the computer system is connected, the method comprising the steps of:

a. establishing, during attack-free operation of the computer system, a regular request-time distribution for all countries of origin of requests to the computer system;
b. monitoring current requests to the computer system;
c. determining the current amount of requests for the at least one country of origin;
d. comparing the current amount of requests for the at least one country of origin with the regular request-time distribution for at least one country of origin; and setting a threshold to differentiate between acceptable request amount deviations and request amounts to be restricted; and
e. restricting the number of requests from this country served by the computer system if it is determined as a result of step d) that the current amount of requests deviates from the threshold during a detected DDoS attack, wherein the number of requests accepted in step e) correlates with the percentage of expected requests according to the regular country-time distribution for this time interval.

**2.** The method of any of any of the preceding claims, wherein step e) comprises the step of rejecting a number of requests from the at least one country.

**3.** The method of claim 2, wherein the number of requests accepted in step e) correlates with the percentage of expected requests according to the regular request-time distribution for this country.

**4.** The method of any of the preceding claims, wherein step e) comprises limiting the bandwidth of the computer system available for the at least one country.

**5.** The method of any of the preceding claims, wherein the regular request-time-distributions for countries are established by monitoring requests during a period of time and combining them for time or time intervals of receipt of the requests and specific for each country.

**6.** The method of any of the preceding claims, wherein the regular request-time-distribution for at least one country is established by approximating a regular request-time-distribution from a comparable computer system with respect to user and time zone.

**7.** The method of any of the preceding claims, wherein the regular request-time-distribution for a country is established by extrapolating the request-time-distribution from a comparable country.

**8.** The method of any of the preceding claims, wherein a request is an IP packet, an e-mail, a DNS request, a FTP download, a VoIP call, or a HTTP request.

**9.** The method of any of the preceding claims, wherein it protects from attacks on an application level.

**10.** System for protecting computer systems from attacks over a network to which the computer system is connected, the system comprising:

means for establishing, during attack-free operation of the computer system, a regular request-time distribution for all countries of origin of requests to the computer system;
means for monitoring current requests to the computer system;
means for determining the current amount of requests for countries of origin;
means for comparing the current amount of requests for the at least one country of origin with the regular request-time distribution for at least one country of origin during a detected DDoS attack; and for setting a threshold to differentiate between acceptable request amount deviations and request amounts to be restricted, and
means for restricting the number of requests from this country served by the computer system if it is determined as a result of step d) that the current amount of requests deviates from the threshold, wherein the number of requests accepted correlates with the percentage of expected requests according to the regular country-time distribution for this time interval.

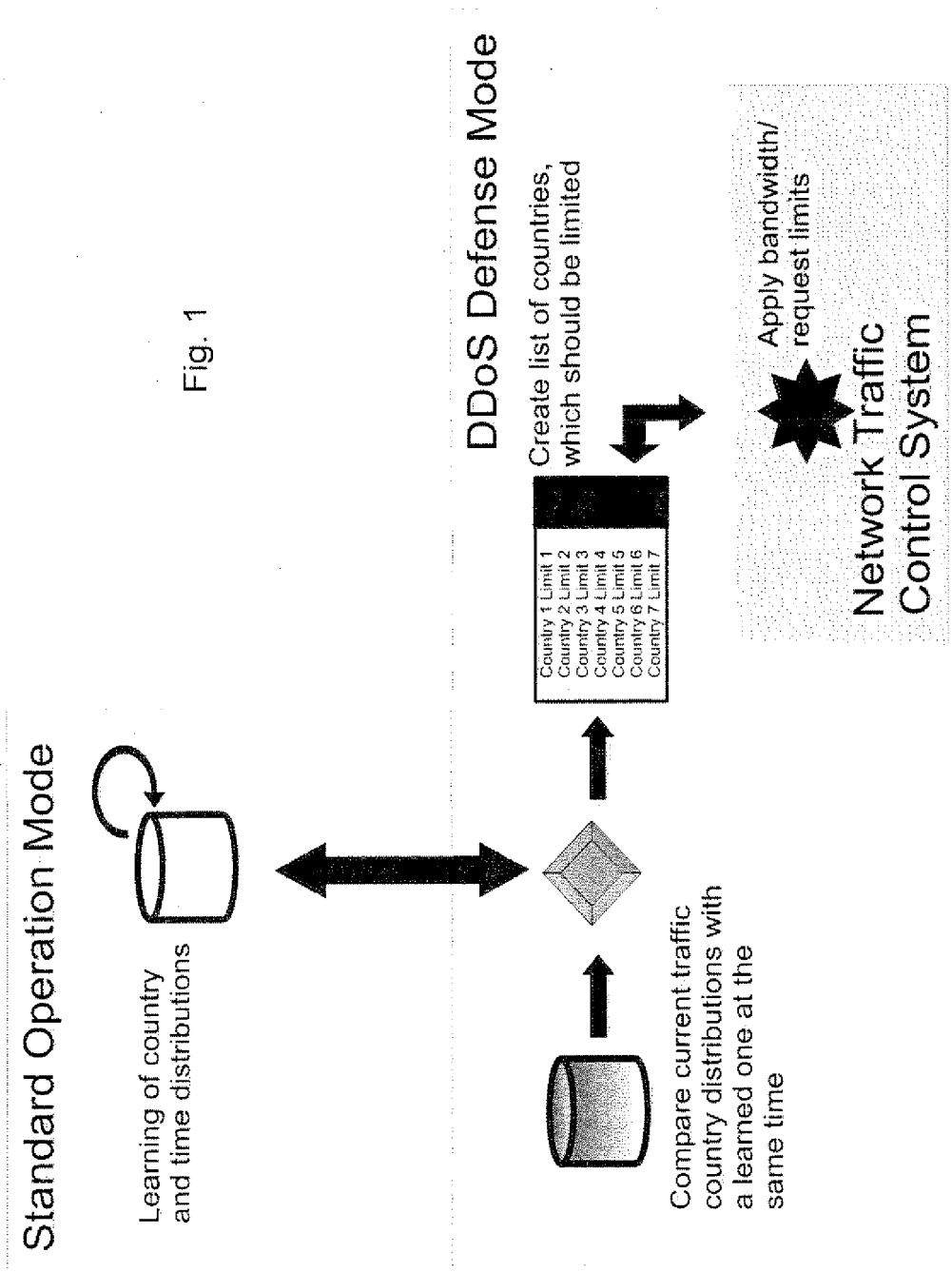
Standard Operation Mode
Learning of country and time distributions
Compare current traffic country distributions with a learned one at the same time
DDoS Defense Mode
Create list of countries, which should be limited
Country 1 Limit 1
Country 2 Limit 2
Country 3 Limit 3
Country 4 Limit 4
Country 5 Limit 5
Country 6 Limit 6
Country 7 Limit 7
Apply bandwidth/ request limits
Network Traffic Control System

Fig. 1

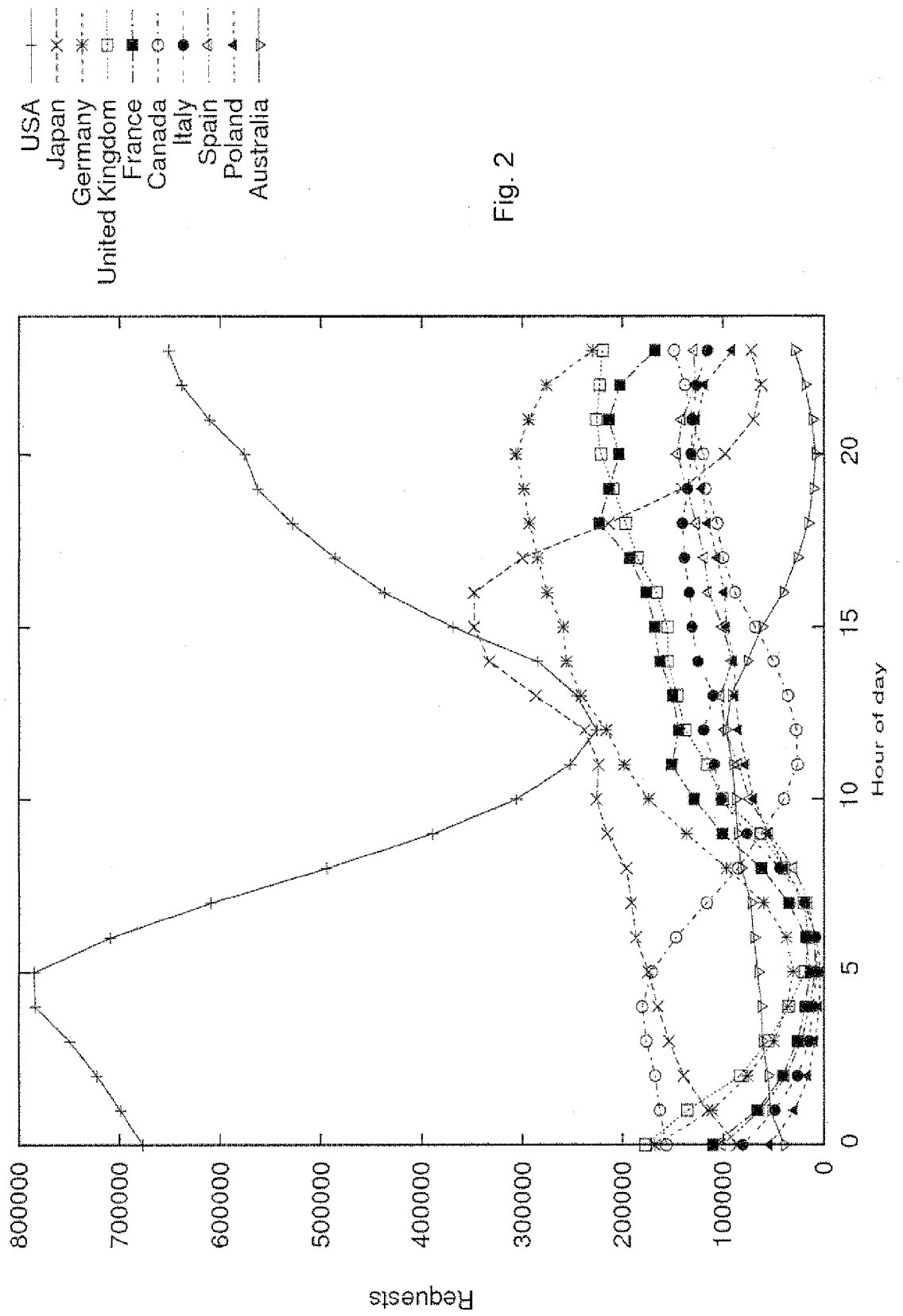
USA
Japan
Germany
United Kingdom
France
Canada
Italy
Spain
Poland
Australia
Requests
800000
700000
600000
500000
400000
300000
200000
100000
0
0
5
10
15
20
Hour of day

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

# EUROPEAN SEARCH REPORT

Application Number
EP 08 15 4389

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (IPC) |
|---|---|---|---|
| X | US 2006/010389 A1 (ROONEY JOHN G [CH] ET AL) 12 January 2006 (2006-01-12)<br>* abstract *<br>* paragraph [0019] - paragraph [0020] *<br>* paragraph [0072] - paragraph [0073] *<br>* paragraph [0083] - paragraph [0086] *<br>* paragraph [0094] *<br>* paragraph [0104] *<br>* claim 1 *<br>* claim 2 *<br>* claim 7 *<br>----- | 1-11 | INV.<br>H04L29/06 |
| X | GARY PACK ET AL: "On Filtering of DDoS Attacks Based on Source Address Prefixes" SECURECOMM AND WORKSHOPS, 2006, IEEE, PI, 1 August 2006 (2006-08-01), pages 1-12, XP031087469<br>ISBN: 978-1-4244-0422-3<br>* page 3, right-hand column, paragraph 2 - paragraph 3 *<br>* page 4, right-hand column, paragraph 4 - page 5, right-hand column, paragraph 1 *<br>* page 6, left-hand column, paragraph 1 *<br>----- | 1-11 | TECHNICAL FIELDS SEARCHED (IPC)<br>H04L |
| A | MIRKOVIC J ET AL: "A TAXONOMY OF DDOS ATTACK AND DDOS DEFENSE MECHANISMS" 1 April 2004 (2004-04-01), COMPUTER COMMUNICATION REVIEW, ACM, NEW YORK, NY, US, PAGE(S) 39 - 53 , XP001224616<br>ISSN: 0146-4833<br>* page 50, left-hand column, paragraph 4 *<br>----- | 1-11 | |
| | -/-- | | |

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| The Hague | 5 December 2008 | Walker Pina, J |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

Europäisches Patentamt
European Patent Office
Office européen des brevets

# EUROPEAN SEARCH REPORT

Application Number
EP 08 15 4389

## DOCUMENTS CONSIDERED TO BE RELEVANT

| Category | Citation of document with indication, where appropriate, of relevant passages | Relevant to claim | CLASSIFICATION OF THE APPLICATION (IPC) |
|---|---|---|---|
| A | MAHAJAN R ET AL: "CONTROLLING HIGH BANDWIDTH AGGREGATES IN THE NETWORK" COMPUTER COMMUNICATION REVIEW, ACM, NEW YORK, NY, US, vol. 32, no. 3, 1 July 2002 (2002-07-01), pages 62-73, XP001133032 ISSN: 0146-4833 * page 64, left-hand column, paragraph 1 * * page 65, left-hand column, paragraph 1 - paragraph 2 * ----- | 1-11 | |

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

| Place of search | Date of completion of the search | Examiner |
|---|---|---|
| The Hague | 5 December 2008 | Walker Pina, J |

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

3

EPO FORM 1503 03.82 (P04C01)

## ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 15 4389

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-12-2008

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2006010389 A1 | 12-01-2006 | CN 1719783 A | 11-01-2006 |
| | | KR 20060049821 A | 19-05-2006 |
| | | US 2008271146 A1 | 30-10-2008 |

## REFERENCES CITED IN THE DESCRIPTION

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

### Non-patent literature cited in the description


- **S. Savage ; D. Wetherall ; A. R. Karlin ; T. Anderson.** Practical network support for IP traceback. *SIGCOMM,* 2000, 295-306 **[0005]**