

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



[12] 发明专利申请公布说明书

[21] 申请号 200710100170.7

H04L 12/26 (2006.01)

H04L 29/08 (2006.01)

H04N 7/18 (2006.01)

H04N 5/225 (2006.01)

[43] 公开日 2008 年 1 月 9 日

[11] 公开号 CN 101102234A

[22] 申请日 2007.6.5

[21] 申请号 200710100170.7

[71] 申请人 北京中星微电子有限公司

地址 100083 北京市海淀区学院路 35 号世宁大厦 15 层

[72] 发明人 付 群 谢 律

[74] 专利代理机构 北京德琦知识产权代理有限公司

代理人 宋志强 麻海明

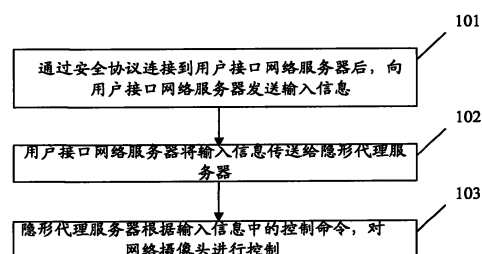
权利要求书 2 页 说明书 9 页 附图 3 页

[54] 发明名称

网络摄像头防监听的控制方法及系统

[57] 摘要

本发明公开了一种网络摄像头防监听的控制方法，该方法建立用户接口网络服务器和隐形代理服务器，该方法还包括：A. 用户端通过安全协议连接到用户接口网络服务器；B. 用户接口网络服务器将输入信息传送给隐形代理服务器；C. 隐形代理服务器根据输入信息中的控制命令，对网络摄像头进行控制。本发明还公开了一种网络摄像头防监听的控制系统。本发明技术方案提高了使用网络摄像头的安全性。



1、一种网络摄像头防监听的控制方法，其特征在于，建立用户接口网络服务器和隐形代理服务器，该方法包括：

- A、用户端通过安全协议连接到用户接口网络服务器；
- B、用户接口网络服务器将输入信息传送给隐形代理服务器；
- C、隐形代理服务器根据输入信息中的控制命令，对网络摄像头进行控制。

2、如权利要求 1 所述的方法，其特征在于，所述用户接口网络服务器为一个或多个；

所述隐形代理服务器为一个或多个。

3、如权利要求 1 所述的方法，其特征在于，步骤 C 所述对网络摄像头进行控制的过程为包括：

- C1、隐形代理服务器向网络摄像头传送输入信息中的控制命令；
- C2、网络摄像头根据控制命令向隐形代理服务器发送相应的反馈信息；
- C3、隐形代理服务器将所述的反馈信息传送给用户接口网络服务器；
- C4、用户接口网络服务器将所述的反馈信息传送给用户端。

4、如权利要求 1 或 3 所述的方法，其特征在于，所述步骤 B 之后，所述步骤 C 之前，该方法进一步包括：

B1、隐形代理服务器判断是否取得对输入信息中指定的网络摄像头的控制，如果是，则执行步骤 C，否则，执行步骤 B2；

B2、隐形代理服务器根据输入信息中验证信息包含的互联网协议地址，采用超文本传输协议查找出与所述互联网协议地址对应的网络摄像头；

B3、隐形代理服务器根据验证信息，进行身份合法性确认，通过确认后产生确认成功的反馈信息，经用户接口网络服务器将反馈信息传送给用户端；

B4、用户端判断是否停止对网络摄像头的控制，如果是，则结束流程，否则，执行步骤 A。

5、如权利要求 3 所述的方法，其特征在于，步骤 A 所述用户端采用统一

资源定位器地址连接到用户接口网络服务器；

步骤 C4 所述用户接口网络服务器通过统一资源定位器地址将所述的反馈信息传送给用户端。

6、如权利要求 3 或 5 所述的方法，其特征在于，步骤 B 所述用户接口网络服务器通过内网或不对外公开的安全途径将输入信息传送给隐形代理服务器；

步骤 C3 所述隐形代理服务器通过内网或不对外公开的安全途径将所述的反馈信息传送给用户接口网络服务器。

7、如权利要求 3 或 5 所述的方法，其特征在于，步骤 C1 所述隐形代理服务器通过动态改变的网络地址向网络摄像头传送输入信息中的控制命令。

8、如权利要求 1 所述的方法，其特征在于，所述安全协议包括安全超文本传输协议或超文本传输协议。

9、一种网络摄像头防监听的控制系统，其特征在于，该系统包括用户端、用户接口网络服务器、隐形代理服务器和网络摄像头；

用户端，用于通过安全协议向用户接口网络服务器发送输入信息；

用户接口网络服务器，用于将用户端发送的输入信息传送给隐形代理服务器；

隐形代理服务器，用于将所述输入信息中的控制命令传送给网络摄像头；

网络摄像头，用于根据所述控制命令产生反馈信息，通过所述隐形代理服务器和所述用户接口服务器将所述反馈信息传送给用户端。

10、如权利要求 9 所述的系统，其特征在于，所述隐形代理服务器包括身份验证模块；

身份验证模块，用于根据所述输入信息中的验证信息进行身份合法性验证，将验证结果通过所述用户接口网络服务器传送给用户端。

网络摄像头防监听的控制方法及系统

技术领域

本发明涉及网络摄像头技术，具体涉及网络摄像头防监听的控制方法及系统。

背景技术

将网络摄像头通过以太网线连接到互联网后，用户端通过互联网协议地址便可直接访问远端的网络摄像头，对网络摄像头进行控制操作。目前，在网络摄像头的使用过程中，部分低档网络摄像头由于自身软、硬件的限制，或者由于网络摄像头所处网络的防火墙的限制，无法对外提供包括安全超文本传输协议（HTTPS，Hypertext Transfer Protocol Secure）在内的业界公认的安全数据传输服务。为了防止监听，现有技术所采用的方法是对用户端和远端的网络摄像头之间传输的数据进行简单的加密，或者通过明文的方式对用户端和远端的网络摄像头之间的数据进行传输，这样，导致了网络监听者很容易发现远端的网络摄像头，并非法对其进行控制。

可见，现有的网络摄像头防监听的控制方法降低了使用网络摄像头的安全性。

发明内容

有鉴于此，本发明提供一种网络摄像头防监听的控制方法，该方法能够提高使用网络摄像头的安全性。

本发明提供一种网络摄像头防监听的控制系统，该系统能够提高使用网络摄像头的安全性。

一种网络摄像头防监听的控制方法，建立用户接口网络服务器和隐形代理服务器，该方法还包括：

- A、用户端通过安全协议连接到用户接口网络服务器；
- B、用户接口网络服务器将输入信息传送给隐形代理服务器；
- C、隐形代理服务器根据输入信息中的控制命令，对网络摄像头进行控制。

所述用户接口网络服务器为一个或多个；

所述隐形代理服务器为一个或多个。

步骤 C 所述对网络摄像头进行控制的过程可以包括：

- C1、隐形代理服务器向网络摄像头传送输入信息中的控制命令；
- C2、网络摄像头根据控制命令向隐形代理服务器发送相应的反馈信息；
- C3、隐形代理服务器将所述的反馈信息传送给用户接口网络服务器；
- C4、用户接口网络服务器将所述的反馈信息传送给用户端。

所述步骤 B 之后，所述步骤 C 之前，该方法可以进一步包括：

B1、隐形代理服务器判断是否取得对输入信息中指定的网络摄像头的控制，如果是，则执行步骤 C，否则，执行步骤 B2；

B2、隐形代理服务器根据输入信息中验证信息包含的互联网协议地址，采用超文本传输协议查找出与所述互联网协议地址对应的网络摄像头；

B3、隐形代理服务器根据验证信息，进行身份合法性确认，通过确认后产生确认成功的反馈信息，经用户接口网络服务器将反馈信息传送给用户端；

B4、用户端判断是否停止对网络摄像头的控制，如果是，则结束流程，否则，执行步骤 A。

步骤 A 所述用户端采用统一资源定位器地址连接到用户接口网络服务器；

步骤 C4 所述用户接口网络服务器通过统一资源定位器地址将所述的反馈信息传送给用户端。

步骤 B 所述用户接口网络服务器通过内网或不对外公开的安全途径将输入信息传送给隐形代理服务器；

步骤 C3 所述隐形代理服务器通过内网或不对外公开的安全途径将所述的反馈信息传送给用户接口网络服务器。

步骤 C1 所述隐形代理服务器通过动态改变的网络地址向网络摄像头传送

输入信息中的控制命令。

所述安全协议包括安全超文本传输协议或超文本传输协议。

一种网络摄像头防监听的控制系统，该系统包括用户端、用户接口网络服务器、隐形代理服务器和网络摄像头；

用户端，用于通过安全协议向用户接口网络服务器发送输入信息；

用户接口网络服务器，用于将用户端发送的输入信息传送给隐形代理服务器；

隐形代理服务器，用于将所述输入信息中的控制命令传送给网络摄像头；

网络摄像头，用于根据所述控制命令产生反馈信息，通过所述隐形代理服务器和所述用户接口服务器将所述反馈信息传送给用户端。

所述隐形代理服务器可以包括身份验证模块；

身份验证模块，用于根据所述输入信息中的验证信息进行身份合法性验证，将验证结果通过所述用户接口网络服务器传送给用户端。

从上述方案可以看出，本发明通过建立用户接口网络服务器和隐形代理服务器，使用户端更加安全、隐蔽地与远端的网络摄像头进行数据传输，而不是像现有技术那样通过简单加密或明文的方式在网络上进行数据传输。从而，提高了使用网络摄像头的安全性。

附图说明

图 1 为本发明网络摄像头防监听的控制方法的示例性流程图；

图 2 为本发明网络摄像头防监听的控制方法一个具体实施例的流程图；

图 3 为本发明网络摄像头防监听的控制系统的结构示意图。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例和附图，对本发明进一步详细说明。

参见图 1，为本发明的网络摄像头防监听的控制方法的示例性流程图，

该方法预先在用户端和网络摄像头之间建立用户接口网络服务器和隐形代理服务器，具体还包括以下步骤：

步骤 101，用户端通过安全协议连接到用户接口网络服务器，向用户接口网络服务器发送输入信息。

步骤 102，用户接口网络服务器将输入信息传送给隐形代理服务器。

步骤 103，隐形代理服务器根据输入信息中的控制命令，对网络摄像头进行控制。

上述的用户接口网络服务器为一个或多个，若为多个时，将该多个用户接口网络服务器组成用户接口网络服务集群，用户接口网络服务器集群内的所有主机以共同的统一资源定位器（URL，Uniform Resource Locator）地址向互联网上的其它主机提供服务，并且，采用安全协议与互联网上的其它主机进行数据传输。这里，所述安全协议为超文本传输协议（HTTP，Hypertext Transfer Protocol）、HTTPS 或类似的安全协议；用户接口服务器集群内的所有主机也就是用户接口服务器集群内的所有用户接口服务器；互联网上的其它主机也就是用户端。用户端通过统一的 URL 地址连接到用户接口网络服务器集群，根据集群具备的服务器分配功能，便可使用户端与用户接口网络服务器集群内的某一用户接口网络服务器相连，然后，进行信息传输。

上述的隐形代理服务器为一个或多个，若为多个时，将该多个隐形代理服务器组成隐形代理服务器集群，隐形代理服务器集群内的所有主机可以不时地动态改变自己的互联网协议地址。隐形代理服务器集群内的所有主机也就是隐形代理服务器内的所有用户接口网络服务器。隐形代理服务器通过动态改变的互联网协议地址与远端的网络摄像头进行信息传输。动态改变互联网协议地址可以通过随机选取互联网协议地址来实现，可以采用等间隔时间地改变互联网协议地址来实现，也可以是其它动态改变互联网协议的方法。

用户接口网络服务器集群与隐形代理服务器集群通过内网或不对外开放并且安全的途径进行信息传输。用户接口网络服务器集群内的用户接口网

络服务器连接到隐形代理服务器集群，根据集群具备的服务器分配功能，便可使用户接口网络服务器与隐形代理服务器集群内的某一隐形代理服务器相连，然后，进行信息传输。

参见图 2，为本发明网络摄像头防监听的控制方法一个具体实施例的流程图，该方法预先建立用户接口网络服务器和隐形代理服务器，还包括以下步骤：

步骤 201，用户端通过安全协议安全地连接到用户接口网络服务器，并取得成功登录。

用户端以用户接口网络服务器集群提供的统一 URL 地址通过安全协议安全地连接到用户接口网络服务器，并采用用户名和密码的方式取得成功登录。安全协议包括 HTTPS 协议、HTTP 协议、或类似的协议，这样提高了用户端和用户接口网络服务器之间信息传输的安全性。

步骤 202，用户接口网络服务器接收用户端传送的输入信息。

用户端通过用户接口网络服务器提供的 WEB 界面向用户接口网络服务器传送输入信息。输入信息包括验证信息或控制命令。验证信息包括远端的网络摄像头的互联网协议地址、以及用来通过网络摄像头确认用户端身份合法性的用户名和密码等。控制命令用于对远端指定的网络摄像头可进行控制操作。

步骤 203，用户接口网络服务器将输入信息传送给隐形代理服务器。

本步骤中，用户接口网络服务器通过内网或不对外公开并且安全的途径将输入信息传送给隐形代理服务器，这样，保证了用户接口网络服务器与隐形代理服务器之间信息传输的安全性。

步骤 204，隐形代理服务器判断是否已经取得对输入信息中指定的网络摄像头的控制，若是执行步骤 205，否则，执行步骤 207。

步骤 205，隐形代理服务器向指定的网络摄像头传送输入信息中的控制命令。

本步骤中，隐形代理服务器可以以固定的互联网协议地址通过 HTTP 协

议向网络摄像头传送控制命令,为了更进一步提高隐形代理服务器与网络摄像头之间信息传输的安全性,也可以采用动态可变的互联网协议地址通过HTTP协议向指定的网络摄像头传送控制命令。动态改变互联网协议地址可以通过随机选取互联网协议地址来实现,可以采用等间隔时间地改变互联网协议地址来实现,也可以是其它动态改变互联网协议的方法。

步骤 206,网络摄像头响应控制命令,根据控制命令向隐形代理服务器发送相应的反馈信息。

本步骤中,若控制命令为传送网络摄像头接收的图像信息,则反馈信息中包括图像信息。当然,控制命令还包括由用户端输入用户接口网络服务器的其他控制命令。

步骤 207,隐形代理服务器根据验证信息中的互联网协议地址,采用HTTP协议查找与互联网协议地址对应的网络摄像头,如果查找成功,则执行步骤 208,否则,连接网络摄像头失败,隐形代理服务器产生连接失败的反馈信息,执行步骤 209。

步骤 208,隐形代理服务器建立与查找到的网络摄像头的连接后,根据用户接口网络服务器传送的验证信息,进行身份合法性确认,若确认成功,表明取得了对该网络摄像头的控制,产生确认成功的反馈信息,执行步骤 209,否则,产生确认失败的反馈信息,执行步骤 209。

步骤 209,隐形代理服务器将反馈信息传送给用户接口网络服务器。

所述的反馈信息包括步骤 206 中向隐形代理服务器传送的反馈信息,步骤 207 中产生的连接失败的反馈信息,以及步骤 208 中的确认成功或确认失败的反馈信息。

本步骤中,隐形代理服务器通过内网或不对外公开并且安全的途径将输入信息传送给用户接口网络服务器,这样,保证了用户接口网络服务器与隐形代理服务器之间信息传输的安全性。

步骤 210,用户接口网络服务器通过安全协议向用户端传送反馈信息。

本步骤中,用户接口网络服务器以用户接口网络服务器集群统一的 URL

地址通过安全协议在用户接口网络服务器提供的 WEB 界面上将反馈信息安全地呈现给用户端。这样，提高了用户端和用户接口网络服务器之间信息传输的安全性。

步骤 211，用户端判断是否停止对摄像头的控制，若是，则结束流程，否则，返回步骤 202。

上述流程中，步骤 207 和 208 为隐形代理服务器取得对网络摄像头控制的过程，步骤 205 和 206 为隐形代理服务器与已经被控制的网络摄像头之间的数据传输过程，步骤 209 和 210 为隐形服务器将反馈信息通过用户接口服务器的过程。

本发明用户接口网路服务器集群内的所有主机有共同的 URL 地址，通过该共同的 URL 地址向用户端提供服务，与用户端进行信息传输。这种以集群为服务的代理层的服务形式，能够以稳定、灵敏和性能可伸缩的方式应对海量级的用户端的服务请求；并且，通过用户端主机丰富的软、硬件资源提供了安全的网络通信服务；以集群为服务的代理层的服务形式，消除了现有技术中用户端为分散的网络摄像头提供升级的困难，使得网络摄像头的生成厂商能够在短时间内在用户界面、安全和性能等方面，为网络摄像头提供新的升级支持。升级时，用户端通过统一 URL 地址将升级命令发送给用户接口网络服务器集群，用户接口网络服务器集群再将升级命令通过隐形代理服务器集群传送给所有的网络摄像头，从而控制网络摄像头进行升级。用户端与用户接口网络服务器通过安全协议与用户进行信息传输，可防止网络监听者通过获取用户端与用户接口网络服务器之间传输的信息。

隐形代理服务器以动态可变的互联网协议地址与网络摄像头进行信息传输，提高隐形代理服务器与网络摄像头之间信息传输的安全性；以集群为服务的代理层的服务形式，能够以稳定、灵敏和性能可伸缩的方式应对海量级的由用户接口网络服务器传送的用户端的服务请求。

用户接口网络服务器集群和隐形代理服务器集群通过内网或其它不对外公开的并且安全的途径进行信息传输，用户接口网络服务器集群通过这种

安全、隐蔽的途径与用户接口网络服务器集群进行信息传输，避免了网络监听者通过用户接口网络服务器集群找到隐形代理服务器集群，从而找到远端网络摄像头的可能。

本发明的技术方案无须对网络摄像头软、硬件及其所处网络的防火墙提出特别要求，便可使用户端更加安全、隐蔽地与远端的网络摄像头进行数据传输，并对其进行控制，这样，提高了使用网络摄像头的安全性。

参见图 3，为本发明网络摄像头防监听的控制系统的结构示意图，该系统包括用户端、用户接口网络服务器、隐形代理服务器和网络摄像头。

用户端，用于通过安全协议向用户接口网络服务器集群内的用户接口网络服务器发送输入信息。安全协议包括 HTTPS 协议或 HTTP 协议。

用户接口网络服务器，用于将用户端发送的输入信息传送给隐形代理服务器。

用户接口网络服务器为一个或多个，若为多个时，该多个用户接口网络服务器组成用户接口网络服务器集群，用户接口网络服务器集群内的用户接口网络服务器通过统一的 URL 地址与用户端进行信息传输。

隐形代理服务器，用于将所述输入信息中的控制命令传送给网络摄像头。隐形代理服务器包括身份验证模块。

身份验证模块，用于根据所述输入信息中的验证信息进行身份合法性验证，将验证结果通过所述用户接口网络服务器传送给用户端。

上述的隐形代理服务器为一个或多个，若为多个时，将该多个隐形代理服务器组成隐形代理服务器集群。隐形代理服务器集群内的所有隐形代理服务器可以以固定的互联网协议地址通过 HTTP 协议向网络摄像头传送控制命令，为了进一步提高信息传输的安全性，也可以以动态可变的互联网协议地址通过 HTTP 协议向网络摄像头传送控制命令，从而对网络摄像头进行控制。用户接口网络服务器集群与隐形代理服务器集群通过内网或其它不对外公开的安全途径进行信息传输。

网络摄像头，用于根据隐形代理服务器传送的控制命令产生反馈信息，

通过隐形代理服务器和用户接口服务器将反馈信息传送给用户端。

以上所述的具体实施例，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

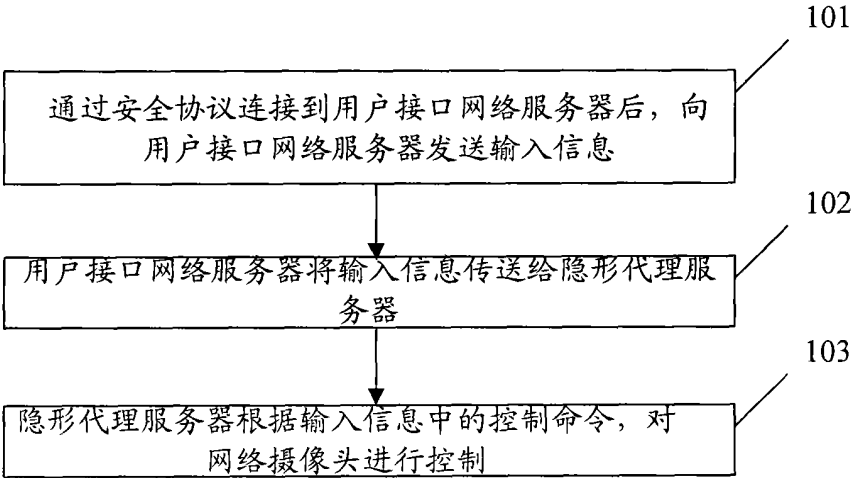


图 1

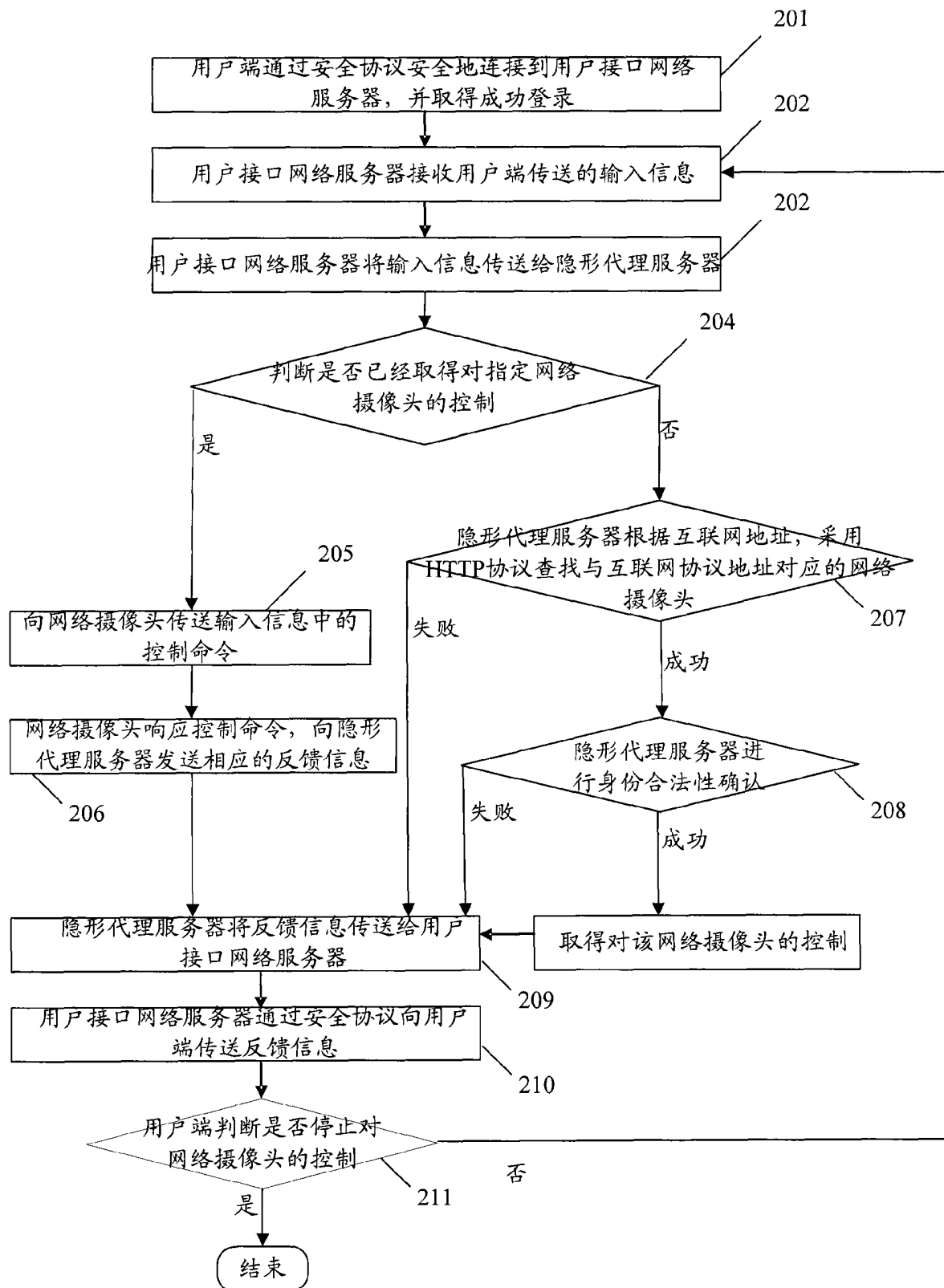


图 2

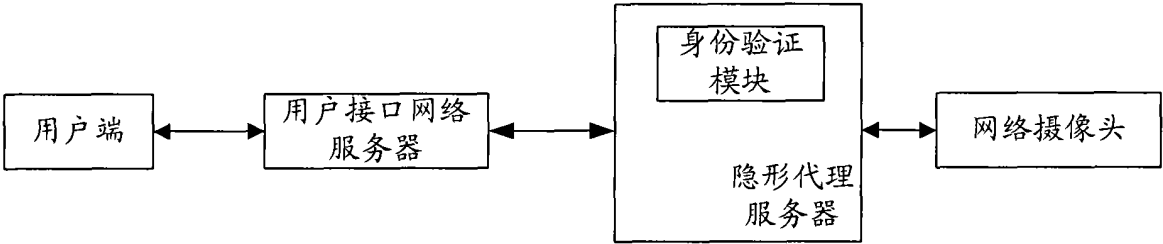


图 3