

(51) International Patent Classification:
H04L 29/06 (2006.01)(21) International Application Number:
PCT/CN2013/090040(22) International Filing Date:
20 December 2013 (20.12.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201310244553.7 19 June 2013 (19.06.2013) 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) Inventors: **NIU, Dongsheng**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN). **WANG, Wanxin**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN). **KONG, Li**; Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518000 (CN).(74) Agent: **ADVANCE CHINA IP LAW OFFICE**; Room 3901, No.85 Huacheng Avenue, Tianhe District, Guangzhou, Guangdong 510623 (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, DEVICE AND SYSTEM FOR DATA DOWNLOADING

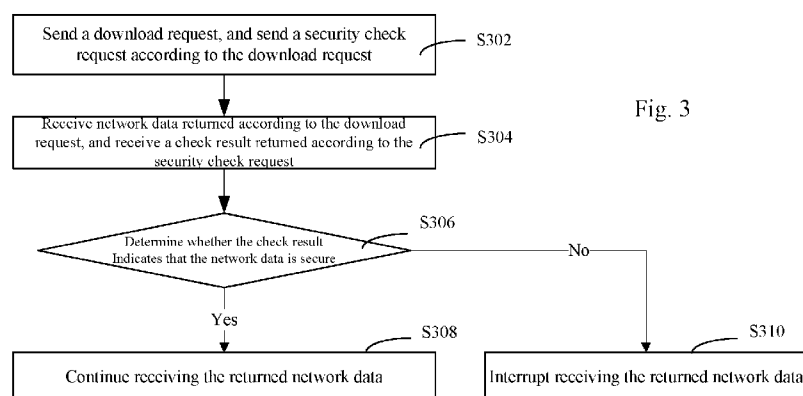


Fig. 3

(57) **Abstract:** A method for data downloading is provided, the method including: sending a download request, and sending a security check request according to the download request; receiving network data returned according to the download request, and receiving a check result returned according to the security check request; and determining whether the check result indicates that the network data is secure; if yes, then continue receiving the returned network data, and if no, interrupt receiving the returned network data. In addition, a device and a system for data downloading are provided. When downloading network data using the above method, device and system, it is necessary to perform security check to the network data. If the network data is secure, continue receiving network data returned according to the download request; and if the network data is insecure, the interrupt receiving network data returned according to the download request. This improves the security of data download.

METHOD, DEVICE AND SYSTEM FOR DATA DOWNLOADING

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims the priority benefit of Chinese Patent Application No. 201310244553.7, filed on June 19, 2013, the contents of which are incorporated by reference herein in their entirety for all purposes.

FIELD OF THE INVENTION

The present disclosure relates generally to the field of data security, and more particularly to a method, device and system for data downloading.

BACKGROUND OF THE INVENTION

With the development of network technology, accessing the network has become a part of people's lives. People are used to access the Internet via a browser installed in a mobile terminal, and download data from the Internet via the browser. For example, download text information from the Internet and store it in the mobile terminal; or, download installation package of applications from the Internet and install them in the mobile terminal.

However, it is found that the data from the network is not absolutely secure, and there may be a virus, which would be a security risk when downloaded to a terminal.

Therefore, heretofore unaddressed needs exist in the art to address the aforementioned deficiencies and inadequacies.

SUMMARY OF THE INVENTION

To address the aforementioned deficiencies and inadequacies, there is a need to provide a method, device and system for data downloading, which can improve the security of data download.

According to one aspect of the disclosure, a method for data downloading includes:

sending a download request, and sending a security check request according to the download request;

receiving network data returned according to the download request, and receiving a check result returned according to the security check request; and

determining whether the check result indicates that the network data is secure; if yes, then continue receiving the returned network data, and if no, interrupt receiving the returned network data.

According to yet another aspect of the disclosure, a device for data downloading includes:

a sending module, configured to send a download request, and to send a security check request according to the download request;

a receiving module, configured to receive network data returned according to the download request, and to receive a check result returned according to the security check request; and

a determining module, configured to determine whether the check result indicates that the network data is secure;

5

When downloading network data using the above method, device and system, it is necessary to perform security check to the network data. If the network data is secure, then continue receiving network data returned according to the download request; and if the network data is insecure, the interrupt receiving network data returned according to the download request. This improves the security of data download.

10

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram showing a system for data downloading according to an embodiment of the present disclosure.

15

Fig. 2 is a schematic diagram showing a system for data downloading according to another embodiment of the present disclosure.

Fig. 3 is a diagram showing a method for data downloading according to an embodiment of the present disclosure.

20

Fig. 4 is a diagram showing a method for data downloading according to another embodiment of the present disclosure.

Fig. 5 is a diagram showing a method for data downloading according to another embodiment of the present disclosure.

Fig. 6 is a diagram showing a method for data downloading according to another embodiment of the present disclosure.

25

Fig. 7 is a diagram showing a method for data downloading according to another embodiment of the present disclosure.

Fig. 8 is a structural schematic diagram showing a device for data downloading according to an embodiment of the present disclosure.

30

DETAILED DESCRIPTION

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.

35

Fig. 1 is a schematic diagram showing a system for data downloading according to an embodiment of the present disclosure. The system for data downloading includes a mobile

terminal 120, a target server 140, and a security server 160. The mobile terminal 120 can be a smart phone, tablet PC, e-book reader, laptop, etc. Network data can be downloaded from the target server 140 via a browser in the mobile terminal 120.

The interaction between components of the system is as follows.

- 5 (1a) The mobile terminal 120 is configured to send to the target server 140 a download request, to send to the security server 160 a security check request, and to receive network data returned from the target server 140 according to the download request.

Specifically, the security check request may contain a link address for downloading the network data. The network data received by the mobile terminal 120 according to the download
10 request is a portion of a complete piece of network data, such as header portion of file data or other portion thereof.

Furthermore, the received network data may also be a complete piece of network data. When the received network data is detected to be insecure, then it may not be saved.

- 15 (1b) The security server 160 is configured to check the security of the network data according to the security check request to obtain a check result, and to return the check result to the mobile terminal 120.

The security server 160 may request the target server 140 for corresponding network data according to the link address for downloading contained in the security check request, and then check the security of the network data corresponding to the link address to obtain a check result.
20 The check result can be that the network data is secure or insecure. Secure network data means that there is no virus in the network.

- (1c) The mobile terminal 120 is further configured to, when it is determined that the check result indicates that the network data is secure, continue receiving network data returned from the target server 140 according to the download request, and when it is determined that the network
25 data is insecure, interrupt receiving network data returned from the target server 140 according to the download request, and to send a prompt of whether to receive the returned network data.

The prompt may be text, picture or a combination thereof. The prompt can be displayed on the mobile terminal 120 in the form of a pop-up window, or in a browser window in the form of web content, or displayed in the form of a prompt bar. When displayed in the form of a pop-up
30 window, its suggesting effect is more pronounced. On the other hand, when displayed in the form of a prompt bar, less data information would be needed to obtain through an asynchronous request, rather than sending a synchronization request to the security server. This saves the network resources.

When the mobile terminal 120 receives a user instruction of continuing receiving the returned
35 network data triggered according to the prompt, it continues receiving the network data returned from the target server 140; when the mobile terminal 120 receives a user instruction of interrupting receiving the returned network data triggered according to the prompt, it interrupts

receiving the network data returned from the target server 140.

When downloading, by a mobile terminal, network data from a target server using the above system, it is necessary to perform security check to the network data. If the network data is secure, then the mobile terminal continues receiving network data downloaded from the target server; and if the network data is insecure, then the mobile terminal interrupts receiving network data downloaded from the target server. This improves the security of data download.

Fig. 2 is a schematic diagram showing a system for data downloading according to another embodiment of the present disclosure. The system includes, in addition to a mobile terminal 120, a target server 140 and a security server 160, a proxy server 130. The interaction between components of the system according to the embodiment is as follows.

(2a) The mobile terminal 120 is configured to send to the proxy server 130 a download request.

(2b) The proxy server 130 is configured to download network data from the target server 140 according to the download request, and to send to the security server 160, a security check request according to the download request.

(2c) The security server 160 is configured to check the security of the network data according to the security check request to obtain a check result, and to return the check result to the proxy server 130.

Specifically, the security check request may contain a link address for downloading the network data.

The security server 160 may request the target server 140 for corresponding network data according to the link address for downloading contained in the security check request, and then check the security of the network data corresponding to the link address to obtain a check result. The check result can be that the network data is secure or insecure. Secure network data means that there is no virus in the network.

(d) The proxy server 130 is further configured to send the check result to the mobile terminal 120.

(2e) The proxy server 130 is further configured to, when it is determined by the mobile terminal 120 that the check result indicates that the network data is secure, continue receiving network data returned from the target server 140 according to the download request, and when it is determined that the check result indicates that the network data is insecure, interrupt receiving network data returned from the target server 140 according to the download request, and to send to the mobile terminal a prompt of whether to receive the returned network data.

Specifically, the mobile terminal 120 is further configured to determine whether the content in a predetermined position of the check result packet indicates that the network data is secure. In the check result packet, the content in a predetermined position can be set as indicating whether the network data is secure, such as content set in the head or tail position of a packet indicating

whether the network data is secure.

The prompt may be text, picture or a combination thereof. The prompt can be displayed on the mobile terminal 120 in the form of a pop-up window, or in a browser window in the form of web content, or displayed in the form of a prompt bar. When displayed in the form of a pop-up
5 window, its suggesting effect is more pronounced. On the other hand, when displayed in the form of a prompt bar, less data information would be needed to obtain through an asynchronous request, rather than sending a synchronization request to the security server, which saves the network resources.

When the mobile terminal 120 receives a user instruction of continuing receiving the returned
10 network data triggered according to the prompt, it continues receiving the network data returned from the target server 140; when the mobile terminal 120 receives a user instruction of interrupting receiving the returned network data triggered according to the prompt, it interrupts receiving the network data returned from the target server 140. When downloading, by the mobile terminal 120, network data from the target server 140 using the above system, it is
15 necessary to download network data from the target server 140 firstly by the proxy server 130, and then initiate a security check request by the proxy server 130 to the security server 160. The security server 160 performs security check to the network data. If the network data is secure, then the proxy server 130 continues receiving network data returned from the target server 140; and if the network data is insecure, then the proxy server 130 interrupts receiving network data
20 returned from the target server 140. The security risk of network data will be firstly assumed by the proxy server 130, which reduces the risk of insecurity on the mobile terminal 120, and improves the security of the data download.

In other embodiments, even if the above system includes the proxy server 130, it is also possible to send a security check request to the security server 160 at the same time of receiving
25 by the proxy server 130 the network data corresponding to the download request. When the network data is secure, the proxy server 130 then receives the downloaded network data from the target server 140. In addition, if the network data requested by the download request exists in the proxy server 130, then directly check to see whether the network data in the proxy server 130 is secure, without the need to download from the target server 140. When it is secure, the network
30 data is returned to the mobile terminal 120.

In other embodiments, the function of the proxy server 130 and the security server 160 may be performed by a computer, such that the mobile terminal 120 sends to the security server 160 a download request, and sends to the security server 160 a security check request according to the download request. The secure server 160 receives network data returned from the target server
35 140 according to the download request, and then performs security check to the network data and returns the check result to the mobile terminal 120. The mobile terminal 120 determines whether the check result indicates that the network data is secure; if yes, then the security server 160

continues receiving network data returned from the target server 140; and if no, then security server 160 interrupts receiving network data returned from the target server 140. The secure network data received by the security server 160 can then be returned to the mobile terminal 120. Thus, the security risk of network data will be firstly assumed by the security server 160, which
5 reduces the risk of insecurity in the mobile terminal 120, and improves the security of the data download.

In addition, when the security server 160 finishes downloading the network data corresponding to the download request, or when the network data corresponding to the download request download request exists in the security server 160, the security server 160 will
10 automatically detects the security of the network data, and returns directly to the mobile terminal 120 the network data when the network data is secure.

In other embodiments, the network data corresponding to the download request may be cached in the security server 160. Next time when the mobile terminal 120 requests to download the same network data, the security server 160 may directly perform security check to the
15 network data to be downloaded, and return the check result more quickly, thus improving the check efficiency.

Fig. 3 is a diagram showing a method for data downloading according to an embodiment of the present disclosure. The method can be applied to a mobile terminal, which can be a smart phone, tablet PC, e-book reader, laptop, etc.

20 The method includes the following steps.

Step S302, sending a download request, and sending a security check request according to the download request.

Specifically, open a browser in the mobile terminal 120, receive a trigger to the download link address in the browser, send a download request to the target server 140, and send a security
25 check request to the security server 160 at the time of sending the download request. The security check request may contain a link address for downloading the network data.

Step S304, receiving network data returned according to the download request, and receiving a check result returned according to the security check request.

Specifically, the mobile terminal 120 receives a portion of the network data returned from the
30 target server 140 according to the download request. The security server 160 requests the target server for network data corresponding to the link according to the security check request, and performs security check to the network data to obtain a corresponding check result. The check result can be that the network data is secure or insecure. Secure network data means that there is no virus in the network.

35 Step S306, determining whether the check result indicates that the network data is secure; if yes, then perform Step S308, and if no, then perform Step S310.

Step S308, continuing receiving the returned network data.

Step S310, interrupting receiving the returned network data.

The mobile terminal 120 determines whether the check result indicates that the network data is secure; if yes, then continue receiving network data returned from the target server 140 according to the download request; and if no, then interrupt receiving network data returned from the target server 140 according to the download request, and send a prompt of whether to receive the returned network data.

Determine whether the content in a predetermined position of the check result packet indicates that the network data is secure. In the check result packet, the content in a predetermined position can be set as indicating whether the network data is secure, such as content set in the head or tail position of a packet indicating whether the network data is secure. Using this way to determine the check result will be more convenient. The prompt may be text, picture or a combination thereof. The prompt can be displayed on the mobile terminal 120 in the form of a pop-up window, or in a browser window in the form of web content, or displayed in the form of a prompt bar. When displayed in the form of a pop-up window, its suggesting effect is more pronounced. On the other hand, when displayed in the form of a prompt bar, less data information would be needed to obtain through an asynchronous request, rather than sending a synchronization request to the security server, which saves the network resources.

Furthermore, the method includes, after the step of sending a prompt of whether to receive the returned network data, the step of: when receiving a user instruction of continuing receiving the returned network data triggered according to the prompt, continue receiving the network data returned from the target server; when receiving a user instruction of interrupting receiving the returned network data triggered according to the prompt, interrupt receiving the network data returned from the target server.

When downloading network data using the above method, it is necessary to perform security check to the network data. If the network data is secure, then continue receiving network data returned according to the download request; and if the network data is insecure, then interrupt receiving network data returned according to the download request. This improves the security of data download. Upon the prompt, whether to receive the returned network data is determined based on the user selection, which is more flexible.

Fig. 4 is a diagram showing a method for data downloading according to another embodiment of the present disclosure. The difference to the method in Fig. 3 lies in the use of a proxy server. That is, download the corresponding network data from a target server using a proxy server, then send a security check request to the security server by the proxy server in place of the mobile terminal, and then download network data from the proxy server by the mobile terminal. As a result, the risk of insecurity on the mobile terminal is reduced.

Step S402, sending to a proxy server 130 a download request, and sending by the proxy server a security check request according to the download request.

Specifically, the mobile terminal 120 sends a download request to the proxy server 130.

Step S402, receiving, by the proxy server 130, network data returned from the target server according to the download request, and receiving the check result returned by the proxy server 130.

5 The proxy server 130 downloads from the target server 140 a portion of the network data according to the download request, sends a security check request to the security server 160 according to the download request, and receives a check result, the result being obtained by checking the security of the network data according to the security check request, and returns the check result to the mobile terminal 120.

10 The security check request may contain a link address for downloading the network data.

The security server 160 may request the target server 140 for corresponding network data according to the link address for downloading contained in the security check request, and then check the security of the network data corresponding to the link address to obtain a check result. The check result can be that the network data is secure or insecure. Secure network data means
15 that there is no virus in the network.

Step S406, determining whether the check result indicates that the network data is secure ; if yes, then perform Step S408, and if no, then perform Step S410.

Specifically, the mobile terminal 120 is further configured to determine whether the content in a predetermined position of the check result packet indicates that the network data is secure. In
20 the check result packet, the content in a predetermined position can be set as indicating whether the network data is secure, such as content set in the head or tail position of a packet indicating whether the network data is secure.

Step S408, continuing receiving, by the proxy server 130, network data returned from the target server 140 according to the download request.

25 Step S410, interrupting receiving, by the proxy server 130, network data returned from the target server 140 according to the download request.

In addition, the method further includes, after interrupting the receiving, the step of: sending a prompt of whether to receive the returned network data.

The prompt may be text, picture or a combination thereof. The prompt can be displayed on the
30 mobile terminal 120 in the form of a pop-up window, or in a browser window in the form of web content, or displayed in the form of a prompt bar. When displayed in the form of a pop-up window, its suggesting effect is more pronounced. On the other hand, when displayed in the form of a prompt bar, less data information would be needed to obtain through an asynchronous request, rather than sending a synchronization request to the security server, which saves the
35 network resources.

Furthermore, the method includes, after sending the prompt, the step of: when receiving a user instruction of continuing receiving the returned network data triggered according to the prompt,

continue receiving the network data returned from the target serve; and when receiving a user instruction of interrupting receiving the returned network data triggered according to the prompt, interrupt receiving the network data returned from the target server.

Fig. 5 is a diagram showing a method for data downloading according to another embodiment of the present disclosure. The difference to the method in Fig. 4 lies in the use of a mobile terminal. That is, the download request and the security check request are all sent by a mobile terminal.

The method for data downloading includes the following steps.

Step S502, sending a download request to a proxy server 130, and sending a security check request to a security server 160 according to the download request.

Step S504, receiving, by the proxy server 130, network data returned from a target server 140 according to the download request, and receiving a check result returned by the security server 160 according to the security check request.

Specifically, the proxy server 130 firstly downloads from the target server 140 a portion of network data according to the download request, and then receives a check result returned by the security server 160 according to the security check request. The security check request may contain a link address for downloading the network data. The security server 160 may request the target server 140 for corresponding network data according to the link address for downloading contained in the security check request, and then check the security of the network data corresponding to the link address to obtain a check result. The check result can be that the network data is secure or insecure, and may be returned directly to a mobile terminal 120 without being forwarded by the proxy server. Secure network data means that there is no virus in the network.

Step S506, determining whether the check result indicates that the network data is secure; if yes, then perform Step S508, and if no, then perform Step S510.

Step S508, continuing receiving, by the proxy server 130, network data returned from the target server 140 according to the download request.

Step S510, interrupting receiving by the proxy server 130 network data returned from the target server 140 according to the download request.

In the above method, the download request is sent by the proxy server 130, and the network data is received also by the proxy server 130. This ensures the security of downloading network data by the mobile terminal 120. On the other hand, the security check request is sent by the mobile terminal 120, and the check result is returned by the security server 160 directly to the mobile terminal. This reduces the intermediate transit links, saving time and network resources.

Fig. 6 is a diagram showing a method for data downloading according to another embodiment of the present disclosure. The difference to the method in Fig. 4 lies in that the mobile terminal sends to the security server the download request and the security check request.

The method for data downloading includes the following steps.

Step S602, sending a download request to a proxy server 130, and sending a security check request to a security server 160 according to the download request.

Step S604, receiving, by the security server 160, network data returned from a target server 140 according to the download request, and receiving a check result returned by the security server 160 according to the security check request.

Specifically, the security server 160 receives network data returned from the target server 140 according to the download request, the network data being a portion of a complete piece of network data. The security check request may include a link address for downloading the network data. The security server 160 may request the target server 140 for corresponding network data according to the link address for downloading contained in the security check request, and then check the security of the network data corresponding to the link address to obtain a check result. The check result can be that the network data is secure or insecure. Secure network data means that there is no virus in the network. Secure network data means that there is no virus in the network. The function of the security server 160 and the proxy server 130 is performed by the security server 160, which saves the hardware and reduces the cost thereby.

In addition, when the security server 160 finishes downloading the network data corresponding to the download request, or when the network data corresponding to the download request download request exists in the security server 160, the security server 160 will automatically detects the security of the network data, and returns directly to the mobile terminal 120 the network data when the network data is secure.

Step S606, determining whether the check result indicates that the network data is secure; if yes, then perform Step S608, and if no, then perform Step S610.

Step S608, continuing receiving, by the security server 160, network data returned from the target server 140 according to the download request.

Step S610, interrupting receiving by the security server 160 network data returned from the target server 140 according to the download request.

In addition, the method further includes, after interrupting the receiving, the step of: sending a prompt of whether to receive the returned network data.

In the above method, the download request is sent by the security server 160, and the network data is received also by the security server 160. This ensures the security of downloading network data by the mobile terminal 120.

In the embodiments of Fig. 4, Fig. 5 and Fig. 6, the respective method includes, after the step of sending a prompt, the step of: when receiving a user instruction of continuing receiving the returned network data triggered according to the prompt, continue receiving the returned network data; when receiving a user instruction of interrupting receiving the returned network data triggered according to the prompt, interrupt receiving the returned network data.

In other embodiments, the network data corresponding to the download request may be cached in the security server 160. Next time when the mobile terminal 120 requests to download the same network data, the security server 160 may directly perform security check to the network data to be downloaded, and return the check result more quickly, thus improving the check efficiency.

In one embodiment, as shown in Fig. 7, a method for data downloading includes the following steps.

Step S702, sending a download request, and sending a security check request according to the download request.

Specifically, a mobile terminal 120 sends to a target server 140 a download request, and sends to a security server 160 a security check request according to the download request.

Step S704, receiving network data returned according to the download request, obtaining a security check result by checking the security of network data according to the security check request, and returning the check request.

Specifically, the mobile terminal 120 receives network data returned from the target server according to the download request. The security server 160 obtains a security check result by checking the security of network data according to the security check request, and returns the check request to the mobile terminal 120.

Step S706, determining whether the check result indicates that the network data is secure; if yes, then perform Step S708, and if no, then perform Step S710.

Step S708, continuing receiving the returned network data.

Step S710, interrupting receiving the returned network data.

Specifically, the mobile terminal 120 determines whether the check result indicates that the network data is secure; if yes, then continue receiving network data returned from the target server 140 according to the download request; and if no, then interrupt receiving network data returned from the target server 140 according to the download request, and send a prompt of whether to receive the returned network data.

The prompt may be text, picture or a combination thereof. The prompt can be displayed on the mobile terminal 120 in the form of a pop-up window, or in a browser window in the form of web content, or displayed in the form of a prompt bar. When displayed in the form of a pop-up window, its suggesting effect is more pronounced. On the other hand, when displayed in the form of a prompt bar, less data information would be needed to obtain through an asynchronous request, rather than sending a synchronization request to the security server, which saves the network resources.

In addition, when receiving a user instruction of continuing receiving the returned network data triggered according to the prompt, the mobile terminal 120 continues receiving the network data returned from the target server 140; when receiving a user instruction of interrupting

receiving the returned network data triggered according to the prompt, the mobile terminal 120 interrupts receiving the network data returned from the target server 140.

Using the above method, when downloading network data from a target server by a mobile terminal, it is necessary to perform security check to the network data by a security server. If the network data is secure, then the mobile terminal continues receiving network data returned according to the download request; and if the network data is insecure, then the mobile terminal interrupts receiving network data returned according to the download request. This improves the security of data download.

In one embodiment, the proxy server firstly downloads from a target server the corresponding network data, and then the proxy server, in place of the mobile terminal, sends a security check request to the security server. The proxy server downloads the network data from the target from the server. When the network data is secure, the mobile terminal then downloads from the proxy server the network data. As a result, the risk of insecurity on the mobile terminal is reduced.

Step S702 includes: sending, by the mobile terminal 120, a download request to the proxy server 130; sending, by the proxy server 130, a security check request to the security server 160 according to the download request.

Step S704 includes: receiving, by the proxy server 130, network data returned from the target server 140 according to the download request; checking, by the security server 160, the security of the network data according to the security check request, and returning the check result to the proxy server 130; sending, by the proxy server 130, the check result to the mobile terminal 120.

Step S706 includes: determine, by the mobile terminal 120, whether the check result indicates that the network data is secure; if yes, then continue receiving, by the proxy server 130, network data returned from the target server 140; and if no, then interrupt receiving, by the proxy server 130, network data returned from the target server 140.

Further, in other embodiments, the mobile terminal 120 may also send the download request to the proxy server 130, and send the security check request to the security server 160 according to the download request. The security server 160 checks the security of the network data according to the security check request, and returns the check result to the mobile terminal 120.

In one embodiment, the mobile terminal sends a download request and a security check request to the security server.

Step S702 includes: the mobile terminal 120 sends a download request to the security server 160, and sends a security check request to the security server 160 according to the download request.

Step S704 includes: the secure server 160 receives network data returned from the target server 140, performs security check to the network data according to the security check request and returns the check result to the mobile terminal 120.

Step S706 includes: the mobile terminal 120 determines whether the check result indicates

that the network data is secure; if yes, then the security server 160 continues receiving network data returned from the target server 140; and if no, then security server 160 interrupts receiving network data returned from the target server 140.

Fig. 8 is a structural schematic diagram showing a device for data downloading according to an embodiment of the present disclosure. The device is implemented on a mobile terminal. The device includes a sending module 820, a receiving module 840 and a determining module 860.

The sending module 820 is configured to send a download request, and send a security check request according to the download request.

Specifically, open a browser in the mobile terminal, and receive a trigger to the download link address in the browser. The sending module 820 sends a download request to the target server 140, and sends a security check request to the security server 160 at the time of sending the download request. The security check request may contain a link address for downloading the network data.

The receiving module 840 is configured to receive the network data returned according to the download request, and receive a check result returned according to the security check request.

Specifically, the receiving module 840 receives a portion of the network data returned from the target server 140 according to the download request. The security server 160 requests the target server for network data corresponding to the link according to the security check request, and performs security check to the network data to obtain a corresponding check result. The check result can be that the network data is secure or insecure. Secure network data means that there is no virus in the network. The receiving module 840 receives the returned check result.

The determining module 860 is configured to determine whether the check result indicates that the network data is secure.

Specifically, the determining module 860 is further configured to determine whether the content in a predetermined position of the check result packet indicates that the network data is secure. In the check result packet, the content in a predetermined position can be set as indicating whether the network data is secure, such as content set in the head or tail position of a packet indicating whether the network data is secure.

The receiving module 840 is also configured to, when the check result is determined as that the check result indicates that the network data is secure, continue receiving network data returned according to the download request, and the check result is determined as that the network data is insecure, interrupt receiving network data returned according to the download request, and send a prompt of whether to receive the returned network data.

The prompt may be text, picture or a combination thereof. The prompt can be displayed on the mobile terminal in the form of a pop-up window, or in a browser window in the form of web content, or displayed in the form of a prompt bar. When displayed in the form of a pop-up window, its suggesting effect is more pronounced. On the other hand, when displayed in the form

of a prompt bar, less data information would be needed to obtain through an asynchronous request, rather than sending a synchronization request to the security server, which saves the network resources.

The receiving module 840 is further configured to, when receiving a user instruction of continuing receiving the returned network data triggered according to the prompt, continue receiving the network data returned from the target server 140, and receiving a user instruction of interrupting receiving the returned network data triggered according to the prompt, interrupt receiving the network data returned from the target server.

When downloading network data using the above device, it is necessary to perform security check to the network data. If the network data is secure, then continue receiving network data returned according to the download request; and if the network data is insecure, then do not receive network data returned according to the download request. This improves the security of data download. Upon the prompt, whether to receive the returned network data is determined based on the user selection, which is more flexible.

Furthermore, in an embodiment, the sending module 820 is further configured to send to a proxy server a download request, and sends, by the proxy server 130 a security check request according to the download request. The receiving module 840 is further configured to receive, by the proxy server 130, network data returned from the target server 140 according to the download request, and receive the check result returned by the proxy server 130. The determining module 860 is further configured to determine whether the check result indicates that the network data is secure; if yes, then the receiving module 840 is further configured to continue receiving, by the proxy server 130, network data returned from the target server 140 according to the download request; and if no, then the receiving module 840 is further configured to interrupt receiving, by the proxy server 130, network data returned from the target server 140 according to the download request, and send a prompt of whether to receive the returned network data.

Specifically, the sending module 820 is further configured to send to the proxy server a download request, and sends, by the proxy server 130, a security check request to the security server 160 according to the download request. The receiving module 840 is further configured to receive the check result obtained by the security server 160 according to the security check request and returned by the proxy server 130.

The above device for data downloading adopts the way of downloading the corresponding network data from a target server using a proxy server, then sending a security check request to the security server by the proxy server in place of the mobile terminal, and then downloading network data from the proxy server by the mobile terminal. As a result, the risk of insecurity on the mobile terminal is reduced.

Furthermore, in an embodiment, the sending module 820 is further configured to send to the proxy server 130 a download request, and sends to the security server 160 a security check

request according to the download request. The receiving module 840 is further configured to receive, by the proxy server 130, network data returned from the target server 140 according to the download request, and receive the check result returned by the security server 160 according to the security check request. The determining module 860 is further configured to determine whether the check result indicates that the network data is secure; if yes, then the receiving module 840 is also configured to continue receiving, by the proxy server 130, network data returned from the target server 140 according to the download request; and if no, then the receiving module 840 is also configured to interrupt receiving, by the proxy server 130, network data returned from the target server 140 according to the download request, and send a prompt of whether to receive the returned network data.

With the above device, the download request is sent by the proxy server, and the network data is received also by the proxy server. This ensures the security of downloading network data by the mobile terminal. On the other hand, the security check request is sent by the mobile terminal, and the check result is returned by the security server directly to the mobile terminal. This reduces the intermediate transit links, saving time and network resources.

Furthermore, in an embodiment, the sending module 820 is further configured to send to the security server a download request, and sends to the security server a security check request according to the download request. The receiving module 840 is further configured to receive, by the security server 160, network data returned from the target server 140 according to the download request, and receive the check result returned upon sending the security check request by the security server. The determining module 860 is further configured to determine whether the check result indicates that the network data is secure; if yes, then the receiving module 840 is also configured to continue receiving, by the security server 160, network data returned from the target server 140 according to the download request; and if no, then the receiving module 840 is also configured to interrupt receiving, by the security server 160, network data returned from the target server 140 according to the download request, and send a prompt of whether to receive the returned network data. The function of the security server and the proxy server is performed by the security server, which saves the hardware and reduces the cost thereby.

It should be noted that for a person skilled in the art, partial or full process to realize the methods in the above embodiments can be accomplished by related hardware instructed by a computer program, the program can be stored in a computer readable storage medium and the program can include the process of the embodiments of the above methods. Wherein, the storage medium can be a disk, a light disk, a Read-Only Memory or a Random Access Memory, etc.

The embodiments are chosen and described in order to explain the principles of the disclosure and their practical application so as to allow others skilled in the art to utilize the disclosure and various embodiments and with various modifications as are suited to the particular use contemplated. Alternative embodiments will become apparent to those skilled in the art to which the present disclosure pertains without departing from its spirit and scope. Accordingly,

the scope of the present disclosure is defined by the appended claims rather than the foregoing description and the exemplary embodiments described therein.

CLAIMS

1. A method for data downloading, comprising:

5 sending a download request, and sending a security check request according to the download request;
receiving network data returned according to the download request, and receiving a check result returned according to the security check request; and
determining whether the check result indicates that the network data is secure; if yes, then continue receiving the returned network data, and if no, interrupt receiving the returned network
10 data.

2. The method of claim 1, wherein the sending further comprises:

sending to a proxy server a download request, and sending, with the proxy server, a security check request according to the download request;
15 the receiving further comprises:
receiving, with the proxy server, network data returned from a target server according to the download request, and receiving a check result returned with the proxy server; and
the determining further comprises:
determining whether the check result indicates that the network data is secure; if yes, then
20 continue receiving, by the proxy server, network data returned from the target server; and if no, then interrupt receiving, by the proxy server, network data returned from the target server.

3. The method of claim 1, wherein the sending further comprises:

sending to a proxy server a download request, and sending to a security server a security
25 check request according to the download request;
the receiving further comprises:
receiving, with the proxy server, network data returned from a target server according to the download request, and receiving a check result returned by the security server; and
the determining further comprises:
30 determining whether the check result indicates that the network data is secure; if yes, then continue receiving, with the proxy server, network data returned from the target server; and if no, then interrupt receiving, with the proxy server, network data returned from the target server.

4. The method of claim 1, wherein the sending further comprises:

35 sending to a security server a download request, and sending to the security server a security check request according to the download request;
the receiving further comprises:

receiving, with the security server, network data returned from a target server according to the download request, and receiving a check result returned by the security server; and

the determining further comprises:

determining whether the check result indicates that the network data is secure; if yes, then
5 continue receiving, with the security server, network data returned from the target server; and if no, then interrupt receiving, with the security server, network data returned from the target server.

5. The method of any one of claims 1 to 4, wherein the determining further comprises:

determining whether the content in a predetermined position of the check result packet indicates that the network data is secure.

10 6. A method for data downloading, comprising:

sending a download request, and sending a security check request according to the download request;

receiving network data returned according to the download request, checking the security of
15 the network data according to the security check request to obtain a check result, and returning the check result; and

determining whether the check result indicates that the network data is secure; if yes, then continue receiving the returned network data, and if no, interrupt receiving the returned network data.

20 7. The method of claim 6, wherein the sending further comprises:

sending, by a mobile terminal, a download request to a proxy server; and

sending, with the proxy server, a security check request to a security server according to the download request;

25 the receiving further comprises:

receiving, with the proxy server, network data returned from a target server according to the download request,

checking, by the security server, the security of the network data according to the security check request to obtain a check result, and returning the check result to the proxy server; and

30 sending, by the proxy server, the check result to the mobile terminal;

the determining further comprises:

determining, by the mobile terminal, whether the check result indicates that the network data is secure; if yes, then continue receiving, with the proxy server, network data returned from the target server; and if no, then interrupt receiving, with the proxy server, network data returned
35 from the target server.

8. The method of claim 6, wherein the sending further comprises:

sending, by a mobile terminal, a download request to a proxy server, and sending to a security server a security check request according to the download request;

the receiving further comprises:

5 receiving, with the proxy server, network data returned from a target server according to the download request, and

checking, by the security server, the security of the network data according to the security check request to obtain a check result, and returning the check result to the mobile terminal;

the determining further comprises:

10 determining whether the check result indicates that the network data is secure; if yes, then continue receiving, with the proxy server, network data returned from the target server; and if no, then interrupt receiving, with the proxy server, network data returned from the target server.

9. The method of claim 6, wherein the sending further comprises:

15 sending, by a mobile terminal, a download request to a security server, and sending to a security server a security check request according to the download request;

the receiving further comprises:

receiving, with the security server, network data returned from a target server according to the download request, and

20 checking, by the security server, the security of the network data according to the security check request to obtain a check result, and returning the check result to the mobile terminal;

the determining further comprises:

determining whether the check result indicates that the network data is secure; if yes, then continue receiving, with the security server, network data returned from the target server; and if no, then interrupt receiving, with the security server, network data returned from the target server.

25

10. A device for data downloading, comprising:

a sending module, configured to send a download request, and to send a security check request according to the download request;

30 a receiving module, configured to receive network data returned according to the download request, and to receive a check result returned according to the security check request; and

a determining module, configured to determine whether the check result indicates that the network data is secure;

35 the receiving module is further configured to, when determining that the check result indicates that the network data is secure, continue receiving network data returned from the target server, and when determining that the check result indicates that the network data is insecure, interrupt receiving the returned network data.

11. The device of claim 10, wherein the sending module is further configured to send to a proxy server a download request, and to send, with the proxy server, a security check request according to the download request;

the receiving module is further configured to receive, with the proxy server, network data returned from a target server according to the download request, and to receive a check result returned with the proxy server;

the determining module is further configured to determine whether the check result indicates that the network data is secure; and

the receiving module is further configured to, when determining that the check result indicates that the network data is secure, continue receiving, with the proxy server, network data returned from the target server, and when determining that the check result indicates that the network data is insecure, interrupt receiving, with the proxy server, network data returned from the target server.

12. The device of claim 10, wherein the sending module is further configured to send to a proxy server a download request, and to send to a security server a security check request according to the download request;

the receiving module is further configured to receive, with the proxy server, network data returned from a target server according to the download request, and receive a check result returned by the security server according to the security check request;

the determining module is further configured to determine whether the check result indicates that the network data is secure; and

the receiving module is further configured to, when determining that the check result indicates that the network data is secure, continue receiving, with the proxy server, network data returned from the target server, and when determining that the check result indicates that the network data is insecure, interrupt receiving, with the proxy server, network data returned from the target server.

13. The device of claim 10, wherein the sending module is further configured to send to a security server a download request, and to send to a security server a security check request according to the download request;

the receiving module is further configured to receive, with the security server, network data returned from a target server, and to receive the check result returned from the target server;

the determining module is further configured to determine whether the check result indicates that the network data is secure; and

the receiving module is further configured to, when determining that the check result indicates that the network data is secure, continue receiving, with the security server, network

data returned from the target server, and when determining that the check result indicates that the network data is insecure, interrupt receiving, with the security server, network data returned from the target server.

14. The device of any of claims 10 to 13, wherein the determining module is further
5 configured to determine whether the content in a predetermined position of the check result packet indicates that the network data is secure.

15. A system for data downloading, comprising a mobile terminal, a security server, and a target server; wherein,

10 the mobile terminal is configured to send to the target server a download request, and to send to the security server a security check request according to the download request, and to receive from the target server network data returned according to the download request;

the security server is configured to check the security of the network data according to the security check request to obtain a check result, and to return the check result to the mobile
15 terminal; and

the mobile terminal is further configured to, when determining that the check result indicates that the network data is secure, continue receiving network data returned from the target server, and when determining that the check result indicates that the network data is insecure, interrupt receiving network data returned from the target server.

20

16. The system of claim 15, wherein the system further comprises a proxy server;

the mobile terminal is further configured to send a download request to the proxy server;

the proxy server is configured to receive network data returned from the target server according to the download request, to send a security check request to the security server
25 according to the download request, to receive a check result sent by the security server and to send the check result to the mobile terminal; and

the mobile terminal is further configured to determining whether the check result indicates that the network data is secure; when determining that the check result indicates that the network data is secure, the proxy server continues receiving network data returned from the target server,
30 and when determining that the check result indicates that the network data is insecure, the proxy server interrupts receiving network data returned from the target server.

17. The system of claim 15, wherein the system further comprises a proxy server;

the mobile terminal is further configured to send a download request to the proxy server,
35 and to send a security check request to the security server according to the download request;

the proxy server is configured to receive network data returned from the target server according to the download request;

the mobile terminal is further configured to receive the check result returned by the security server according to the security check result, and to determine whether the check result indicates that the network data is secure; and

5 the proxy server is further configured to, when the mobile terminal determines that the check result indicates that the network data is secure, continue receiving network data returned from the target server, and when the mobile terminal determines that the check result indicates that the network data is insecure, interrupt receiving network data returned from the target server.

10 18. The system of claim 15, wherein the mobile terminal is further configured to send a download request to the security server, to send a security check request to the security server according to the download request, to receive the check result returned according to the security check request, and to determine whether the check result indicates that the network data is secure;

15 the security server is configured to receive the network data returned from the target server according to the download request; and

the security server is further configured to, when the mobile terminal determines that the check result indicates that the network data is secure, continue receiving network data returned from the target server, and when the mobile terminal determines that the check result indicates that the network data is insecure, interrupt receiving network data returned from the target server.

20

19. The system of any one of claims 15 to 18, wherein the mobile terminal is further configured to determine whether the content in a predetermined position of the check result packet indicates that the network data is secure.

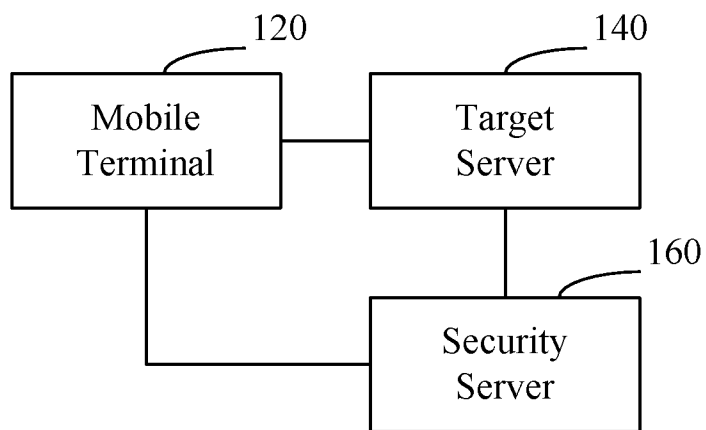


Fig. 1

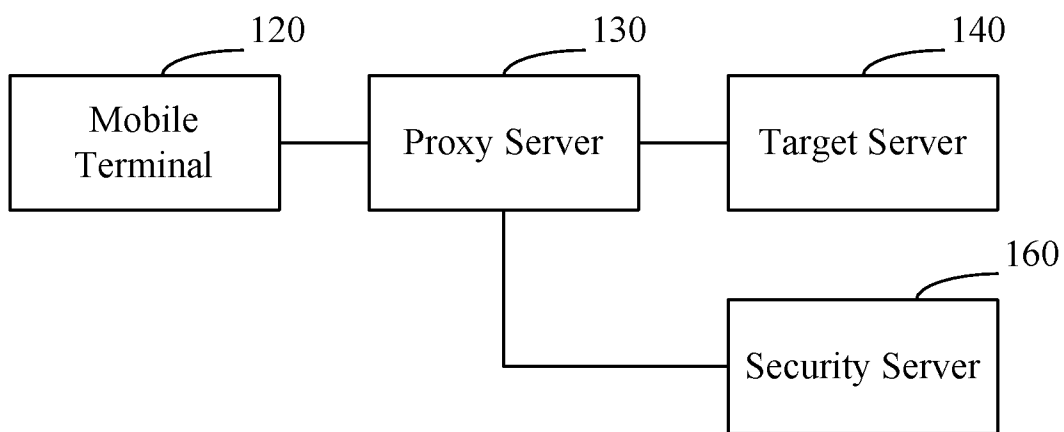


Fig. 2

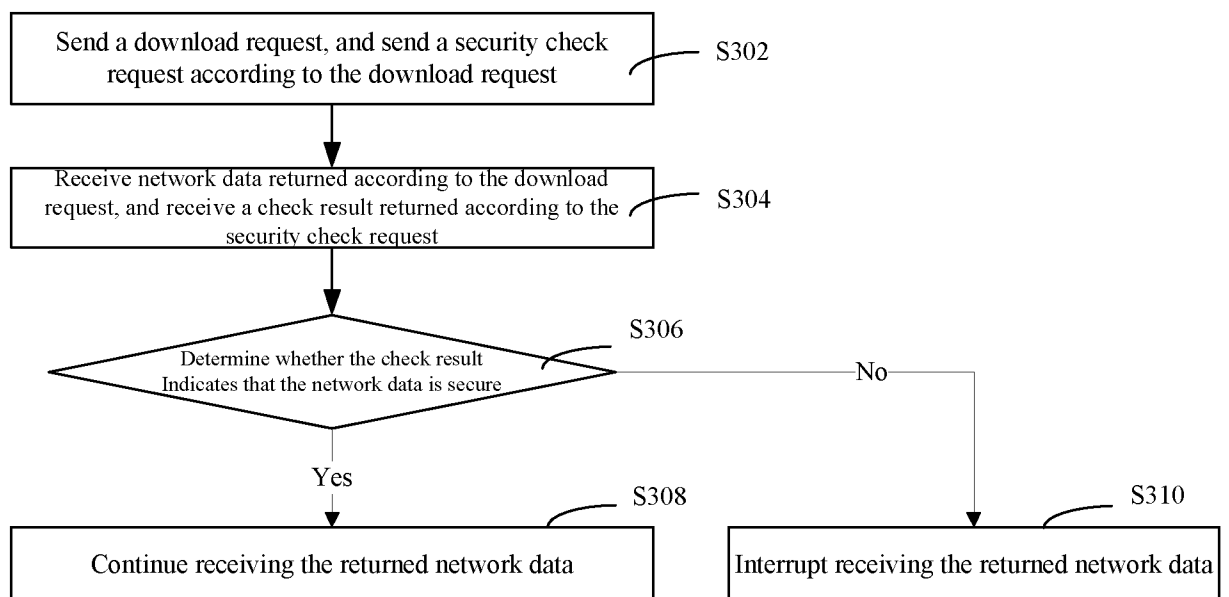


Fig. 3

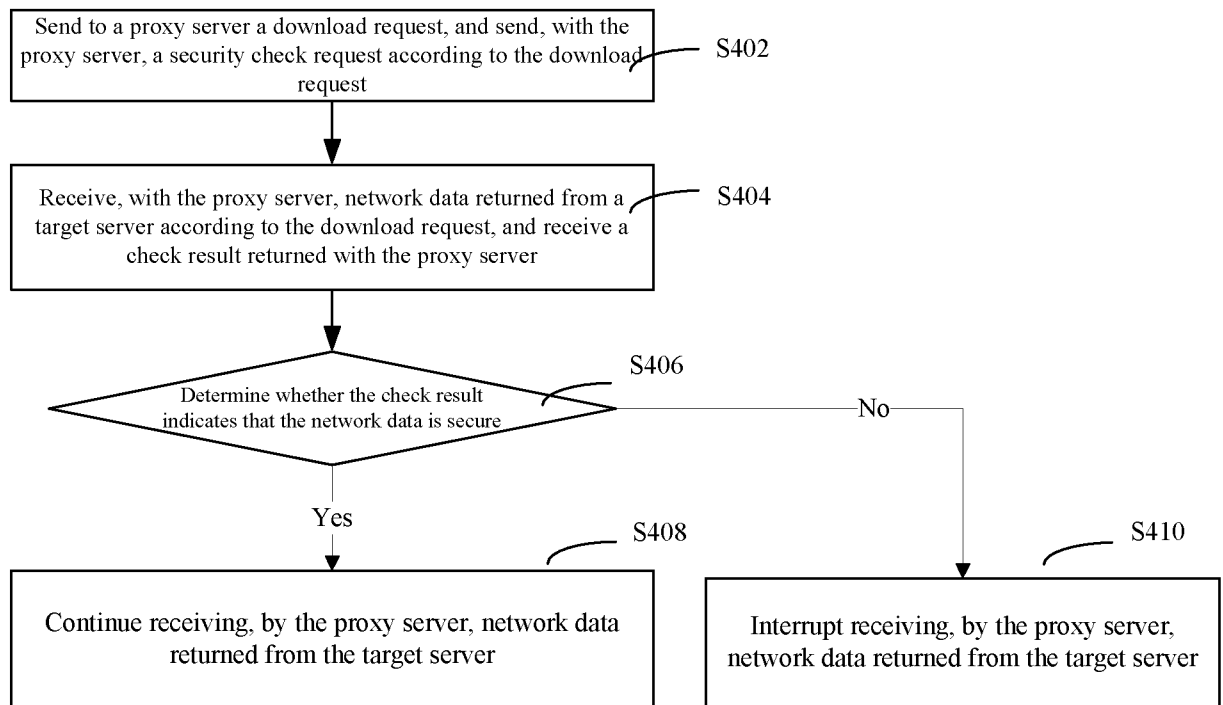


Fig. 4

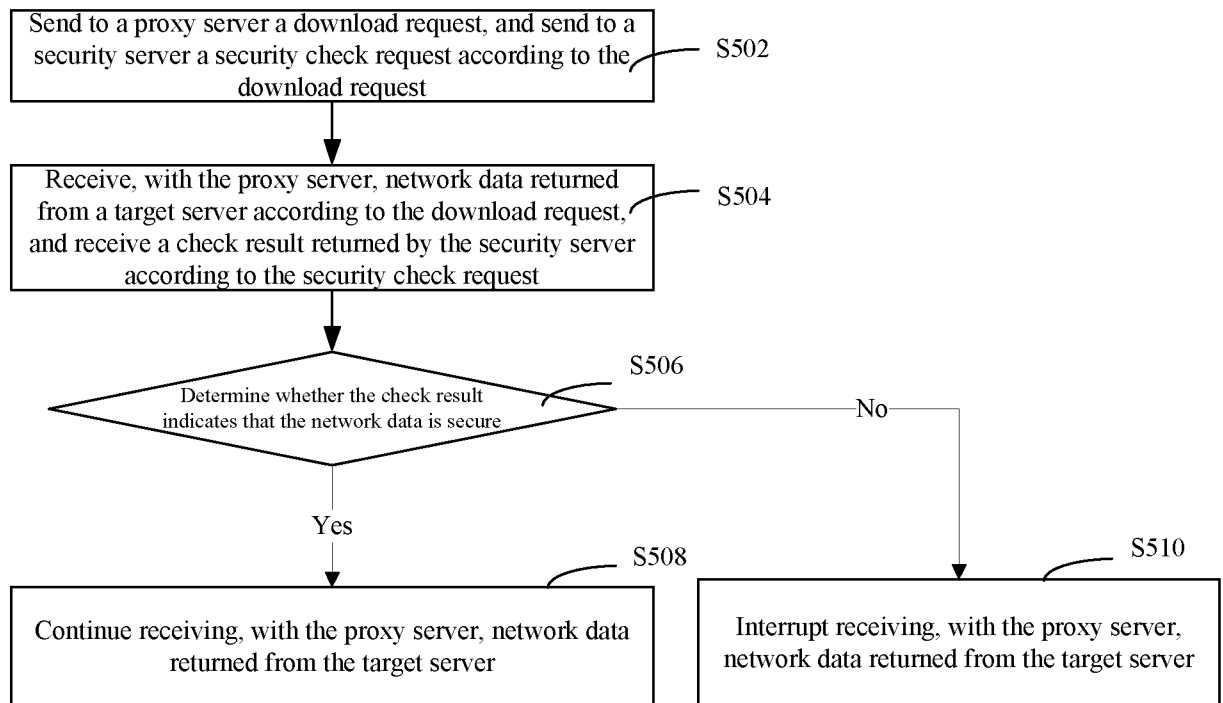


Fig. 5

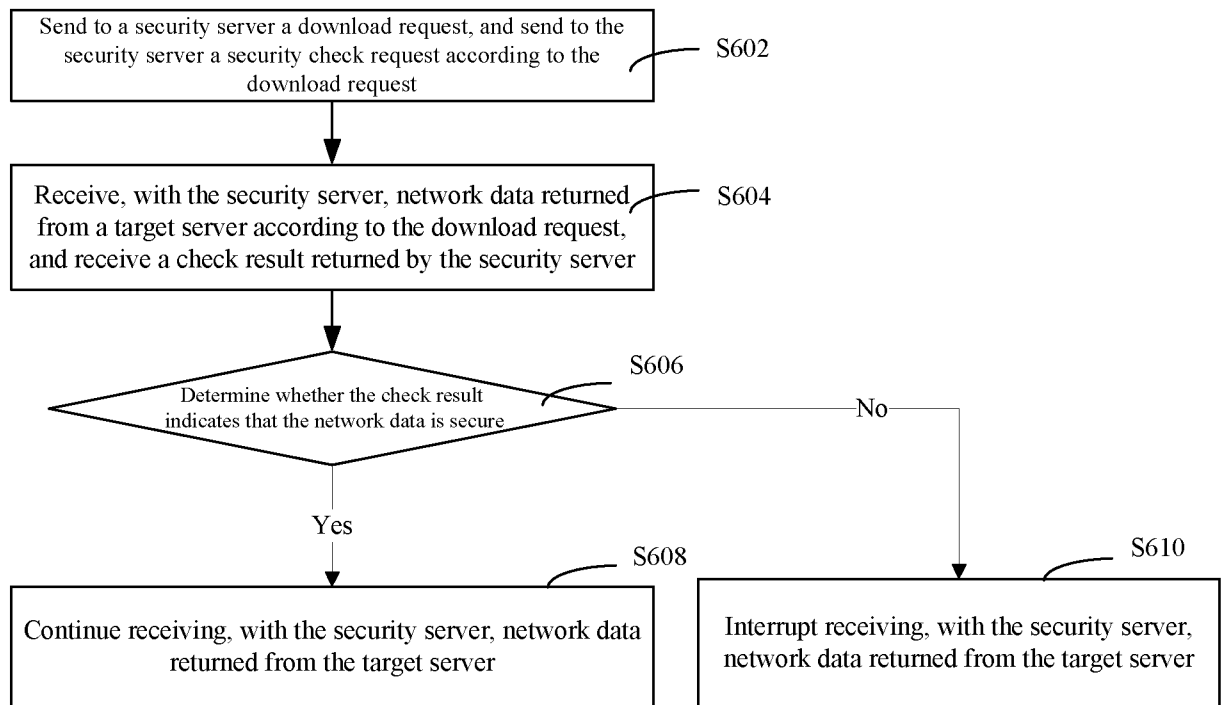


Fig. 6

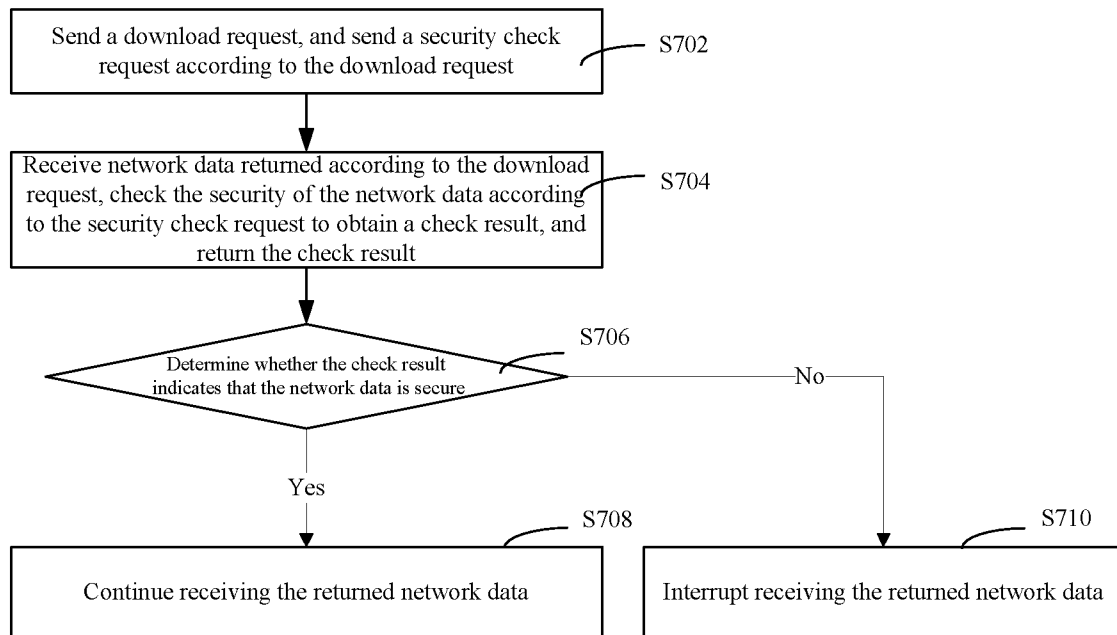


Fig. 7

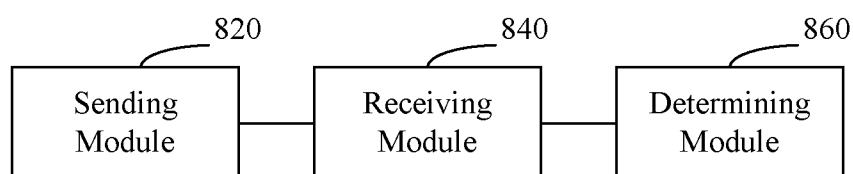


Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/090040

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (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, CNKI, CNTXT, DWPI, VEN: mobile, smart, phone, download+, secure+, request, server, proxy, browser, virus

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102255915 A (ZTE CORPORATION) 23 November 2011 (23.11.2011) see description, paragraphs [0002], [0004], [0005], [0029]-[0034], [0037], [0050]	1, 5, 6, 10, 14, 15, 19
Y	Idem	2-4, 7-9, 11-13, 16-18
Y	CN 101325533 A (SHENZHEN GAOZHENG SOFTWARE CORPORATION LIMITED) 17 December 2008 (17.12.2008) see description, page 1 lines 16-21, page 3 lines 5-8, figure 1	2-4, 7-9, 11-13, 16-18
A	US 2011231517 A1 (SRINIVASAN et al.) 22 September 2011 (22.09.2011) the whole document	1-19

☐ 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 13 March 2014 (13.03.2014)	Date of mailing of the international search report 27 Mar. 2014 (27.03.2014)
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 LI, Xiaoqian Telephone No. (86-10)62089456

International application No.
PCT/CN2013/090040

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