(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
7 February 2008 (07.02.2008)

PCT

(10) **International Publication Number**
WO 2008/016442 A2

(51) **International Patent Classification:**
G06F 21/20 (2006.01)

(21) **International Application Number:** PCT/US2007/014815

(22) **International Filing Date:** 26 June 2007 (26.06.2007)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**

60/816,714	27 June 2006 (27.06.2006)	US
60/860,719	22 November 2006 (22.11.2006)	US

(71) **Applicant** *(for all designated States except US):* **THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OFNEW YORK** [US/US]; 535 West 116 Street, 412 Low Memorial Library, New York, NY 10027 (US).

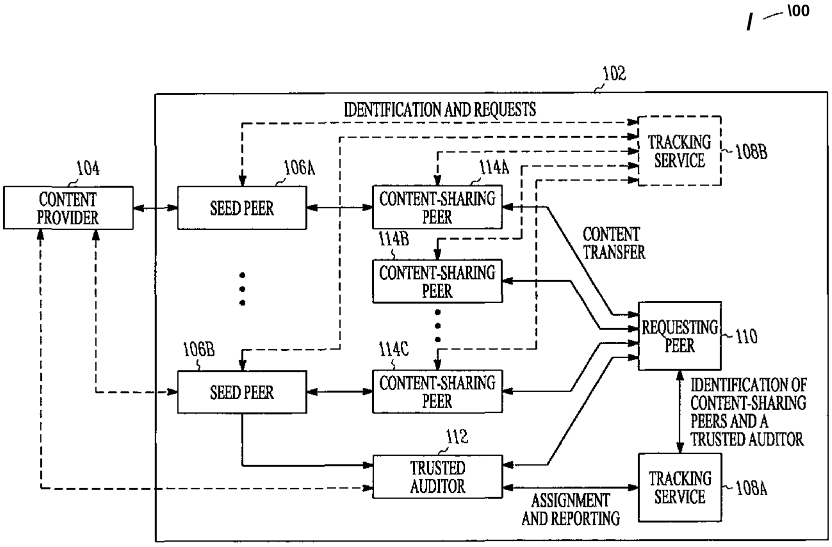
(71) **Applicants and**
(72) **Inventors: SHERMAN, Alexander** [US/US]; 792 Columbus Avenue #8L, New York, NY 10025 (US). **STAVROU, Angelos** [GR/US]; 527 W 113 Street #4F, New York, NY 10025 (US). **NIEH, Jason** [US/US]; 2700 Broadway #11 B, New York, NY 10025 (US). **STEIN, Clifford** [US/US]; 180 Sussex Road, Tenafly, NJ 07670 (US). **KEROMYTIS, Angelos** [GR/US]; 423 W. 120 Street #98, New York, NY 10027 (US). **CHAWLA, Japinder, Singh** [IN/US]; 189 Claremont Avenue #55, New York, NY 10027 (US). **SARMA, Justin** [US/US]; 57 Undercliff Road, Montclair, NJ 07042 (US).

(74) **Agents: STEFFEY, Charles, E.** et al.; Schwegman, Lundberg & Woessner, P.A., P.O. Box 2938, Minneapolis, MN 55402 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind cf national protection available):* AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK,

[Continued on next page]

(54) **Title:** A TRUSTED P2P SYSTEM FOR PAID OR OTHER CONTENT DELIVERY



(57) **Abstract:** A peer-to-peer content delivery system includes trusted auditors to report inappropriate peer behavior. This permits punishment or banishment. The trusted auditors can mimic peer behavior. The trusted auditors can be used in an existing peer-to-peer system, or in a system in which users share content anonymously via layer of inteπnediate nodes. The intermediate nodes can be inhibited from having an entirety of content they help to transfer. Vendors can leverage peer-to-peer transfer capacity and keep the same level of trust of customers as in traditional content distribution models. Infrastructure costs and end-user cost can be lowered. The intermediate nodes can be incentivized to contribute a portion of their transfer capacity, such as via electronic payments, and electronic payment transactions ma be facilitated by a bank service. Efficiency, security or reliability can be enhanced through queuing, pipelining, encryption and direct-download recovery capabilities.

LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

A TRUSTED P2P SYSTEM FOR PAID OR OTHER CONTENT DELIVERY

CROSS-REFERENCE TO RELATED PATENT DOCUMENTS

This patent application claims the benefit of priority, under 35 U.S.C. Section 119(e), to Sherman et al. U.S. Provisional Patent Application Serial Number 60/816,714, entitled "A TRUSTED P2P SYSTEM FOR PAID CONTENT DELIVERY," filed on June 27, 2006 (Attorney Docket No. 2413.002PRV); and Sherman ct al. U.S. Provisional Patent Application Serial Number 60/860,7 19, entitled "P2P DELIVERY OF PAID OR OTHER CONTENT," filed on November 22, 2006 (Attorney Docket No. 2413.017PRV).

U.S. Provisional Patent Application Serial Number 60/816,714 and U.S. Provisional Patent Application Serial Number 60/860,719 are hereby incorporated by reference herein in their entireties.

STATEMENT REGARDING FEDERALLY-SPONSORED RESEARCH

The invention was made with the support of National Science Foundation Grant No. CCR-00-93047. The U.S. Government has certain rights in the invention.

TECHNICAL FIELD

This document pertains generally to digital content-sharing through a peer-to-peer (P2P) network and more particularly, but not by way of limitation, to a trusted P2P system for paid or other content delivery.

BACKGROUND

Peer-to-peer content-sharing is a powerful and efficient distribution model due to its ability to leverage peers' transfer capacity. However, companies that sell digital content such as music, video or movies typically rely on "direct download" methods. In direct download, users download content either from the vendor's website directly or via a contracted CDN (content delivery network). Content providers are hesitant to rely on peer-to-peer systems for paid content distribution as free-of-charge content-sharing is common in current peer-to-peer models. This is sometimes referred to as the "free rider" problem.

The content providers' concern is well-justified as existing peer-to-peer users can easily foπn free content-sharing communities. Examples of such communities use Kazaa or BitTorrent, in which requested content is subdivided and transferred upon request from multiple content-sharing peers. Some systems require payment before a user can enter the peer-to-peer network, such as MoveDigital. However, once a user has access to the content on the network, she may directly share the purchased content with other users on other networks, without authorization from the content provider. Once these users learn of one another and know that they have similar interests, they can easily form a private community for free future sharing of similar content. This is sometimes referred to as a "darknet."

OVERVIEW

The present system can provide cost-effective distribution capabilities of a decentralized peer-to-peer approach, and can maintain sufficient trust and security for paid content distribution. The system can include authentication or one or more trusted auditors (TAs). TAs can serve as sentinels: they can assume the role of a content source, a content destination, or an inappropriately behaving system *(e.g.,* luring other inappropriately behaving peers to either probe them or to respond to their probes). When TAs detect, record, and report inappropriate behavior, a variety of measures may be taken, including punishment or removal from participation in the network. Authentication and TAs can even be layered onto an existing peer-to-peer system, if desired. Using the system, content vendors can leverage peer-to-peer transfer capacity while effectively maintaining the same level of trust towards their customers as in traditional models of content distribution. As a result, a content provider can reduce its infrastructure costs and lower the costs for the end-users.

In some examples, the system can be structured such that users share content with a degree of anonymity with respect to other content-sharing peers via a layer of intermediate nodes. The intermediate nodes can be inhibited from possessing an entirety of the content that they help to transfer. The intermediate nodes can be provided with an incentive to contribute a portion of their transfer capacity, such as via electronic payment. Electronic payment transactions can be facilitated by a bank service. The efficiency, security, or reliability of the content transfer can be increased, such as through queuing, pipelining, encryption, or direct-download recovery.

Example 1 describes a method. In this example, the method comprises: seeding a peer-to-peer networked digital content-sharing system with content from a content provider; providing requested content to be transferred from a content-sharing peer to a requesting peer; identifying a content-sharing peer to participate in transferring the requested content; recognizing an identified peer as trustworthy; assigning a recognized trustworthy identified peer as a trusted auditor; and detecting, using the trusted auditor, an instance of an inappropriate behavior.

In Example 2, the method of Example 1 optionally comprises assigning a number of trusted auditors as a function of a number of inappropriately behaving peers.

In Example 3, the method of at least one of Examples 1-2 optionally comprises: receiving payment from the requesting peer for the content to be transferred; and, in response to receiving payment, authorizing content delivery to the requesting peer.

In Example 4, the method of at least one of Examples 1-3 optionally comprises selecting a number of trusted auditors to provide or enhance a profit of the providing requested content to the requesting peer.

In Example 5, the method of at least one of Examples 1-4 optionally comprises assigning at least 6% of a total number of content-sharing and requesting peers as trusted auditors, and receiving at least twice the value of an expended transfer capacity of a content sharing instance as payment for the content sharing instance.

In Example 6, the method of at least one of Examples 1-5 optionally comprises inhibiting transfer of requested content without an authorization for content delivery.

In Example 7, the method of at least one of Examples 1-6 optionally comprises reporting, by a trusted auditor, to the tracking service an inappropriate behavior of a content-sharing peer or requesting peer.

In Example 8, the method of at least one of Examples 1-7 optionally comprises mimicking, by a trusted auditor, a behavior of a content-sharing peer or a requesting peer to conceal an identity of the trusted auditor.

In Example 9, the method of at least one of Examples 1-8 optionally comprises mimicking, by a trusted auditor, an inappropriate behavior of (1) a content-sharing peer, (2) a requesting peer, or (3) an outside system probing a content-sharing or a requesting peer.

In Example 10, the method of at least one of Examples 1-9 optionally comprises removing a content-sharing or requesting peer from participation in the peer-to-peer network in response to an instance of at least one inappropriate behavior.

In Example 11, the method of at least one of Examples 1-10 optionally comprises penalizing a content-sharing or requesting peer in response to an instance of at least one inappropriate behavior.

In Example 12, the method of at least one of Examples 1-1 1 optionally comprises varying an address of a trusted auditor to conceal an identity of the trusted auditor.

In Example 13, the method of at least one of Examples 1-12 optionally comprises monitoring traffic generated by a trusted auditor, comparing the traffic to a threshold value, and adjusting behavior of the trusted auditor when the traffic exceeds the threshold value.

In Example 14, the method of at least one of Examples 1-13 optionally comprises authenticating at least one request or response made over the peer-to-peer network.

Example 15 comprises a system. In this example, the system includes: a pool of peer-to-peer networked digital content-sharing peers, including a requesting peer to receive requested content from another peer; a content-sharing peer, configured to host at least some of the requested content; a content provider, configured to deliver an entirety of the requested content; a tracking service, configured to provide content-sharing peer node identification; and a trusted auditor, configured to be recognized as trustworthy by the tracking service, configured to participate in the pool of peer-to-peer networked digital content-sharing peers, configured to be assigned by the tracking service to a content-sharing session, and configured to record an instance of inappropriate behavior.

In Example 16, the system of Example 15 optionally comprises the tracking service being configured to assign a number of trusted auditors as a function of a total number of inappropriately behaving peers.

In Example 17, the system of at least one of Examples 15-16 optionally comprises the content provider being configured to receive a content purchase request, and, in response, to provide an authorization of content delivery to the requesting peer.

In Example 18, the system of at least one of Examples 15-17 optionally comprises the tracking service and content-sharing peers being configured to inhibit transfer of requested content without an authorization for content delivery.

In Example 19, the system of at least one of Examples 15-18 optionally comprises a specified number of trusted auditors, wherein the number of trusted auditors is a function of a number of peers.

In Example 20, the system of at least one of Examples 15-19 optionally comprises the number of the trusted auditors being specified to be at least 10% of an expected or detected number of inappropriate users.

In Example 21, the system of at least one of Examples 15-20 optionally comprises the trusted auditor being configured to report to the tracking service an instance of inappropriate behavior of (1) a content-sharing peer or (2) a requesting peer.

In Example 22, the system of at least one of Examples 15-21 optionally comprises the trusted auditor being configured to conceal its identity by mimicking behavior of (1) a content-sharing peer or (2) a requesting peer.

In Example 23, the system of at least one of Examples 15-22 optionally comprises the trusted auditor being configured to mimic inappropriate behavior of (1) a content-sharing peer, (2) a requesting peer, or (3) an outside system probing a content-sharing peer or a requesting peer.

In Example 24, the system of at least one of Examples 15-23 optionally comprises the tracking service comprises a violation tracking service that is configured to remove a content-sharing or a requesting peer from participation in the peer-to-peer network in response to at least one instance of inappropriate behavior by the content-sharing or requesting peer.

In Example 25, the system of at least one of Examples 15-24 optionally comprises a violation tracking service that is configured to penalize a content-sharing or requesting peer in response to at least one instance of inappropriate behavior by the content-sharing or requesting peer.

In Example 26, the system of at least one of Examples 15-25 optionally comprises the trusted auditor comprising a variable address.

In Example 27, the system of at least one of Examples 15-26 optionally comprises a trusted auditor. In this example, the trusted auditor comprises: a traffic monitor, configured to monitor a volume of probing traffic generated by the trusted auditor; and a comparator, coupled to the traffic monitor, the comparator configured to compare the traffic generated by the trusted auditor against a threshold value, and wherein the trusted auditor is configured to adjust its activity when the traffic exceeds the threshold value.

In Example 28, the system of at least one of Examples 15-27 optionally comprises the network being configured to provide at least one authentication of a request or a response.

Example 29 describes a system. In this example, the system comprises: means for seeding a peer-to-peer networked digital content-sharing system with content from a content provider; means for providing requested content to be transferred from a content-sharing peer to a requesting peer; means for identifying a content-sharing peer to participate in transferring the requested content; means for recognizing an identified peer as trustworthy; means for assigning a recognized trustworthy identified peer as a trusted auditor; and means for detecting an instance of inappropriate behavior of a peer.

Example 30 describes a machine readable medium. In this example, the machine readable medium includes instructions that, when performed by the machine, cause the machine to: seed a peer-to-peer networked digital content-sharing system with content from a content provider; provide requested content to be transferred from a content-sharing peer to a requesting peer; identify a content-sharing peer to participate in transferring the requested content; recognize an identified peer as trustworthy; assign a recognized trustworthy identified peer as a trusted auditor; and detect an instance of an inappropriate behavior.

Example 31 describes a method. In this example, the method comprises: providing requested content to be transferred by a peer-to-peer networked digital content-sharing system from a content-sharing peer to a requesting peer; subdividing the content into chunks; delivering chunks from a content-sharing peer to a requesting peer through an inteπnediate node; identifying an intermediate node and a content-sharing peer to participate in transferring the requested content; assigning an intermediate node to separate a content-sharing peer from a requesting peer during the transferring of the requested content; and inhibiting an intermediate node from accessing an entirety of the requested content.

In Example 32, the method of Example 3 1 optionally comprises limiting a number of assigned intermediate nodes, which separate a content-sharing peer from a requesting peer during the transferring of the requested content, to a value that is less than or equal to an outdegree parameter value.

In Example 33, the method of at least one of Examples 31-32 optionally comprises receiving payment from the requesting peer for the content to be transferred; and, in response to the receiving payment, authorizing content delivery to the requesting peer.

In Example 34, the method of at least one of Examples 3 1-33 optionally comprises electronically crediting the requesting peer in response to the receiving payment from the requesting peer.

In Example 35, the method of at least one of Examples 3 1-34 optionally comprises paying an intermediate node for a chunk of requested content and, in response, transferring the requested content.

In Example 36, the method of at least one of Examples 3 1-35 optionally comprises receiving a request and payment for transfer of a block of multiple chunks of requested content.

In Example 37, the method of at least one of Examples 3 1-36 optionally comprises bidding, by an intermediate node against other intermediate nodes, for participating in a content transfer.

In Example 38, the method of at least one of Examples 31-37 optionally comprises constructing at least one distributed hash table (DHT) and identifying a peer or node to a peer or node using the DHT.

In Example 39, the method of at least one of Examples 3 1-38 optionally comprises providing decentralized tracking of the identified peer or inteπnediate node.

In Example 40, the method of at least one of Examples 31-39 optionally comprises seeding a network of peer-to-peer networked digital content-sharing peers with an entirety of the requested content.

In Example 41, the method of at least one of Examples 31-40 optionally comprises transferring at·least some of the requested content by direct download when the requesting peer fails to receive an entirety of the requested content from the pool of peer-to-peer networked content-sharing peers.

In Example 42, the method of at least one of Examples 31-41 optionally comprises providing multiple versions of the requested content, and inhibiting an intermediate node from receiving at least one version of the requested content.

In Example 43, the method of at least one of Examples 31-42 optionally comprises monitoring by the requesting peer the content transfer rate from a first intermediate node, comparing transfer rate to a threshold value, and requesting a corresponding chunk of digital content from a second intermediate node when the content transfer rate is below the threshold value.

In Example 44, the method of at least one of Examples 31-43 optionally comprises storing a content request to an intermediate node in a request queue, and transferring the content from the content request when the intermediate node becomes available.

In Example 45, the method of at least one of Examples 31-44 optionally comprises removing from the pool of intermediate nodes an intermediate node that fails to deliver requested content for which the intermediate node has been paid.

In Example 46, the method of at least one of Examples 31-45 optionally comprises detecting an instance of inappropriate behavior of an intermediate node or requesting peer.

In Example 47, the method of at least one of Examples 31-46 optionally comprises penalizing a detected instance of inappropriate behavior of an intermediate node or a requesting peer.

In Example 48, the method of at least one of Examples 31-47 optionally comprises auditing members of the pool of peer-to-peer networked content-sharing peers by a trusted auditor, the auditing comprising at least one of (1) mimicking an intermediate node, a content-sharing peer, or a requesting peer, or (2) probing the intermediate node, the content-sharing peer, or the requesting peer.

In Example 49, the method of at least one of Examples 31-48 optionally comprises assigning at least one trusted auditor to interact with a requesting peer, a content-sharing peer, or an intermediate node during a content transfer session.

In Example 50, the method of at least one of Examples 31-49 optionally comprises encrypting a content-sharing transaction on the peer-to-peer networked digital content-sharing system.

Example 50 describes a system. In this example, the system comprises a pool of peer-to-peer networked digital content-sharing peers. The pool includes a requesting peer, to receive requested content, a content sharing peer, and an intermediate node that separates the requesting peer from the content sharing peer. A content provider is configured to deliver the content from the content sharing peer to the requesting peer via the inteπnediate node, wherein the content-sharing peer has access to at least some of the content, and wherein the intermediate node is configured to transfer a chunk of the content from the content sharing peer or the intennediate node to the requesting peer. A tracking service is configured to provide (1) peer or intermediate node identification and (2) chunk identification, and wherein the tracking service is configured to inhibit an inteπnediate node from access to an entirety of the requested content.

In Example 52, the system of Example 5 1 optionally comprises an outdegree parameter indicating a number of first level intermediate nodes that a requesting peer is permitted to contact, and indicating a number of second level intermediate nodes to participate in the delivery of content to the requesting peer through the first level intermediate nodes.

In Example 53, the system of at least one of Examples 51-52 optionally is configured to provide paid content to the requesting peer.

In Example 54, the system of at least one of Examples 51-53 optionally comprises a bank service configured to receive a content purchase request, and, in response, to provide an authorization of content delivery to the requesting peer.

In Example 55, the system of at least one of Examples 51-54 optionally comprises a bank service that is configured to provide an electronic credit to the requesting peer upon a content purchase by the requesting peer.

In Example 56, the system of at least one of Examples 51-55 optionally comprises an intermediate node that is configured to receive a payment for a chunk of requested content to be transferred by the intermediate node in exchange for content transfer capacity provided by the intermediate node.

In Example 57, the system of at least one of Examples 51-56 optionally comprises the intermediate node being configured to provide multiple chunks of the requested content in response to a block request from the requesting peer, wherein an identity of the requesting peer is authenticated before providing the multiple chunks.

In Example 58, the system of at least one of Examples 51-57 optionally comprises the intermediate node being configured to bid against at least one other intermediate node to provide the content transfer capacity.

In Example 59, the system of at least one of Examples 51-58 optionally comprises the tracking service being configured to provide dynamic peer or node identification information for a peer or an intermediate node using at least one distributed hash table (DHT).

In Example 60, the system of at least one of Examples 51-59 optionally comprises at least two decentralized nodes.

In Example 61, the system of at least one of Examples 51-60 optionally comprises a seed peer in the pool of peer-to-peer networked digital content-sharing peers, the seed peer comprising an entirety of the requested content.

In Example 62, the system of at least one of Examples 51-61 optionally comprises a direct download provider configured to provide direct download of the requested content when the requesting peer is unable to receive an entirety of the requested content from the pool of peer-to-peer networked content-sharing peers.

In Example 63, the system of at least one of Examples 51-62 optionally comprises the content provider being configured to provide multiple versions of the requested content, and wherein the tracking service is configured to inhibit an intermediate node from receiving at least one version of the requested content.

In Example 64, the system of at least one of Examples 51-63 optionally includes a requesting peer that comprises: a content transfer rate monitor that is configured to monitor a content transfer rate from a first intermediate node; a comparator, coupled to the content transfer rate monitor, the comparator configured to compare the content transfer rate to a threshold value. In this example, the requesting peer is configured to request a corresponding chunk of digital content from a second intermediate node when the content transfer rate is below the threshold value.

In Example 65, the system of at least one of Examples 51-64 optionally comprises a request queue associated with the intermediate node, wherein the request queue is configured to store a pending content request until the intermediate node becomes available to transfer content in response to the pending content request.

In Example 66, the system of at least one of Examples 51-65 optionally comprises the tracking service being configured to remove from the pool of intermediate nodes an intermediate node that fails to deliver requested content for which the intermediate node has been paid by a requesting peer or intermediate node.

In Example 67, the system of at least one of Examples 51-66 optionally comprises a violation tracking service that detects an instance of inappropriate behavior by an intermediate node or requesting peer.

In Example 68, the system of at least one of Examples 51-67 optionally comprises the violation tracking service being configured to penalize in response to an instance of inappropriate behavior.

In Example 69, the system of at least one of Examples 51-68 optionally comprises a trusted auditor interacting with the pool of peer-to-peer networked content-sharing peers, the trusted auditor configured to mask its identity by at least one of (1) mimicking an intermediate node, a content-sharing peer, or a requesting peer, or (2) probing the intermediate node, the content-sharing peer, or the requesting peer.

In Example 70, the system of at least one of Examples 51-69 optionally comprises at least one trusted auditor interacting, during a given content transfer session, with a requesting peer, a content-sharing peer, or an intermediate node.

In Example 71, the system of at least one of Examples 51-70 optionally comprises at least one secure network connection providing encryption of a content transfer session.

Example 72 describes a system comprising: means for providing requested content to be transferred by a peer-to-peer networked digital content-sharing system from a content-sharing peer to a requesting peer; means for subdividing the content into chunks; means for delivering chunks from a content-sharing peer to a requesting peer through an intermediate node; means for identifying intermediate nodes and content-sharing peers to participate in transferring the requested content; means for assigning an intermediate node to separate a content-sharing peer from a requesting peer during the transferring of the requested content; and means for inhibiting an intermediate node from accessing an entirety of the requested content.

Example 72 describes a machine readable medium including instructions that, when performed by the machine, cause the machine to: provide requested content to be transferred by a peer-to-peer networked digital content-sharing system from a content-sharing peer to a requesting peer; subdivide the content into chunks; deliver chunks from a content-sharing peer to a requesting peer through an intermediate node; identify intermediate nodes and content-sharing peers to participate in transferring the requested content; assign an intermediate node to separate a content-sharing peer from a requesting peer during the transferring of the requested content; and inhibit an intermediate node from accessing an entirety of the requested content.

This overview is intended to provide an overview of subject matter of the present patent application. It is not intended to provide an exclusive or exhaustive explanation of the invention. The detailed description is included to provide further information about the present patent application.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings, which are not necessarily drawn to scale, like numerals may describe similar components in different views. Like numerals having different letter suffixes may represent different instances of similar components. The drawings illustrate generally, by way of example, but not by way of limitation, various embodiments discussed in the present document.

FIG. 1 is a block diagram illustrating generally an example of a system including a pool of peer-to-peer networked digital content-sharing peers.

FIG. 2 is a block diagram illustrating generally an example of a relationship between a tracking service and multiple assigned trusted auditors amongst a pool including a mix of inappropriately behaving and appropriately behaving (neutral) content-sharing and requesting peers.

FIG. 3 illustrates generally portions of an example of the tracking service inhibiting a transfer of requested content in the absence of an authorization provided by the content provider.

FIG. 4 is similar to FlG. 3, but illustrates generally portions of an example of actions of different participants in the peer-to-peer network during a purchase request, authorization, request for content, content-sharing peer identification, content-delivery request, and delivery of requested content.

FIG. 5 is a diagram illustrating generally portions of an example of the participation of a trusted auditor during an instance of an inappropriate request.

FIG. 6 is a diagram, similar to FIG. 5, but illustrating generally portions of an example of the participation of a trusted auditor, mimicking a content-sharing peer, during an instance of an inappropriate request.

FIG. 7 is a diagram illustrating generally an example of a pool of nodes on a peer-to-peer network incorporating intermediate nodes.

FIG. 8 is a block diagram illustrating generally an example of a typical system including content-sharing peers and requesting peers in a peer-to-peer network containing intermediate nodes, and in which some of the nodes can be assigned as trusted auditors.

FIG. 9 is a diagram illustrating generally an example of the relationship between different participants in a peer-to-peer network in which the requesting peer interacts with a bank service.

FIG. 10 is a diagram, similar to FIG. 9, but illustrating generally an example of multiple levels of intermediate nodes, and in which the bank service provides an electronic credit to the requesting peer, and the requesting peer provides an electronic payment to an intermediate node for usage of the intermediate node's transfer capacity to deliver a chunk of requested content.

FIG. 11 is an example of a plot from an economic analysis of two different content distribution methods showing a comparison between various proportions of inappropriately-behaving peers on a peer-to-peer network in the absence of trusted auditors and the resulting profit to a content provider, as compared the profit realized from a direct-download model.

FIG. 12 is an example of a plot from an economic analysis of two different content distribution methods showing a comparison between various proportions of inappropriately-behaving peers on a peer-to-peer network with the addition of an assigned 10: 1 ratio of trusted auditors to inappropriately-behaving peers and in which an inappropriately-behaving peer is assumed to be warned, but allowed to continue participating in the peer-to-peer network.

FIG. 13 is an example of a plot from an economic analysis of two different content distribution methods showing a comparison between various proportions of inappropriately-behaving peers on a peer-to-peer network with the addition of an assigned 10: 1 ratio of trusted auditors to inappropriately-behaving peers and in which an inappropriately-behaving peer is assumed to be forced to use a direct-download method of obtaining content, and is no longer participating in the peer-to-peer network.

DETAILED DESCRIPTION

FIG. 1 is a block diagram illustrating generally an example of a system 100 including a pool of peer-to-peer networked digital content-sharing peers 102. The content sharing peers 102 are communicatively coupled *(e.g.,* by a communicative link such as an optical, wired or wireless computer network) through a computer network to a content provider 104, such as via a seed peer 106. The seed peer 106, in turn, is communicatively coupled through the peer-to-peer network 102 to a content-sharing peer 114 and a trusted auditor 112. The peer-to-peer network can include additional content-sharing peers 114, which are coupled to a requesting peer 110. This can enhance the content transfer rate beyond a typical rate sustained by a single content-sharing peer 114. In some examples, it can even enhance the content transfer rate beyond the rate sustainable by the content provider 104 in a direct-download transfer. Using the content transfer capacity of multiple content sharing peers 114 can reduce the cost to the content provider 104 per content transfer session of the content transfer capacity.

In the example of FIG. 1, a tracking service 108A is communicatively coupled to the requesting peer 110, and to a trusted auditor 112. A tracking service 108B is communicatively coupled through the peer-to-peer network 102 to the seed peer 106A, and content-sharing peer 114A. Although FIG. 1 shows an example in which the tracking services 108A and 108B are separate services, in another example, they can be combined as the same tracking service. In still another example, 108A and 108B could be instances of a larger number of separate tracking services distributed within the peer-to-peer network 102. In certain examples, the tracking services 108A, 108B use consistent hashing or a distributed hashing table (DHT) to provide a look-up service associating a given content request with a location or network address corresponding to the location of the request. For example, the content request can be a cryptographically-encoded key derived from a filename or other identifier for a given piece of content, and such that the encoded key can be provided to the DHT, which can then return the corresponding network address for the requested content, or the content itself. Each encoded key represents a portion of a "keyspace" of all possible keys. The DHT can be used by assigning portions of the keyspace of possible keys to certain nodes, and in the present subject matter, such nodes can be the tracking services 108. When a content-sharing peer 114 enters or leaves the network 102, the tracking service 108 associated with the keyspace corresponding to the content-sharing peer 114 re-computes the hashing table corresponding to the tracking service's 108 portion of the keyspace, but other tracking services 108 need not re-compute their corresponding tables. In particular, the usage of a DHT as opposed to other types of hashing tables reduces the need to modify the entire hashing table *(e.g.,* the relationship between all content keys and their corresponding location on the network) when a content-sharing peer 114 enters or leaves the peer-to-peer network 102. This enhances reliability of the peer-to-peer network 102 when there is a large keyspace corresponding to a wide variety of available content, and where there is a large pool of peers 106, 112, 114, 110.

In FIG. 1, a trusted auditor 112 is communicatively coupled to the content provider 104. The trusted auditor 112 is owned and operated by (or otherwise operating in affiliation with) the content provider 104. In the example shown in FIG. 1 two seed peers 106A, 106B are included. The content provider 114 can provide multiple seed peers 106 distributed within the peer-to-peer network 102. The content provider 114, seed peers 106A, 106B, tracking services 108A, 108B, trusted auditor 112, content-sharing peers 114A, 114B, 114C, and requesting peer 110 can communicate such as by using authenticated or encrypted messages over TCP connections on a network. For example, communication can use SSL and an RC4 cipher during a TCP connection session. Examples of requested content include music files, movie files, music video files, software files, files including previously broadcast television programs, or distributed streaming content.

FIG. 2 is a block diagram illustrating generally an example within the peer-to-peer network 102, in which the tracking service 108 is communicatively coupled to an assigned trusted auditor 112A. The particular trusted auditor 112A is assigned by the tracking service 108 to a peer 200A, such as a content-sharing peer 114 or a requesting peer 110. In certain circumstances, the trusted auditor 112A can be communicatively coupled to an inappropriately behaving content sharing or requesting peer 202A. The trusted auditor 112A can be configured to mimic a content-sharing peer 114 or a requesting peer 110, such as described below. However, the trusted auditor 112A can be configured to record or report instances of inappropriate requests. In certain examples, additional trusted auditors 112B, 112C, and 112D, are communicatively coupled to additional peers 200B, 200C, 200D, 200E, 200F, 200G, 200H, 2001, and 200J. In order to enhance the likelihood of recording an instance of inappropriate behavior, the tracking service 108 can communicate with a number of trusted auditors 112. The number of trusted auditors 112 can be selected using an expected or measured number of inappropriately behaving peers 202 participating in the peer-to-peer network 102. The address of the trusted auditor 112A can be assigned in a way that helps conceal that a node is a trusted auditor 112A *(e.g.,* affiliated with a content provider 104) rather than an unaffiliated or independent content-sharing peer 114 or requesting peer 110. Different trusted auditors 112 can be assigned to the same or different content transfer sessions on the peer-to-peer network 102. In certain examples, a trusted auditor 112 can operate passively, rather than as an active participant in the content transfer session on the peer-to-peer network 102. A passive trusted auditor 112 can observe other participants 200, 202, such as to detect or record an instance of an inappropriate request. In certain examples a trusted auditor 112 can operate actively, such as by probing a requesting peer 110, or a content-sharing peer 114. In certain examples, a trusted auditor 112 can participate actively by probing a requesting peer 110, or a content-sharing peer 114 in a manner resembling or mimicking previously observed behavior of (1) a inappropriately behaving requesting peer 110 or content-sharing peer 114, or (2) of an outside system probing the peer-to-peer network 102. For example, such probing can be using a TCP network connection to generate messages directed at a content-sharing 114 or requesting peer 110 and then listening to the reply from the peer being probed, or flooding a content-sharing 114 or requesting peer 110 with a large number of malformed TCP requests. Probing can also be attempting to participate with a peer (such as an inappropriately behaving peer 202) in a separate content-sharing session following a different protocol, and attempting to exchange content originally transferred via the peer-to-peer network 102, but without authorization or payment. In certain examples, a trusted auditor 112 can be inhibited from probing if desired, such as when the probing would generate excessive traffic on the peer-to-peer network 102. For example, if the observed inappropriate behavior is a "denial of service" attack in which a node excessively barrages one or more other nodes with excessive communications to thwart communications by others, then the trusted auditor 112 can be configured to always or eventually inhibit creating its own "denial of service" attack, such as when doing so would be associated with an unacceptable volume of network traffic in its attempt to mimic inappropriate behavior.

FIG. 3 is a diagram illustrating generally portions of an example of a requesting peer 110 requesting content at 300 without first obtaining an authorization from the tracking service 108. At 302, in response, the tracking service 108 inhibits a transfer of requested content because of the absence of an authorization. For example, inhibiting transfer can be simply not replying to the request, or replying with an error message, or recording an instance of an inappropriate request and preventing further participation in the peer-to-peer network 102.

FIG. 4 is a diagram, similar to FIG. 3, but illustrating generally an example in which at 400 the requesting peer 110 issues a content purchase request. At 402, the content provider 104 provides an authorization of content delivery back to the requesting peer 110. At 404, the requesting peer 110, with authorization, requests the content from the tracking service 108. At 406, the tracking service 108 provides content-sharing peer identification to the requesting peer 110. At 408, the requesting peer 110 uses such content-sharing peer identification to request content delivery from a content-sharing peer 114. At 410, the content-sharing peer 114 delivers the requested content to the requesting peer 110. In an example, the authorization uses strong authentication, such as checking for the presence of valid temporary public/private key pair and a signed credential *(e.g.,* a public-key certificate) provided by an authenticating entity, such as a content provider 104 or a bank service 900 (see FIG. 9 for example of a bank service 900). In the absence of a valid public/private key pair and signed credential, the tracking service 108 inhibits transfer of requested content, such as in FIG. 3.

In certain examples, at 404, the requesting peer 110 makes more than one content delivery request to more than one content-sharing peer 114. This can help increase the content transfer rate. In certain examples, a content-sharing peer 114 is actually a trusted auditor 112 mimicking the behavior of a non-auditor content-sharing peer 114. This increases the likelihood of recording an instance of an inappropriate behavior. In an example, the requesting peer 110 is actually a trusted auditor 112 mimicking a requested peer. In another example, the content-sharing peer 114 is actually a trusted auditor 112 mimicking a content-sharing peer.

FIG. 5 is a diagram illustrating generally portions of an example of a sequence of events on a peer-to-peer network 102. In this example, at 500, a trusted auditor 112 is assigned to report instances of an inappropriate request for content or other inappropriate behavior to a tracking service 108. At 502, an inappropriate request is made by a requesting peer 110 or a content-sharing peer 114. At 504, this results in recording of the instance of the inappropriate behavior. At 506,the instance of the inappropriate request is reported to the tracking service 108. At 508, the tracking service 108 responds by penalizing or removing the inappropriately behaving peer 202 from participation in the peer-to-peer network 102. In certain examples, inappropriate behavior includes a malformed request, a request deviating from an accepted protocol, a request using an invalid or expired credential *(e.g.,* an expired signed certificate, an invalid signed certificate, an expired key, or an invalid key), a request using an invalid session identifier, a request involving an improper port *{e.g.,* a TCP network port that is not recognized for a legitimate use of the peer-to-peer network 102), a request using an invalid protocol message, or the like. Either requesting peers 110 or content-sharing peers 114 can be penalized or removed by the tracking service 108 in response to a report at 506.

In an example, a penalty to an inappropriately behaving peer 202 is "banishment" from the peer-to-peer network 102 to a direct-download system. This prevents the inappropriately behaving peer 202 from realizing a benefit offered by the peer-to-peer network, such as enhanced content transfer capacity, reduced download pricing, or the like. The "banishment" can be of fixed duration. The "banishment" can also depend on observed later behavior of the inappropriately behaving peer 202 *(e.g.,* improving reputation, "good behavior", or the like).

FIG. 6 is a diagram illustrating generally portions of an example of a sequence of events on a peer-to-peer network 102. In this example, at 600, a trusted auditor 112 is assigned to participate in a content-sharing session. At 602, the trusted auditor 112 participates in the content-sharing session by mimicking a content-sharing peer 114. At 604, an inappropriate request is made by a requesting peer 110. At 504, the inappropriate request instance is recorded, such as by the trusted auditor 112. At 506, the instance of the inappropriate request is reported to the tracking service 108. At 508, the tracking service 108 responds by penalizing or removing the inappropriately behaving peer 202 from participation in the content-sharing of the peer-to-peer network 102. Similarly to FIG. 6, a trusted auditor 112 can be assigned to participate in a content-sharing session by mimicking a requesting peer 110, and can correspondingly record an inappropriate request instance and report such an instance to the tracking service 108.

FIG. 7 is a diagram illustrating generally an example of a pool of nodes on a peer-to-peer network 750 (a "graph" of an example of a peer-to-peer network). In this example, a requesting peer HOA communicates with two intermediate nodes 806A, 806D. A communicative coupling 710 between the requesting peer 110 and an inteπnediate node, 806A can be established, for example, by requesting node identification information from a tracking service 108 *(e.g.,* in response to a request for content, a tracking service provides node addressing information for use on a TCP network). Similarly, intermediate node 806A establishes communicative coupling 720 with another intennediate node 806B. Inteπnediate node 806B then establishes its own communicative coupling 730 with a content-sharing peer 114A possessing at least some of the requested content. Other content-sharing peers 114B, 114C, 114D possess other portions of the requested content.

In certain examples, more than one intermediate node 806 can be identified to the requesting peer 110, for example intermediate node 806D, with the number of identified intermediate nodes 806 corresponding to an "outdegree" parameter. The outdegree parameter sets the number of intermediate nodes 806 to which a requesting peer 110 can directly connect during a content transfer session, and in the case of multiple levels of inteπnediate nodes, 806B, 806C, 806E, 806F, the parameter can also specify the number of other intermediate nodes 806 to which an intermediate node 806 can connect directly, for instance through a communication session through a TCP session over a computer network. "Level" refers to the degree of separation between the intermediate node 806A and the requesting peer 110. First level implies that the intermediate node 806 is directly communicatively coupled to a requesting peer 110, for example through a TCP network session. Similarly, second-level implies that the content-sharing peer 114 and a given second level intermediate node 806 are communicatively separated by a first level intermediate node 806.

FIG. 8 is a block diagram illustrating generally an example of a system 800, including a pool of peer-to-peer networked digital content-sharing peers 802. In this example, a requesting peer IIOA communicates with at least one first-level intermediate node 806A. The first-level intermediate node 806A communicates with a second-level intermediate node 806B. The second level intermediate node 806B communicates with at least one content-sharing peer 114C having some of the requested content provided by a content provider 104 for the requesting peer HOA. In this manner, the requesting peer IIOA is likely to be unaware of the identity of the content-sharing peer 114C due to the intervening inteπnediate nodes 806 and the lack of a direct communicative coupling between the requesting peer HOA and the content-sharing peer 114C provided by the peer-to-peer network 802. The protocol of the peer-to-peer network 802 can be used to inhibit direct communication between the requesting peer HOA and the content-sharing peer 114C. In the example in FIG. 8, an inteπnediate node 806 has been assigned as a trusted auditor 804A. This enhances the security of the peer-to-peer network 802. The trusted auditor 804A can be communicatively coupled to the content-sharing peer 114B and a first-level intermediate node 806A, with the intermediate node 806A connected to the requesting peer HOA.

The peer-to-peer network 802 can support multiple independent content transfer sessions. This can involve more than one content-sharing peer 114 and more than one requesting peer H Oconcurrently engaged in different content transfer sessions. In this example, the content-sharing peer 114A, the requesting peers HOB and HOD and the inteπnediate node 806F are not participating in a content-sharing session with the other members specifically shown. Also, in this example, the content-sharing peers 114D and 114E communicate with intermediate nodes 806C and 806E respectively, which in turn communicate with an intermediate node 806D and a trusted auditor 804C, which are both communicatively coupled to a requesting peer HOC for a second content transfer session occurring on the peer-to-peer network 802. As discussed with respect to FIG. 1, FIG. 2, and FIG. 5, in this example, a trusted auditor 804A conceals its identity by mimicking the behavior of an intermediate node 806. In this example, the inappropriate behaviors and penalties as described with respect to FIG. 1, FIG. 2, and FIG. 5 can similarly apply. In addition, there is the possibility of inappropriate behavior on the part of an intermediate node 806A, resulting in penalty or removal of the inteπnediate node 806A, such as for similar behaviors that would result in a penalty or removal of a content-sharing peer 114 or a requesting peer 110. An additional inappropriate behavior of an inteπnediate node 806A, which can be recorded or reported by a trusted auditor 804A, is a failure to transfer requested content to a requesting peer IIOA after receipt by the intermediate node 806A of an electronic payment. For example, if requesting peer HOA were instead a trusted auditor 804, such an assignment can be used to detect intermediate node 806A failing to transfer requested content.

In FIG 8., an intermediate node 806A is shown communicating to both a trusted auditor 804A and an intermediate node 806B. In one example, the intermediate node 806A is configured with a request queue. This can help accommodate the intermediate node 806B handling multiple queued content transfer requests. It can increase the content transfer rate through "pipelining." If the intermediate node 806A is busy handling a previous pending content request, a requesting node, such as intermediate node 806B, can be inhibited from consuming further content transfer capacity by repeatedly requesting content transfers and receiving "BUSY" indications from intermediate node 806A. This permits the intermediate node 806A to handle a previous pending request, such as a content transfer request from trusted auditor 804A.

There can also be a communication link between the content provider 104 and the requesting peers 11OA, HOB, HOC, and HOD. This can provide direct-download capability, such as in the event that one of the requesting peers 11OA, 11OB, HOC, or HOD is unable to receive an entirety of the requested content using the peer-to-peer network 802. This "recovery" capability allows the content provider 104 to offer enhanced availability of requested content to encourage participation in the peer-to-peer network 102, even when the reliability of the peer-to-peer network 802 is less than perfect. The number of missing "chunks" is likely to be small (where a "chunk" is a portion of at least some of the requested content). Therefore, providing the "recovery" capability is unlikely to result in significantly increased load on the content provider 104.

FIG. 9 is a diagram illustrating generally portions of an example of a sequence of events on a peer-to-peer network 802. In this example, at 902, a request for content by a requesting peer 110 is made to a bank service 900. At 904, in response, the bank service 900 provides a content delivery authorization. At 906, the requesting peer 110 then provides a request for content with authorization to a tracking service 108. At 908, in response, the tracking service 108 provides node identification to the requesting peer 110. At 910, the node identification enables the requesting peer 110 to request content from an intermediate node 806. At 912, the intermediate node 806 responds with a request to the tracking service 108 for node and content chunk identification. At 914, the tracking service 108 responds with node and chunk identification. At 916, this enables the intermediate node 806 to request a chunk of content from a content-sharing peer 114. At 918, the content-sharing peer 114 responds with a transfer of a chunk of requested content. At 920, the intermediate node 806 responds by transferring the content that it received from the content-sharing peer 114 to the requesting peer 110. In this example, the content-sharing peer 114 has only some of the requested content. This allows a content provider to inhibit an intermediate node 806 from accessing an entirety of the requested content. This avoids a form of free-loading in which participating intermediate nodes 806 can acquire the entirety of the content for their own use, or for redistribution. In certain examples, the intermediate node 806 may not be able to establish contact with a content-sharing peer 114 having the desired content. This may occur, for example, when the peer has exited the network 802, or does not have the requested chunk. In certain examples, the tracking service 108 does not identify specific chunks to be transferred by an inteπnediate node 806. Instead, the tracking service 108 identifies chunks that an intermediate node 806 is forbidden to transfer. The intermediate node 806 can use a download heuristic in which it requests a chunk from a content-sharing peer 114 without prior knowledge as to whether the content-sharing peer 114 has the requested chunk. Instead, the intermediate node 806 discovers amongst a list of assigned content sharing peers 114 those peers 114 that have the requested chunk *(e.g.,* traverses the "graph" formed by the pool of nodes and connections 750 as shown in FIG. 7). hi an example, the content-sharing peer 114 transmits a different randomly-selected chunk than the requested chunk, where the different chunk is still part of the requested content {*e.g.,* sending a different piece of the requested content than was originally requested). This increases the efficiency of the peer-to-peer network 802 by allowing content-sharing peers 114 with only small proportions of the entirety of the requested content to propagate such content to other nodes, increasing the chance that during a future content transfer session, additional content-sharing peers 114 have a greater proportion of the chunks making up the requested content.

In certain examples, the requesting peer 110 can repeat the actions starting at 906, but requesting the corresponding content from a different intermediate node 806 than had been previously contacted. If the requesting peer 110 has multiple content chunk requests pending from a variety of intermediate nodes 806, it may be that at least one intermediate node 806 will fail to respond with the requested content, or will respond slowly. A "boosting" effect of requesting similar content from an alternate intermediate node 806 can help increase the content transfer rate. Particularly near the end of a given content transfer session, this can improve throughput and increase the likelihood of a successful transfer to the requesting peer 110 of an entirety of the requested content. In an example, the requesting peer 110 can monitor the content transfer rate. If the rate falls below a threshold value, the requesting peer 110 can initiate such "boosting" by contacting an alternate intermediate node 806 with a request for similar content.

One concern a content provider 104 can have is that the roles of the participating nodes will vary from one content session to another. In some cases a content-sharing peer 114 will become a requesting peer 110 for a later session. Similarly, in certain examples, the requesting peer 110 will have previously participated as an intermediate node 806 in a prior content transfer session. The content provider can impose restrictions on what content an intermediate node 806 is allowed to transfer, with emphasis on preventing an intermediate node 806 from obtaining content without payment or authorization by virtue of being "in the middle" during a prior transfer session. For example, the content provider 104 can save at least one "reserved" version of the requested content that is qualitatively similar, but distinct from the version of the requested content that the requesting peer 110 had previously transferred as an intermediate node. At 906 when the requesting peer 110 attempts to transfer this requested content, the content provider 104 at 908, through the tracking service 108, can identify an intermediate node 806 that can transfer a different version of the requested content. This protects the interests of a content provider 104 in preventing an intermediate node 806 from appropriating content, for example, without authorization or payment, since the content provider 104 can render useless any previously transferred "chunks" of content that happened to be stored by the requesting peer 110 from its prior role as an intermediate node 806. Without the reserved version, the requesting peer 110 can aggregate previously stored chunks of content with chunks of requested content presently being transferred to acquire an entirety of the content. The requesting peer 110 can then terminate the content transfer session early, and report failure, while in fact the transfer has been successful. This can result in reduction or denial of due compensation to the content provider 104. However, if the requesting peer 110 stores chunks during a previous transfer session, and the content provider 104 at 908 selects the reserved version such that the previously stored chunks are not part of the reserved version, the value of the previously-stored chunks is diminished and the content provider 104 is more likely to have accurate information regarding the success or failure of content transfer *(e.g.,* such information can be used in future content transfer session by the content provider 908 to determine which version of content is to be transferred).

FIG. 10 is a diagram illustrating generally portions of an example of a sequence of events on a peer-to-peer network 802. At 950, a requesting peer 110 requests purchase of content from a bank service 900. At 904, in response, the bank service 900 provides an authorization of content delivery. At 952, also in response to a content purchase request, the bank service 900 provides an electronic credit to the requesting peer 110. This can include crediting an electronic account held by the requesting peer 110, or issuing the requesting peer 110 one or more negotiable electronic "coins" to be used in later transactions. At 906, the requesting peer 110 provides a request for content with authorization to a tracking service 108. At 908, in response, the tracking service 108 provides node identification to the requesting peer 110. At 954A, this enables the requesting peer 110 to request content from and provide an electronic payment to an intermediate node 806A. In an example, the electronic payment includes the intermediate node 806A contacting the bank service 900 with a signed credential or policy allowing the intermediate node 806A to authenticate the validity of the electronic payment offered by the requesting peer 110. In certain examples, the electronic payment includes transfer of one or more negotiable "electronic coins." An electronic coin can be configured as an electronic token *(e.g.,* a certificate) redeemable by the holder for cash *(e.g.,* currency, a negotiable instrument, or the like) from a bank service 900. The electronic payment provides an incentive for an inteπnediate node 806A to contribute its transfer capacity in the content transfer session, even though it does not have access to an entirety of the content. In the absence of the benefit of access to an entirety of the content being transferred, an inteπnediate node 806 may have little reason to remain as a participant in the peer-to-peer network 802. At 912, the inteπnediate node 806A responds with a request to the tracking service 108 for node and content chunk identification. At 914, the tracking service 108 responds with node and chunk identification. In an example, the intermediate node 806A can then directly contact a content-sharing peer 114, such as in FIG 9. At 954B, the first-level intermediate node 806A requests content and provides electronic payment to the identified second-level intermediate node 806B. In some examples, the intermediate node 806B can itself proceed through a series of requests to the tracking service 108, such as to identify additional intermediate nodes or a content-sharing peer 114. In this example, the intermediate node 806B makes a content delivery request and electronic payment to a content-sharing peer 114. At 956A, the content sharing peer 114 delivers a chunk of requested content to the intermediate node 806B. At 956B, the intermediate node 806B delivers a chunk of requested content to intermediate node 806A. At 956C, the intermediate node 806A delivers a chunk of requested content to the requesting peer HOC. In certain examples, an electronic payment is made for each chunk of content transferred, and is made to each participating intermediate node 806A, 806B and to the content-sharing peer

114. The requesting peer 110 can provide sufficient electronic payment such that an intermediate node 806A can keep a portion of the payment and pass on the remainder to the next intermediate node 806B or to the content-sharing peer 114. For example, assuming two intermediate nodes 806A, 806B and a single content-sharing peer 114, the requesting peer 110 at 954A provides three units of electronic payment, the intermediate node 806A can keep one unit of payment, then at 954B can request content from intermediate node 806B with two units of payment, and similarly intermediate node 806B keeps one unit of payment and at 954C submits a content request to the requesting peer 114 with one unit of payment. In some examples, a requesting peer 110 can make a single payment and a block request for multiple chunks of content. In response, multiple chunks of content are transferred by intermediate nodes 806A, 806B and a content sharing peer 114. A block request can help increase the content transfer rate by reducing the protocol overhead associated with payment and content requests.

In an example, at 952, the bank service 900 can provide an electronic credit in excess of the minimum credit required for the requesting peer 110 to transfer an entirety of the requested content. Such a minimum credit can correspond to the number of intermediate node 806 and content sharing peer 114 "edges" traversed by the requested content through the series of connections between the content-sharing peer 114, intermediate node 806A, and 806B, multiplied by the number of chunks to be transferred. This permits a micro-payment to be made to each participant for each chunk transferred by each peer or node in the network 802. The excess (above the minimum credit) can be used by the requesting peer 110 to recover from a situation in which an inappropriately behaving intermediate node 806A, or 806B, or content-sharing peer 114 fails to deliver requested content after receiving an electronic payment. In such a case, the excess credit can be used to make another request along a different pathway. The bank service at 900 can invalidate a requesting peer's 110 remaining excess credit from a given content transfer session after the entirety of the requested content is successfully transferred to the requesting peer 110. In certain examples, the intermediate node 806A bids against other similar identified intermediate nodes 806, and the requesting peer 110 offers electronic payment to the intermediate node 806 providing more desirable bid with respect to the other bidding intermediate nodes 806. A bid can be deemed more desirable based on one or more characteristics, such as if the bid requests less payment, promises reduced latency *(e.g.,* the time it takes an individual node to respond to a request), the bidder has a good reputation, or can the bidder can provide increased content transfer rate *(e.g.,* the sustained data transfer rate available from a particular node).

FIG. 11 is a plot of an economic analysis 150 using an analytical model of two different content distribution methods employing a fixed cost for transfer capacity (labeled as "bandwidth"). FIG. 11 shows a comparison between various proportions of inappropriately-behaving peers 202 on a peer-to-peer network 102 and the resulting profit to a content provider 104 in the absence of trusted auditors 112. The profit realized from a direct-download model is used as basis for comparison. The content provider 104 profit-per-download 152 is plotted for each model against the content provider 104 profit before bandwidth cost 154. In this example, the resulting profit line from a direct-download method 156 intersects the line 158 representing the peer-to-peer network 102 performance when it includes 60% inappropriately behaving peers 202 (m=60%). This indicates that at a certain threshold 160 of expected profit, the peer-to-peer distribution model may be less profitable than a direct-download method, in the absence of trusted auditors 112. Another line 162 shows that for a proportion of 80% inappropriately behaving peers 202, the cross-over threshold is correspondingly reduced 170. The peer-to-peer network 102 remains consistently more profitable if the number of inappropriately-behaving peers 202 is further reduced to 40% as shown 164, or to 20% as shown 166, or to nothing (an ideal scenario) 168.

FIG. 11 shows in summary that on an existing peer-to-peer network 102, the absence of trusted auditors can erode the economic benefit to a content provider 104 of the usage of a peer-to-peer network 102 rather than direct-download network for content distribution once the proportion of inappropriately behaving peers 202 reaches a certain threshold. The model does not address illicit content sharing that occurs outside of the peer-to-peer network 102. However, such transfers could be separately addressed, such as through digital rights management mechanism.

FIG. 12 is a plot of an economic analysis 250 using an analytical model of two different content distribution methods employing a fixed cost for transfer capacity (labeled as "bandwidth"). FIG. 12 shows a comparison between various proportions of inappropriately-behaving peers 202 on a peer-to-peer network 102 and the resulting profit to a content provider 104. This can be modeled by the steady-state result of a Markov decision process in which inappropriately-behaving peers 202 seek to form clusters of two peers ("growth factor" = 2), a 5% "renewal rate" of additional inappropriately behaving peers 202 appears each later download session, and with an assigned 10: 1 ratio of trusted auditors 112 to inappropriately-behaving peers 202. The profit realized from a direct-download model can be used as basis for comparison. In this model, an inappropriately-behaving peer 202 is warned, but allowed to continue participating in the peer-to-peer network 102 (a "conservative" policy on the part of the content provider 104).

The content provider 104 profit-per-download 152 is plotted for each model against the content provider 104 profit before bandwidth cost 154. In the range plotted, the resulting profit line from a direct-download method 156 no longer crosses the line 258 representing the peer-to-peer network 102 performance when there are 60% inappropriately-behaving peers 202 (m=60%). This shows that the direct-download model for content distribution is expected to be consistently less profitable for the content provider 104 under the conditions shown. Even at a proportion of 90% inappropriately-behaving peers 202, the profit line shows 260 that the content provider 104 would need to expect a much greater profit than is shown in the range plotted before the content provider 104 would realize more profit using the direct-download model. The range plotted 250 makes the assumption that at the highest profit level plotted, the content provider 104 is attempting to gross twice for each content transfer session as is consumed on transfer capacity (bandwidth) expense, namely four units of profit before bandwidth cost, and two units of bandwidth cost per content transfer session. The peer-to-peer network 102 remains consistently and correspondingly more profitable if the number of inappropriately-behaving peers 202 is further reduced to 80% as shown 262, or to 40% as shown 264, or to 20% as shown 266, or finally to nothing (an ideal scenario) 168.

FIG 12 shows in summary that on a peer-to-peer network 102, the presence of 10: 1 ratio of trusted auditors 112 to inappropriately-behaving peers 202 can enhance the economic benefit to a content provider 104 of usage of a peer-to-peer network 102 rather than direct-download network for content distribution. The model does not address illicit content transfers occurring outside of the peer-to-peer network 102, but such out-of-network or out-of-band transfers can be separately addressed, such as through a digital rights management mechanism.

FIG. 13 is a plot of an economic analysis 250 using an analytical model of two different content distribution methods employing a fixed cost for transfer capacity (labeled as "bandwidth"). FIG. 13 shows a comparison between various proportions of inappropriately-behaving peers 202 on a peer-to-peer network 102 and the resulting profit to a content provider 104. This can be modeled by the steady-state result of a Markov decision process wherein inappropriately-behaving peers 202 seek to form clusters of two peers, ("growth factor" = 2), a 5% "renewal rate" of additional inappropriately behaving peers 202 appears each subsequent download session, and with an assigned 10:1 ratio of trusted auditors 112 to inappropriately-behaving peers 202. The profit realized from a direct-download model can be used as basis for comparison. FIG. 13 differs from FIG. 12 in that an inappropriately-behaving peer 202 that is detected is forced to use a direct-download method of obtaining content, and is no longer participating in the peer-to-peer network 102 (an "aggressive" policy on the part of the content provider).

The content provider 104 profit-per-download 152 is plotted for each model against the content provider 104 profit before bandwidth cost 154. In the range plotted, the resulting profit line from a direct-download method 156 does not cross the line 358 representing the peer-to-peer network 102 performance when there are 60% inappropriately-behaving peers 202 (m=60%), showing that the direct-download model for content distribution can be consistently less profitable for the content provider 104 under the conditions shown. At a proportion of 90%

inappropriately-behaving peers **202,** the profit line **360** roughly overlaps the line representing direct-download **156** as expected under the new "aggressive" policy, showing a break-over **370** wherein direct-download can become marginally more profitable. The peer-to-peer network **102** can remain correspondingly more profitable if the number of inappropriately-behaving peers **202** is further reduced to 80% as shown at 362, or to 40% as shown at 364, or to 20% as shown at 366, or finally to nothing at **168.**

FIG 13 shows in summary that on a peer-to-peer network, the presence of 10: 1ratio of trusted auditors **112** to inappropriately-behaving peers **202** can enhance the economic benefit to a content provider of usage of a peer-to-peer network **102** rather than direct-download network for content distribution even if an "aggressive" policy is imposed that forces many of the peer-to-peer network participants onto a direct-download model if they have been detected behaving inappropriately. The model does not address out-of-network ("out of band") transfers, but such transfers might be separately addressed, such as through a digital rights management mechanism.

The above detailed description includes references to the accompanying drawings, which form a part of the detailed description. The drawings show, by way of illustration, specific embodiments in which the invention can be practiced. These embodiments are also referred to herein as "examples." All publications, patents, and patent documents referred to in this document are incorporated by reference herein in their entirety, as though individually incorporated by reference. In the event of inconsistent usages between this document and those documents so incorporated by reference, the usage in the incorporated reference(s) should be considered supplementary to that of this document; for irreconcilable inconsistencies, the usage in this document controls.

In this document, the terms "a" or "an" are used, as is common in patent documents, to include one or more than one, independent of any other instances or usages of "at least one" or "one or more." In this document, the term "or" is used to refer to a nonexclusive or, such that "A or B" includes "A but not B," "B but not A," and "A and B," unless otherwise indicated. In the appended claims, the terms "including" and "in which" are used as the plain-English equivalents of the respective terms "comprising" and "wherein." Also, in the following claims, the terms "including" and "comprising" are open-ended, that is, a system, device, article, or process that includes elements in addition to those listed after such a term in a claim are still deemed to fall within the scope of that claim. Moreover, in the following claims, the terms "first," "second," and "third," etc. are used merely as labels, and are not intended to impose numerical requirements on their objects.

Method examples described herein can be machine or processor-implemented at least in part. Some examples can include a processor-readable medium or machine-readable medium encoded with instructions operable to configure an electronic device to perform methods as described in the above examples. An implementation of such methods can include code, such as microcode, assembly language code, a higher-level language code, or the like. Such code can include processor readable instructions for performing various methods. The code may form portions of processor program products. Further, the code may be tangibly stored on one or more volatile or non-volatile processor-readable media during execution or at other times. These processor-readable media may include, but are not limited to, hard disks, removable magnetic disks, removable optical disks *(e.g.,* compact disks and digital video disks), magnetic cassettes, memory cards or sticks, random access memories (RAMs), read only memories (ROMs), and the like.

The above description is intended to be illustrative, and not restrictive. For example, the above-described examples (or one or more aspects thereof) may be used in combination with each other. Other embodiments can be used, such as by one of ordinary skill in the art upon reviewing the above description. The Abstract is provided to comply with 37 C.F.R. §1.72(b), to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. Also, in the above Detailed Description, various features may be grouped together to streamline the disclosure. This should not be interpreted as intending that an unclaimed disclosed feature is essential to any claim. Rather, inventive subject matter may lie in less than all features of a particular disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separate embodiment. The scope of the invention should be detennined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

WHAT IS CLAIMED IS:

1. A method comprising:

seeding a peer-to-peer networked digital content-sharing system with content from a content provider;

providing requested content to be transferred from a content-sharing peer to a requesting peer;

identifying a content-sharing peer to participate in transferring the requested content;

recognizing an identified peer as trustworthy;

assigning a recognized trustworthy identified peer as a trusted auditor; and

detecting, using the trusted auditor, an instance of an inappropriate behavior.

2. The method of claim 1, comprising assigning a number of trusted auditors as a function of a number of inappropriately behaving peers.

3. The method of claim 1, comprising:

receiving payment from the requesting peer for the content to be transferred; and

in response to receiving payment, authorizing content delivery to the requesting peer.

4. The method of claim 3, comprising selecting a number of trusted auditors to provide or enhance a profit of the providing requested content to the requesting peer.

5. The method of claim 3, comprising:

assigning at least 6% of a total number of content-sharing and requesting peers as trusted auditors; and

receiving at least twice the value of an expended transfer capacity of a content sharing instance as payment for the content sharing instance.

6. The method of claim 1, comprising inhibiting transfer of requested content without an authorization for content delivery.

7. The method of claim 1, comprising:

reporting, by a trusted auditor, to the tracking service an inappropriate behavior of a content-sharing peer or requesting peer.

8. The method of claim 7, comprising:

mimicking, by a trusted auditor, a behavior of a content-sharing peer or a requesting peer to conceal an identity of the trusted auditor.

9. The method of claim 8, comprising:

mimicking, by a trusted auditor, an inappropriate behavior of (1) a content-sharing peer, (2) a requesting peer, or (3) an outside system probing a content-sharing or a requesting peer.

10. The method of claim 7, 8, or 9, comprising:

removing a content-sharing or requesting peer from participation in the peer-to-peer network in response to an instance of at least one inappropriate behavior.

11. The method of claim 7, 8, or 9, comprising:

penalizing a content-sharing or requesting peer in response to an instance of at least one inappropriate behavior.

12. The method of claim 1, comprising:

varying an address of a trusted auditor to conceal an identity of the trusted auditor.

13. The method of claim 1, comprising:

monitoring traffic generated by a trusted auditor;

comparing the traffic to a threshold value; and

adjusting behavior of the trusted auditor when the traffic exceeds the threshold value.

14. The method of claim 1, comprising authenticating at least one request or response made over the peer-to-peer network.

15. A system comprising:

a pool of peer-to-peer networked digital content-sharing peers, including a requesting peer to receive requested content from another peer;

a content-sharing peer, configured to host at least some of the requested content;

a content provider, configured to deliver an entirety of the requested content;

a tracking service, configured to provide content-sharing peer node identification; and

a trusted auditor, configured to be recognized as trustworthy by the tracking service, configured to participate in the pool of peer-to-peer networked digital content-sharing peers, configured to be assigned by the tracking service to a content-sharing session, and configured to record an instance of inappropriate behavior.

16. The system of claim 15, wherein the tracking service is configured to assign a number of trusted auditors as a function of a total number of inappropriately behaving peers.

17. The system of claim 15, wherein the content provider is configured to receive a content purchase request, and, in response, to provide an authorization of content delivery to the requesting peer.

18. The system of claim 17, wherein the tracking service and content-sharing peers are configured to inhibit transfer of requested content without an authorization for content delivery.

19. The system of claim 17, comprising a specified number of trusted auditors, wherein the number of trusted auditors is a function of a number of peers.

20. The system of claim 17, wherein a number of the trusted auditors is specified to be at least 10% of an expected or detected number of inappropriate users.

21. The system of claim 15, wherein the trusted auditor is configured to report to the tracking service an instance of inappropriate behavior of (1) a content-sharing peer or (2) a requesting peer.

22. The system of claim 21, wherein the trusted auditor is configured to conceal its identity by mimicking behavior of (1) a content-sharing peer or (2) a requesting peer.

23. The system of claim 22, wherein the trusted auditor is configured to mimic inappropriate behavior of (1) a content-sharing peer, (2) a requesting peer, or (3) an outside system probing a content-sharing peer or a requesting peer.

24. The system of claim 21, 22, or 23, wherein the tracking service comprises a violation tracking service that is configured to remove a content-sharing or a requesting peer from participation in the peer-to-peer network in response to at least one instance of inappropriate behavior by the content-sharing or requesting peer.

25. The system of claim 21, 22, or 23, wherein the tracking service comprises a violation tracking service that is configured to penalize a content-sharing or requesting peer in response to at least one instance of inappropriate behavior by the content-sharing or requesting peer.

26. The system of claim 15, wherein the trusted auditor comprises a variable address.

27. The system of claim 15, wherein the trusted auditor comprises:

a traffic monitor, configured to monitor a volume of probing traffic generated by the trusted auditor; and

a comparator, coupled to the traffic monitor, the comparator configured to compare the traffic generated by the trusted auditor against a threshold value, and wherein the trusted auditor is configured to adjust its activity when the traffic exceeds the threshold value.

28. The system of claim 15, wherein the network is configured to provide at least one authentication of a request or a response.

29. A system comprising:

means for seeding a peer-to-peer networked digital content-sharing system with content from a content provider;

means for providing requested content to be transferred from a content-sharing peer to a requesting peer;

means for identifying a content-sharing peer to participate in transferring the requested content;

means for recognizing an identified peer as trustworthy;

means for assigning a recognized trustworthy identified peer as a trusted auditor; and

means for detecting an instance of inappropriate behavior of a peer.

30. A machine readable medium including instructions that, when performed by the machine, cause the machine to:

seed a peer-to-peer networked digital content-sharing system with content from a content provider;

provide requested content to be transferred from a content-sharing peer to a requesting peer;

identify a content-sharing peer to participate in transferring the requested content;

recognize an identified peer as trustworthy;

assign a recognized trustworthy identified peer as a trusted auditor; and

detect an instance of an inappropriate behavior.

31. A method comprising:

providing requested content to be transferred by a peer-to-peer networked digital content-sharing system from a content-sharing peer to a requesting peer;

subdividing the content into chunks;

delivering chunks from a content-sharing peer to a requesting peer through an intermediate node;

identifying an intermediate node and a content-sharing peer to participate in transferring the requested content;

assigning an intermediate node to separate a content-sharing peer from a requesting peer during the transferring of the requested content; and

inhibiting an intermediate node from accessing an entirety of the requested content.

32. The method of claim 31, comprising limiting a number of assigned intermediate nodes, which separate a content-sharing peer from a requesting peer during the transferring of the requested content, to a value that is less than or equal to an outdegree parameter value.

33. The method of claim 31, comprising:

receiving payment from the requesting peer for the content to be transferred; and

in response to the receiving payment, authorizing content delivery to the requesting peer.

34. The method of claim 33, comprising electronically crediting the requesting peer in response to the receiving payment from the requesting peer.

35. The method of claim 34, comprising paying an intermediate node for a chunk of requested content and, in response, transferring the requested content.

36. The method of claim 31, comprising receiving a request and payment for transfer of a block of multiple chunks of requested content.

37. The method of claim 31, comprising bidding, by an intermediate node against other intermediate nodes, for participating in a content transfer.

38. The method of claim 31, comprising constructing at least one distributed hash table (DHT) and identifying a peer or node to a peer or node using the DHT.

39. The method of claim 31, comprising providing decentralized tracking of the identified peer or intermediate node.

40. The method of claim 31, comprising seeding a network of peer-to-peer networked digital content-sharing peers with an entirety of the requested content.

41. The method of claim 31, comprising transferring at least some of the requested content by direct download when the requesting peer fails to receive an entirety of the requested content from the pool of peer-to-peer networked content-sharing peers.

42. The method of claim 31, comprising providing multiple versions of the requested content, and inhibiting an intermediate node from receiving at least one version of the requested content.

43. The method of claim 31, comprising monitoring by the requesting peer the content transfer rate from a first inteπnediate node, comparing transfer rate to a threshold value, and requesting a corresponding chunk of digital content from a second intermediate node when the content transfer rate is below the threshold value.

44. The method of claim 31, comprising storing a content request to an intermediate node in a request queue, and transferring the content from the content request when the inteπnediate node becomes available.

45. The method of claim 31, comprising removing from the pool of intermediate nodes an inteπnediate node that fails to deliver requested content for which the intermediate node has been paid.

46. The method of claim 31, comprising detecting an instance of inappropriate behavior of an intermediate node or requesting peer.

47. The method of claim 46, comprising penalizing a detected instance of inappropriate behavior of an intermediate node or a requesting peer.

48. The method of claim 31, comprising auditing members of the pool of peer-to-peer networked content-sharing peers by a trusted auditor, the auditing comprising at least one of (1) mimicking an intermediate node, a content-sharing peer, or a requesting peer, or (2) probing the intermediate node, the content-sharing peer, or the requesting peer.

49. The method of claim 31, comprising assigning at least one trusted auditor to interact with a requesting peer, a content-sharing peer, or an intermediate node during a content transfer session.

50. The method of claim 31, comprising encrypting a content-sharing transaction on the peer-to-peer networked digital content-sharing system.

51. A system comprising:

a pool of peer-to-peer networked digital content-sharing peers, the pool including:

a requesting peer, to receive requested content;

a content sharing peer; and

an intermediate node that separates the requesting peer from the content sharing peer;

a content provider, configured to deliver the content from the content sharing peer to the requesting peer via the intermediate node, wherein the content-sharing peer has access to at least some of the content, and wherein the intermediate node is configured to transfer a chunk of the content from the content sharing peer or the intermediate node to the requesting peer; and

a tracking service, configured to provide (1) peer or intermediate node identification and (2) chunk identification, and wherein the tracking service is configured to inhibit an intermediate node from access to an entirety of the requested content.

52. The system of claim 51, comprising an outdegree parameter indicating a number of first level intermediate nodes that a requesting peer is permitted to contact, and indicating a number of second level intermediate nodes to participate in the delivery of content to the requesting peer through the first level intermediate nodes.

53. The system of claim 51, wherein the system is configured to provide paid content to the requesting peer.

54. The system of claim 53, including a bank service configured to receive a content purchase request, and, in response, to provide an authorization of content delivery to the requesting peer.

55. The system of claim 54, wherein the bank service is configured to provide an electronic credit to the requesting peer upon a content purchase by the requesting peer.

56. The system of claim 55, wherein an intermediate node is configured to receive a payment for a chunk of requested content to be transferred by the intermediate node in exchange for content transfer capacity provided by the intermediate node.

57. The system of claim 51, wherein the intermediate node is configured to provide multiple chunks of the requested content in response to a block request from the requesting peer, wherein an identity of the requesting peer is authenticated before providing the multiple chunks.

58. The system of claim 51, wherein the intermediate node is configured to bid against at least one other intermediate node to provide the content transfer capacity.

59. The system of claim 51, wherein the tracking service is configured to provide dynamic peer or node identification information for a peer or an intermediate node using at least one distributed hash table (DHT).

60. The system of claim 51, wherein the tracking service comprises at least two decentralized nodes.

61. The system of claim 51, comprising a seed peer in the pool of peer-to-peer networked digital content-sharing peers, the seed peer comprising an entirety of the requested content.

62. The system of claim 51, comprising a direct download provider configured to provide direct download of the requested content when the requesting peer is unable to receive an entirety of the requested content from the pool of peer-to-peer networked content-sharing peers.

63. The system of claim 51, wherein the content provider is configured to provide multiple versions of the requested content, and wherein the tracking service is configured to inhibit an intermediate node from receiving at least one version of the requested content.

64. The system of claim 51, wherein the requesting peer comprises:

a content transfer rate monitor that is configured to monitor a content transfer rate from a first intermediate node;

a comparator, coupled to the content transfer rate monitor, the comparator configured to compare the content transfer rate to a threshold value; and
wherein the requesting peer is configured to request a corresponding chunk of digital content from a second inteπnediate node when the content transfer rate is below the threshold value.

65. The system of claim 51, comprising a request queue associated with the intermediate node, wherein the request queue is configured to store a pending content request until the intermediate node becomes available to transfer content in response to the pending content request.

66. The system of claim 51, wherein the tracking service is configured to remove from the pool of intermediate nodes an intermediate node that fails to deliver requested content for which the intermediate node has been paid by a requesting peer or intermediate node.

67. The system of claim 51, wherein the tracking service comprises a violation tracking service that detects an instance of inappropriate behavior by an intermediate node or requesting peer.

68. The system of claim 67, wherein the violation tracking service is configured to penalize in response to an instance of inappropriate behavior.

69. The system of claim 51, comprising a trusted auditor interacting with the pool of peer-to-peer networked content-sharing peers, the trusted auditor configured to mask its identity by at least one of (1) mimicking an intermediate node, a content-sharing peer, or a requesting peer, or (2) probing the intermediate node, the content-sharing peer, or the requesting peer.

70. The system of claim 69, wherein during a given content transfer session, at least one trusted auditor interacts with a requesting peer, a content-sharing peer, or an intermediate node.

71. The system of claim 51, comprising at least one secure network connection providing encryption of a content transfer session.

72. A system comprising:

means for providing requested content to be transferred by a peer-to-peer networked digital content-sharing system from a content-sharing peer to a requesting peer;

means for subdividing the content into chunks;

means for delivering chunks from a content-sharing peer to a requesting peer through an intermediate node;

means for identifying intermediate nodes and content-sharing peers to participate in transferring the requested content;

means for assigning an intermediate node to separate a content-sharing peer from a requesting peer during the transferring of the requested content; and means for inhibiting an intermediate node from accessing an entirety of the requested content.

73. A machine readable medium including instructions that, when performed by the machine, cause the machine to:

provide requested content to be transferred by a peer-to-peer networked digital content-sharing system from a content-sharing peer to a requesting peer;

subdivide the content into chunks;

deliver chunks from a content-sharing peer to a requesting peer through an inteπnediate node;

identify inteπnediate nodes and content-sharing peers to participate in transferring the requested content;

assign an intermediate node to separate a content-sharing peer from a requesting peer during the transferring of the requested content; and

inhibit an intermediate node from accessing an entirety of the requested content.

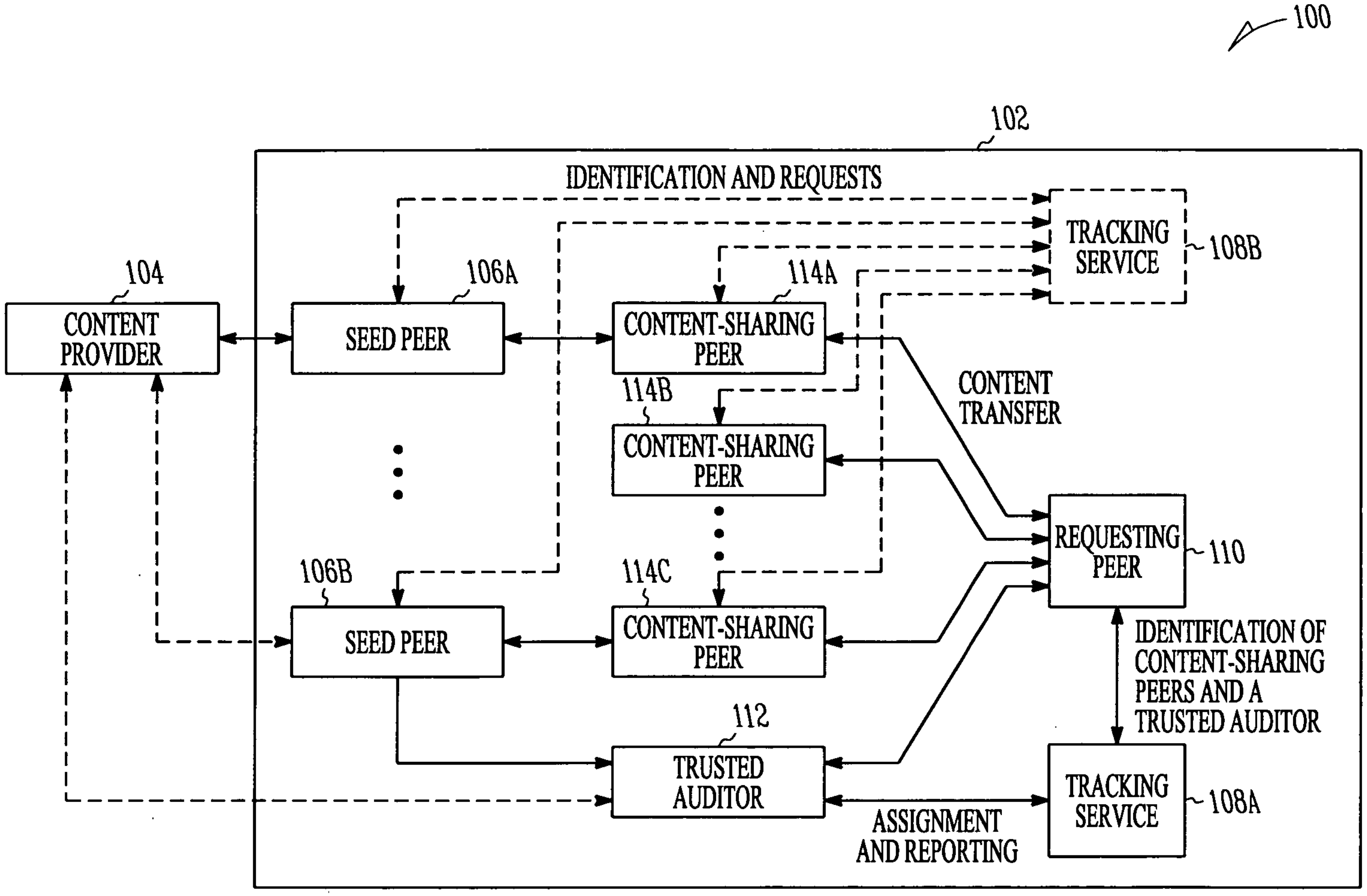

100
102
IDENTIFICATION AND REQUESTS
TRACKING SERVICE
108B
104
CONTENT PROVIDER
106A
SEED PEER
114A
CONTENT-SHARING PEER
114B
CONTENT-SHARING PEER
CONTENT TRANSFER
REQUESTING PEER
110
106B
SEED PEER
114C
CONTENT-SHARING PEER
IDENTIFICATION OF CONTENT-SHARING PEERS AND A TRUSTED AUDITOR
112
TRUSTED AUDITOR
ASSIGNMENT AND REPORTING
TRACKING SERVICE
108A

FIG. 1

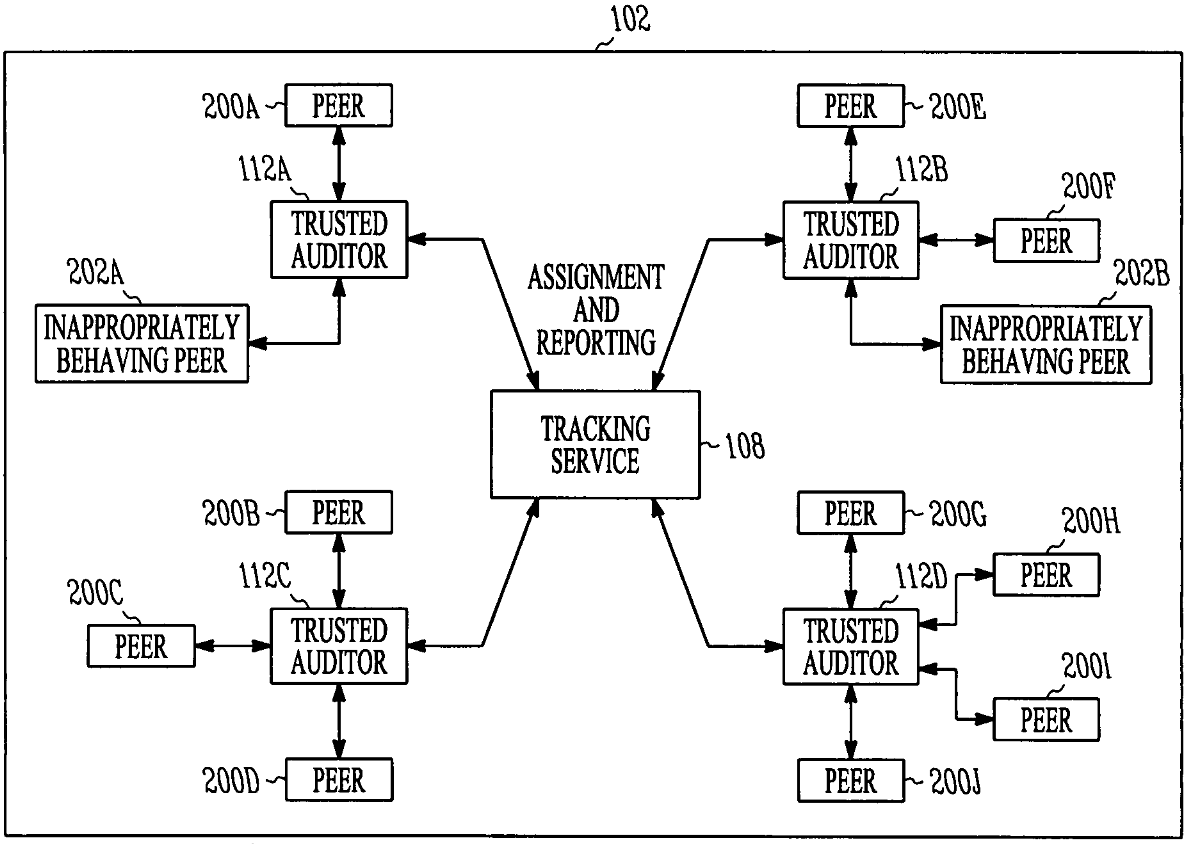

102
200A
PEER
112A
TRUSTED AUDITOR
202A
INAPPROPRIATELY BEHAVING PEER
ASSIGNMENT AND REPORTING
PEER
200E
112B
TRUSTED AUDITOR
200F
PEER
202B
INAPPROPRIATELY BEHAVING PEER
TRACKING SERVICE
108
200B
PEER
112C
200C
PEER
TRUSTED AUDITOR
200D
PEER
PEER
200G
200H
112D
PEER
TRUSTED AUDITOR
200I
PEER
PEER
200J

FIG. 2

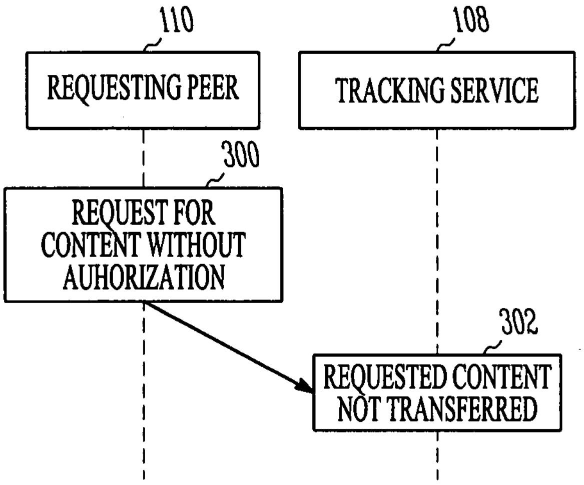

110
REQUESTING PEER
108
TRACKING SERVICE
300
REQUEST FOR CONTENT WITHOUT AUHORIZATION
302
REQUESTED CONTENT NOT TRANSFERRED

FIG. 3

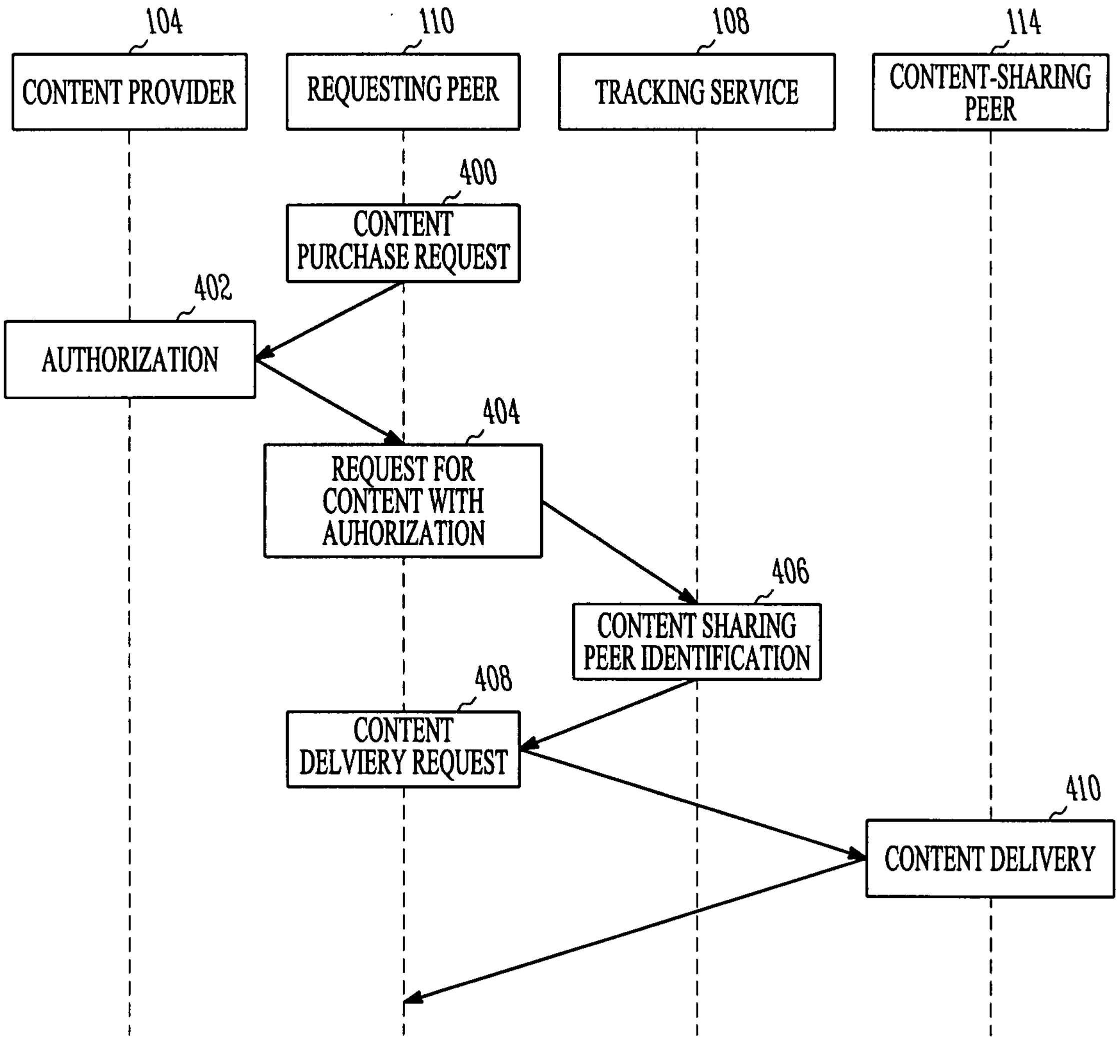

104
CONTENT PROVIDER
110
REQUESTING PEER
108
TRACKING SERVICE
114
CONTENT-SHARING PEER
400
CONTENT PURCHASE REQUEST
402
AUTHORIZATION
404
REQUEST FOR CONTENT WITH AUHORIZATION
406
CONTENT SHARING PEER IDENTIFICATION
408
CONTENT DELVIERY REQUEST
410
CONTENT DELIVERY

FIG. 4

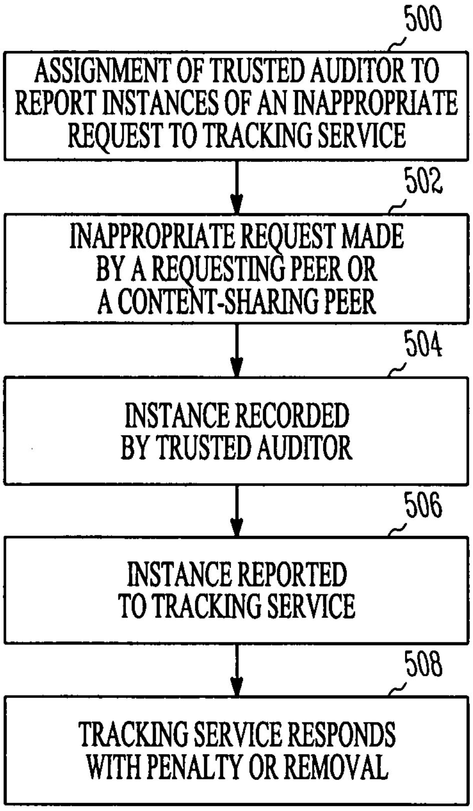

500
ASSIGNMENT OF TRUSTED AUDITOR TO REPORT INSTANCES OF AN INAPPROPRIATE REQUEST TO TRACKING SERVICE
502
INAPPROPRIATE REQUEST MADE BY A REQUESTING PEER OR A CONTENT-SHARING PEER
504
INSTANCE RECORDED BY TRUSTED AUDITOR
506
INSTANCE REPORTED TO TRACKING SERVICE
508
TRACKING SERVICE RESPONDS WITH PENALTY OR REMOVAL

FIG. 5

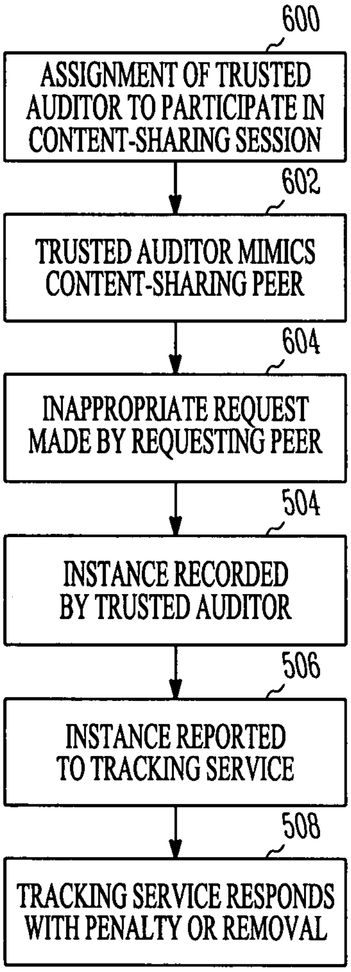

600
ASSIGNMENT OF TRUSTED AUDITOR TO PARTICIPATE IN CONTENT-SHARING SESSION
602
TRUSTED AUDITOR MIMICS CONTENT-SHARING PEER
604
INAPPROPRIATE REQUEST MADE BY REQUESTING PEER
504
INSTANCE RECORDED BY TRUSTED AUDITOR
506
INSTANCE REPORTED TO TRACKING SERVICE
508
TRACKING SERVICE RESPONDS WITH PENALTY OR REMOVAL

FIG. 6

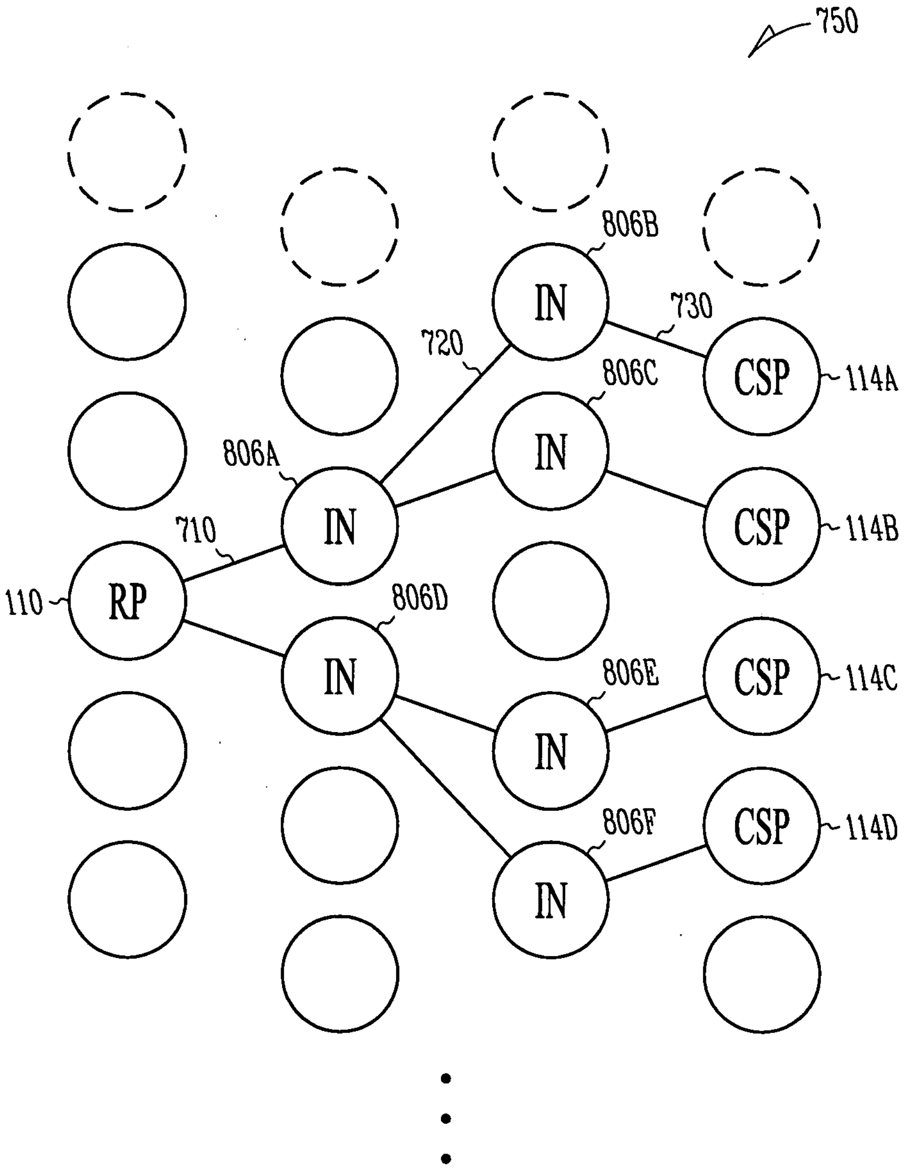

750
806B
IN
730
720
CSP
114A
806C
IN
806A
IN
CSP
114B
710
110
RP
806D
IN
806E
CSP
114C
IN
806F
CSP
114D
IN

FIG. 7

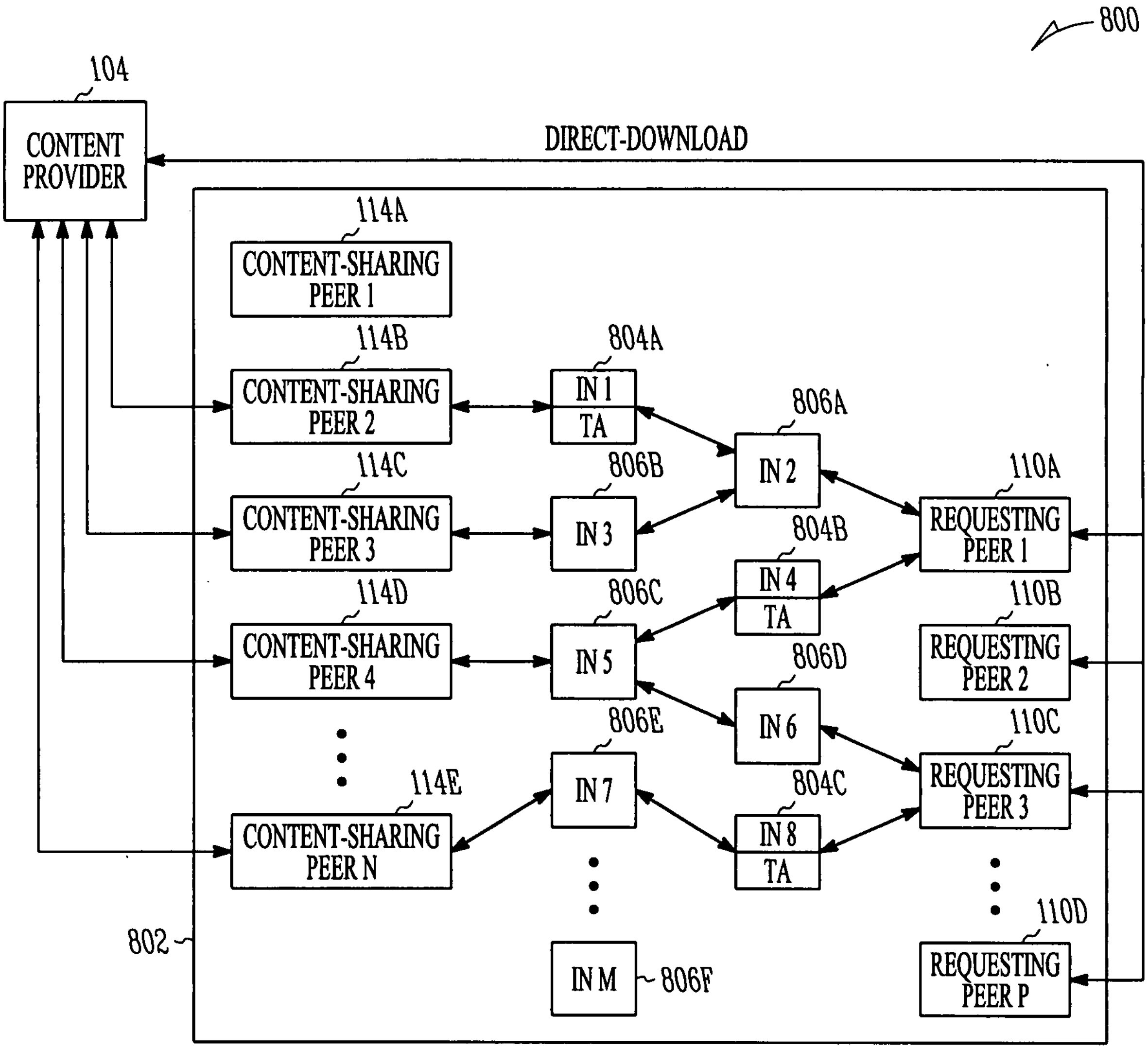

800
104
CONTENT PROVIDER
DIRECT-DOWNLOAD
114A
CONTENT-SHARING PEER 1
114B
CONTENT-SHARING PEER 2
114C
CONTENT-SHARING PEER 3
114D
CONTENT-SHARING PEER 4
114E
CONTENT-SHARING PEER N
804A
IN 1
TA
806A
IN 2
806B
IN 3
804B
IN 4
TA
806C
IN 5
806D
IN 6
806E
IN 7
804C
IN 8
TA
IN M
806F
110A
REQUESTING PEER 1
110B
REQUESTING PEER 2
110C
REQUESTING PEER 3
110D
REQUESTING PEER P
802

FIG. 8

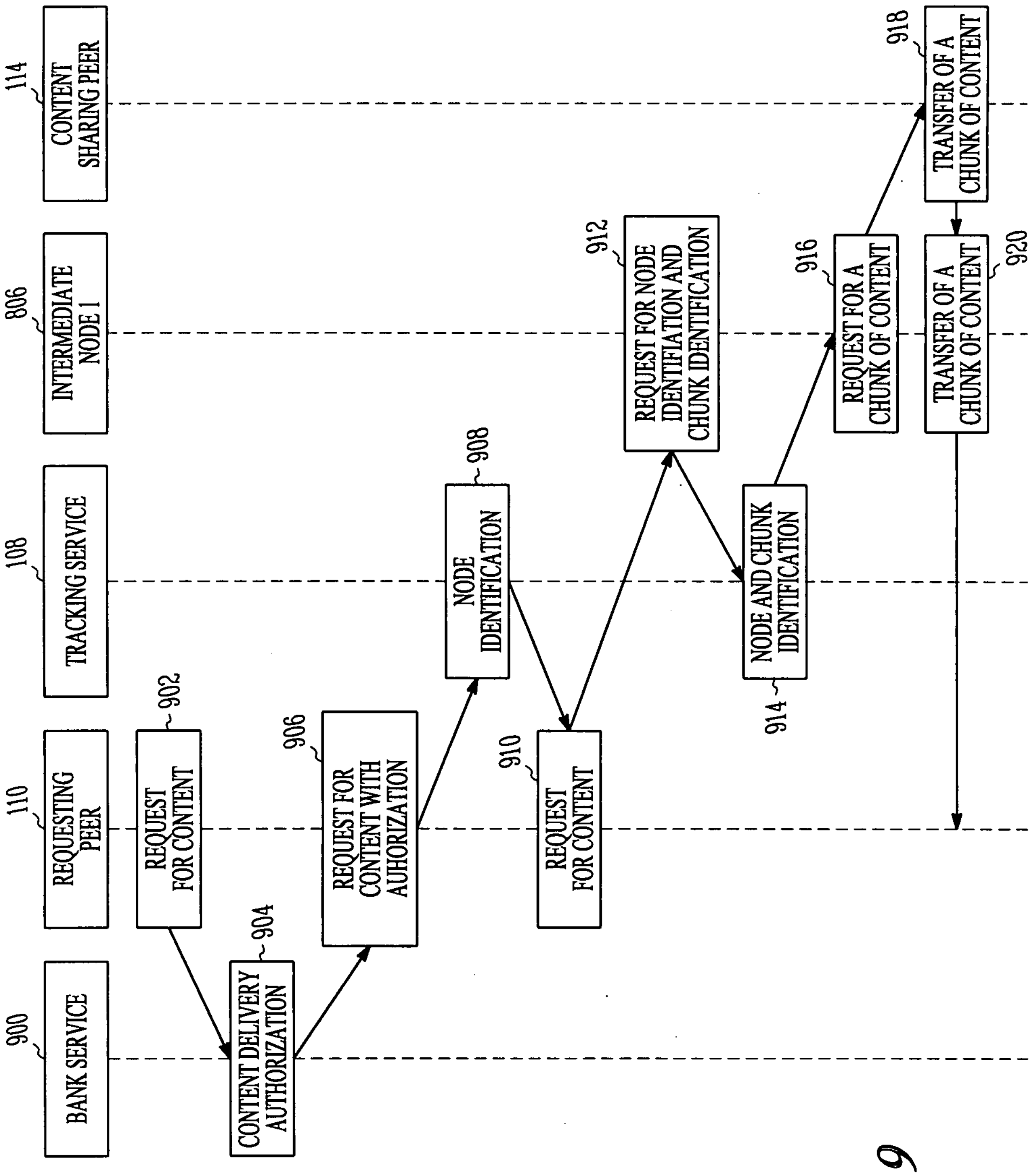

900
BANK SERVICE
110
REQUESTING PEER
108
TRACKING SERVICE
806
INTERMEDIATE NODE 1
114
CONTENT SHARING PEER
902
REQUEST FOR CONTENT
904
CONTENT DELIVERY AUTHORIZATION
906
REQUEST FOR CONTENT WITH AUHORIZATION
908
NODE IDENTIFICATION
910
REQUEST FOR CONTENT
912
REQUEST FOR NODE IDENTIFIATION AND CHUNK IDENTIFICATION
914
NODE AND CHUNK IDENTIFICATION
916
REQUEST FOR A CHUNK OF CONTENT
918
TRANSFER OF A CHUNK OF CONTENT
920
TRANSFER OF A CHUNK OF CONTENT

FIG. 9

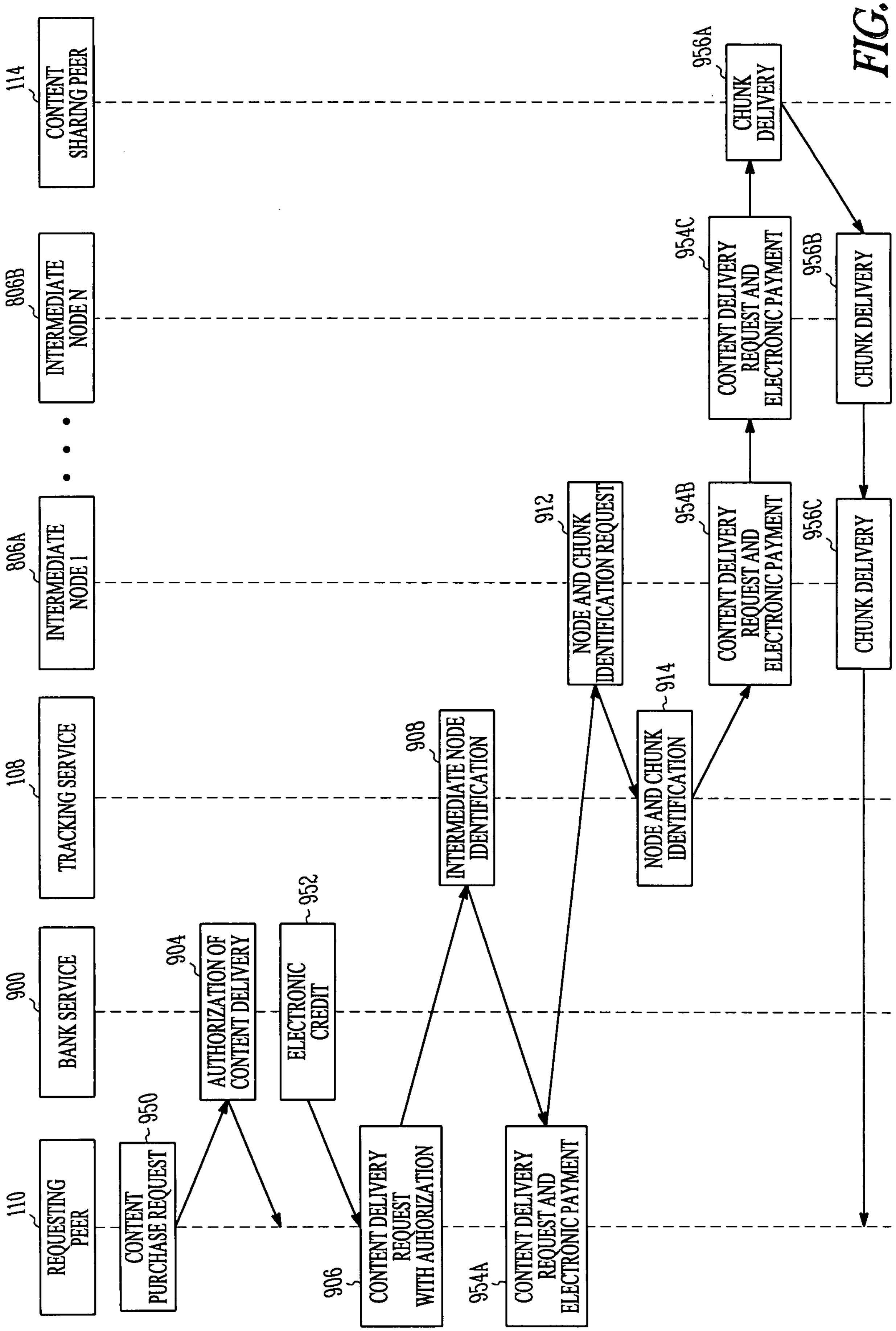

110
REQUESTING PEER
900
BANK SERVICE
108
TRACKING SERVICE
806A
INTERMEDIATE NODE 1
806B
INTERMEDIATE NODE N
114
CONTENT SHARING PEER
950
CONTENT PURCHASE REQUEST
904
AUTHORIZATION OF CONTENT DELIVERY
952
ELECTRONIC CREDIT
906
CONTENT DELIVERY REQUEST WITH AUHORIZATION
908
INTERMEDIATE NODE IDENTIFICATION
954A
CONTENT DELIVERY REQUEST AND ELECTRONIC PAYMENT
912
NODE AND CHUNK IDENTIFICATION REQUEST
914
NODE AND CHUNK IDENTIFICATION
954B
CONTENT DELIVERY REQUEST AND ELECTRONIC PAYMENT
954C
CONTENT DELIVERY REQUEST AND ELECTRONIC PAYMENT
956A
CHUNK DELIVERY
956B
CHUNK DELIVERY
956C
CHUNK DELIVERY

FIG. 10

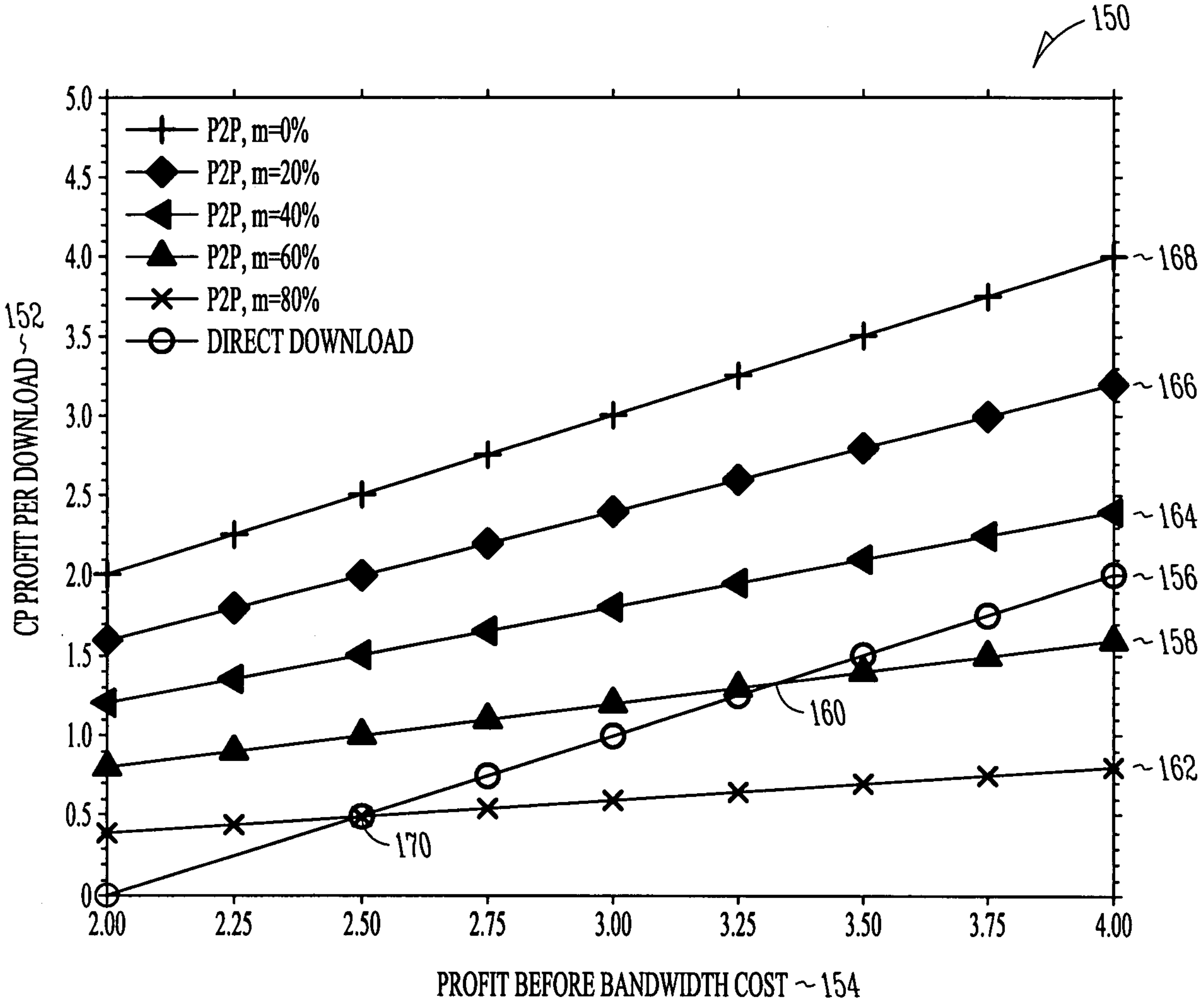

150
P2P, m=0%
P2P, m=20%
P2P, m=40%
P2P, m=60%
P2P, m=80%
DIRECT DOWNLOAD
CP PROFIT PER DOWNLOAD ~ 152
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0
2.00
2.25
2.50
2.75
3.00
3.25
3.50
3.75
4.00
PROFIT BEFORE BANDWIDTH COST ~ 154
168
166
164
156
158
160
162
170

FIG. 11

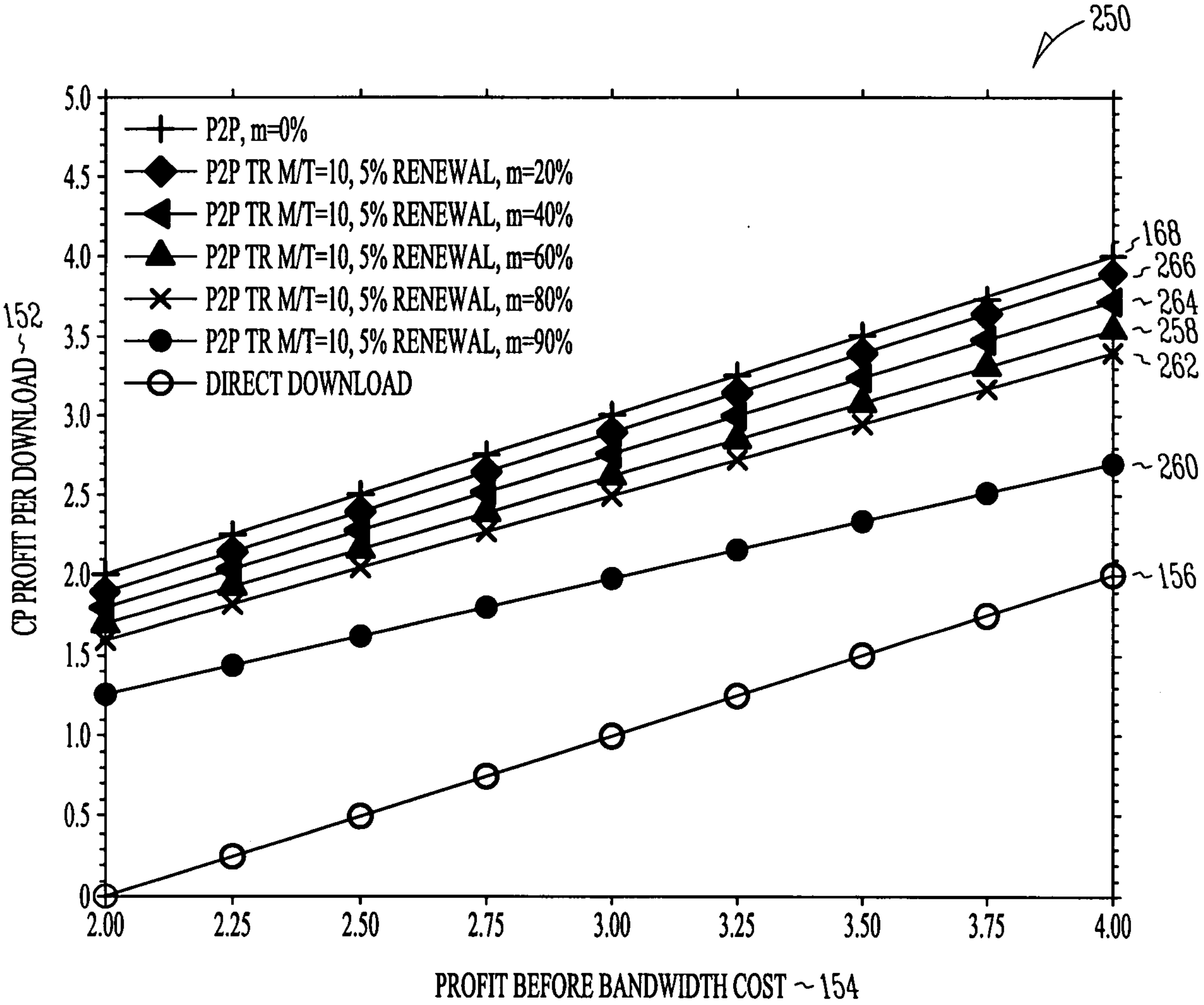

250
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0
CP PROFIT PER DOWNLOAD
152
P2P, m=0%
P2P TR M/T=10, 5% RENEWAL, m=20%
P2P TR M/T=10, 5% RENEWAL, m=40%
P2P TR M/T=10, 5% RENEWAL, m=60%
P2P TR M/T=10, 5% RENEWAL, m=80%
P2P TR M/T=10, 5% RENEWAL, m=90%
DIRECT DOWNLOAD
168
266
264
258
262
260
156
2.00
2.25
2.50
2.75
3.00
3.25
3.50
3.75
4.00
PROFIT BEFORE BANDWIDTH COST ~ 154

FIG. 12

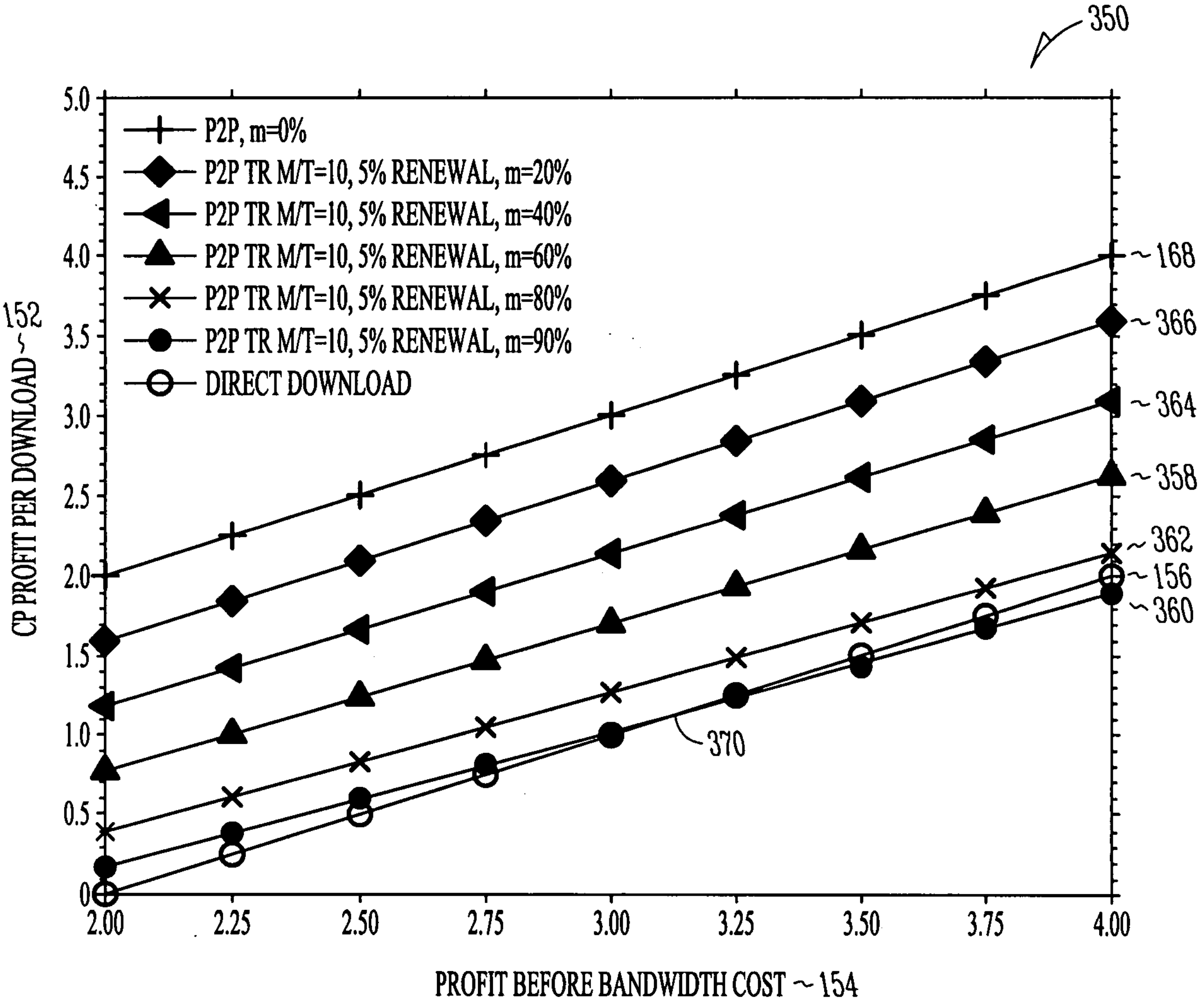

350
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0
CP PROFIT PER DOWNLOAD ~ 152
2.00
2.25
2.50
2.75
3.00
3.25
3.50
3.75
4.00
PROFIT BEFORE BANDWIDTH COST ~ 154
+ P2P, m=0%
◆ P2P TR M/T=10, 5% RENEWAL, m=20%
◀ P2P TR M/T=10, 5% RENEWAL, m=40%
▲ P2P TR M/T=10, 5% RENEWAL, m=60%
× P2P TR M/T=10, 5% RENEWAL, m=80%
● P2P TR M/T=10, 5% RENEWAL, m=90%
○ DIRECT DOWNLOAD
168
366
364
358
362
156
360
370

FIG. 13