(12) **United States Patent**
**Saridakis**

(10) **Patent No.: US 8,874,691 B2**
(45) **Date of Patent: Oct. 28, 2014**

(54) **SYSTEM AND METHOD FOR ESTABLISHING PEER TO PEER CONNECTIONS BETWEEN PCS AND SMART PHONES USING NETWORKS WITH OBSTACLES**

(75) Inventor: **Titos Saridakis**, Espoo (FI)

(73) Assignee: **Core Wireless Licensing S.A.R.L.**, Luxembourg (LU)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2411 days.

(21) Appl. No.: **11/158,710**

(22) Filed: **Jun. 22, 2005**

(65) **Prior Publication Data**

US 2006/0294213 A1 Dec. 28, 2006

(51) **Int. Cl.**
***G06F 15/16*** (2006.01)
***H04L 29/08*** (2006.01)
***H04L 29/06*** (2006.01)

(52) **U.S. Cl.**
CPC .............. ***H04L 67/104*** (2013.01); ***H04L 67/02*** (2013.01); ***H04L 67/28*** (2013.01); ***H04L 63/029*** (2013.01)
USPC .............................. **709/219**; 709/217; 726/12

(58) **Field of Classification Search**
CPC ..................................................... G06F 15/173
USPC ............................ 709/217, 219, 245; 726/12
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 6,685,093 | B2 * | 2/2004 | Challa et al. | 235/462.46 |
| 6,789,119 | B1 * | 9/2004 | Zhu et al. | 709/227 |
| 7,003,463 | B1 * | 2/2006 | Maes et al. | 704/270.1 |
| 7,028,091 | B1 * | 4/2006 | Tripathi et al. | 709/230 |
| 7,200,668 | B2 * | 4/2007 | Mak et al. | 709/230 |
| 7,222,306 | B2 * | 5/2007 | Kaasila et al. | 715/801 |
| 7,257,837 | B2 * | 8/2007 | Xu et al. | 726/12 |
| 7,274,658 | B2 * | 9/2007 | Bornstein et al. | 370/227 |
| 7,296,288 | B1 * | 11/2007 | Hill et al. | 726/2 |
| 7,318,073 | B2 * | 1/2008 | Shields et al. | 707/202 |
| 7,346,925 | B2 * | 3/2008 | Marcjan | 726/12 |
| 2002/0023143 | A1 | 2/2002 | Stephenson et al. | |
| 2002/0147810 | A1 | 10/2002 | Traversat et al. | |
| 2003/0105812 | A1 | 6/2003 | Flowers, Jr. et al. | |
| 2003/0131258 | A1 * | 7/2003 | Kadri | 713/201 |
| 2003/0187631 | A1 | 10/2003 | Masushige et al. | |

(Continued)

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| JP | 2003273937 | 9/2003 |

OTHER PUBLICATIONS

International Search report for PCT Application PCT/IB2006/001660.

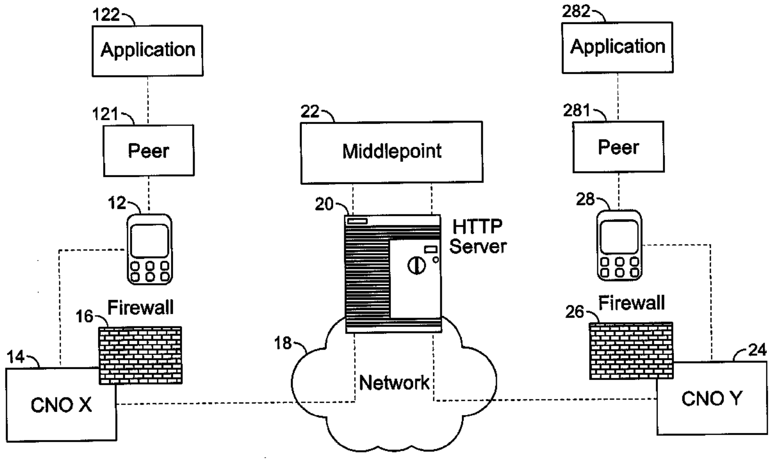
(Continued)

*Primary Examiner* — Emmanuel L Moise
*Assistant Examiner* — Marie Georges Henry
(74) *Attorney, Agent, or Firm* — Winstead PC

(57) **ABSTRACT**

A method of circumventing network obstacles to provide a peer-to-peer communication channel between peers utilizing hypertext transfer protocol (HTTP) includes communicating a HTTP request from a peer device to a relay through a network including an obstacle where the HTTP request is intended for another peer device. The method further includes communicating a HTTP response from the relay to the peer device and establishing a communication channel between the peer device and the another peer device via the relay. The communication channel permits the peer device and the another peer device to send and receive data.

**18 Claims, 2 Drawing Sheets**



## (56) References Cited

### U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 2003/0210694 | A1 * | 11/2003 | Jayaraman et al. ........... | 370/392 |
| 2004/0162871 | A1 | 8/2004 | Pabla et al. | |
| 2006/0075116 | A1 * | 4/2006 | Chitilian et al. ............. | 709/227 |
| 2006/0215684 | A1 | 9/2006 | Capone | |

### OTHER PUBLICATIONS

Office Action in Korean Patent Application No. 10-2008-7001593, dated Mar. 11, 2010 (with English translation).

Office Action in Japanese Patent Application No. 2008-517620, dated Feb. 14, 2011 (refer to the non-patent literature document submitted in the IDS filed Dec. 30, 2010, for the listing in References 1-3).

Ford, B. et al., "Peer-to-Peer (P2P) communication across Network Address Translators (NAT)", No. 2, Mar. 1, 2004, 33 pages.

Baset, Salman A. et al., "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol", Sep. 15, 2004, 13 pages.

Office Action in Japanese Patent Application No. 2008-517620, mailed Oct. 4, 2010.

* cited by examiner

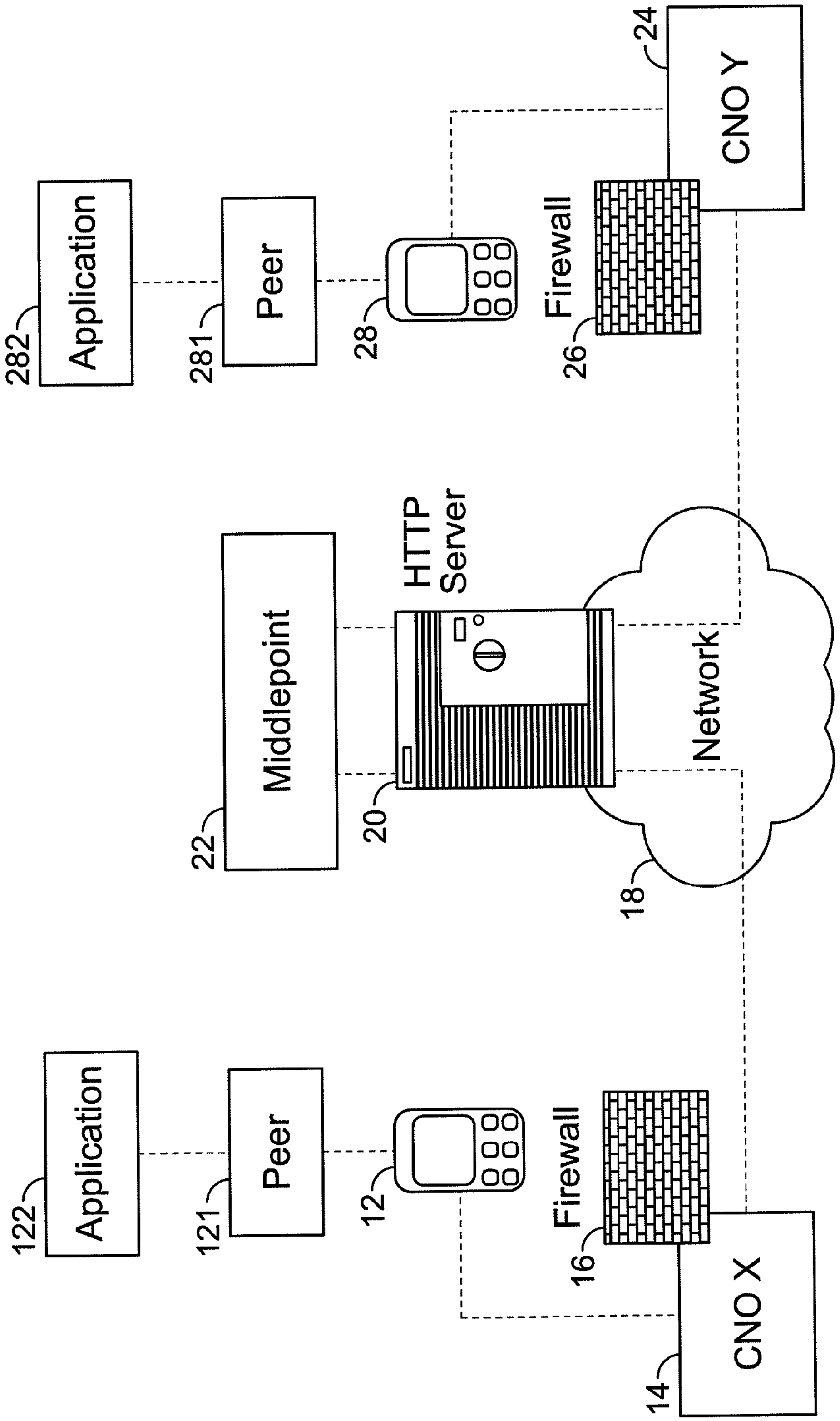

282
Application
281
Peer
28
Firewall
26
24
CNO Y
22
Middlepoint
20
HTTP Server
Network
18
122
Application
121
Peer
12
Firewall
16
14
CNO X

FIG. 1

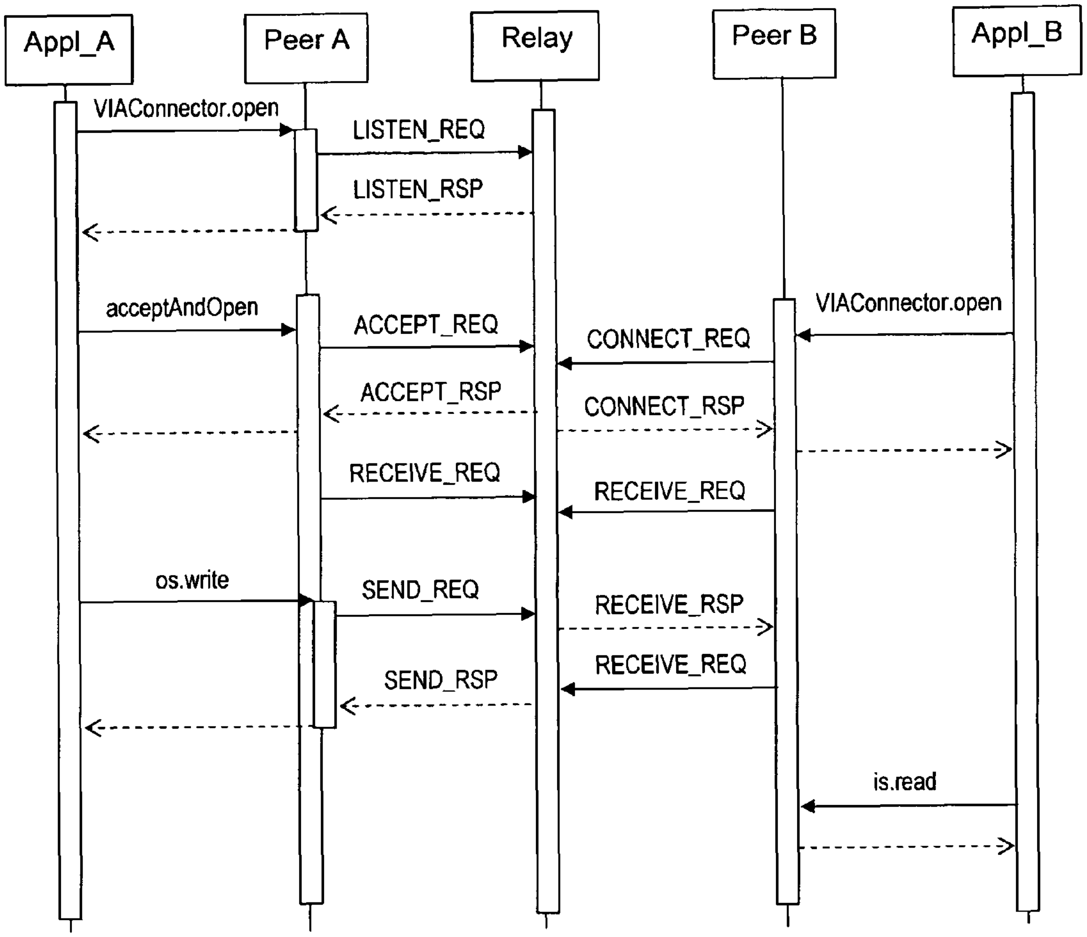

Appl_A
Peer A
Relay
Peer B
Appl_B
VIAConnector.open
LISTEN_REQ
LISTEN_RSP
acceptAndOpen
ACCEPT_REQ
ACCEPT_RSP
VIAConnector.open
CONNECT_REQ
CONNECT_RSP
RECEIVE_REQ
RECEIVE_REQ
os.write
SEND_REQ
SEND_RSP
RECEIVE_RSP
RECEIVE_REQ
is.read

FIG. 2

# SYSTEM AND METHOD FOR ESTABLISHING PEER TO PEER CONNECTIONS BETWEEN PCS AND SMART PHONES USING NETWORKS WITH OBSTACLES

## BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to firewalls and peer to peer connections. More specifically, the present invention relates to a system and method for establishing peer to peer (P2P) connections between PCS and smart phones or other devices, including personal computers, over a network that obstructs the straightforward establishment of such P2P connections using means such as firewalls and network address translation (NAT) servers.

2. Description of the Related Art

This section is intended to provide a background or context. The description herein may include concepts that could be pursued, but are not necessarily ones that have been previously conceived or pursued. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the claims in this application and is not admitted to be prior art by inclusion in this section.

The majority of devices on the Internet, whether stationary (e.g., personal computers) or mobile (e.g., smart phones), are connected to the Internet through network connections offered by some Internet Service Provider (ISP) or some Cellular Network Operator (CNO). The traditional model for accessing content over the Internet is centered around Web servers: content is placed by content providers on Web servers operated by service providers (often ISPs and CNOs assume both roles of content and service provider); then, users interested in specific content access the corresponding Web server(s) to obtain it. In this content distribution model, the users who may possess some content cannot offer it directly to other users, unless they place it on some Web server.

An alternative to this content-distribution model centered on Web servers is the peer-to-peer (P2P) model. Here, the user may directly share with other users the content he or she possesses. Each P2P protocol (Napster, Gnutella, Chord, FastTrack, etc) comes with a content location service, centralized or distributed, which permits the location of the peer(s) that contain a specified content. Using such a location service, a user looking for some specific content may connect to the device of another user who offers the content in question and retrieve it from there.

In order for P2P protocols to work over the Internet, the establishment of a connection between two peers at the edges of the Internet (e.g., PCs or smart-phones) must be possible. It is not a trivial task to satisfy this requirement, especially taking into consideration the constraints imposed by firewalls and NAT servers that are used by ISPs and CNOs to protect and control their networks.

Firewalls are used to control the data traffic that goes through them. In practice, the great majority of such firewalls allow only solicited HTTP traffic to reach a smart phone or a PC, while plain IP traffic (over TCP or UDP) is blocked. Even if a smart phone has an HTTP server, an HTTP request sent by a remote device to that server would not go through these firewalls, since the HTTP message is unsolicited by the receiving smart phone. Consequently, for such strict firewall policies, there is no straightforward way to establish a P2P

NAT servers also create obstacles to a P2P connection, especially for the case where one peer is a smart phone that roams across different CNOs while connected to the Internet. In that case, while the smart phone would be connected to a P2P overlay network, it will change its IP address and consequently it will lose all socket connections that have been established to its previous IP address.

Previous attempts have been made to provide solutions to the problem of establishing P2P connections in an environment including firewalls and NAT servers, both in the fixed and in the mobile Internet cases. In the fixed Internet, a peer (PC) is assigned a possibly different IP address by a NAT server every time it connects to the network. However, as long as the peer remains connected to the network, the IP address is not changed. Hence, the problem of changing IP address while connected to the network does not appear in the fixed Internet and, consequently, existing P2P protocols do not provide solutions for such cases. However, in applications connected to the Internet by way of a mobile device, a smart phone that roams may change its IP address while being connected to the network. As such, P2P protocols from the fixed Internet cannot operate correctly.

In the fixed Internet, corporate networks can include firewalls that implement the strict security policy of allowing only solicited HTTP traffic to reach a PC connected in the corporate network. Similarly, many cellular network operator (CNO) firewalls implement the same strict security policy. A number of solutions to P2P connections despite the presence of CNO firewalls have been proposed in the context of SIP deployment, since SIP traffic faces the same constraints from the firewalls as any other, unsolicited HTTP traffic. These solutions rely on the dynamic allocation of pinholes on the firewalls to allow SIP traffic to go through. Such solutions create another case of specific traffic, similar to the solicited HTTP traffic. They are not a generic solution to the establishment of P2P connections.

There is a need to establish peer to peer (P2P) connections between PCs and smart phones despite the obstacles imposed by firewalls, which allow only solicited HTTP traffic to go though, and by NAT servers, which change the IP address of roaming smart phones. Further, there is a need for a reliable peer-to-peer communication protocol that works in a network environment including a firewall without relying on special firewall features.

## SUMMARY OF THE INVENTION

In general, exemplary embodiments described herein establish peer to peer connections between personal computers (PCs) and smart phones despite the obstacles imposed by firewalls, which allow only solicited HTTP traffic to go through, and by network address translation (NAT) servers, which change the IP address of roaming smart phones. Exemplary embodiments utilize an HTTP-based protocol that does message relaying. The purpose of the protocol is to enable a socket connection between two terminals despite firewalls between them. The protocol uses HTTP requests and responses to relay the messages between the peers without expecting any favorable behavior from the firewalls (e.g., opening "pinholes" for specific TCP (transmission control protocol) or UDP (user datagram protocol) traffic).

One exemplary embodiment relates to a method of circumventing network obstacles to provide a peer-to-peer communication channel between peers utilizing hypertext transfer protocol (HTTP). This method can include communicating a

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

### FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

### E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

**WHAT WILL YOU BUILD?** | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.