



US 20190089610A1

(19) **United States**

(12) **Patent Application Publication**  
**Chan**

(10) **Pub. No.: US 2019/0089610 A1**

(43) **Pub. Date: Mar. 21, 2019**

(54) **PARALLEL COMPUTATIONAL  
FRAMEWORK AND APPLICATION SERVER  
FOR DETERMINING PATH CONNECTIVITY**

**H04L 12/24** (2006.01)

**H04L 29/08** (2006.01)

(52) **U.S. Cl.**

**CPC** ..... **H04L 43/065** (2013.01); **G06F 17/3064**  
(2013.01); **G06N 7/005** (2013.01); **H04L**  
**43/045** (2013.01); **H04L 67/22** (2013.01);  
**H04L 43/0805** (2013.01); **H04L 43/16**  
(2013.01); **H04L 41/14** (2013.01)

(71) Applicant: **www.TrustScience.com Inc.**, Edmonton  
(CA)

(72) Inventor: **Leo M. Chan**, Edmonton (CA)

(21) Appl. No.: **16/195,946**

(22) Filed: **Nov. 20, 2018**

#### **Related U.S. Application Data**

(63) Continuation of application No. 15/953,011, filed on  
Apr. 13, 2018, now Pat. No. 10,187,277, which is a  
continuation of application No. 15/623,103, filed on  
Jun. 14, 2017, now abandoned, which is a continu-  
ation of application No. 15/224,063, filed on Jul. 29,  
2016, now abandoned, which is a continuation of  
application No. 13/503,352, filed on Aug. 28, 2012,  
now Pat. No. 9,443,004, filed as application No.  
PCT/CA2010/001658 on Oct. 22, 2010.

(60) Provisional application No. 61/254,313, filed on Oct.  
23, 2009.

#### **Publication Classification**

(51) **Int. Cl.**

**H04L 12/26** (2006.01)

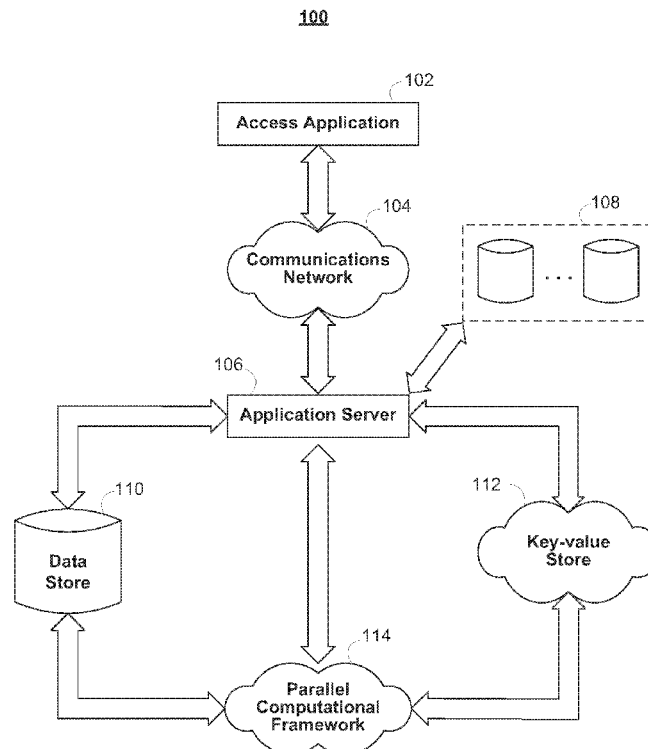
**G06F 17/30** (2006.01)

**G06N 7/00** (2006.01)

(57)

#### **ABSTRACT**

Systems and methods for social graph data analytics to determine the connectivity between nodes within a community are provided. A user may assign user connectivity values to other members of the community, or connectivity values may be automatically harvested or assigned from third parties or based on the frequency of interactions between members of the community. Connectivity values may represent such factors as alignment, reputation, status, and/or influence within a social graph of a network community, or the degree of trust. The paths connecting a first node to a second node may be retrieved, and social graph data analytics may be performed on the retrieved paths. For example, a network connectivity value may be determined from all or a subset of all of the retrieved paths. Network connectivity values and/or other social graph data may be outputted to third-party processes, services, and ratings agencies for use in initiating automatic transactions, making automated network-based or real-world decisions, determining or verifying the identity of a node within the community, scoring or ranking nodes, or making credit-granting decisions.



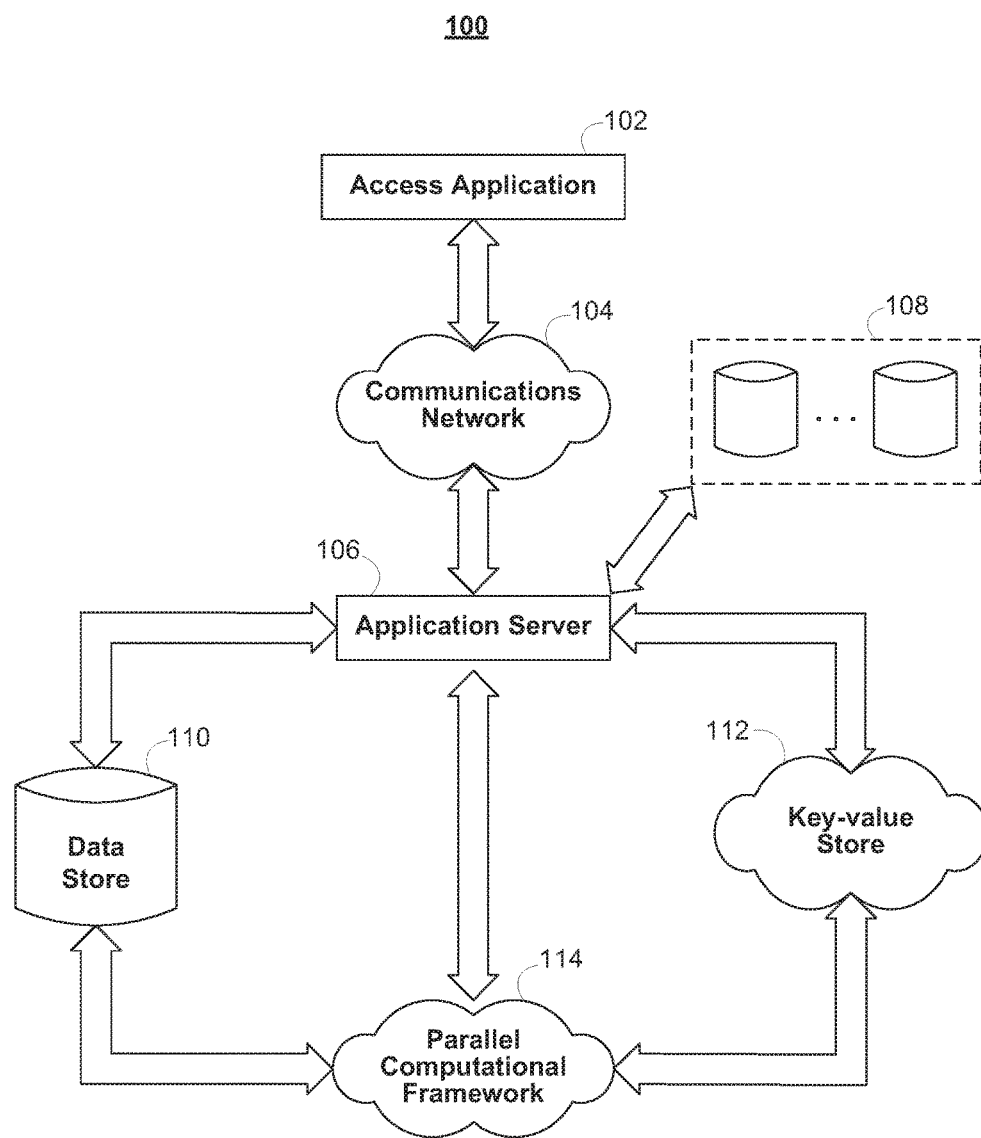


FIG. 1

200

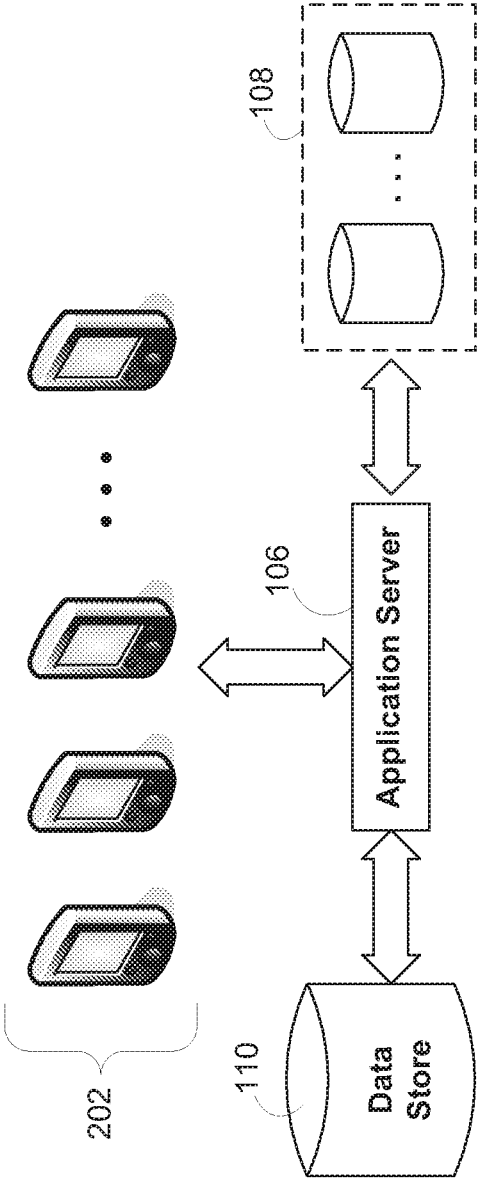


FIG. 2

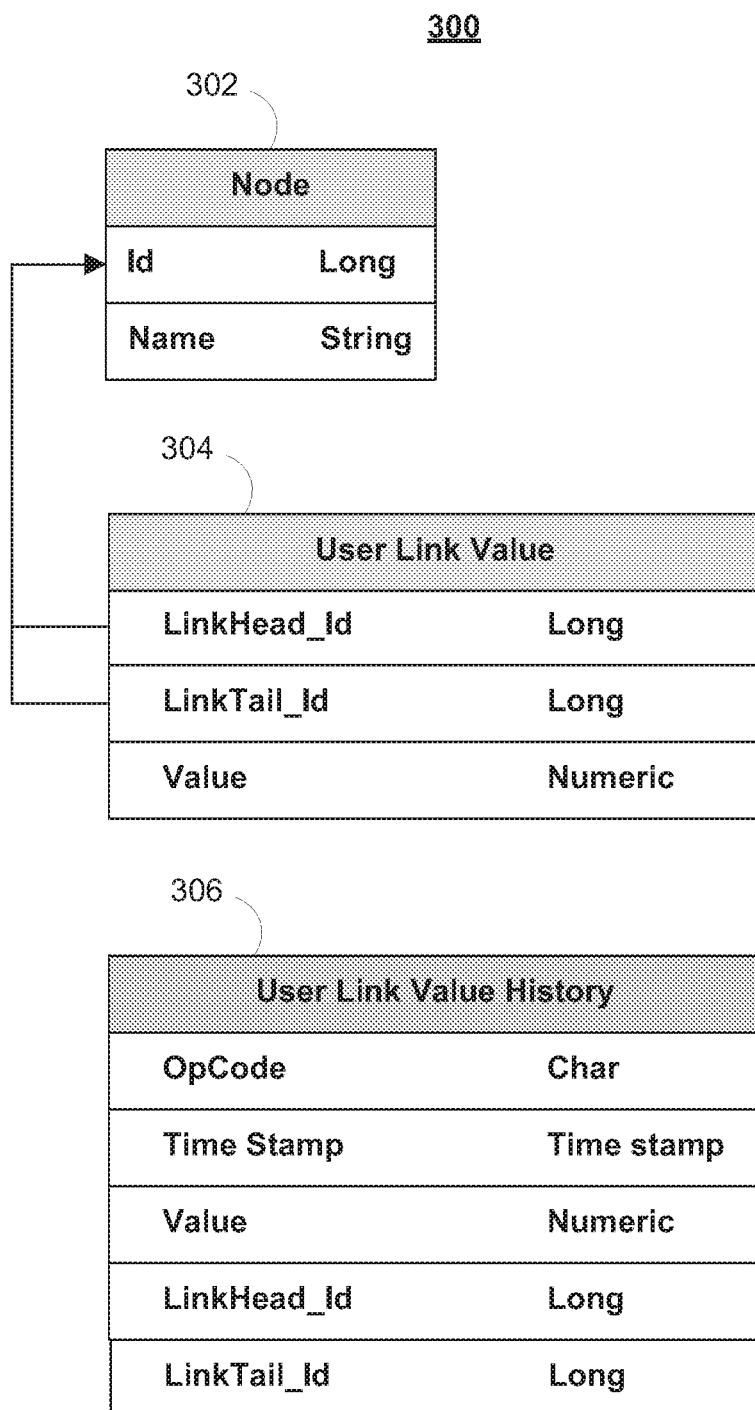


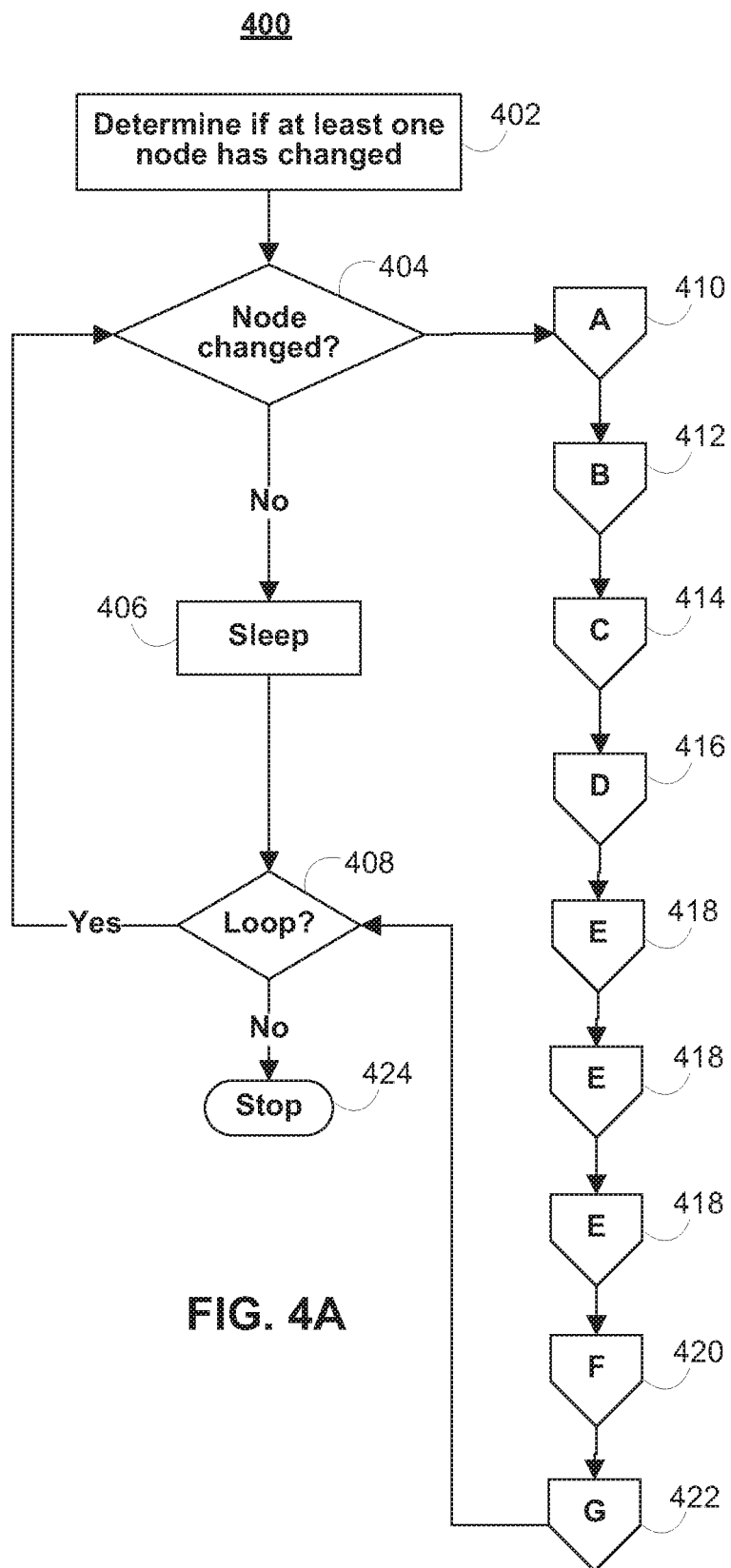
FIG. 3A

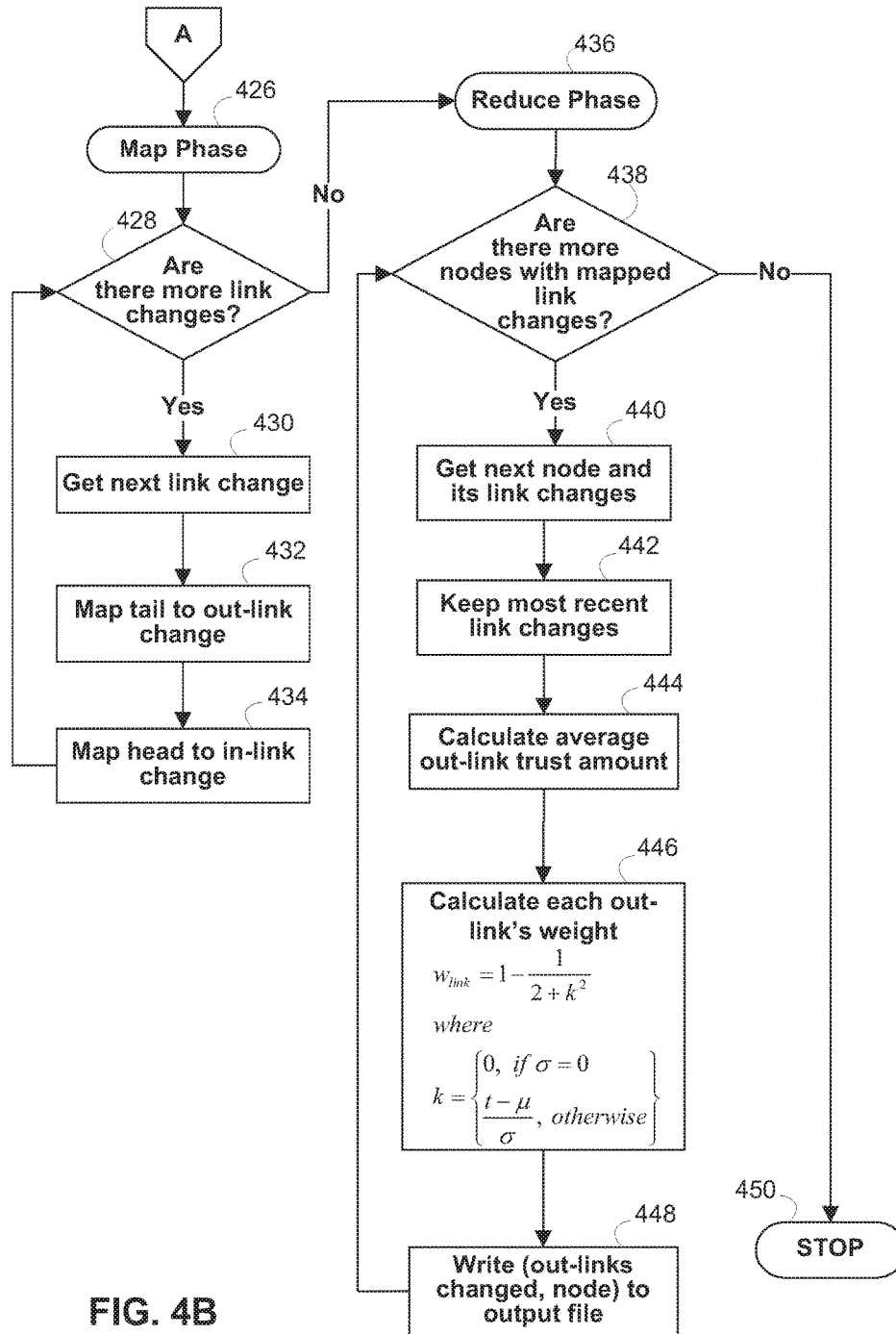
310

312

	<b>Node Table</b>	
314	<b>RowId</b>	<b>64-bit Integer</b>
316	<b>"info:inlinks"</b>	<b>List</b>
318	<b>"info:outlinks"</b>	<b>List</b>
320	<b>"inBucket:" + source node id</b>	<b>List</b>
322	<b>"outBucket:" + target node id</b>	<b>List</b>

**FIG. 3B**





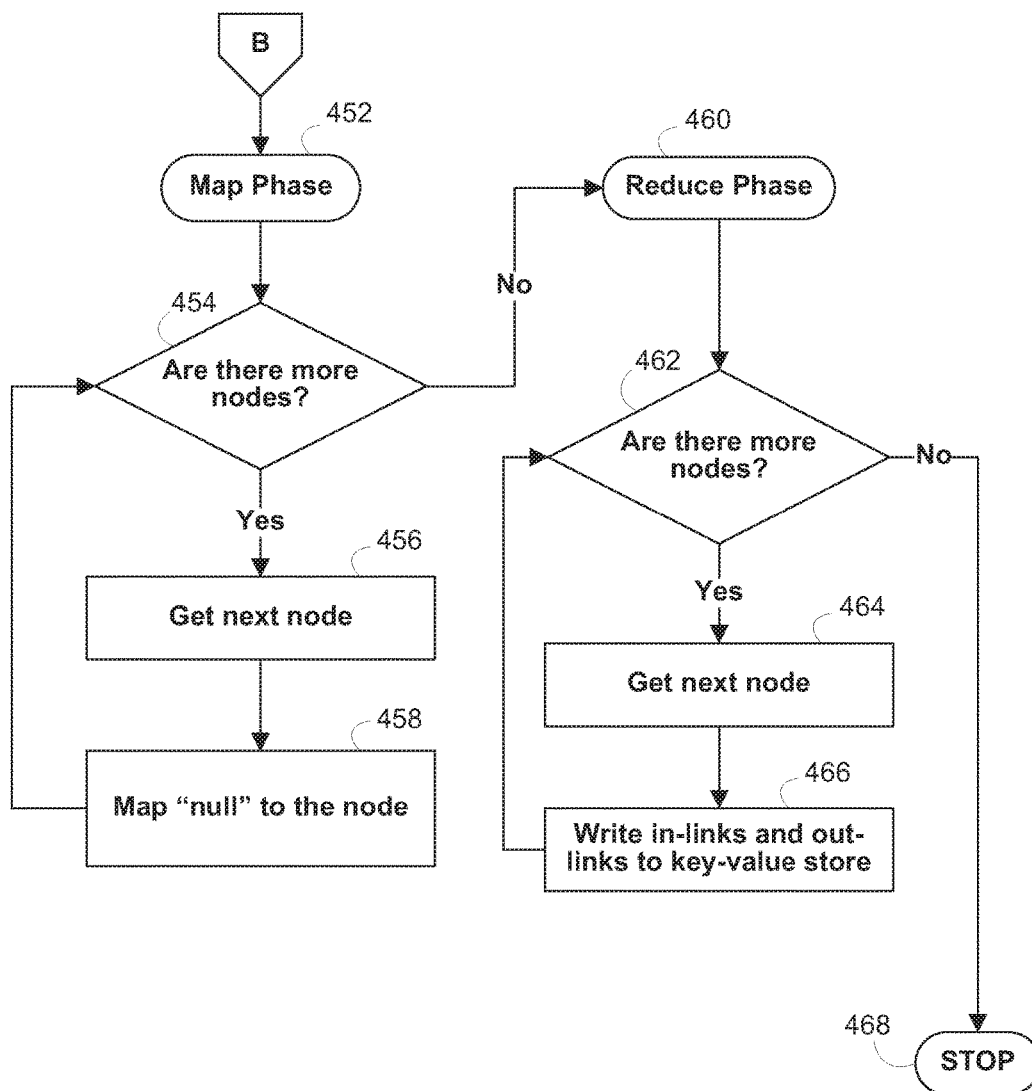


FIG. 4C



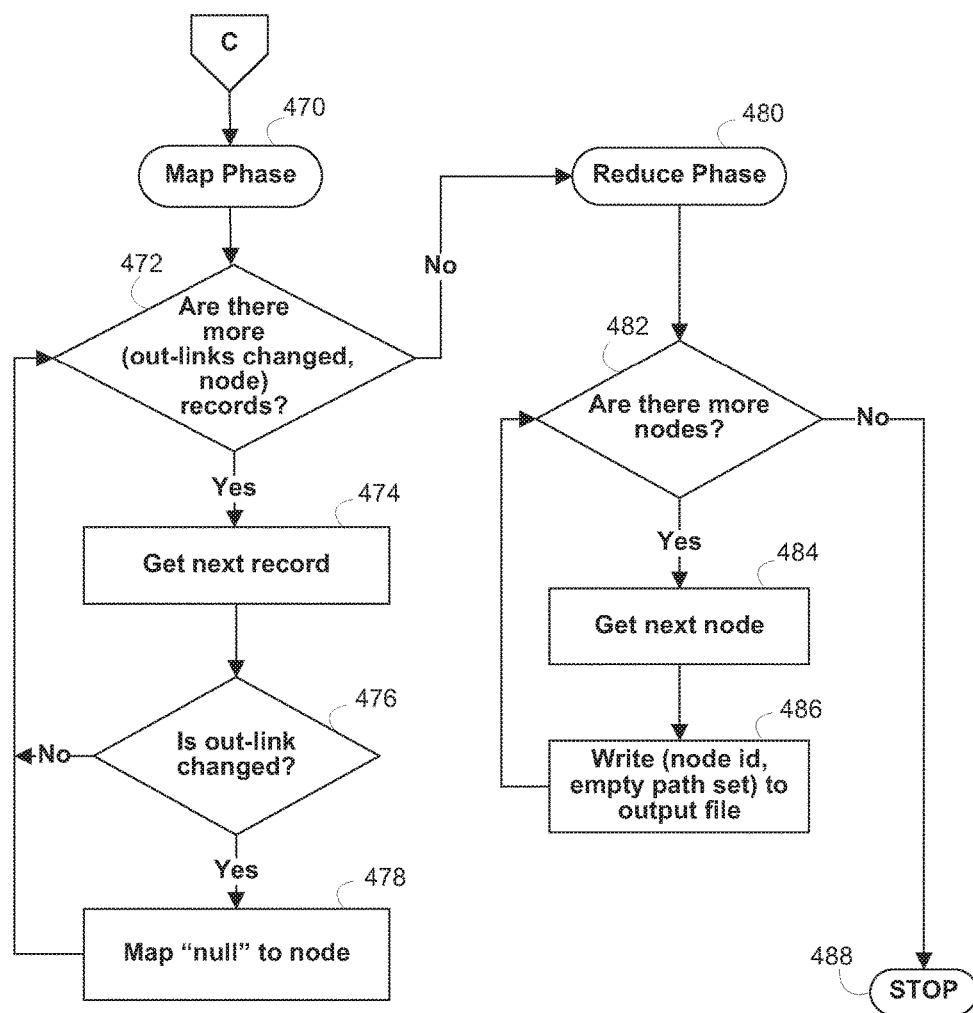


FIG. 4D

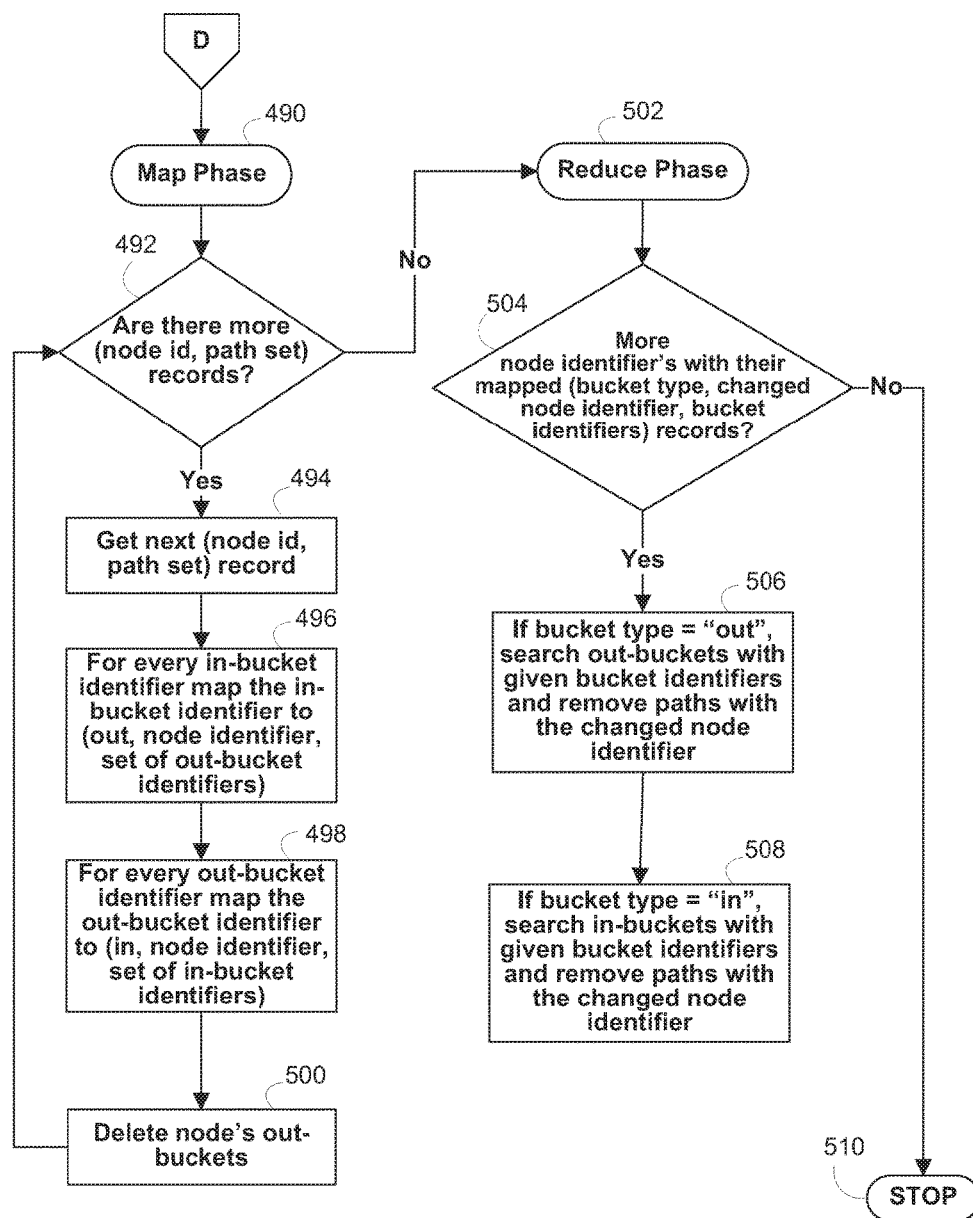


FIG. 4E

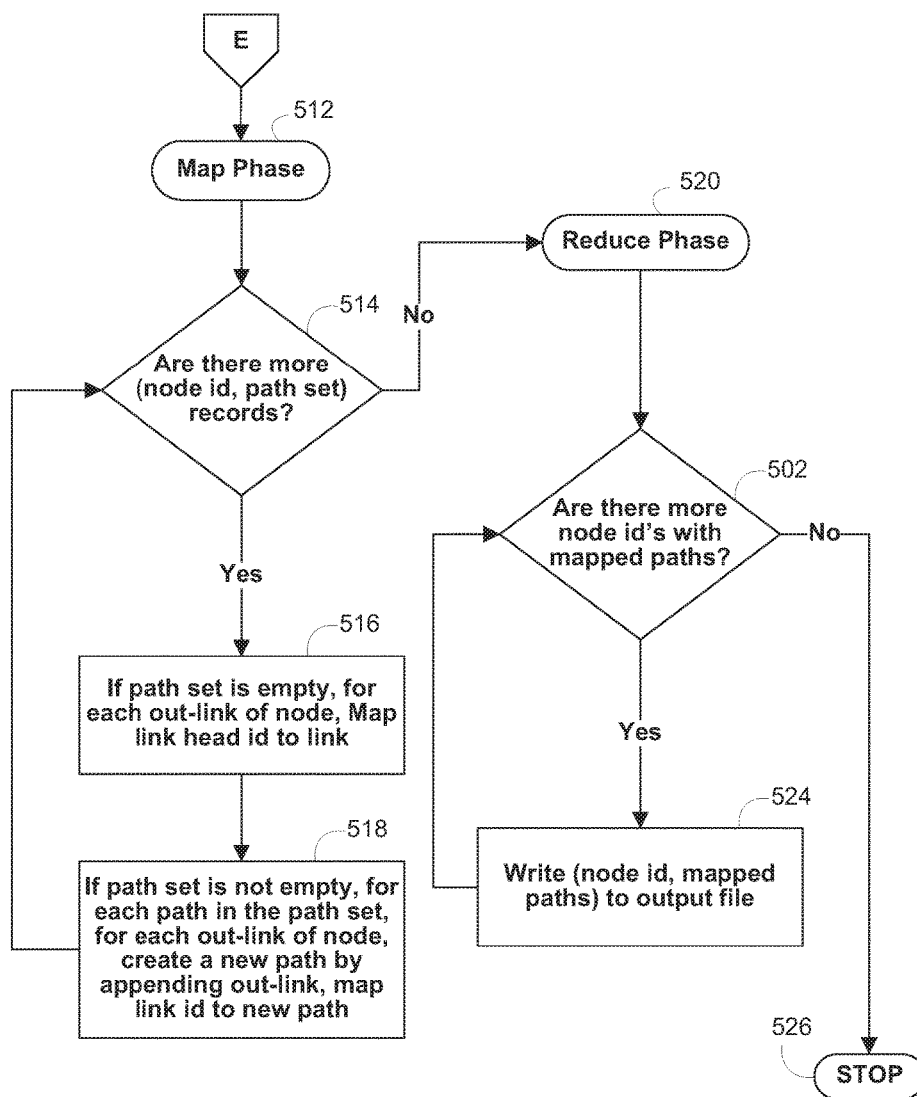
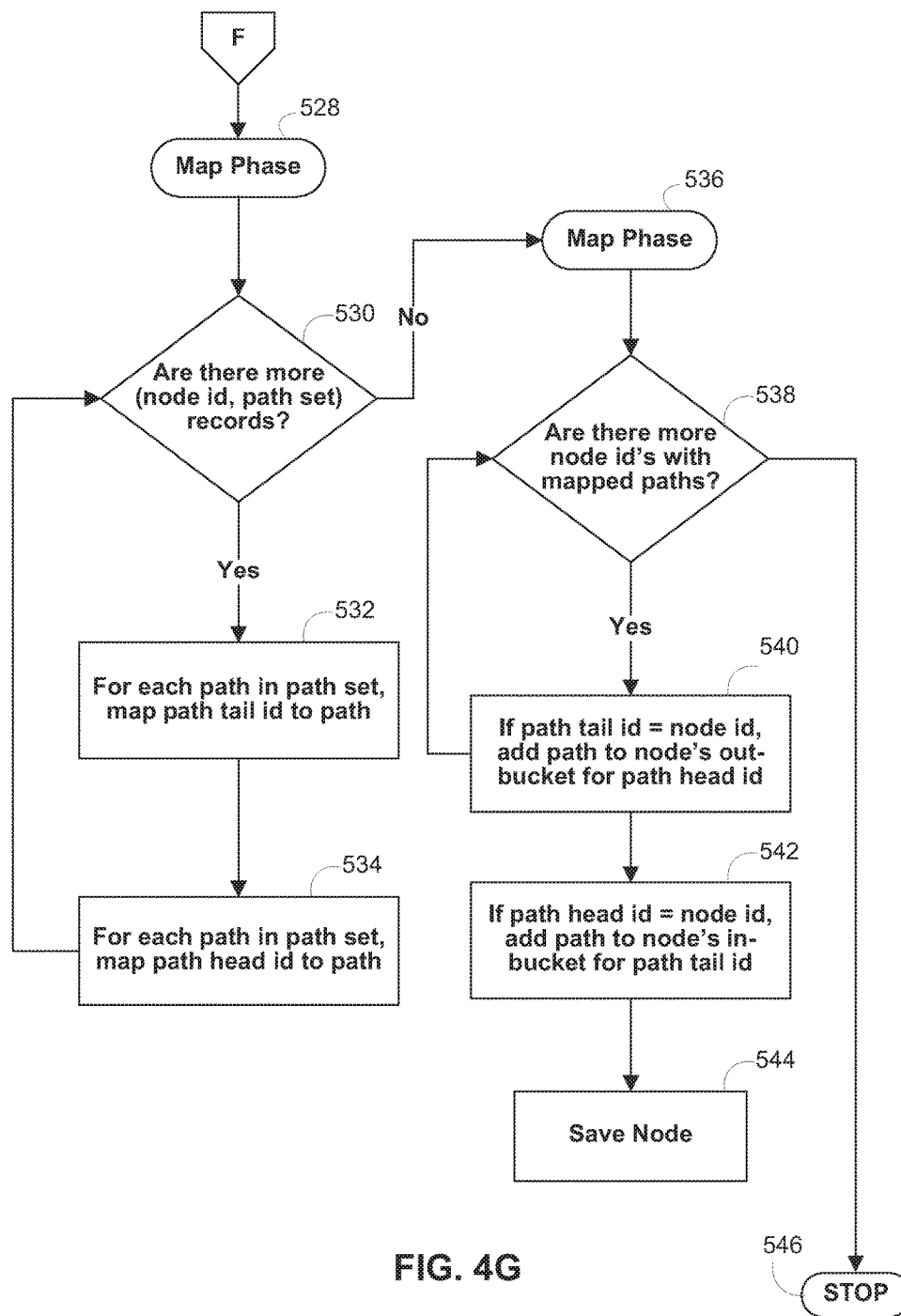
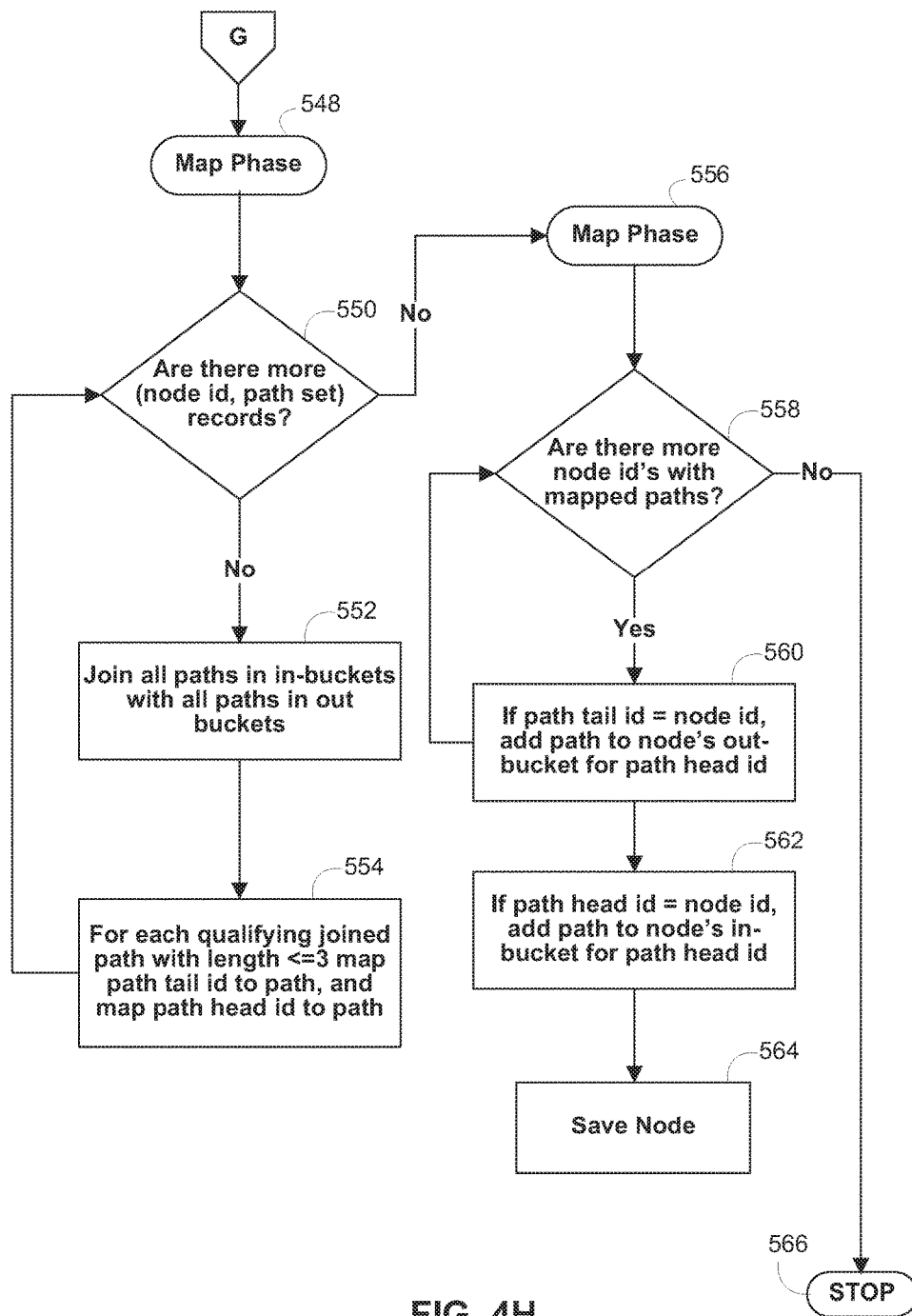
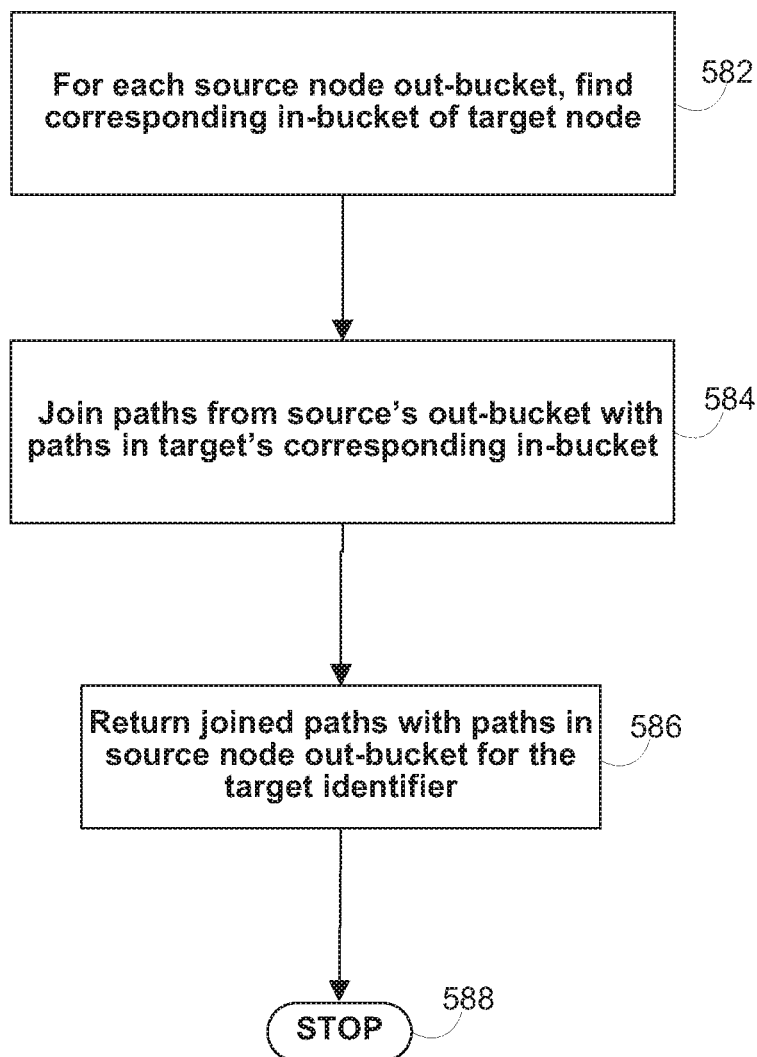


FIG. 4F





580



**FIG. 5**

# **PARALLEL COMPUTATIONAL FRAMEWORK AND APPLICATION SERVER FOR DETERMINING PATH CONNECTIVITY**

## **CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application is a continuation of U.S. patent application Ser. No. 15/953,011, filed Apr. 13, 2018 entitled “SCORING USING DISTRIBUTED DATABASE WITH ENCRYPTED COMMUNICATIONS FOR CREDIT-GRANTING AND IDENTIFICATION VERIFICATION”: which is a continuation of U.S. patent application Ser. No. 15/623,103, filed Jun. 14, 2017 entitled “SOCIAL GRAPH DATA ANALYTICS” which is a continuation of U.S. patent application Ser. No. 15/224,063, filed on Jul. 29, 2016 entitled “SOCIAL GRAPH DATA ANALYTICS”, which is a continuation of U.S. patent application Ser. No. 13/503,352, filed Aug. 28, 2012, entitled “SOCIAL GRAPH DATA ANALYTICS”, which is a national stage filing under 35 U.S.C. § 371 of International Application No. PCT/CA2010/001658, filed Oct. 22, 2010, which claims the benefit to U.S. Provisional Application Ser. No. 61/254,313, filed Oct. 23, 2009. The above applications are incorporated herein by reference.

## **BACKGROUND OF THE INVENTION**

[0002] This invention relates generally to networks of individuals and/or entities and network communities and, more particularly, to systems and methods for determining trust scores or connectivity within or between individuals and/or entities or networks of individuals and/or entities.

[0003] The connectivity, or relationships, of an individual or entity within a network community may be used to infer attributes of that individual or entity. For example, an individual or entity's connectivity within a network community may be used to determine the identity of the individual or entity (e.g., used to make decisions about identity claims and authentication), the trustworthiness or reputation of the individual or entity, or the membership, status, and/or influence of that individual or entity in a particular community or subset of a particular community.

[0004] An individual or entity's connectivity within a network community, however, is difficult to quantify. For example, network communities may include hundreds, thousands, millions, billions or more members. Each member may possess varying degrees of connectivity information about itself and possibly about other members of the community. Some of this information may be highly credible or objective, while other information may be less credible and subjective.

## **BACKGROUND OF THE INVENTION**

[0005] This invention relates generally to networks of individuals and/or entities and network communities and, more particularly, to systems and methods for determining trust scores or connectivity within or between individuals and/or entities or networks of individuals and/or entities.

[0006] The connectivity, or relationships, of an individual or entity within a network community may be used to infer attributes of that individual or entity. For example, an individual or entity's connectivity within a network community may be used to determine the identity of the individual or entity (e.g., used to make decisions about identity

claims and authentication), the trustworthiness or reputation of the individual or entity, or the membership, status, and/or influence of that individual or entity in a particular community or subset of a particular community.

[0007] An individual or entity's connectivity within a network community, however, is difficult to quantify. For example, network communities may include hundreds, thousands, millions, billions or more members. Each member may possess varying degrees of connectivity information about itself and possibly about other members of the community. Some of this information may be highly credible or objective, while other information may be less credible and subjective. proportional to the number of subpaths, or relationships, connecting the two nodes, among other possible measures. Using the number of subpaths as a measure, a path with one or more intermediate nodes between the first node  $n_1$  and the second node  $n_2$  may be scaled by an appropriate number (e.g., the number of intermediate nodes) and this scaled number may be used to calculate the connectivity rating.

[0008] In some embodiments, weighted links are used in addition or as an alternative to the subpath counting approach. Processing circuitry may be configured to assign a relative user weight to each path connecting a first node  $n_1$  and a second node  $n_2$  within a network community. A user connectivity value may be assigned to each link. For example, a user or entity associated with node  $n_1$  may assign user connectivity values for all outgoing paths from node  $n_1$ . In some embodiments, the connectivity values assigned by the user or entity may be indicative of that user or entity's trust in the user or entity associated with node  $n_2$ . The link values assigned by a particular user or entity may then be compared to each other to determine a relative user weight for each link.

[0009] The relative user weight for each link may be determined by first computing the average of all the user connectivity values assigned by that user or node (i.e., the out-link values). If  $t_i$  is the user connectivity value assigned to link  $i$ , then the relative user weight,  $w_i$ , assigned to that link may be given in accordance with:

$$w_i = 1 + (t_i - \bar{t})^2 \quad (1)$$

[0010] In some embodiments, an alternative relative user weight,  $w'_i$ , may be used based on the number of standard deviations,  $\sigma$ , the user connectivity value differs from the average value assigned by that user or node. For example, the alternative relative user weight may be given in accordance with:

$$w'_i = 1 - \frac{1}{2 + k^2} \text{ where } k = \begin{cases} 0, & \text{if } \sigma = 0 \\ \frac{t_i - \bar{t}}{\sigma}, & \text{otherwise} \end{cases} \quad (2)$$

[0011] To determine the overall weight of a path, in some embodiments, the weights of all the links along the path may be multiplied together. The overall path weight may then be given in accordance with:

$$w_{path} = \prod(w_i) \quad (3)$$

or

$$w_{path} w'_{path} = \prod(w'_i) \quad (4)$$

[0012] The connectivity value for the path may then be defined as the minimum user connectivity value of all the links in the path multiplied by the overall path weight in accordance with:

$$l_{path} = w_{path} \times l_{min} \quad (5)$$

[0013] In some embodiments, only “qualified” paths are used to determine connectivity values. A qualified path may be a path whose path weight is greater than or equal to some threshold value. As described in more detail below, any suitable threshold function may be used to define threshold values. The threshold function may be based, at least in some embodiments, on empirical data, desired path keep percentages, or both. In some embodiments, threshold values may depend on the length,  $l$ , of the path. For example, an illustrative threshold function specifying the minimum path weight for path  $p$  may be given in accordance with:

$$\text{threshold}(p) = \begin{cases} 0.5, & \text{if } l = 1 \\ 0.428, & \text{if } l = 2 \\ 0.289, & \text{if } l = 3 \\ 0.220, & \text{if } l = 4 \\ 0.216, & \text{if } l = 5 \\ 0.192, & \text{if } l = 6 \end{cases} \quad (6)$$

[0014] To determine path connectivity values, in some embodiments, a parallel computational framework or distributed computational framework (or both) may be used. For example, in one embodiment, a number of core processors implement an Apache Hadoop or Google MapReduce cluster. This cluster may perform some or all of the distributed computations in connection with determining new path link values and path weights.

[0015] The processing circuitry may identify a changed node within a network community. For example, a new outgoing link may be added, a link may be removed, or a user connectivity value may have been changed. In response to identifying a changed node, in some embodiments, the processing circuitry may re-compute link, path, and weight values associated with some or all nodes in the implicated network community or communities.

[0016] In some embodiments, only values associated with affected nodes in the network community are recomputed after a changed node is identified. If there exists at least one changed node in the network community, the changed node or nodes may first undergo a prepare process. The prepare process may include a “map” phase and “reduce” phase. In the map phase of the prepare process, the prepare process may be divided into smaller sub-processes which are then distributed to a core in the parallel computational framework cluster. For example, each node or link change (e.g., tail to out-link change and head to in-link change) may be mapped to a different core for parallel computation. In the reduce phase of the prepare process, each out-link’s weight may be determined in accordance with equation (1). Each of the out-link weights may then be normalized by the sum of the out-link weights (or any other suitable value). The node table may then be updated for each changed node, its in-links, and its out-links.

[0017] After the changed nodes have been prepared, the paths originating from each changed node may be calculated. Once again, a “map” and “reduce” phase of this

process may be defined. During, this process, in some embodiments, a depth-first search may be performed of the node digraph or node tree. All affected ancestor nodes may then be identified and their paths recalculated.

[0018] In some embodiments, to improve performance, paths may be grouped by the last node in the path. For example, all paths ending with node  $n_1$  may be grouped together, all paths ending with node  $n_2$  may be grouped together, and so on. These path groups may then be stored separately (e.g., in different columns of a single database table). In some embodiments, the path groups may be stored in columns of a key-value store implementing an HBase cluster (or any other compressed, high performance database system, such as BigTable).

[0019] In some embodiments, one or more threshold functions may be defined. The threshold function or functions may be used to determine the maximum number of links in a path that will be analyzed in a connectivity determination or connectivity computation. Threshold factors may also be defined for minimum link weights, path weights, or both. Weights falling below a user-defined or system-defined threshold may be ignored in a connectivity determination or connectivity computation, while only weights of sufficient magnitude may be considered.

[0020] In some embodiments, a user connectivity value may represent the degree of trust between a first node and a second node. In one embodiment, node  $n_1$  may assign a user connectivity value of  $l_1$  to a link between it and node  $n_2$ . Node  $n_2$  may also assign a user connectivity value of  $l_2$  to a reverse link between it and node  $n_1$ . The values of  $l_1$  and  $l_2$  may be at least partially subjective indications of the trustworthiness of the individual or entity associated with the node connected by the link. For example, one or more of the individual or entity’s reputation within the network community (or some other community), the individual or entity’s alignment with the trusting party (e.g., political, social, or religious alignment), past dealings with the individual or entity, and the individual or entity’s character and integrity (or any other relevant considerations) may be used to determine a partially subjective user connectivity value indicative of trust. A user (or other individual authorized by the node) may then assign this value to an outgoing link connecting the node to the individual or entity. Objective measures (e.g., data from third-party ratings agencies or credit bureaus) may also be used, in some embodiments, to form composite user connectivity values indicative of trust. The subjective, objective, or both types of measures may be automatically harvested or manually inputted for analysis.

[0021] In some embodiments, a decision-making algorithm may access the connectivity values in order to make automatic decisions (e.g., automatic network-based decisions, such as authentication or identity requests) on behalf of a user. Connectivity values may additionally or alternatively be outputted to external systems and processes located at third-parties. The external systems and processes may be configured to automatically initiate a transaction (or take some particular course of action) based, at least in part, on received connectivity values. For example, electronic or online advertising may be targeted to subgroups of members of a network community based, at least in part, on network connectivity values.

[0022] In some embodiments, a decision-making algorithm may access the connectivity values to make decisions prospectively (e.g., before an anticipated event like a request



for credit). Such decisions may be made at the request of a user, or as part of an automated process (e.g., a credit bureau's periodic automated analysis of a database of customer information). This prospective analysis may allow for the initiation of a transaction (or taking of some particular action) in a fluid and/or dynamic manner.

**[0023]** In some embodiments, connectivity values may be used to present information to the user. This information may include, but is not limited to, static and/or interactive visualizations of connectivity values within a user's associated network community or communities. In some embodiments, this information may allow the user to explore or interact with an associated network community or communities, and encourage and/or discourage particular interactions within a user's associated network community or communities. In some embodiments, this information may explicitly present the user with the connectivity values. For example, a percentage may indicate how trustworthy another individual and/or entity is to a user. In some embodiments, the information may implicitly present the user with a representation of the connectivity values. For example, an avatar representing another individual and/or entity may change in appearance based on how trustworthy that individual and/or entity is to a user.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0024]** The above and other features of the present invention, its nature and various advantages will be more apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings, and in which:

**[0025]** FIG. 1 is an illustrative block diagram of a network architecture used to support connectivity within a network community in accordance with one embodiment of the invention;

**[0026]** FIG. 2 is another illustrative block diagram of a network architecture used to support connectivity within a network community in accordance with one embodiment of the invention;

**[0027]** FIGS. 3A and 3B show illustrative data tables for supporting connectivity determinations within a network community in accordance with one embodiment of the invention;

**[0028]** FIGS. 4A-4H show illustrative processes for supporting connectivity determinations within a network community in accordance with one embodiment of the invention; and

**[0029]** FIG. 5 shows an illustrative process for querying all paths to a target node and computing a network connectivity value in accordance with one embodiment of the invention.

#### DETAILED DESCRIPTION

**[0030]** Systems and methods for determining the connectivity between nodes in a network community are provided. As defined herein, a "node" may include any user terminal, network device, computer, mobile device, access point, robot, or any other electronic device capable of being uniquely identified within a network community. For example, nodes may include robots (or other machines) assigned unique serial numbers or network devices assigned unique network addresses. In some embodiments, a node may also represent an individual human being, entity (e.g.,

a legal entity, such as a public or private company, corporation, limited liability company (LLC), partnership, sole proprietorship, or charitable organization), concept (e.g., a social networking group), animal, or inanimate object (e.g., a car, aircraft, or tool). As also defined herein, a "network community" may include a collection of nodes and may represent any group of devices, individuals, or entities.

**[0031]** For example, all or some subset of the users of a social networking website or social networking service (or any other type of website or service, such as an online gaming community) may make up a single network community. Each user may be represented by a node in the network community. As another example, all the subscribers to a particular newsgroup or distribution list may make up a single network community, where each individual subscriber may be represented by a node in the network community. Any particular node may belong in zero, one, or more than one network community, or a node may be banned from all, or a subset of, the community. To facilitate network community additions, deletions, and link changes, in some embodiments, a network community may be represented by a directed graph, or digraph, weighted digraph, tree, or any other suitable data structure.

**[0032]** FIG. 1 shows illustrative network architecture 100 used to support the connectivity determinations within a network community. A user may utilize access application 102 to access application server 106 over communications network 104. For example, access application 102 may include a standard web browser, application server 106 may include a web server, and communications network 104 may include the Internet. Access application 102 may also include proprietary applications specifically developed for one or more platforms or devices. For example, access application 102 may include one or more instances of an Apple iOS, Android, or WebOS application or any suitable application for use in accessing application 106 over communications network 104. Multiple users may access application service 106 via one or more instances of access application 102. For example, a plurality of mobile devices may each have an instance of access application 102 running locally on the devices. One or more users may use an instance of access application 102 to interact with application server 106.

**[0033]** Communications network 104 may include any wired or wireless network, such as the Internet, WiMax, wide area cellular, or local area wireless network. Communications network 104 may also include personal area networks, such as Bluetooth and infrared networks. Communications on communications network 104 may be encrypted or otherwise secured using any suitable security or encryption protocol.

**[0034]** Application server 106, which may include any network server or virtual server, such as a file or web server, may access data sources 108 locally or over any suitable network connection. Application server 106 may also include processing, circuitry (e.g., one or more microprocessors), memory (e.g., RAM, ROM, and hybrid types of memory), storage devices (e.g., hard drives, optical drives, and tape drives). The processing circuitry included in application server 106 may execute a server process for supporting the network connectivity determinations of the present invention, while access application 102 executes a corresponding client process. The processing circuitry included in application server 106 may also perform any of the calculations and computations described herein in connection

with determining network connectivity. In some embodiments, a computer-readable medium with computer program logic recorded thereon is included within application server **106**. The computer program logic may determine the connectivity between two or more nodes in a network community and it may or may not output such connectivity to a display screen or data store.

**[0035]** For example, application server **106** may access data sources **108** over the Internet, a secured private LAN, or any other communications network. Data sources **108** may include one or more third-party data sources, such as data from third-party social networking services, third-party ratings bureaus, and document issuers (e.g., driver's license and license plate issuers, such as the Department of Motor Vehicles). For example, data sources **108** may include user and relationship data (e.g., "friend" or "follower" data) from one or more of Facebook, MySpace, openSocial, Friendster, Bebo, hi5, Orkut, PerfSpot, Yahoo! 360, Gmail, Yahoo! Mail, Hotmail, other email-based services and accounts, LinkedIn, Twitter, Google Buzz, Really Simple Syndication readers, or any other social networking website or information service. Data sources **108** may also include data stores and databases local to application server **106** containing relationship information about users accessing application server **106** via access application **102** (e.g., databases of addresses, legal records, transportation passenger lists, gambling patterns, political affiliations, vehicle license plate or identification numbers, universal product codes, news articles, business listings, and hospital or university affiliations).

**[0036]** Application server **106** may be in communication with one or more of data store **110**, key-value store **112**, and parallel computational framework **114**. Data store **110**, which may include any relational database management system (RDBMS), file server, or storage system, may store information relating to one or more network communities. For example, one or more of data tables **300** (FIG. 3A) may be stored on data store **110**. Data store **110** may store identity information about users and entities in the network, community, an identification of the nodes in the network community, user link and path weights, user configuration settings, system configuration settings, and/or any other suitable information. There may be one instance of data store **110** per network community, or data store **110** may store information relating to a plural number of network communities. For example, data store **110** may include one database per network community, or one database may store information about all available network communities (e.g., information about one network community per database table).

**[0037]** Parallel computational framework **114**, which may include any parallel or distributed computational framework or cluster, may be configured to divide computational jobs into smaller jobs to be performed simultaneously, in a distributed fashion, or both. For example, parallel computational framework **114** may support data-intensive distributed applications by implementing a map/reduce computational paradigm where the applications may be divided into a plurality of small fragments of work, each of which may be executed or re-executed on any core processor in a cluster of cores. A suitable example of parallel computational framework **114** includes an Apache Hadoop cluster.

**[0038]** Parallel computational framework **114** may interface with key-value store **112**, which also may take the form

of a cluster of cores. Key-value store **112** may hold sets of key-value pairs for use with the map/reduce computational paradigm implemented by parallel computational framework **114**. For example, parallel computational framework **114** may express a large distributed computation as a sequence of distributed operations on data sets of key-value pairs. User-defined map/reduce jobs may be executed across a plurality of nodes in the cluster. The processing and computations described herein may be performed, at least in part, by any type of processor or combination of processors. For example, various types of quantum processors (e.g., solid-state quantum processors and light-based quantum processors), artificial neural networks, and the like may be used to perform massively parallel computing and processing.

**[0039]** In some embodiments, parallel computational framework **114** may support two distinct phases, a "map" phase and a "reduce" phase. The input to the computation may include a data set of key-value pairs stored at key-value store **112**. In the map phase, parallel computational framework **114** may split, or divide, the input data set into a large number of fragments and assign each fragment to a map task. Parallel computational framework **114** may also distribute the map tasks across the cluster of nodes on which it operates. Each map task may consume key-value pairs from its assigned fragment and produce a set of intermediate key-value pairs. For each input key-value pair, the map task may invoke a user defined map function that transmutes the input into a different key-value pair. Following the map phase, parallel computational framework **114** may sort the intermediate data set by key and produce a collection of tuples so that all the values associated with a particular key appear together. Parallel computational framework **114** may also partition the collection of tuples into a number of fragments equal to the number of reduce tasks.

**[0040]** In the reduce phase, each reduce task may consume the fragment of tuples assigned to it. For each such tuple, the reduce task may invoke a user-defined reduce function that transmutes the tuple into an output key-value pair. Parallel computational framework **114** may then distribute the many reduce tasks across the cluster of nodes and provide the appropriate fragment of intermediate data to each reduce task.

**[0041]** Tasks in each phase may be executed in a fault-tolerant manner, so that if one or more nodes fail during a computation the tasks assigned to such failed nodes may be redistributed across the remaining nodes. This behavior may allow for load balancing and for failed tasks to be re-executed with low runtime overhead.

**[0042]** Key-value store **112** may implement any distributed file system capable of storing large files reliably. For example key-value store **112** may implement Hadoop's own distributed file system (DFS) or a more scalable column-oriented distributed database, such as HBase. Such file systems or databases may include BigTable-like capabilities, such as support for an arbitrary number of table columns.

**[0043]** Although FIG. 1, in order to not over-complicate the drawing, only shows a single instance of access application **102**, communications network **104**, application server **106**, data source **108**, data store **110**, key-value store **112**, and parallel computational framework **114**, in practice, network architecture **100** may include multiple instances of one or more of the foregoing components. In addition, key-value store **112** and parallel computational framework

**114** may also be removed, in some embodiments. As shown in network architecture **200** of FIG. 2, the parallel or distributed computations carried out by key-value store **112** and/or parallel computational framework **114** may be additionally or alternatively performed by a cluster of mobile devices **202** instead of stationary cores. In some embodiments, cluster of mobile devices **202**, key-value store **112**, and parallel computational framework **114** are all present in the network architecture. Certain application processes and computations may be performed by cluster of mobile devices **202** and certain other application processes and computations may be performed by key-value store **112** and parallel computational framework **114**. In addition, in some embodiments, communication network **104** itself may perform some or all of the application processes and computations. For example, specially-configured routers or satellites may include processing circuitry adapted to carry out some or all of the application processes and computations described herein.

**[0044]** Cluster of mobile devices **202** may include one or more mobile devices, such as PDAs, cellular telephones, mobile computers, or any other mobile computing device. Cluster of mobile devices **202** may also include any appliance (e.g., audio/video systems, microwaves, refrigerators, food processors) containing a microprocessor (e.g., with spare processing time), storage, or both. Application server **106** may instruct devices within cluster of mobile devices **202** to perform computation, storage, or both in a similar fashion as would have been distributed to multiple fixed cores by parallel computational framework **114** and the map/reduce computational paradigm. Each device in cluster of mobile devices **202** may perform a discrete computational job, storage job, or both. Application server **106** may combine the results of each distributed job and return a final result of the computation.

**[0045]** FIG. 3A shows illustrative data tables **300** used to support the connectivity determinations of the present invention. One or more of tables **300** may be stored in, for example, a relational database in data store **110** (FIG. 1). Table **302** may store an identification of all the nodes registered in the network community. A unique identifier may be assigned to each node and stored in table **302**. In addition, a string name may be associated with each node and stored in table **302**. As described above, in some embodiments, nodes may represent individuals or entities, in which case the string name may include the individual or person's first and/or last name, nickname, handle, or entity name.

**[0046]** Table **304** may store user connectivity values. In some embodiments, user connectivity values may be assigned automatically by the system (e.g., by application server **106** (FIG. 1)). For example, application server **106** (FIG. 1) may monitor all electronic interaction (e.g., electronic communication, electronic transactions, or both) between members of a network community. In some embodiments, a default user connectivity value (e.g., the link value 1) may be assigned initially to all links in the network community. After electronic interaction is identified between two or more nodes in the network community, user connectivity values may be adjusted upwards or downwards depending on the type of interaction between the nodes and the result of the interaction. For example, each simple email exchange between two nodes may automatically increase or decrease the user connectivity values connecting those two

nodes by a fixed amount. More complicated interactions (e.g., product or service sales or inquires) between two nodes may increase or decrease the user connectivity values connecting those two nodes by some larger fixed amount. In some embodiments, user connectivity values between two nodes may always be increased unless a user or node indicates that the interaction was unfavorable, not successfully completed, or otherwise adverse. For example, a transaction may not have been timely executed or an email exchange may have been particularly displeasing. Adverse interactions may automatically decrease user connectivity values while all other interactions may increase user connectivity values (or have no effect). In addition, user connectivity values may be automatically harvested using outside sources. For example, third-party data sources (such as ratings agencies and credit bureaus) may be automatically queried for connectivity information. This connectivity information may include completely objective information, completely subjective information, composite information that is partially objective and partially subjective, any other suitable connectivity information, or any combination of the foregoing.

**[0047]** In some embodiments, user connectivity values may be manually assigned by members of the network community. These values may represent, for example, the degree or level of trust between two users or nodes or one node's assessment of another node's competence in some endeavor. As described above, user connectivity values may include a subjective component and an objective component in some embodiments. The subjective component may include a trustworthiness "score" indicative of how trustworthy a first user or node finds a second user, node, community, or subcommunity. This score or value may be entirely subjective and based on interactions between the two users, nodes, or communities. A composite user connectivity value including subjective and objective components may also be used. For example, third-party information may be consulted to form an objective component based on, for example, the number of consumer complaints, credit score, socio-economic factors (e.g., age, income, political or religious affiliations, and criminal history), or number of citations/hits in the media or in search engine searches. Third-party information may be accessed using communications network **104** (FIG. 1). For example, a third-party credit bureau's database may be polled or a personal biography and background information, including criminal history information, may be accessed from a third-party database or data source (e.g., as part of data sources **108** (FIG. 1) or a separate data source) or input directly by a node, user, or system administrator.

**[0048]** Table **304** may store an identification of a link head, link tail, and user connectivity value for the link. Links may or may not be bidirectional. For example, a user connectivity value from node  $n_1$  to node  $n_2$  may be different (and completely separate) than a link from node  $n_2$  to node  $n_1$ . Especially in the trust context described above, each user can assign his or her own user connectivity value to a link (i.e., two users need not trust each other an equal amount in some embodiments).

**[0049]** Table **306** may store an audit log of table **304**. Table **306** may be analyzed to determine which nodes or links have changed in the network community. In some embodiments, a database trigger is used to automatically insert an audit record into table **306** whenever a change of the data in table

**304** is detected. For example, a new link may be created, a link may be removed, or a user connectivity value may be changed. This audit log may allow for decisions related to connectivity values to be made prospectively (i.e., before an anticipated event). Such decisions may be made at the request of a user, or as part of an automated process, such as the processes described below with respect to FIG. 5. This prospective analysis may allow for the initiation of a transaction (or taking of some particular action) in a fluid and/or dynamic manner. After such a change is detected, the trigger may automatically create anew row in table **306**. Table **306** may store an identification of the changed node, and identification of the changed link head, changed link tail, and the user connectivity value to be assigned to the changed link. Table **306** may also store a timestamp indicative of the time of the change and an operation code. In some embodiments, operation codes may include “insert,” “update,” or “delete” operations, corresponding to whether a link was inserted, a user connectivity value was changed, or a link was deleted, respectively. Other operation codes may be used in other embodiments.

**[0050]** FIG. 3B shows illustrative data structure **310** used to support the connectivity determinations of the present invention. In some embodiments, data structure **310** may be stored using key-value store **112** (FIG. 1), while tables **300** are stored in data store **110** (FIG. 1). As described above, key-value store **112** (FIG. 1) may implement an HBase storage system and include BigTable support. Like a traditional relational database management system, the data shown in FIG. 3B may be stored in tables. However, the BigTable support may allow for an arbitrary number of columns in each table, whereas traditional relational database management systems may require a fixed number of columns.

**[0051]** Data structure **310** may include node table **312**. In the example shown in FIG. 3B, node table **312** includes several columns. Node table **312** may include row identifier column **314**, which may store 64-bit, 128-bit, 256-bit, 512-bit, or 1024-bit integers and may be used to uniquely identify each row (e.g., each node) in node table **312**. Column **316** may include a list of all the incoming links for the current node. Column **318** may include a list of all the outgoing links for the current node. Node table **312** may also include one or more “bucket” columns **320** and **322**. These columns may store a list of paths that connect, for example, a source node to the current node, the current node to a target node, or both. As described above, grouping paths by the last node in the path (e.g., the target node), the first node in the path (e.g., the source node), or both, may facilitate connectivity computations. As shown in FIG. 3B, in some embodiments, to facilitate scanning, bucket column names may include the target node identifier appended to the end of the “bucket” column name.

**[0052]** FIGS. 4A-4H show illustrative processes for determining the connectivity of nodes within a network community. FIG. 4A shows process **400** for updating a connectivity graph (or any other suitable data structure) associated with a network community. As described above, in some embodiments, each network community is associated with its own connectivity graph, digraph, tree, or other suitable data structure. In other embodiments, a plurality of network communities may share one or more connectivity graphs (or other data structure).

**[0053]** In some embodiments, the processes described with respect to FIG. 4A-4H may be executed to make decisions prospectively (i.e., before an anticipated event). Such decisions may be made at the request of a user, or as part of an automated process, such as the processes described below with respect to FIG. 5. This prospective analysis may allow for the initiation of a transaction (or taking of some particular action) in a fluid and/or dynamic manner.

**[0054]** In some embodiments, the processes described with respect to FIG. 4A-4H may be executed to provide information to a user. Such presentations may be made at the request of a user, or as part of an automated presentation. This information may include, but is not limited to, static and/or interactive visualizations of connectivity values within a user’s associated network community or communities. In some embodiments, this information may be integrated into explorations of or interactions within a user’s associated network community or communities. Providing this information to a user may allow the user to better understand what other individuals and/or entities they may trust within a network community, and/or may encourage and/or discourage particular interactions within a user’s associated network community or communities.

**[0055]** At step **402**, a determination is made whether at least one node has changed in the network community. As described above, an audit record may be inserted into table **306** (FIG. 3) after a node has changed. By analyzing table **306** (FIG. 3), a determination may be made (e.g., by application server **106** of FIG. 1) that a new link has been added, an existing link has been removed, or a user connectivity value has changed. If, at step **404**, it is determined that a node has changed, then process **400** may continue to step **410** (shown in FIG. 4B) to process the changed links, step **412** (shown in FIG. 4C) to save the nodes with changed links, step **414** (shown in FIG. 4D) to create path set input files, step **416** (shown in FIG. 4E) to remove paths with changed nodes, one or more iterations of step **418** (shown in FIG. 4F) to grow paths by one link at a time, step **420** (shown in FIG. 4G) to save the paths that have grown by one or more links, and step **422** (shown in FIG. 4H) to join paths that go through changed nodes. It should be noted that more than one step or task shown in FIGS. 4B, 4C, 4D, 4E, 4F, 4G, and 4H may be performed in parallel using, for example, a cluster of cores. For example, multiple steps or tasks shown in FIG. 4B may be executed in parallel or in a distributed fashion, then multiple steps or tasks shown in FIG. 4C may be executed in parallel or in a distributed fashion, then multiple steps or tasks shown in FIG. 4D may be executed in parallel or in a distributed fashion, then multiple steps or tasks shown in FIG. 4E may be executed in parallel or in a distributed fashion, and so on. In this way, overall latency associated with process **400** may be reduced.

**[0056]** As described above, step **418** may be executed one or more times. This step may be operative to grow paths by a single link. Each iteration of step **418** may take as input the results of a previous iteration of step **418** so that paths may grow by more than one link, if desired. In the example of FIG. 4A, three iterations of step **418** are shown. Thus, process **400** may generate paths with lengths less than or equal to three. In other embodiments, more or fewer iterations of step **418** may allow process **400** to generate paths with more or fewer

[0057] If a node change is not detected at step 404, then process 400 enters a sleep mode at step 406. For example, in some embodiments, an application thread or process may continuously check to determine if at least one node or link has changed in the network community. In other embodiments, the application thread or process may periodically check for changed links and nodes every  $n$  seconds, where  $n$  is any positive number. After the paths are calculated that go through a changed node at step 416 or after a period of sleep at step 406, process 400 may determine whether or not to loop at step 408. For example, if all changed nodes have been updated, then process 400 may stop at step 418. If, however, there are more changed nodes or links to process, then process 400 may loop at step 408 and return to step 404.

[0058] In practice, one or more steps shown in process 400 may be combined with other steps, performed in any suitable order, performed in parallel (e.g., simultaneously or substantially simultaneously), or removed.

[0059] FIGS. 4B-4H each include processes with a “map” phase and “reduce” phase. As described, above, these phases may form part of a map/reduce computational paradigm carried out by parallel computational framework 114 (FIG. 1), key-value store 112 (FIG. 1), or both. As shown in FIG. 4B, in order to process link changes, map phase 426 may include determining if there are any more link changes at step 428; retrieving the next link change at step 430, mapping the tail to out-link change at step 432, and mapping the head to in-link change at step 434.

[0060] If there are no more link changes at step 428, then, in reduce phase 436, a determination may be made at step 438 that there are more nodes with mapped link changes to process. If so, then the next node and its link changes may be retrieved at step 440. The most recent link changes may be preserved at step 442 while any intermediate link changes are replaced by more recent changes. For example, the timestamp stored in table 306 (FIG. 3) may be used to determine the time of every link or node change. At step 444, the average out-link user connectivity value may be calculated. For example, if node  $n_1$  has eight out-links with assigned user connectivity values, these eight user connectivity values may be averaged at step 444. At step 446, each out-link's weight may be calculated in accordance with equation (1) or (2) above. At step 448, an output file may be created or appended with the out-links changed and corresponding changed node identifier. For example, one or more (out-links changed, node identifier) records may be written to the output file. Although the term “file” is sometimes used herein, the output need not be in a literal file or even file format. For example, any output stream, whether or not it is recorded, may be used. In some embodiments, some or all of the output file may be passed directly to a calling application, process, or function from a returning application, process, or function in the form of a stream or object return value. If there are no more nodes and link changes to process at step 438, the process may stop at step 450.

[0061] As shown in FIG. 4C, in order to save nodes with changed links, map phase 452 may include determining if there are any more changed nodes at step 454, retrieving the next changed node at step 456, and mapping “null” to the node at step 458.

[0062] If there are no more changed nodes at step 454, then, in reduce phase 460, a determination may be made at step 462 that there are more nodes to process. If so, then the next node may be retrieved at step 464. At step 466, the

in-links and out-links associated with the node may be written to a key-value store (e.g., key-value store 112 of FIG. 1). As described above, the key-value store may implement an HBase cluster (or any other compressed, high performance database system, such as BigTable). If there are no more nodes to, process at step 462, the process may stop at step 468.

[0063] As shown in FIG. 4D, in order to create path set input files, map phase 470 may include determining if there are any more (out-links changed, node identifier) records in the output file created or appended at step 448 (FIG. 4B). If so, the next record may be retrieved at step 474. At step 476, a determination may be made if an out-link has changed. If so, then at step 478 a “null” value may be mapped to the node. Otherwise, map phase 470 may return to step 472 to determine if there are any more (out-links changed, node identifier) records in the output file.

[0064] If there are no more changed records at step 472, then, in reduce phase 480, a determination may be made at step 482 that there are more node to process. If so, then the next node may be retrieved at step 484. At step 486, new records may be written to the output file. In some embodiments, the records written at step 486 may include records of the form (node identifier, empty path set for the node identifier). If there are no more nodes to process at step 482, the process may stop at step 488.

[0065] As shown in FIG. 4E, in order to remove paths with changed nodes, map phase 490 may include determining if there are any more (node identifier, path set) records in the output file at step 492 and retrieving the next such record at step 494. At step 496, for every “in” bucket identifier, the “in” bucket identifier may be mapped to a record of the form (out bucket type, node identifier, set of “out” bucket identifiers) (or any other suitable form). At step 498, for every “out” bucket identifier, the “out” bucket identifier may be mapped to a record of the form (in bucket type, node identifier, set of “in” bucket identifiers) (or any other suitable form). At step 500, the node's “out” buckets may be deleted, and the process may return to step 492 to determine if there are more records to process.

[0066] If there are no more records at step 492, then, in reduce phase 502, a determination may be made at step 504 that there are more node identifiers with their mapped (bucket type, changed node identifier, bucket identifiers) records to process. If so, then at step 506, if the bucket type is “out”, out-buckets with the given bucket identifiers may be searched and paths with the changed node identifier may be removed. At step 508, if the bucket type is “in”, in-buckets with the given bucket identifiers may be searched and paths with the changed node identifier may be removed. If there are no more records to process at step 504, the process may stop at step 510.

[0067] As shown in FIG. 4F, in order to grow paths by one link, map phase 512 may include determining if there are any more (node identifier, path set) records in the output file at step 514. If so, then at step 516, if the path set is empty, for each out-link of the node, a link head identifier may be mapped to the link. At step 518, if the path set is not empty, then for each path  $n$  in the path set, and for each out-link of a node, anew path may be created by appending (out-link, map link head identifier) to the new path.

[0068] If there are no more records at step 514, then, in reduce phase 520, a determination may be made at step 522 that there are more node identifiers with mapped paths to

process. If so, then at step 524, new records of the form (node identifier, mapped paths) (or any other suitable form) may be written to the output file. If there are no more records to process at step 522, the process may stop at step 526.

[0069] The process shown in FIG. 4F may be executed one or more times, with the result of growing path lengths by one link for each execution. As shown in FIG. 4A, in some embodiments, three iterations of the process shown in FIG. 4F are used to grow paths by three links. In other embodiments, more or fewer iterations are used.

[0070] As shown in FIG. 4G, in order to save the new paths, map phase 528 may include determining if there are any more (node identifier, path set) records in the output file at step 530. If so, then at step 532, for each path in the path set, the path tail identifier may be mapped to the path. At step 534, for each path in the path set, the path head identifier may be mapped to the path.

[0071] If there are no more records at step 530, then, in reduce phase 536, a determination may be made at step 538 that there are more node identifiers with mapped paths to process. If so, then at step 540, if the path tail identifier equals the node identifier, then that path may be added to the node's "out" bucket for the path head identifier. At step 542, if the path head identifier equals the node identifier, then that path may be added to the node's "in" bucket for the path tail identifier. At step 544, the node may be saved. If there are no more records to process at step 538, the process may stop at step 546.

[0072] As shown in FIG. 4H, in order to join paths that go through changed nodes, map phase 548 may include determining if there are any more (node identifier, path set) records in the output file at step 550. If so, then at step 552, all paths in "in" buckets may be joined with all paths in "out" buckets. At step 554, for each qualified joined path with length less than or equal to three (or the number of iterations of the process shown in FIG. 4F), the path tail identifier may be mapped to the path, and the path head identifier may also be mapped to the path.

[0073] If there are no more records at step 550, then, in reduce phase 556, a determination may be made at step 558 that there are more node identifiers with mapped paths to process. If so, then at step 560, if the path tail identifier equals the node identifier, then that path may be added to the node's "out" bucket for the path head identifier. At step 562, if the path head identifier equals the node identifier, then that path may be added to the node's "in" bucket for the path tail identifier. At step 564, the node may be saved. If there are no more records to process at step 558, the process may stop at step 566.

[0074] FIG. 5 shows illustrative process 580 for supporting a user query for all paths from a first node to a target node. For example, a first node (representing, for example, a first individual or entity) may wish to know how connected the first node is to some second node (representing, for example, a second individual or entity) in the network community. In the context of trust described above (and where the user connectivity values represent, for example, at least partially subjective user trust values), this query may return an indication of how much the first node may trust the second node. In general, the more paths connecting the two nodes may yield a greater (or lesser if, for example, adverse ratings are used) network connectivity value (or network trust amount).

[0075] At step 582, for each source node "out" bucket, the corresponding "in" bucket of target nodes may be located. For example, column 320 of node table 312 (both of FIG. 3B) may be accessed at step 582. Paths from the source node's "out" bucket may then be joined with paths in the target node's "in" bucket at step 584. Joined paths with paths in the source node's "out" bucket may then be returned for the target node's identifier. Process 580 may stop at step 588.

[0076] Having returned all paths between the source and target node (of length less than or equal to three, or any other suitable value depending on the number of iterations of the process shown in FIG. 4F), a network connectivity value may be computed. The path weights assigned to the paths returned at step 586 may then be summed. The path weights may be normalized by dividing each path weight by the computed sum of the path weights. A network connectivity value may then be computed. For example, each path's user connectivity value may be multiplied by its normalized path weight. The network connectivity value may then be computed in some embodiments in accordance with:

$$t_{network} = \sum t_{path} \times w_{path} \quad (7)$$

where  $t_{path}$  is the user connectivity value for a path (given in accordance with equation (5)) and  $w_{path}$  is the normalized weight for that path. The network connectivity value may then be held, output by processing circuitry of application server 106, and/or stored on data store 110 (FIG. 1). In addition, a decision-making algorithm may access the network connectivity value in order to make automatic decisions (e.g., automatic network-based decisions, such as authentication or identity requests) on behalf of the user. Network connectivity values may additionally or alternatively be outputted to external systems and processes located at third-parties. The external systems and processes may be configured to automatically initiate a transaction (or take some particular course of action) based, at least in part, on the received network connectivity values. For example, some locales or organizations may require identity references in order to apply for a document (e.g., a passport, driver's license, group or club membership card, etc.). The identity reference or references may vouch that an individual actually exists and/or is the individual the applicant is claiming to be. Network connectivity values may be queried by the document issuer (e.g., a local government agency, such as the Department of Motor Vehicles or a private organization) and used as one (or the sole) metric in order to verify the identity of the applicant, the identity of an identity reference, or both. In some embodiments, network connectivity values may be used as an added assurance of the identity of an applicant or reference in conjunction with more traditional forms of identification (e.g., document verification and knowledge-based identity techniques). If the document issuer (or some other party trusted by the document issuer) has a set of strong paths from the applicant or reference, this may indicate a higher degree of confidence in the identity of the applicant or reference. Such an indication may be outputted to the third-party system or process.

[0077] As another example, credit-granting decisions may be made by third parties based, at least in part, network connectivity values. One or more queries for a network connectivity value may be automatically executed by the credit-granting institution (e.g., a bank, private financial institution, department store) as part of the credit application process. For example, a query for a network connectivity

value between the applicant and the credit-granting institution itself (or its directors, board members, etc.) and between the applicant and one or more trusted nodes may be automatically executed as part of the credit application process. The one or more network connectivity values returned to the credit-granting institution may then be used as an input to a proprietary credit-granting decision algorithm. In this way, a credit-granting decision may be based on a more traditional component (e.g., occupation, income, repayment delinquencies, and credit score) and a network connectivity component. Each component may be assigned a weight and a weighted sum or weighted average may be computed. The weighted sum or average may then be used directly to make an automatic credit-granting decision for the applicant. The weights assigned to each component of the weighted sum or average may be based on such factors as the applicant's credit history with the financial institution, the amount of credit requested, the degree of confidence in the trusted nodes, any other suitable factor, or any combination of the foregoing factors.

**[0078]** In practice, one or more steps shown in process 580 may be combined with other steps, performed in any suitable order, performed in parallel (e.g., simultaneously or substantially simultaneously), or removed. In addition, as described above, various threshold functions may be used in order to reduce computational complexity. For example, a threshold function defining the maximum number of links to traverse may be defined. Paths containing more than the threshold specified by the threshold function may not be considered in the network connectivity determination. In addition, various threshold functions relating to link and path weights may be defined. Links or paths below the threshold weight specified by the threshold function may not be considered in the network connectivity determination.

**[0079]** Although process 580 describes a single user query for all paths from a first node to a target node, in actual implementations groups of nodes may initiate a single query for all the paths from each node in the group to a particular target node. For example, multiple members of a network community may all initiate a group query to a target node. Process 580 may return an individual network connectivity value for each querying node in the group or a single composite network connectivity value taking into account all the nodes in the querying group. For example, the individual network connectivity values may be averaged to form a composite value or some weighted average may be used. The weights assigned to each individual network connectivity value may be based on seniority in the community (e.g., how long each node has been a member in the community), rank, or social stature. In addition, in some embodiments, a user may initiate a request for network connectivity values for multiple target nodes in a single query. For example, node  $n_1$  may wish to determine network connectivity values between it and multiple other nodes. For example, the multiple other nodes may represent several candidates for initiating a particular transaction with node  $n_1$ . By querying for all the network connectivity values in a single query, the computations may be distributed in a parallel fashion to multiple cores so that some or all of the results are computed substantially simultaneously.

**[0080]** In addition, queries may be initiated in a number of ways. For example, a user (represented by a source node) may identify another user (represented by a target node) in order to automatically initiate process 580. A user may

identify the target node in any suitable way, for example, by selecting the target node from a visual display, graph, or tree, by inputting or selecting a username, handle, network address, email address, telephone number, geographic coordinates, or unique identifier associated with the target node, or by speaking a predetermined command (e.g., "query node 1" or "query node group 1, 5, 9" where 1, 5, and 9 represent unique node identifiers). After an identification of the target node or nodes is received, process 580 may be automatically executed. The results of the process (e.g., the individual or composite network connectivity values) may then be automatically sent to one or more third-party services or processes as described above.

**[0081]** In an embodiment, a user may utilize access application 102 to generate a user query that is sent to access application server 106 over communications network 104 (see also, FIG. 1) and automatically initiate process 580. For example, a user may access an Apple iOS, Android, or WebOS application or any suitable application for use in accessing application 106 over communications network 104. The application may display a searchable list of relationship data related to that user (e.g., "friend" or "follower" data) from one or more of Facebook, MySpace, openSocial, Friendster, Bebo, hi5, Orkut, PerfSpot, Yahoo! 360, LinkedIn, Twitter, Google Buzz, Really Simple Syndication readers or any other social networking website or information service. In some embodiments, a user may search for relationship data that is not readily listed—i.e., search Facebook, Twitter, or any suitable database of information for target nodes that are not displayed in the searchable list of relationship data. A user may select a target node as described above (e.g., select an item from a list of usernames representing a "friend" or "follower") to request a measure of how connected the user is to the target node. Using the processes described with respect to FIGS. 3 and 4A-H, this query may return an indication of how much the user may trust the target node. The returned indication may be displayed to the user using any suitable indicator. In some embodiments, indicator may be a percentage that indicates how trustworthy the target node is to the user.

**[0082]** In some embodiments, a user may utilize access application 102 to provide manual assignments of at least partially subjective indications of how trustworthy the target node is. For example, the user may specify that he or she trusts a selected target node (e.g., a selected "friend" or "follower") to a particular degree. The particular degree may be in the form of a percentage that represents the user's perception of how trustworthy the target node is. The user may provide this indication before, after, or during process 580 described above. The indication provided by the user (e.g., the at least partially subjective indications of trustworthiness) may then be automatically sent to one or more third-party services or processes as described above. In some embodiments, the indications provided by the user may cause a node and/or link to change in a network community. This change may cause a determination to be made that at least one node and/or link has changed in the network community, which in turn triggers various processes as described with respect to FIGS. 3 and 4A-4H.

**[0083]** In some embodiments, a user may utilize access application 102 to interact with or explore a network community. For example, a user may be presented with an interactive visualization that includes one or more implicit or explicit representations of connectivity values between

the user and other individuals and/or entities within the network community. This interactive visualization may allow the user to better understand what other individuals and/or entities they may trust within a network community, and/or may encourage and/or discourage particular interactions within a user's associated network community or communities.

**[0084]** In some embodiments, a path counting approach may be used in addition to or in place of the weighted link approach described above. Processing circuitry (e.g., of application server **106** (FIG. 1)) may be configured to count the number of paths between a first node  $n_1$  and a second node  $n_2$  within a network community. A connectivity rating  $R_{n_1n_2}$  may then be assigned to the nodes. The assigned connectivity rating may be proportional to the number of paths, or relationships, connecting the two nodes. A path with one or more intermediate nodes between the first node  $n_1$  and the second node  $n_2$  may be scaled by an appropriate number (e.g., the number of intermediate nodes) and this scaled number may be used to calculate the connectivity rating.

**[0085]** Each equation presented above should be construed as a class of equations of a similar kind, with the actual equation presented being one representative example of the class. For example, the equations presented above include all mathematically equivalent versions of those equations, reductions, simplifications, normalizations, and other equations of the same degree.

**[0086]** The above described embodiments of the invention are presented for purposes of illustration and not of limitation. The following claims give additional embodiments of the present invention.

What is claimed is:

**1.** A method for determining the network connectivity between a first node and a second node connected to the first node by at least one path, the method comprising:

storing a first list that identifies outgoing paths from the first node;

storing a second list that identifies incoming paths to the second node;

joining paths to the second node from the first node, wherein joining paths comprises accessing the first list and the second list; and

using processing circuitry to determine a network connectivity indication based, at least in part, on the joined paths.

**2.** The method of claim **1** further comprising accessing a link threshold value, wherein joining paths to the second node from the first node comprises joining only those paths containing fewer links than the accessed link threshold value.

**3.** The method of claim **1** further comprising accessing a path weight threshold value, wherein joining paths to the second node from the first node comprises joining only those paths with a normalized path weight above the accessed path weight threshold value.

**4.** The method of claim **1** wherein the processing circuitry determines a normalized path weight for each identified path by dividing a product of the link weights of each link in an identified path by a sum of the path weights of all identified paths.

**5.** The method of claim **1** wherein the processing circuitry determines a user connectivity value for each identified path

by multiplying the path weight for an identified path and a minimum connectivity value assigned to a link in the identified path.

**6.** The method of claim **5** wherein the user connectivity value represents a subjective user trust value or competency assessment.

**7.** The method of claim **1** further comprising using the processing circuitry to access third-party ratings data, wherein the network connectivity indication based, at least in part, on the third-party ratings information.

**8.** The method of claim **1** wherein joining paths to the second node from the first node comprises accessing data from a social networking service.

**9.** The method of claim **1** further comprising outputting the network connectivity indication to a requesting third-party process.

**10.** The method of claim **9** further comprising automatically making at least one network-based decision based, at least in part, on the outputted network connectivity indication.

**11.** An application server for determining the network connectivity between a first node and a second node connected to the first node by at least one path, the application server comprising

a storage device configured to:

store a first list that identifies outgoing paths from the first node;

store a second list that identifies incoming paths to the second node; and

processing circuitry configured to:

join paths to the second node from the first node, wherein joining paths comprises accessing the first list and the second list; and

determine a network connectivity indication based, at least in part, on the joined paths.

**12.** The system of claim **11** wherein the processing circuitry is further configured to access a link threshold value, wherein joining paths to the second node from the first node comprises joining only those paths containing fewer links than the accessed link threshold value.

**13.** The system of claim **11** wherein the processing circuitry is further configured to access a path weight threshold value, wherein joining paths to the second node from the first node comprises joining only those paths with a normalized path weight above the accessed path weight threshold value.

**14.** The system of claim **1** wherein the processing circuitry is further configured to determine a normalized path weight for each identified path by dividing a product of the link weights of each link in an identified path by a sum of the path weights of all identified paths.

**15.** The system of claim **11** wherein the processing circuitry is further configured to determine a user connectivity value for each identified path by multiplying the path weight for an identified path and a minimum connectivity value assigned to a link in the identified path.

**16.** The system of claim **15** wherein the user connectivity value represents a subjective user trust value or competency assessment.

**17.** The system of claim **11** wherein the processing circuitry is further configured to access third-party ratings data, wherein the network connectivity indication is based, at least in part, on the third-party ratings information.



**18.** The system of claim **11** wherein joining paths to the second node from the first node comprises accessing data from a social networking service.

**19.** The system of claim **11** wherein the processing circuitry is further configured to output the network connectivity indication to a requesting third-party process.

**20.** The system of claim **19** wherein the processing circuitry is further configured to automatically make at least one network-based decision based, at least in part, on the outputted network connectivity indication.

**21.** A system for determining the network connectivity between a first node and a second node connected to the first node by at least one path, the system comprising:

means for storing a first list that identifies outgoing paths from the first node;

means for storing a second list that identifies incoming paths to the second node;

means for joining paths to the second node from the first node, wherein joining paths comprises accessing the first list and the second list; and

means for determining a network connectivity indication based, at least in part, on the joined paths.

**22.** The system of claim **21** wherein the system further comprises means for accessing a link threshold value, wherein the means for joining paths to the second node from the first node comprises means for joining only those paths containing fewer links than the accessed link threshold value.

**23.** The system of claim **21** wherein the system further comprises means for accessing a path weight threshold value, wherein the means for joining paths to the second

node from the first node comprises means for joining only those paths with a normalized path weight above the accessed path weight threshold value.

**24.** The system of claim **21** wherein the system further comprises means for determining a normalized path weight for each identified path by dividing a product of the link weights of each link in an identified path by a sum of the path weights of all identified paths.

**25.** The system of claim **21** wherein the system further comprises means for determining a user connectivity value for each identified path by multiplying the path weight for an identified path and a minimum connectivity value assigned to a link in the identified path.

**26.** The system of claim **25** wherein the user connectivity value represents a subjective user trust value or competency assessment.

**27.** The system of claim **21** wherein the system further comprises means for accessing third-party ratings data, wherein the network connectivity indication is based, at least in part, on the third-party ratings information.

**28.** The system of claim **21** wherein joining paths to the second node from the first node comprises accessing data from a social networking service.

**29.** The system of claim **21** wherein the system further comprises means for outputting the network connectivity indication to a requesting third-party process.

**30.** The system of claim **29** wherein the system further comprises means for automatically making at least one network-based decision based, at least in part, on the outputted network connectivity indication.

\* \* \* \* \*