



- (51) International Patent Classification:
H04L 12/24 (2006.01)
- (21) International Application Number:
PCT/CN2013/087748
- (22) International Filing Date:
25 November 2013 (25.11.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
201210527650.2 10 December 2012 (10.12.2012) CN
- (71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).
- (72) Inventors: **LIN, Jie**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **ZHANG, Xi**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN). **YANG, Jing**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044 (CN).
- (74) Agent: **DEQI INTELLECTUAL PROPERTY LAW CORPORATION**; 7/F, Xueyuan International Tower, No. 1 Zhichun Road, Haidian District, Beijing 100083 (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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, 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, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

(54) Title: METHOD AND APPARATUS FOR RESTRICTING NETWORK APPLICATIONS

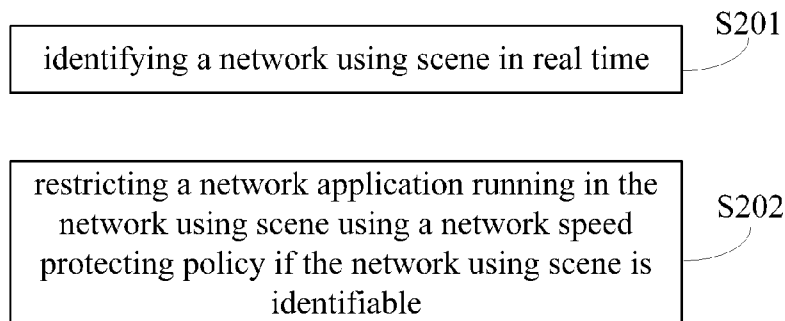


Fig. 2

(57) Abstract: Various examples of the present disclosure provide a method and an apparatus for restricting network applications to increase network speed of the local device. According to the method, a network using scene is identified; a network application running in the network using scene is restricted using a network speed protecting policy corresponding to the network using scene identified.

METHOD AND APPARATUS FOR RESTRICTING NETWORK APPLICATIONS

Related documents

[0001] The present invention claims priority of Chinese patent application No. 201210527650.2 titled “method and apparatus for restricting network applications” and filed on October 10, 2012 with the Patent Office of the People’s Republic of China, the disclosure of which is incorporated by reference in its entirety for all purposes.

Technical Field

[0002] The present disclosure relates to Web applications, and particularly to a method and an apparatus for restricting network applications.

Background

[0003] Software technology has undergone drastic changes with the rapid growth in the Internet. For example, once-prevailing stand-alone software and local network software are evolving into Internet software. The currently popular Internet “cloud” technology is also driving the development of software towards the direction of “Internet connected”. Some general-purpose operating systems such as Windows, etc., do not adopt a completely free competition mechanism for software to access network resources, but allow the software which first seized the resources to use the resources. Therefore, the software that started later may not function properly because it is unable to obtain adequate resources. For example, online game software are generally sensitive to changes in network bandwidth and network delay, and a sudden increase in network resource occupancy by other applications may greatly affect the fluency of online gaming and may even make the user fall off-line in severe cases.

[0004] A conventional solution is to store a black list of processes whose network speed is restricted in a local device. When a process consumes a large amount of network resources, the process is added into the black list and then ended. As such, network resources previously occupied by the process become available, and network speed is increased.

Summary

[0005] Various examples of the present disclosure provide a method and an apparatus for restricting network applications to increase network speed of a local application.

[0006] A method for restricting network applications may include:

a current network using scene is identified;

a network application is restricted using a network speed protecting policy corresponding to the network using scene.

[0007] An apparatus for restricting network applications may include: a scene identifying module and an application restricting module.

The scene identifying module identifies a current network using scene in real time;

The application restricting module restricts a network application using a network speed protecting policy corresponding to the network using scene identified by the scene identifying module.

[0008] The mechanism of examples of the present disclosure monitors the network using scene when a user device accesses the network and adopts a network speed protecting policy corresponding to the scene identified to restrict network applications. Therefore, targeted protection and restriction of network applications are implemented, which do not restrict a regular network application but restrict an application which is automatically started and consumes a large amount of network resources. The network speed of a local application can be increased.

Brief Description of the Drawings

[0009] Features of the present disclosure are illustrated by way of example and not limited in the following figures, in which like numerals indicate like elements, in which:

Fig. 1 is a schematic diagram illustrating an example of a computing device;

Fig. 2 is a flowchart illustrating a method for restricting network applications according to an example of the present disclosure;

Figs. 3a, 3b, 3c, 3d, 3e, 3f, 3g, 3h, 3i and 4 are schematic diagrams respectively illustrating several examples of an apparatus for restricting network applications.

Detailed Descriptions

[0010] For simplicity and illustrative purposes, the present disclosure is described by referring mainly to an example thereof. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present disclosure. It will be readily apparent however, that the present disclosure may be practiced without limitation to these specific details. In other instances, some methods and structures have not been described in detail so as not to unnecessarily obscure the present disclosure. As used herein, the term “includes” means includes but not limited to, the term “including” means including but not limited to. The term “based on” means based at least in part on. Due to characteristics of the Chinese language, quantities of an element, unless specifically mentioned, may be one or a plurality of, or at least one.

[0011] In an example, a computing device may execute methods and software systems of the present application. Fig. 1 is a schematic diagram illustrating an example of a computing device. As shown in Fig.1, computing device 100 may be capable of executing a method and apparatus of the present disclosure. The computing device 100 may, for example, be a device such as a personal desktop computer or a portable device, such as a laptop computer, a tablet computer, a cellular telephone, or a smart phone. The computing device 100 may also be a server that connects to the above devices locally or via a network.

[0012] The computing device 100 may vary in terms of capabilities or features. Claimed subject matter is intended to cover a wide range of potential variations. For example, the computing device 100 may include a keypad/keyboard 156. It may also include a display 154, such as a liquid crystal display (LCD), or a display with a high degree of functionality, such as a touch-sensitive color 2D or 3D display. In contrast, however, as another example, a web-enabled computing device 100 may include one or more physical or virtual keyboards, and mass storage medium 130.

[0013] The computing device 100 may also include or may execute a variety of operating systems 141, including an operating system, such as a WindowsTM or LinuxTM, or a mobile operating system, such as iOSTM, AndroidTM, or Windows MobileTM. The computing device 100 may include or may execute a variety of possible applications 142, such as a network speed protecting application 145.

[0014] Further, the computing device 100 may include one or more non-transitory processor-readable storage media 130 and one or more processors 122 in communication with the non-transitory processor-readable storage media 130. For example, the non-transitory processor-readable storage media 130 may be a RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of non-transitory storage medium known in the art. The one or more non-transitory processor-readable storage media 130 may store sets of instructions, or units and/or modules that include the sets of instructions, for conducting operations described in the present application. The one or more processors may be configured to execute the sets of instructions and perform the operations in examples of the present application.

[0015] Fig. 2 is a flowchart illustrating a method for restricting network applications according to an example of the present disclosure. The entity that executes the method may be the network speed protecting application 145 in the computing device 100, e.g., a user device and the like. As shown in Fig. 2, the method may include the following procedures.

[0016] In block S201, a current scene of network usage (which is also referred to as network using scene) is identified in real time.

[0017] Different network using scenes may have different requirements for network resources, e.g., an online video scene and an online game scene generally require more bandwidth or I/O resources and are more sensitive to network delay than a webpage browsing scene. Therefore, the current network using scene is identified before restrictions are applied to network applications. The real-time identifying refers to an act of identifying a network using scene when a user starts using a network.

[0018] In an example, a uniform resource locator (URL) is monitored in real time to identify the network using scene. The URL is an identity describing the address of a webpage or other resources in the Internet. When a user accesses network resources using a browser in the user device, the system may identify the current network using scene by monitoring the URL currently being visited in real time. For example, when it is determined the user is visiting *.youku.com via a browser, it can be determined the network using scene is an online video scene.

[0019] In another example, the network using scene may be identified in real time by monitoring the software the user switches on/off in real time. That is, the switching on/off of software may be used for determining the network using scene. For example, when a user starts a QQ car racing process, it can be determined that the current network using scene is an online game scene.

[0020] New network using scenes may be recorded and network using scenes may be subdivided from time to time. Sometimes, a user may be in two different network using scenes at the same time. For example, a user may be playing an online game while listening to online music. This situation is related to user habits. Therefore, an interface may be provided by the user device for the user to select applications that are allowed to run in a network using scene. A network using scene may be identified by monitoring a URL and switching on/off of applications at the same time.

[0021] When a user accesses the network by using a client application, capabilities of the user device may also affect the network speed of an application running in the user device. Restricting the network speed of a user device with low capabilities may result in lower performances of the machine. In an example, besides monitoring the network using scene in real time, capabilities including hardware capabilities and software capabilities of the user device are also identified and classified. Hardware capabilities may include capabilities of a CPU, a memory, a video card, a hard drive and the like of the user device. Software capabilities may include an operating system of the user device. Information on the hardware capabilities and software capabilities is reported to a background module in the user device. The background module may classify the capabilities of the user device into ranks such as high, medium, low, and so on. If a user device is classified to have low capabilities, information may be displayed to prompt the user to switch off a process and/or a service that is occupying network resources when the user device accesses the network.

[0022] In block S202, if the scene is identifiable, a network speed protecting policy corresponding to the scene is adopted to restrict network applications running in the network using scene.

[0023] In an example, an auxiliary policy may be adopted to restrict network applications running in the scene; and/or, a black/white list policy may be used for restricting processes running in the scene. Restricting processes using the black/white list

policy may involve classifying processes running in the network using scene. In an example, when a user accesses the network under a certain network using scene, a network speed protecting application in the user device may monitor usage of network by other processes running in the network using scene, and report monitoring results to a background module. The background module classifies the processes. For example, the processes may be classified by using the name of the company producing the software, e.g., Microsoft, Xunlei and the like. Then the processes are further classified by using the name of the product to obtain application categories. If a process belongs to a known category, the process may be put into a black list or a white list. If a process does not belong to any known category, manual work is required to determine whether the process is related to the current network using scene and possibly provide a score. As such, the background module may generate a score for each of all the processes representing the correlation between the process and the network using scene. A process may be added into the white list or the black list according to the score of the process using one or multiple pre-defined thresholds. When a user enters a certain network using scene, the network speed protecting application in the user device may automatically provide a prompt message to suggest the user to adopt a network speed protecting policy associated with the scene.

[0024] Processes may be restricted according to the classification result after the processes in a network using scene are classified, i.e., if a process running in a scene belongs to the white list of the scene, the process is not restricted; if the process belongs to the black list of the scene, the process is ended; if the process belongs to a gray list, network resources consumed by the process are restricted. Taking the network using scene being a user playing an online game (e.g., a QQ car racing game) as an example, processes running in the online game scene which are necessary to the running of the online game, e.g., a system process, a gaming process, a gaming subprocess, an application accompanying the game (e.g., a game accelerator and the like) and etc., belong to a white list and thus are not restricted by the network speed protecting application in the user device. Processes running in the online gaming scene which are not necessary to the running of the online game and occupy a lot of system resources belong to a black list. The network speed protecting application in the user device may apply a restricting policy to the processes in the black list, e.g., directly ending the

process or ending the process and the like. Processes belonging to a gray list, e.g., an unknown process or a third party process that the user does not wish to be ended, may be restricted according to a network speed restricting policy.

[0025] Restricting network applications running in an identifiable network using scene by using an auxiliary policy may involve not restricting the speed of a suspended process, not restricting an application which is manually started by the user, restricting or ending a process running in a user device with low capabilities, and so on. Still taking the user playing an online game as an example, when the user has started an online game process but is not playing the game, i.e., the online game process is suspended, the network speed protecting application does not restrict the network speed of the online game process in the online game scene. When the user has started the online game process and then manually starts another application that also consumes network resources, the network speed protecting application in the user device does not restrict the network speed of the application manually started by the user in the online game scene. When the user has started an online game process but the user device has low capabilities, processes running in the user device are restricted or ended to ensure there are enough resources for running the online game in the device.

[0026] The auxiliary policy and/or the black/white list policy may be network speed protecting policies stored in a local policy center or obtained from a cloud server in real time. In an example, network speed protecting policies in a server in the cloud may be obtained by using a cloud hub.

[0027] The mechanism of examples of the present disclosure monitors the network using scene in real time when a user device accesses the network, and adopts a network speed protecting policy corresponding to the scene identified to restrict network applications if the scene is identifiable. Therefore, targeted protection and restriction of network applications are implemented, which do not restrict a regular network application but restrict an application which is automatically started and consumes a large amount of network resources. The network speed of an application can be increased.

[0028] Fig. 3a is a schematic diagram illustrating a structure of an apparatus for restricting network applications according to an example of the present disclosure. Only those features related with the implementation of the mechanism are illustrated for simplicity. The apparatus as shown in Fig. 3a may be a network speed protecting software

installed in a user device. The apparatus may include a scene identifying module 301 and an application restricting module 302.

[0029] A scene identifying module 301 is configured to identify a current network using scene in real time;

[0030] an application restricting module 302, configured to restrict a network application using a network speed protecting policy corresponding to the network using scene identified by the scene identifying module 301.

[0031] In an example, the scene identifying module 301 may include a first identifying module 3011 as shown in Fig. 3b.

[0032] The first identifying module 3011 is configured to monitor a URL in real time to identify the network using scene.

[0033] In an example, the scene identifying module 301 may include a second identifying module 3012 as shown in Fig. 3c.

[0034] The second identifying module 3012 is configured to monitor switching on/off of an application in real time to identify the network using scene.

[0035] As shown in Fig. 3d, the scene identifying module 301 in the apparatus may include the first identifying module 3011 and the second identifying module 3012.

[0036] In an example, the application restricting module 302 may include a first restricting module 3021 as shown in Fig. 3e.

[0037] The first restricting module 3021 is configured to restrict a network application running in the network using scene by using an auxiliary policy. For example, the auxiliary policy may include any or any combination of: not restrict the speed of a suspended process, not restricting an application which is manually started by the user, restricting or ending a process running in a user device with low capabilities.

[0038] In an example, the application restricting module 302 may include a second restricting module 3022 as shown in Fig. 3f.

[0039] The second restricting module 3022 is configured to restrict a process running in the network using scene using a black/white list policy.

[0040] In an example, the apparatus may include the first restricting module 3021 and the second restricting module 3022, as shown in Fig. 3g.

[0041] In an example, the second restricting module 3022 may include a classifying module 3221, a first process handling module 3222, a process ending module 3223 and a second process handling module 3224, as shown in Fig. 3h and Fig. 3i.

[0042] The classifying module 3221 is configured to classify processes running in the network using scene.

[0043] The first process handling module 3222 is configured to apply no restriction on a process running in the network using scene if the process belongs to a white list.

[0044] The process ending module 3223 is configured to end a process running in the network using scene if the process belongs to a black list.

[0045] The second process handling module 3224 is configured to restrict a network speed obtained by a process running in the network using scene if the process belongs to a gray list.

[0046] Fig. 4 is a schematic diagram illustrating a structure of an apparatus for restricting network applications according to an example of the present disclosure. The apparatus may include a scene identifying module 401, an application restricting module 402, a capability identifying module 403 and a prompting module 404.

[0047] Functions of the scene identifying module 401 and the application restricting module 402 may be similar to those of the scene identifying module 301 and the application restricting module 302.

[0048] The capability identifying module 403 is configured to identify and classify capabilities of a user device. The categories of user device capabilities may include high, medium and low.

[0049] The prompting module 404 is configured to prompt the user to end a process and/or a service that consumes network resources if the capability identifying module 403 determines the user device has low capabilities when the user device is accessing the network.

[0050] It should be understood that in the above processes and structures, not all of the procedures and modules are necessary. Certain procedures or modules may be omitted

according to the needs. The order of the procedures is not fixed, and can be adjusted according to the needs. The modules are defined based on function simply for facilitating description. In implementation, a module may be implemented by multiple modules, and functions of multiple modules may be implemented by the same module. The modules may reside in the same device or distribute in different devices. The “first”, “second” in the above descriptions are merely for distinguishing two similar objects, and have no substantial meanings.

[0051] In various embodiments, a hardware module may be implemented mechanically or electronically. For example, a hardware module may include dedicated circuitry or logic that is permanently configured (e.g., as a special-purpose processor, such as a field programmable gate array (FPGA) or an application-specific integrated circuit (ASIC)) to perform certain operations. A hardware module may also include programmable logic or circuitry (e.g., as encompassed within a general-purpose processor or other programmable processor) that is temporarily configured by software to perform certain operations. It will be appreciated that the decision to implement a hardware module mechanically, in dedicated and permanently configured circuitry, or in temporarily configured circuitry (e.g., configured by software) may be driven by cost and time considerations.

[0052] A machine-readable storage medium is also provided, which is to store instructions to cause a machine to execute a method as described herein. Specifically, a system or apparatus having a storage medium which stores machine-readable program codes for implementing functions of any of the above examples and which may make the system or the apparatus (or CPU or MPU) read and execute the program codes stored in the storage medium. In addition, instructions of the program codes may cause an operating system running in a computer to implement part or all of the operations. In addition, the program codes implemented from a storage medium are written in a storage device in an extension board inserted in the computer or in a storage in an extension unit connected to the computer. In this example, a CPU in the extension board or the extension unit executes at least part of the operations according to the instructions based on the program codes to realize the technical scheme of any of the above examples.

[0053] The storage medium for providing the program codes may include floppy disk, hard drive, magneto-optical disk, compact disk (such as CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-RAM, DVD-RW, DVD+RW), magnetic tape drive, Flash card, ROM

and so on. Optionally, the program code may be downloaded from a server computer via a communication network.

[0054] The scope of the claims should not be limited by the embodiments set forth in the examples, but should be given the broadest interpretation consistent with the description as a whole.

Claims

1. A method for restricting network applications, comprising:

identifying a current network using scene;

restricting a network application using a network speed protecting policy corresponding to the network using scene.
2. The method of claim 1, wherein the identifying a current network using scene in real time comprises:

monitoring a uniform resource locator (URL) to identify the network using scene;
and/or

monitoring switching on/off of an application to identify the network using scene.
3. The method of claim 1, further comprising:

identifying capabilities of a user device, and classifying the capabilities into one of categories including high capabilities, medium capabilities and low capabilities;

prompting a user to end a process and/or a service that is occupying network resources when the user device accesses the network if the user device is classified into the category of low capabilities.
4. The method of claim 1, wherein restricting a network application using a network speed protecting policy comprises:

adopting an auxiliary policy to restrict a network application running in the network using scene; and/or

adopting a black/white list policy to restricting a process running in the network using scene.
5. The method of claim 4, wherein the adopting an auxiliary policy to restrict a network application running in the network using scene comprises: restricting network speeds obtained by processes except for a suspended process, restricting applications except for an application which is manually started by the user, restricting or ending a process running in a user device having low capabilities;

wherein adopting a black/white list policy to restricting a process running in the network using scene comprises:

classifying processes running in the network using scene;

applying no restricting policy to a process belonging to a white list running in the network using scene;

ending a process belonging to a black list running in the network using scene; and

restricting a network speed obtained by a process belonging to a gray list running in the network using scene.

6. An apparatus for restricting network applications, comprising:

a scene identifying module, configured to identify a current network using scene ;

an application restricting module, configured to restrict a network application using a network speed protecting policy corresponding to the network using scene identified by the scene identifying module.

7. The apparatus of claim 6, wherein the scene identifying module comprises:

a first identifying module, configured to monitor a uniform resource locator (URL) to identify the network using scene; and/or

a second identifying module, configured to monitor switching on/off of an application to identify the network using scene.

8. The apparatus of claim 6, further comprising:

a capability identifying module, configured to identify and classify capabilities of a user device into categories including high capabilities, medium capabilities and low capabilities; and

a prompting module, configured to prompt the user to end a process and/or a service that consumes network resources if the capability identifying module identifies the user device has low capabilities when the user device accesses the network.

9. The apparatus of claim 6, wherein the application restricting module comprises:

a first restricting module, configured to adopt an auxiliary policy to restrict the network application running in the network using scene; and/or

a second restricting module, configured to restrict a process running in the network using scene using a black/white list policy.

10. The apparatus of claim 9, wherein the first restricting module is configured to restrict network speeds obtained by processes except for a suspended process, restrict applications except for an application which is manually started by the user, restricting or end a process running in a user device having low capabilities; and

wherein the second restricting module comprises:

a classifying module, configured to classify processes running in the network using scene;

a first process handling module, configured to apply no restriction on a process running in the network using scene if the process belongs to a white list;

a process ending module, configured to end a process running in the network using scene if the process belongs to a black list;

a second process handling module, configured to restrict a network speed obtained by a process running in the network using scene if the process belongs to a gray list.

1/5

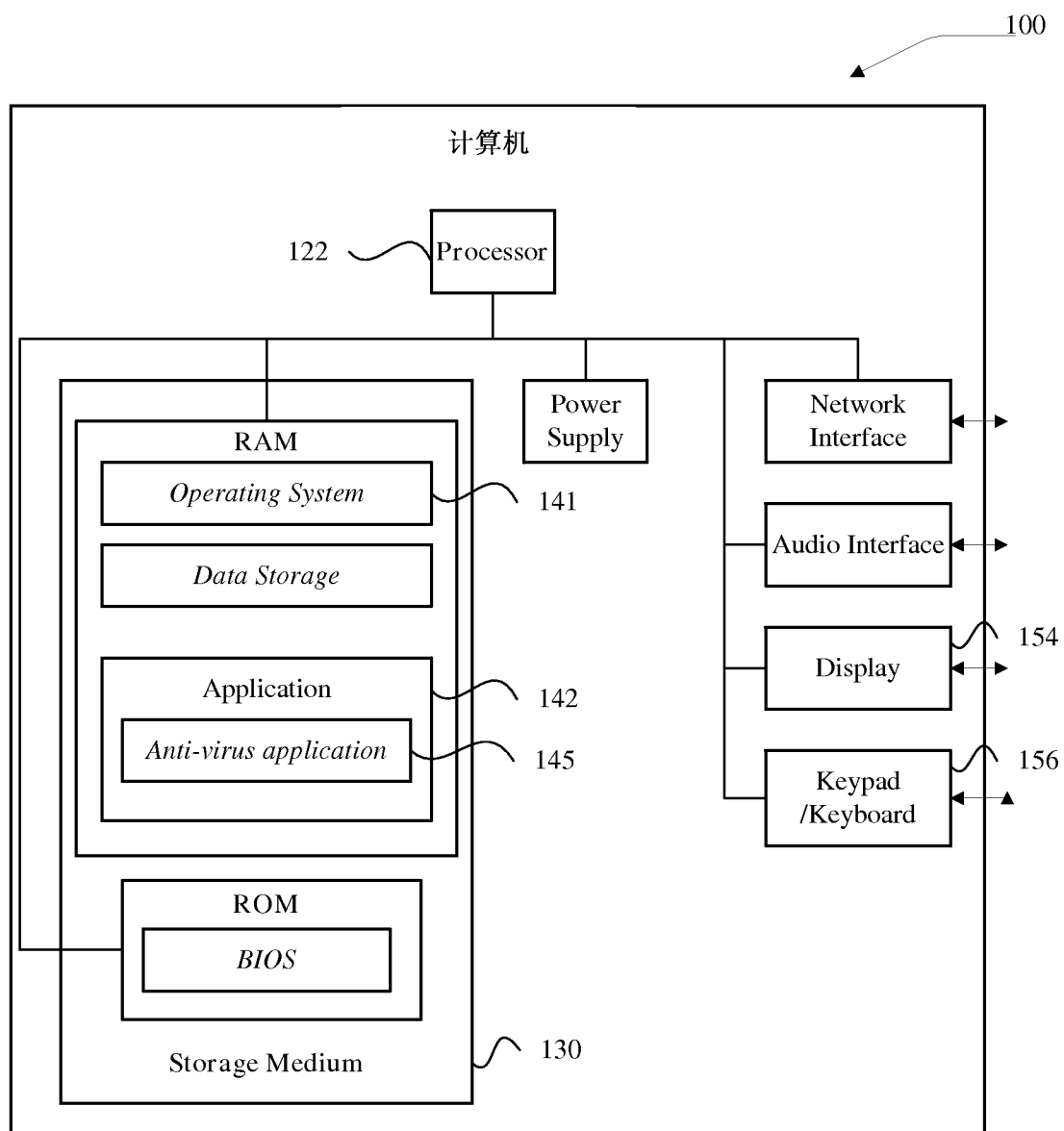


Fig. 1

2/5

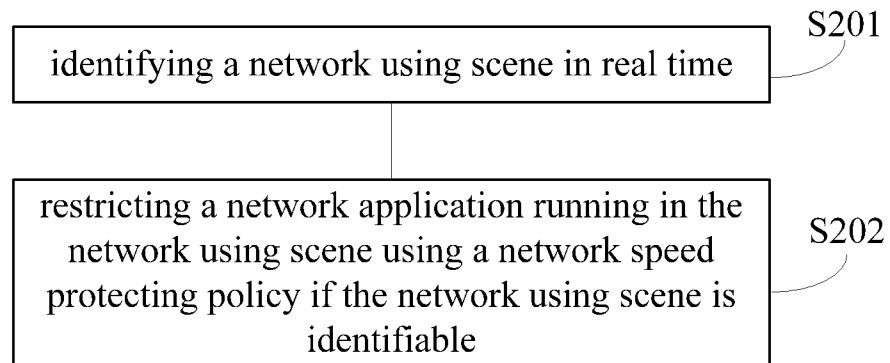


Fig. 2

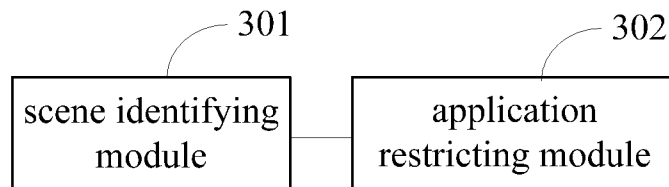


Fig. 3a

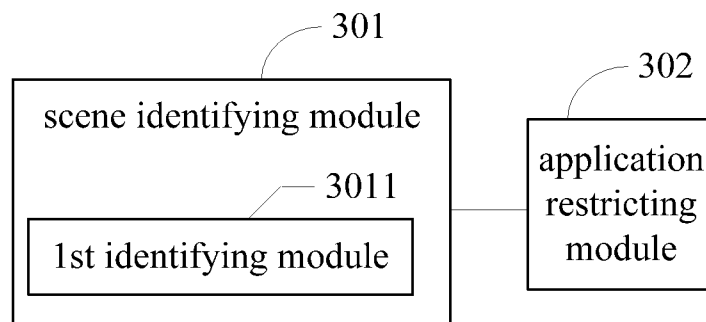


Fig. 3b

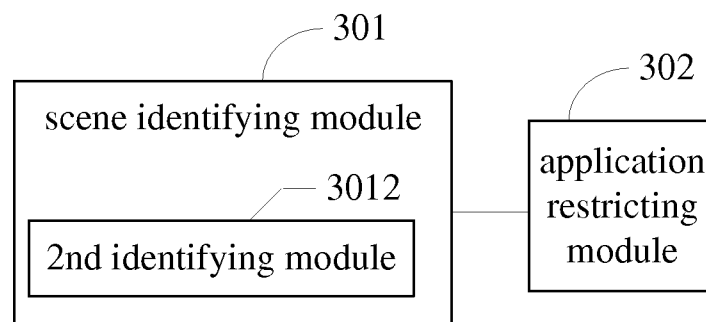


Fig. 3c

3/5

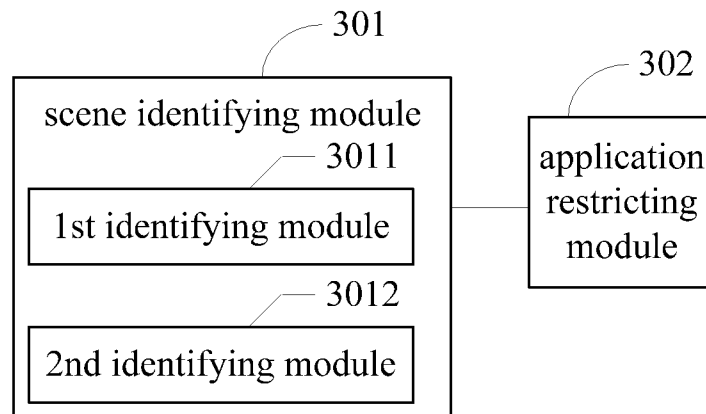


Fig. 3d

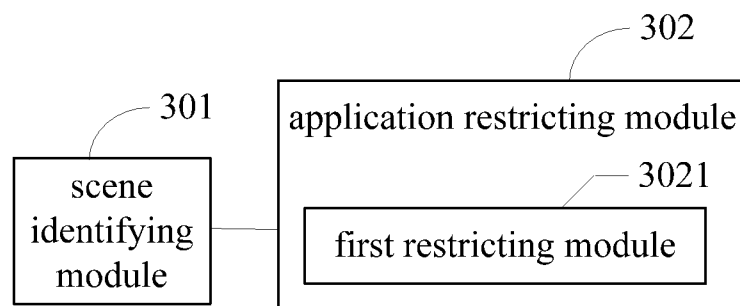


Fig. 3e

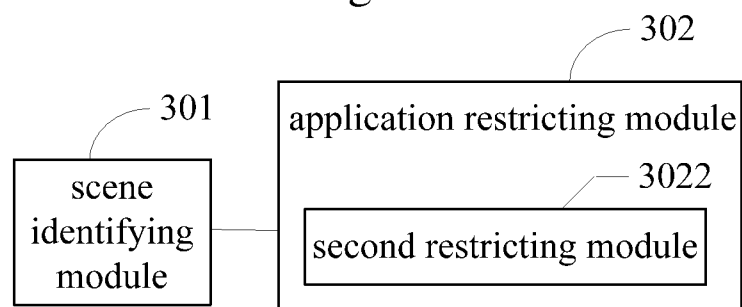


Fig. 3f

4/5

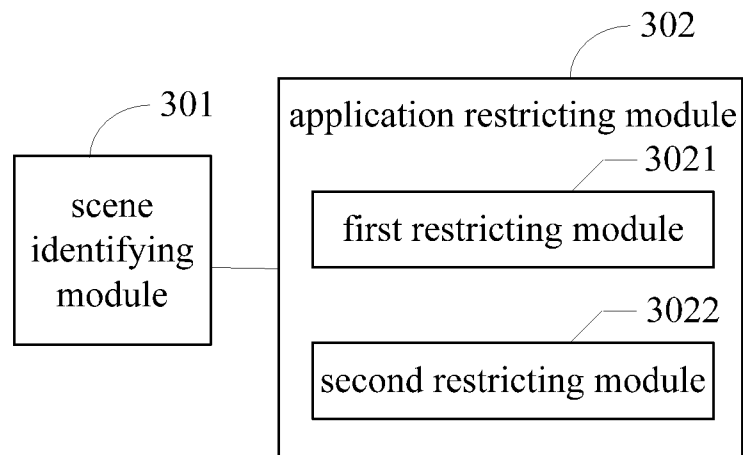


Fig. 3g

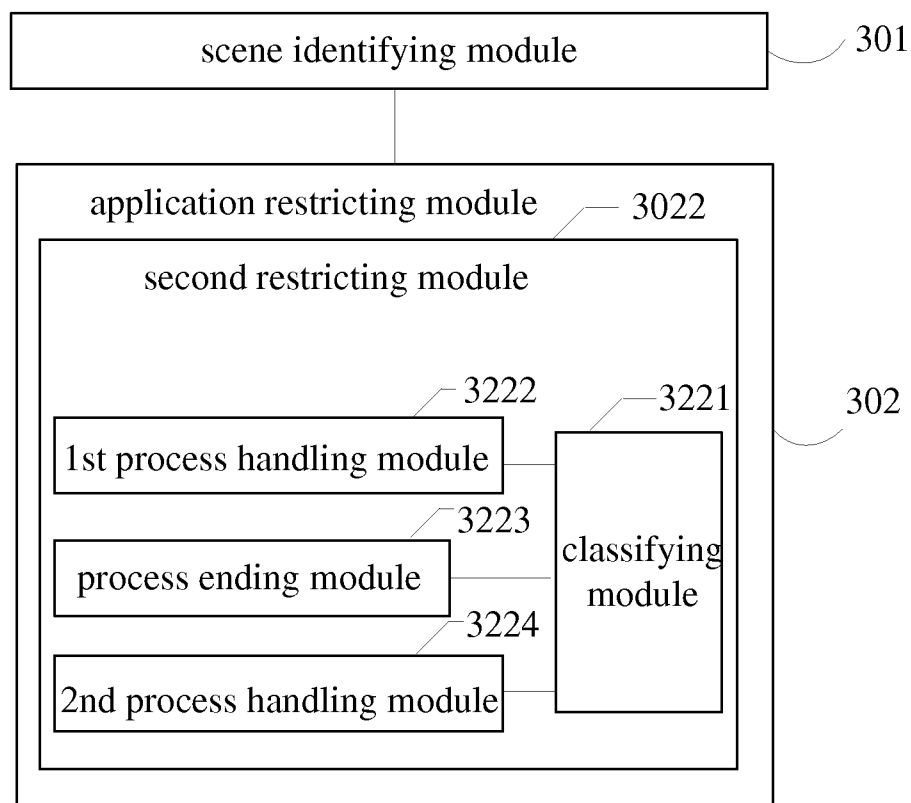


Fig. 3h

5/5

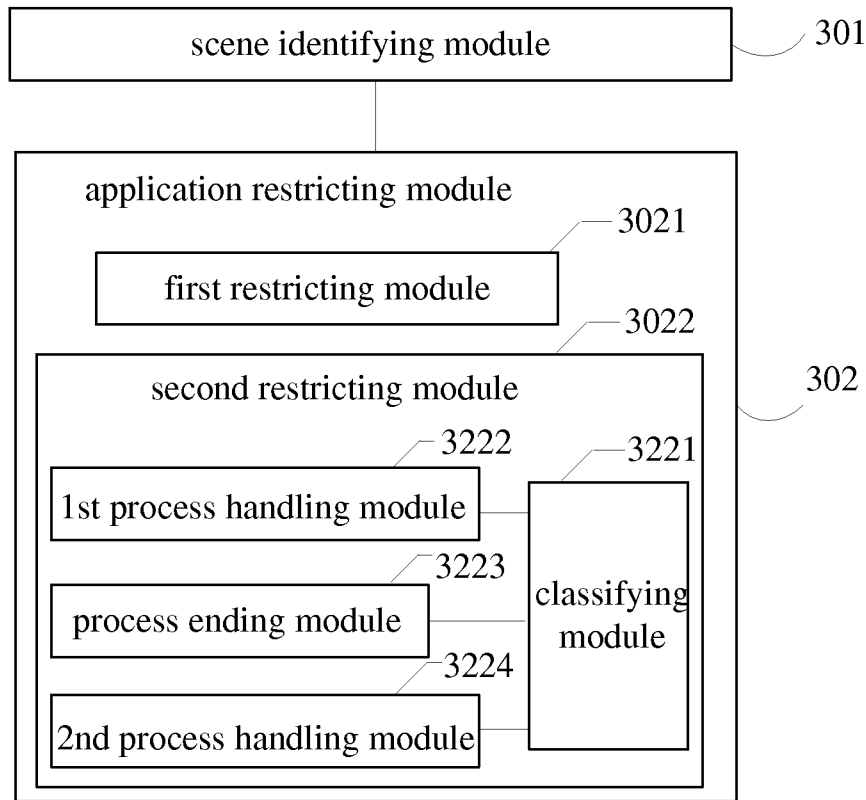


Fig. 3i

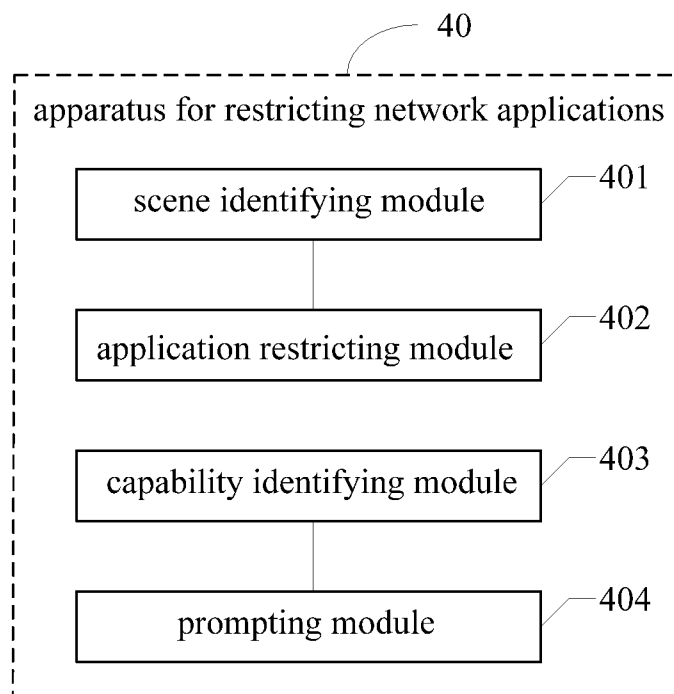


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/087748

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24 (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

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)

CPRSABS, CNTXT, CNKI, VEN: application, program, restrict, limit, network, speed, monitor, rate, process, stop, switch, identify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102209107 A (QIZHI SOFTWARE BEIJING CO., LTD.) 05 October 2011 (05.10.2011), the description paragraphs [0086]-[0100]	1-2, 6-7
A	CN 101431473 A (SHENZHEN THUNDER NETWORK TECHNOLOGY CO., LTD.) 13 May 2009 (13.05.2009), the whole document	1-10
A	CN 102111333 A (SHANGHAI JUXIN NETWORK TECHNOLOGY CO., LTD.) 29 June 2011 (29.06.2011), the whole document	1-10
A	WO 2008039033 A1 (HOIDE CO., LTD.) 03 April 2008 (03.04.2008), the whole document	1-10

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

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 15 February 2014 (15.02.2014)	Date of mailing of the international search report 06 Mar. 2014 (06.03.2014)
--	--

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
ZHOU, Dan
Telephone No. (86-10)62089390

International application No.
PCT/CN2013/087748

Form PCT/ISA /210 (patent family annex) (July 2009)