



(51) International Patent Classification:
G06F 9/46 (2006.01)

(21) International Application Number:
PCT/CN2013/082265

(22) International Filing Date:
26 August 2013 (26.08.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201210305259.8 24 August 2012 (24.08.2012) CN

(71) Applicant: **TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED** [CN/CN]; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(72) Inventor: **XIAO, Quanhao**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).

(74) Agent: **BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.**; A-1-102, He Jing Yuan, Ji Men Li, Xueyuan Road, Haidian District, Beijing 100088 (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, 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 SYSTEM FOR NETWORKING CONTROL OF APPLICATION PROGRAMS

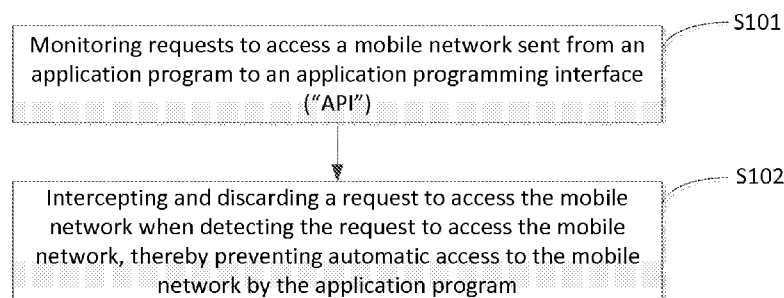


FIG. 1

(57) Abstract: The present disclosure provides method and system for networking control of application programs, and belongs to the field of computer technology. The method comprises: monitoring requests to access a mobile network sent from an application program to an application programming interface; intercepting and discarding a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program. The present disclosure accomplishes effective control of an application program's access to a mobile network, reduces communication flow of terminal users, and enhances privacy security of the terminal users.



PCT PATENT APPLICATION

FOR

Method and System for Networking Control of Application Programs

Cross Reference to Related Application

[0001] This application claims the priority benefit of Chinese Patent Application No. 201210305259.8, filed August 24, 2012, the contents of which are incorporated by reference herein in their entirety for all purposes.

Technical Field

[0002] The present disclosure relates generally to the technological field of computers, and more particularly, to a method and system for networking control of application programs.

Background

[0003] With the intelligentization of mobile terminals (such as smartphones and tablet PCs, etc.), many application programs for mobile terminals emerge one after another. Some software can establish network connection using a mobile terminal's wireless network without obtaining permission from or reminding a terminal user, and upload the terminal user's application program data or even private data to specific servers, thereby increasing the terminal user's communication flows and reducing the privacy security of the terminal user.

Summary of the Disclosure

[0004] The present disclosure discloses a method and system for networking control of application programs to solve the following problem: existing technology cannot provide an effective application program networking control method, which causes an increase in a terminal user's communication flows and reduces privacy security of the terminal user.

[0005] According to the present disclosure, an application program networking control method comprises:

[0006] monitoring requests to access a mobile network sent from an application program to an application programming interface (“API”), and

[0007] intercepting and discarding a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0008] The present disclosure also discloses an application program networking control system, the system comprising:

[0009] a request monitoring unit that monitors request to access a mobile network sent from an application to an API, and

[0010] a request discarding unit that intercepts and discards a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0011] By monitoring requests to access a mobile network sent from an application program to an API, and intercepting and discarding a request to access the mobile network when detecting the request to access the mobile network, automatic access to the mobile network by the application program can be prevented, thereby accomplishing effective control of the application program’s access to the mobile network, reducing communication flows of terminal users, and enhancing privacy security of the terminal users.

Brief Description of the Drawings

[0012] FIG. 1 is a schematic diagram illustrating an example of the flow of an application program networking control method according to various embodiments.

[0013] FIG. 2 is a schematic diagram illustrating an example of the flow of an application program networking control method according to various embodiments.

[0014] FIG. 3 is a schematic diagram illustrating an example of an arrangement of an application program networking control system according to various embodiments.

[0015] FIG. 4 is a schematic diagram illustrating an example of an arrangement of an application program networking control system according to various embodiments.

[0016] FIG. 5 is a schematic diagram illustrating an example of an arrangement of an application program networking control system according to various embodiments.

Detailed Description

[0017] In the following description of embodiments, reference is made to the accompanying drawings which form a part hereof, and in which it is shown by way of illustration specific embodiments of the disclosure that can be practiced. It is to be understood that other embodiments can be used and structural changes can be made without departing from the scope of the disclosed embodiments.

[0018] FIG. 1 is a schematic diagram illustrating an example of the flow of an application program networking control method according to various embodiments. The method can comprise:

[0019] Step S101: monitoring requests to access a mobile network sent from an application program to an application programming interface (“API”).

[0020] According to some embodiments, monitoring requests to access a mobile network sent from an application program to an API comprises monitoring the API, wherein the API is associated with access to the mobile network. According to some embodiments, monitoring requests to access a mobile network sent from an application program to an API comprises monitoring whether the application program has sent any request to access the mobile network to the API, wherein the API is associated with access to the mobile network. The mobile network can be a second generation mobile communication network, a third generation mobile communication network, or a fourth generation mobile communication network. Examples of a mobile network include, but are not limited to, a General Packet Radio Service (“GPRS”) network, a Wideband Code Division Multiple Access (“WCDMA”) network, a Code Division Multiple Access 2000 (“CDMA2000”) network, a Time Division-Synchronous Code Division Multiple Access (“TD-SCDMA”) network, and a Time Division Long Term Evolution (“TD-LTE”) network.

[0021] Step S102: intercepting and discarding a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0022] According to some embodiments, when detecting a request to access the mobile network sent from an application program to an API, the request to access the mobile network can be intercepted and discarded, thereby preventing automatic access to or an operation of uploading data to the mobile network. According to these embodiments, communication flows brought about by the application program's visiting the mobile network can be reduced. This can protect user privacy to some extent.

[0023] After discarding a request to access the mobile network, a networking failure message can be returned to the application program to prompt that the application program cannot access the requested mobile network. By way of example only, corresponding networking failure identification information can be returned to a thread or a process of the application program that sent the request to access the mobile network. After receiving the identification information, the application program can output corresponding networking failure prompt message to remind a terminal user.

[0024] FIG. 2 is a schematic diagram illustrating an example of the flow of an application program networking control method according to various embodiments. The method can comprise:

[0025] Step S201: setting one or more networking control commands allowing or prohibiting access to a mobile network.

[0026] According to some embodiments, setting one or more networking control commands allowing or prohibiting access to a mobile network can allow a terminal user to conveniently and independently set whether to prohibit access to the mobile network with respect to each application program.

[0027] Step S202: monitoring requests to access the mobile network sent from an application program to an API.

[0028] According to some embodiments, monitoring requests to access the mobile network sent from an application program to an API can comprise monitoring via a set HOOK function.

[0029] Step S203: determining whether there is a set networking control command prohibiting access to the mobile network when detecting a request to access the mobile network. If yes, then proceed with Step S204. If no, then proceed with Step S205.

[0030] According to some embodiments, monitoring requests to access a mobile network sent from an application program to an API comprises monitoring the API, wherein the API is associated with access to the mobile network. According to some embodiments, monitoring requests to access a mobile network sent from an application program to an API comprises monitoring whether the application program has sent any request to access the mobile network to the API, wherein the API is associated with access to the mobile network. When detecting a request to access the mobile network, a determination can be made as to whether there is a networking control command prohibiting access to the mobile network set by a user.

[0031] Step S204: intercepting and discarding the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0032] According to some embodiments, when detecting a request to access a mobile network sent from an application program to an API using a set HOOK function, a HOOK subprogram can be sent to the request to force the end of the transmission of the request, i.e., to discard the request, thereby preventing automatic access to the mobile network by the application program.

[0033] Step S205: sending the request to access the mobile network to the API.

[0034] According to some embodiments, when a terminal user allows an application program to access a mobile network, a request to access the mobile network sent from the application program can be sent to an API associated with access to the mobile network, enabling the application program to access the mobile network.

[0035] According to some embodiments, by setting one or more networking control commands allowing or prohibiting access to a mobile network, a terminal user can independently set whether to prohibit access to the mobile network with respect to each application program.

This increases the controllability of application programs' mobile network access. When detecting a request to access a mobile network prohibited by a set networking control command, the request to access the mobile network can be intercepted and discarded, thereby preventing automatic access to the mobile network by an application program. This accomplishes effective control of application programs' mobile network access, reduces a terminal user's communication flows, and enhances the terminal user's privacy security.

[0036] Persons of ordinary skill in the art can readily appreciate that all or part of the steps of the methods described in the embodiments above can be executed by relevant hardware instructed by a program that may be stored in a computer-readable memory medium. The readable memory medium may be, for example, a read-only memory ("ROM"), a random access memory ("RAM"), a magnetic disk or a compact disc.

[0037] FIG. 3 is a schematic diagram illustrating an example of an arrangement of an application program networking control system according to various embodiments. As illustrated in FIG. 3, an application program networking control system 3 can comprise a request monitoring unit 31 and a request discarding unit 32, wherein

[0038] The request monitoring unit 31 monitors requests to access a mobile network sent from an application program to an API.

[0039] According to some embodiments, the request monitoring unit 31 monitors the API, wherein the API is associated with access to the mobile network. According to some embodiments, the request monitoring unit 31 monitors whether the application program has sent any request to access the mobile network to the API, wherein the API is associated with access to the mobile network.

[0040] The request discarding unit 32 intercepts and discards a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0041] According to some embodiments, when detecting a request to access the mobile network sent from an application program to an API, the request discarding unit 32 can intercept and discard the request to access the mobile network, thereby preventing automatic access to or an operation of uploading data to the mobile network. According to these embodiments,

communication flows brought about by the application program's visiting the mobile network can be reduced. This can protect user privacy to some extent.

[0042] FIG. 4 is a schematic diagram illustrating an example of an arrangement of an application program networking control system according to various embodiments. As illustrated in FIG. 4, an application program networking control system 4 can comprise: a setting unit 41, a request monitoring unit 42, a request discarding unit 43, an information returning unit 44, and a request sending unit 45, wherein

[0043] The setting unit 41 sets one or more networking control commands allowing or prohibiting access to a mobile network.

[0044] According to some embodiments, setting one or more networking control commands allowing or prohibiting access to a mobile network can allow a terminal user to conveniently and independently set whether to prohibit access to the mobile network with respect to each application program.

[0045] The request monitoring unit 42 monitors requests to access the mobile network sent from an application program to an API.

[0046] The request discarding unit 43 intercepts and discards a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0047] According to some embodiments, when a networking control command allowing or prohibiting access to the mobile network is set by the setting unit 41, the request discarding unit 43 can comprise a request discarding subunit 431 that intercepts and discards a request to access the mobile network prohibited by a networking control command when detecting the request to access the mobile network.

[0048] The information returning unit 44 sends a networking failure message to the application program.

[0049] The request sending unit 45 sends a request to access the mobile network to the API when detecting the request to access the mobile network if access to the mobile network is allowed by a set networking control command.

[0050] FIG. 5 is a schematic diagram illustrating an example of an arrangement of an application program networking control system according to various embodiments. As illustrated in FIG. 5, an application program networking control system 5 can comprise: a setting unit 51, a request monitoring unit 52, a request discarding unit 53, an information returning unit 54, and a request sending unit 55, wherein

[0051] The setting unit 51 sets one or more networking control commands allowing or prohibiting access to a mobile network.

[0052] According to some embodiments, setting one or more networking control commands allowing or prohibiting access to a mobile network can allow a terminal user to conveniently and independently set whether to prohibit access to the mobile network with respect to each application program.

[0053] The request monitoring unit 52 monitors requests to access the mobile network sent from an application program to an API.

[0054] According to some embodiments, monitoring requests to access the mobile network sent from an application program to an API can comprise monitoring via a set HOOK function. According to these embodiments, the request monitoring unit 52 can comprise a request monitoring subunit 521 that monitors requests to access the mobile network sent from the application program to the API via the set HOOK function.

[0055] The request discarding unit 53 intercepts and discards a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

[0056] According to some embodiments, when detecting a request to access a mobile network sent from an application program to an API using a set HOOK function, a HOOK subprogram can be sent to the request to force the end of the transmission of the request, i.e., to discard the request. According to these embodiments, the request discarding unit 53 can comprise a request discarding subunit 531 that intercepts and discards a request to access the mobile network via the set HOOK function when detecting the request to access the mobile network.

[0057] The information returning unit 54 sends a networking failure message to the application program.

[0058] The request sending unit 55 sends a request to access the mobile network to the API when detecting the request to access the mobile network if access to the mobile network is allowed by a set networking control command.

[0059] According to some embodiments, when detecting a request to access the mobile network sent from an application program to an API, the request discarding unit 32 can intercept and discard the request to access the mobile network, thereby preventing automatic access to or an operation of uploading data to the mobile network. According to these embodiments, communication flows brought about by the application program's visiting the mobile network can be reduced. This can protect user privacy to some extent.

[0060] The methods disclosed herein can be executed by a mobile terminal and the systems disclosed herein can be part of a mobile terminal. A mobile terminal can be a mobile phone, a tablet PC, a media player, etc. Examples of mobile terminals that can be used in accordance with various embodiments include, but are not limited to, a tablet PC (including, but not limited to, Apple iPad and other touch-screen devices running Apple iOS, Microsoft Surface and other touch-screen devices running the Windows operating system, and tablet devices running the Android operating system), a mobile phone, a smartphone (including, but not limited to, an Apple iPhone, a Windows Phone and other smartphones running Windows Mobile or Pocket PC operating systems, and smartphones running the Android operating system, the Blackberry operating system, or the Symbian operating system), an e-reader (including, but not limited to, Amazon Kindle and Barnes & Noble Nook), a laptop computer (including, but not limited to, computers running Apple Mac operating system, Windows operating system, Android operating system and/or Google Chrome operating system), a media player (including, but not limited to, Apple iPod and Microsoft Zoom), or an on-vehicle device running any of the above-mentioned operating systems or any other operating systems, , or any other mobile Internet device ("MID") or intelligent communication terminal, all of which are well known to those skilled in the art.

[0061] Although the disclosed embodiments have been fully described with reference to the accompanying drawings, it is to be noted that various changes and modifications will become

apparent to those skilled in the art. Such changes and modifications are to be understood as being included within the scope of the disclosed embodiments as defined by the appended claims.

WHAT IS CLAIMED IS:

1. An application program networking control method comprising:
monitoring requests to access a mobile network sent from an application program to an API, and
intercepting and discarding a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.
2. The method of claim 1, comprising:
sending a networking failure message to the application program after intercepting and discarding the request to access the mobile network.
3. The method of claim 1, comprising:
setting one or more networking control commands allowing or prohibiting access to the mobile network before monitoring the requests to access the mobile network sent from the application program to the API.
4. The method of claim 3, wherein intercepting and discarding the request to access the mobile network when detecting the request to access the mobile network comprises:
intercepting and discarding the request to access the mobile network when detecting the request to access the mobile network if and only if there is a set networking control command prohibiting access to the mobile network.
5. The method of claim 1, wherein the mobile network comprises at least one of: a GPRS network, a WCDMA network, a CDMA2000 network, a TD-SCDMA network, and a TD-LTE network.
6. The method of claim 1, wherein

monitoring the requests to access the mobile network sent from the application program to the API comprises monitoring the requests to access the mobile network sent from the application program to the API via a set HOOK function, and

intercepting and discarding the request to access the mobile network when detecting the request to access the mobile network comprises intercepting and discarding a request to access the mobile network via the set HOOK function when detecting the request to access the mobile network.

7. An application program networking control method comprising:

setting one or more networking control commands allowing or prohibiting access to a mobile network,

monitoring requests to access the mobile network sent from an application program to an API, and

sending a request to access the mobile network to the API when detecting the request to access the mobile network if and only if there is a set networking control command allowing access to the mobile network.

8. The method of claim 7, wherein the mobile network comprises at least one of: a GPRS network, a WCDMA network, a CDMA2000 network, a TD-SCDMA network, and a TD-LTE network.

9. An application program networking control method comprising:

setting one or more networking control commands allowing or prohibiting access to a mobile network,

monitoring requests to access the mobile network sent from an application program to an API, and

sending a request to access the mobile network to the API when detecting the request to access the mobile network if there is no set networking control command prohibiting access to the mobile network.

10. The method of claim 9, wherein the mobile network comprises at least one of: a GPRS network, a WCDMA network, a CDMA2000 network, a TD-SCDMA network, and a TD-LTE network.

11. An application program networking control system comprising:
a request monitoring unit that monitors request to access a mobile network sent from an application to an API, and
a request discarding unit that intercepts and discards a request to access the mobile network when detecting the request to access the mobile network, thereby preventing automatic access to the mobile network by the application program.

12. The system of claim 11, comprising:
an information returning unit that sends a networking failure message to the application program.

13. The system of claim 11, comprising:
a setting unit that sets one or more networking control commands allowing or prohibiting access to the mobile network.

14. The system of claim 13, wherein the request discarding unit comprises:
a request discarding subunit that intercepts and discards the request to access the mobile network when detecting the request to access the mobile network if and only if there is a set networking control command prohibiting access to the mobile network.

15. The system of claim 13, comprising:
a request sending unit that sends the request to access the mobile network to the API when detecting the request to access the mobile network if and only if there is a set networking control command allowing access to the mobile network.

16. The system of claim 13, comprising:

a request sending unit that sends the request to access the mobile network to the API when detecting the request to access the mobile network if there is no set networking control command prohibiting access to the mobile network.

17. The system of claim 11, wherein the mobile network comprises at least one of: a GPRS network, a WCDMA network, a CDMA2000 network, a TD-SCDMA network, and a TD-LTE network.

18. The system of claim 11, wherein
the request monitoring unit comprises a request monitoring subunit that monitors the requests to access the mobile network sent from the application program to the API via a set HOOK function, and

the request discarding unit comprises a request discarding subunit that intercepts and discards the request to access the mobile network via the set HOOK function when detecting the request to access the mobile network.

1/5

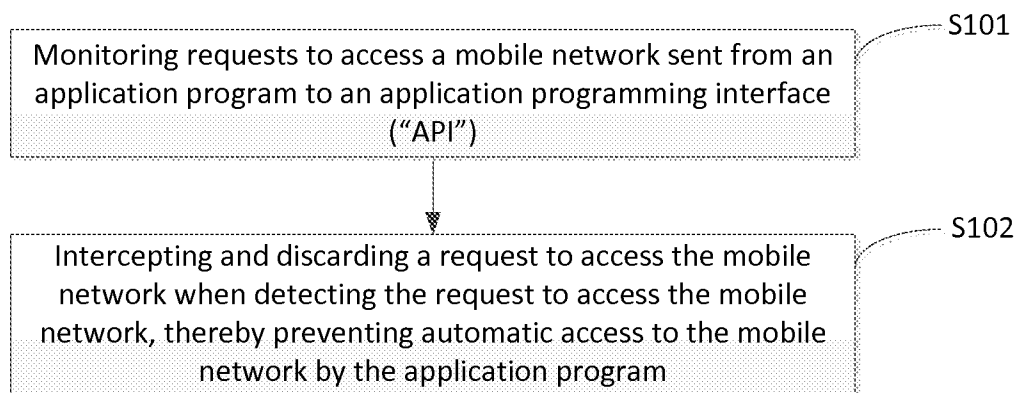


FIG. 1

2/5

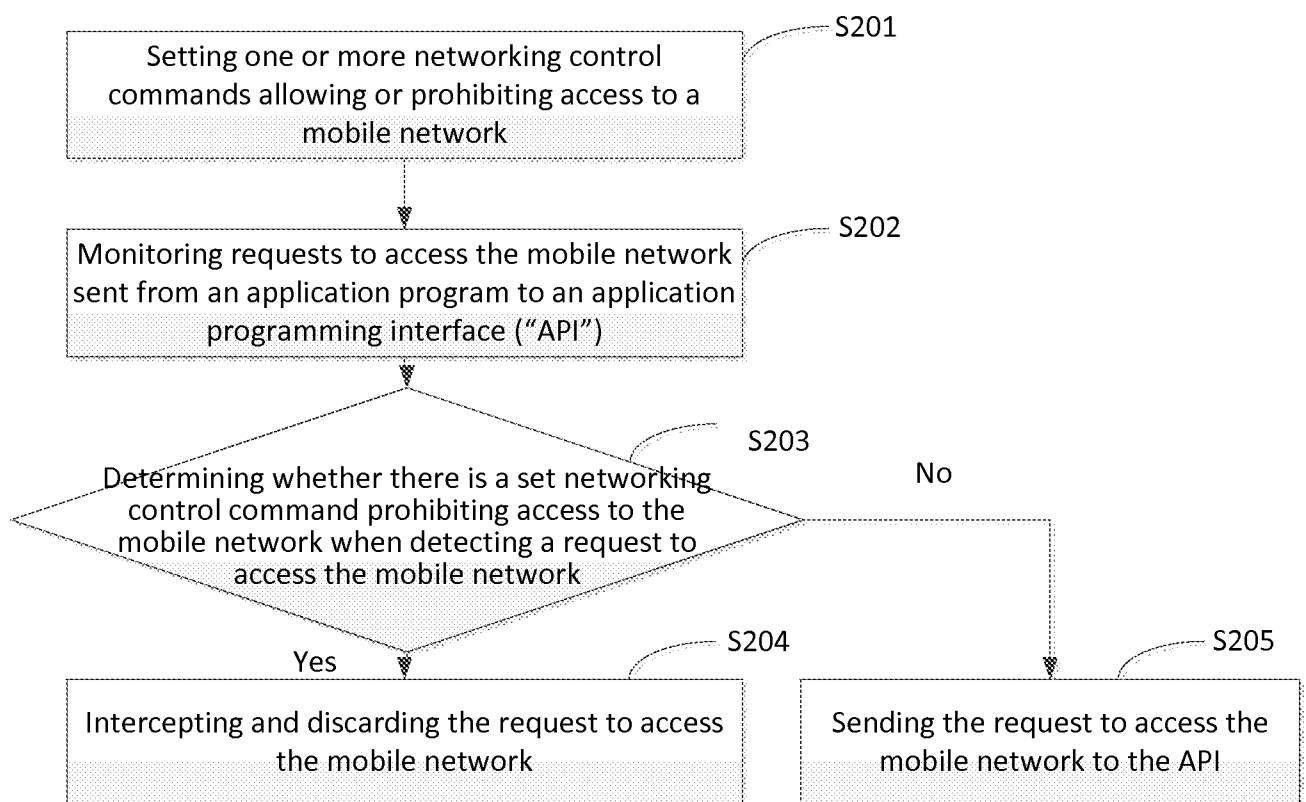


FIG. 2

3/5

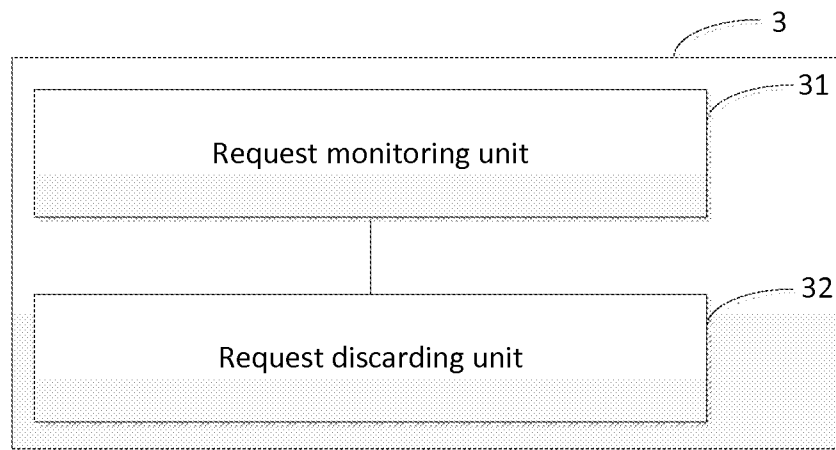


FIG. 3

4/5

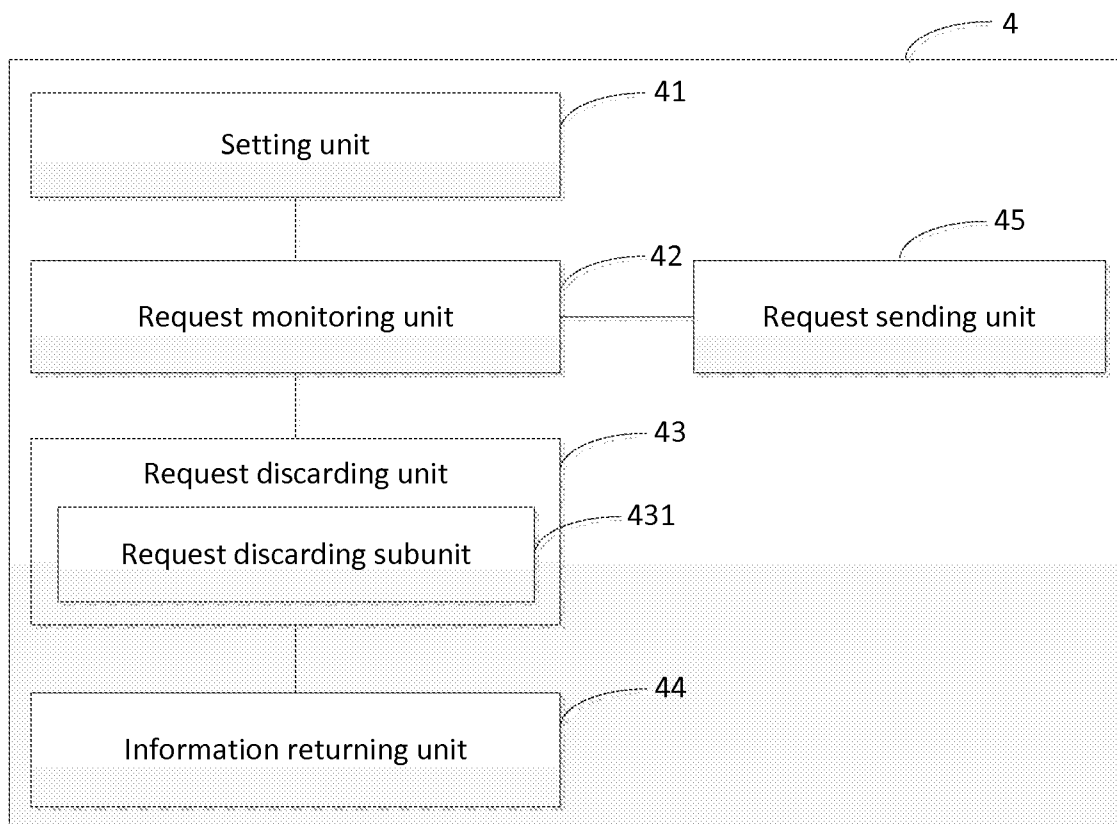


FIG. 4

5/5

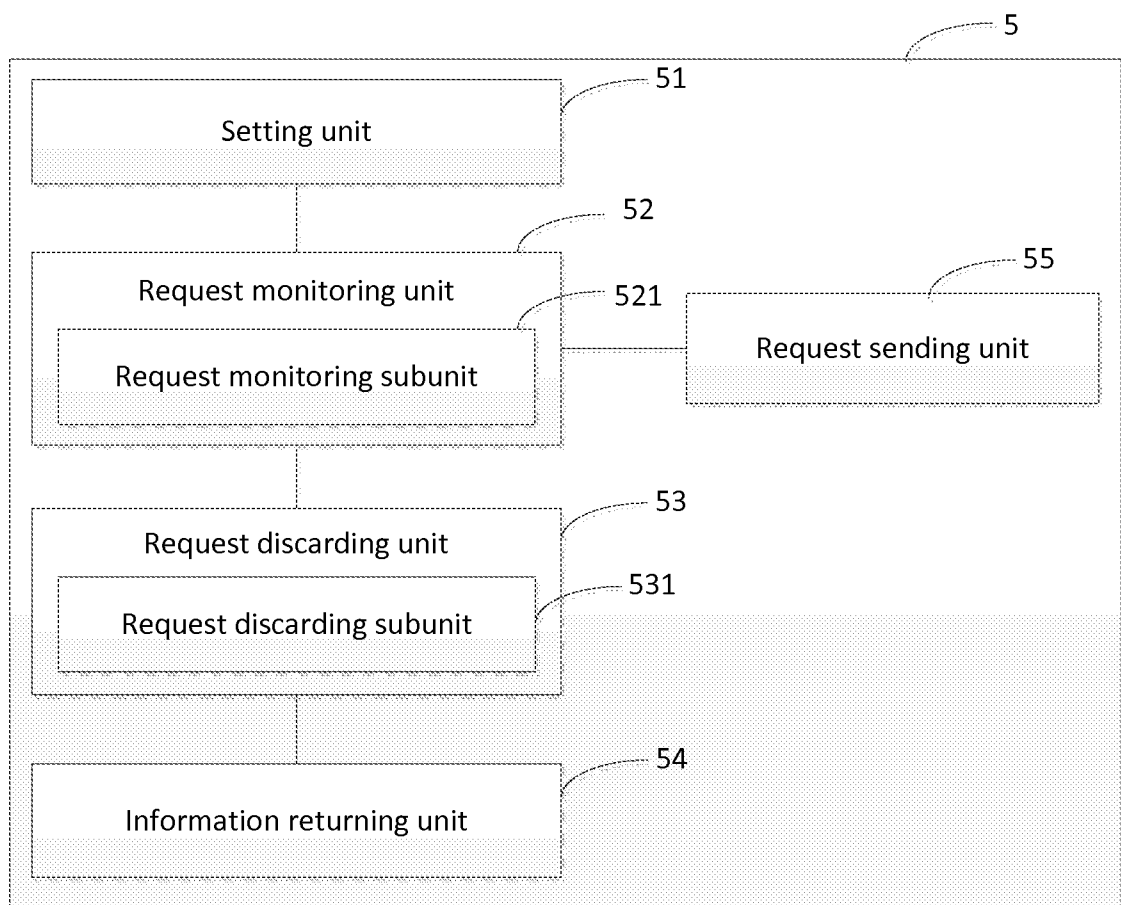


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/082265

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/46(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: G06F 9/-

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)

CNPAT,CNKI,WPLEPODOC: application, program, network+, monitor+, request+, mobile, access+, API, intercept+, prevent+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101355459A (BEIJING INSTITUTE OF TECHNOLOGY) 28 January 2009(28.01.2009) See description, page 2, paragraph 2 to page 5, paragraph 1 and figures 1-5	1-18
A	CN102257760A (NORTEL NETWORKS LTD.) 23 November 2011(23.11.2011) See the whole document	1-18
A	US2005/0195774A1 (CHENNIKARA Jasmine et al.) 08 September 2005(08.09.2005) See the whole document	1-18
A	US2008/0177647A1 (VEENSTRA John W.) 24 July 2008(24.07.2008) See the whole document	1-18

☐ 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 06 November 2013 (06.11.2013)	Date of mailing of the international search report 05 Dec. 2013 (05.12.2013)
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 BAI,Lushuang Telephone No. (86-10)62413918

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/082265

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101355459A	28.01.2009	None	
CN102257760A	23.11.2011	US2010/0161960A1	24.06.2010
		WO2010/069058A1	24.06.2010
		EP2359529A1	24.08.2011
		CA2746341A1	24.06.2010
		KR20110098824A	01.09.2011
		JP2012512573A	31.05.2012
		INCHENP201104154E	07.09.2012
		RU2011124586A	27.01.2013
US2005/0195774A1	08.09.2005	WO2005/084320A2	15.09.2005
US2008/0177647A1	24.07.2008	WO2008/089340A2	24.07.2008