(12) UK Patent Application (19) GB (11) 2461596 (13) A

(43) Date of A Publication 13.01.2010

(21) Application No: 0812351.5

(22) Date of Filing: 07.07.2008

(51) INT CL:
H04N 1/00 (2006.01) *G08B 13/196* (2006.01)
H04N 7/18 (2006.01)

(56) Documents Cited:
WO 2007/073314 A3 WO 2006/072994 A1
JP 2006086940 A JP 2003110560 A
TW 000251412 B US 20050055727 A1

(58) Field of Search:
INT CL **H04N**
Other: **Online: WPI, EPODOC**

(71) Applicant(s):
View Network Solutions Ltd
(Incorporated in the United Kingdom)
79 Chiltern Drive, BERRYLANDS, KT5 8LR,
United Kingdom

(72) Inventor(s):
Conrad Charles Spiteri
Tang Zheng

(74) Agent and/or Address for Service:
Atkinson & Company Intellectual Property Limited
37-41 Gower Street, LONDON, WC1E 6HH,
United Kingdom

(54) Abstract Title: **IP network camera and server system**

(57) An IP network camera 2 and a server system 5 is shown. The camera has detection means to detect the presence of a local internet connection and generation means to generate a predetermined outbound server address communication with the camera logging on upon detection of the local internet connection. The server is programmed with the server address and has initiation means to receive a communication from the camera and to validate the camera credentials and to send the camera log on confirmation. In use, the camera receives the confirmation and opens a TCP/UDP or other session with the server. A 6 user can communicate with the camera using the server as a relay and fooling the camera into thinking the commands come are a response to camera requests and overcomes security devices such as firewalls and network address translation. When the user requests to view live video, in order to minimize server bandwidth, the server will ask the camera and the client computer to start a connectionless UDP session with each other without having the data pass directly through the server.

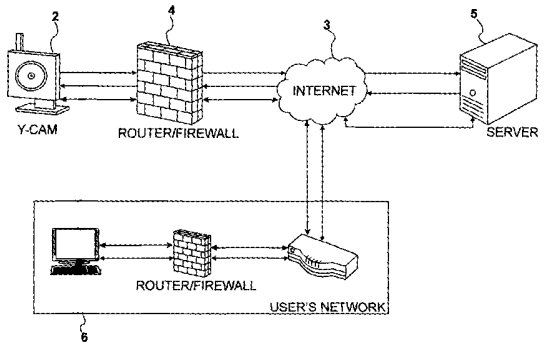

Figure 1

GB 2461596 A

The claims were filed later than the filing date but within the period prescribed by Rule 22(1) of the Patents Rules 2007.

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

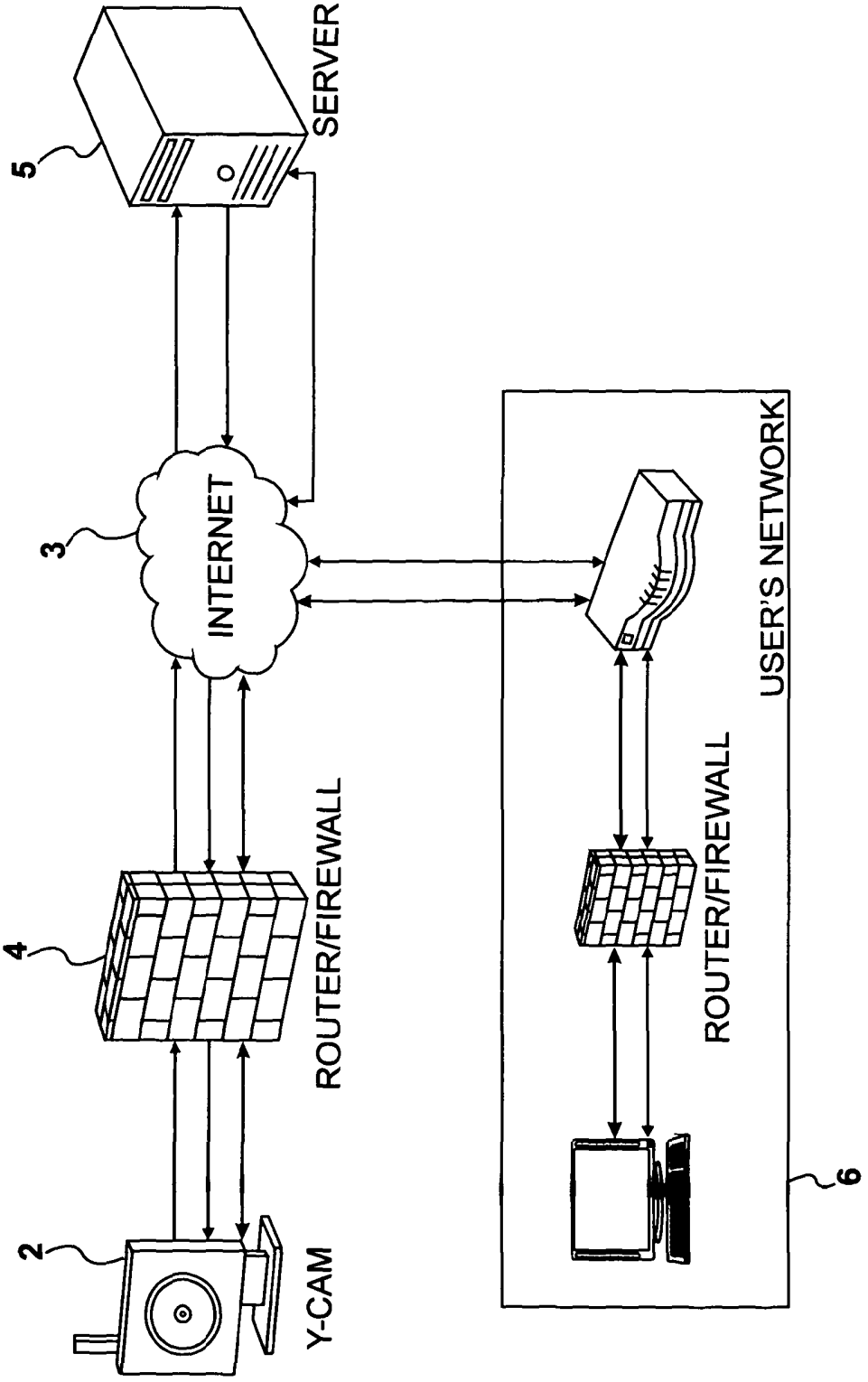
SERVER
5
INTERNET
3
ROUTER/FIREWALL
4
Y-CAM
2
USER'S NETWORK
ROUTER/FIREWALL
6

Figure 1

Title: IP Network Camera and Server System

The present invention relates to an IP network camera and remote server system, especially for use as a security/monitoring system.

The protocols used for communicating over IP networks usually conflict with most network security devices such as firewalls and network address translation (NATs). These devices work to protect the network from intruders getting into the organisation's private data resources. Firewalls examine the IP address and destination port of each data packet received from the outside world. Firewalls are often configured so that if a computer on the inside of the firewall requests data from a computer on the outside of the firewall (i.e. an outbound connection), for example if a user downloads a file from a website, the firewall will let the data from the computer outside the firewall pass. However this is only if it sends the data packets to the same IP address and port number of the computer on the inside of the firewall that originated the request.

It is known to place remote IP cameras in locations and transfer images and pictures taken by the camera onto a server for storage and retrospective viewing. There are a number of remote monitoring and storage services available in the market and they mainly use one of two available methods.

In the first method the camera uploads snapshots at regular intervals through an internet connection to an FTP server where the images are processed and compiled into a video. This method is not dependant on any firewalls along the connection between the camera and the server (since it is an outbound connection). Its main disadvantage is the lack of ability of the server to configure the camera or change upload intervals and other setting.

The second method is to allow the server to communicate with the camera directly in order to retrieve video streams and modify any setting. This is a much more flexible solution, however any firewalls in between the server and the camera will block access to the camera and specific ports need to be opened manually for this system to work. This makes it much less user friendly than the FTP method.

The invention seeks to provide a solution to this problem to allow a camera to form a "plug and view" connection to a remote server through a local internet connection and allow communication from the server to control the camera without need for adjustment to any firewalls or other security measures.

According to the present invention there is provided IP network camera and server system comprising:

a) a camera having detection means to detect the presence of a local internet connection, and generation means to generate an outbound predetermined server address communication with camera credentials upon detection of a local internet connection,

b) a server programmed with said server address, said server having initiation means to receive a server address communication from the camera and to validate the camera credentials and to send said camera "log on" confirmation,
in use the camera upon receipt of confirmation opening a TCP/UDP or other session with said server.

An embodiment of the invention will now be described with reference to the accompanying drawing.

Referring to the drawing there is shown a system 1. System 1 has a camera 2 in use connected to a local internet connection 3 through a firewall 4. Camera 2 may connect to the internet through a wireless connection. Camera 2 communicates with a server 5 with a server address. The system works as follows.

When the camera 2 is turned "on", detection means in the camera 2 detects the presence of a local internet connection 3, and generation means in the camera generates an outbound predetermined server address communication only upon detection of a local internet connection (a routine within the software (firmware) would contain the pre-programmed IP address of the server 5). When the server 5 is discovered the camera 2 sends the server 5 camera credentials (login details).

Server 5 has initiation means to receive the server address communication from the camera and to validate the camera credentials, including checking account details, and to send said camera "log on" confirmation.

The camera, upon receipt of confirmation, opens a TCP/UDP or other session with the said server. This allows the remote user 6 to send commands to the camera using the server as a relay station (Dashed lines) since commands from the server to the camera are sent as a form of reply to the cameras requests. This will fool the firewall into thinking that the commands are being requested by the camera which is located behind the firewall. The server may also request video and/or audio streams from the camera for storage or other audio/video manipulation purposes. At any point the user may require to view the live video, however, having a large number of cameras streaming audio and/or video through one or more servers will consume a very high amount of bandwidth. In order to keep bandwidth consumption to a minimum on the server side, when the user requests to view live video, the server will ask the camera and the client computer to start a connectionless UDP session with each other without having the data pass directly through the server (Dotted Lines).

This is achieved by having the remote user request a video session from the server (Dashed Lines). The server contacts the camera and sends the IP address and UDP port number of the user. The camera will try to contact the user but this is blocked by the user's firewall, however the camera's firewall doesn't know that. It now thinks that anything which comes from the user IP and UDP port is addressed to the camera's IP address and is legitimate. On the other hand, the server will pass the camera's IP address and UDP port to the user, who will attempt to contact the camera. The camera's firewall sees the recognised sender address and passes the apparent response on to the camera. This will allow data to flow between the camera and the user with both firewalls thinking that the device on their respective networks initiated the communication (Dotted Lines).

As the camera initiates communication with the server, it is therefore immune to any firewalls or other security devices since the connection is outbound. When the server receives a pre-determined set of strings (commands) that identify and validate the camera, the server is able to request various items from the camera such as video stream and still images. The server will also be able to change settings within the camera by returning various strings to the camera. For example the server may create a file or a set of strings in a pre-determined location. The camera will search for the file or strings in that location, compare its settings with the settings generated by the server and proceed to change its setting if they are different.

It will be appreciated that once a session has been opened and the camera has punched a "hole" through the firewall or router, communication between the camera and server can take place without further obstruction. This has effectively solved any potential configuration problems for the user and made the system truly plug and play.

The invention may take a form different to that specifically described above. It is envisaged that system may include a number of cameras each at the same or different locations, and each camera addressing the same server.

Further modifications will be apparent to those skilled in the art without departing from the scope of the present invention.

Claims

1. A camera for transmitting image data over the internet, comprising:

an image data generating device configured to generate image data in an active state and to disable image data generation in a passive state;

a network device configured to establish a connection to the internet via a local network so as to communicate with a server, wherein:

said network device transfers image data to said server during said active state; and

said network device maintains a session with the server during said passive state.

2. An IP network camera and server system comprising:

a camera having detection means to detect the presence of a local Internet connection, and generation means to generate an outbound predetermined server address communication with camera credentials upon detection of a local Internet connection; and

a server programmed with said server address, said server having initiation means to receive a server address communication from the camera and to validate the camera credentials and to send said camera "log on" confirmation,

such that, when in use,

the camera upon receipt of confirmation opens a TCP/UDP or other session with the server.

Application No: GB0812351.5 **Examiner:** Richard Baines

Claims searched: 2 **Date of search:** 3 June 2009

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	2	US2005/0055727 A1 (PENTAX) - abstract, figure and paragraphs 15, 71, 81, 82 & 88
X	2	WO2007/073314 A3 (AXIS) - abstract, figure and paragraphs 41, 61, 65 & 72
X	2	JP2006086940 A (MEGACHIPS) - abstract
X	2	TW251412 B (AIRWAVE) - abstract
X	2	JP2003110560 A (SANYO) - abstract
A	-	WO2006/072994 A1 (SYSTEMK) - abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

H04N

The following online and other databases have been used in the preparation of this search report

Online: WPI, EPODOC

International Classification:

Subclass	Subgroup	Valid From
H04N	0001/00	01/01/2006
G08B	0013/196	01/01/2006
H04N	0007/18	01/01/2006