

# **AUTOMATIC NETWORK TOPOLOGY DETECTION AND FRAUD DETECTION**

## **CROSS REFERENCE TO RELATED APPLICATIONS**

5   **[0001]**   This application claims priority to European Patent Application No. 12165026.1, filed April 20, 2012, and entitled "Automatic electric network topology detection and instantaneous fraud detection," which is incorporated herein by reference.

## **BACKGROUND**

10   **[0002]**   With the rapid expansion of metropolitan cities and the expansive growth of population, distribution networks for utilities such as electricity, gas and water, etc., have become unprecedentedly complicated. New metering devices, such as electricity meters, are added to the distribution networks to serve new areas and/or replace obsolete metering devices, while outdated metering devices are removed from the  
15   distribution networks. Given the tremendous number of metering devices in the distribution networks and the dynamics of the distribution networks, utility service providers find it impractical, if not impossible, to determine the topologies associated with the distribution networks, i.e., which metering device is connected to which junction node (e.g., a transformer in electricity service, etc.), for example.

20   **[0003]**   Furthermore, without an accurate and up-to-date knowledge of the topologies of the distribution networks, the utility service providers may overlook fraud

and/or leakage that occurs in the networks, thereby incurring losses to the utility service providers.

#### **BRIEF DESCRIPTION OF THE DRAWINGS**

**[0004]** The detailed description is set forth with reference to the accompanying  
5 figures. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The use of the same reference numbers in different figures indicates similar or identical items.

**[0005]** FIG. 1 illustrates an example environment usable to implement an example network topology detection and fraud detection system.

10 **[0006]** FIG. 2 illustrates the example network topology detection and fraud detection system of FIG. 1 in more detail.

**[0007]** FIG. 3 illustrates an example method of network topology detection.

**[0008]** FIG. 4 illustrates an example method of fraud detection.

#### **DETAILED DESCRIPTION**

##### 15 **Overview**

**[0009]** As noted above, existing utility service providers find it impractical, if not impossible, to determine topologies associated with distribution networks for providing utility services. Furthermore, without an accurate and up-to-date knowledge of the topologies of the distribution networks, determination of fraud and/or leakage in the  
20 networks is prone to errors and erroneously reports false positives and false negatives, thus causing a waste of resources to investigate these false positives and false negatives.

**[0010]** This disclosure describes a network topology detection and fraud detection system. The system enables automated detection of a topology of a network associated with a given node (i.e., detection of a topology of a network with the given node as a root node of the network). For example, given a node, the system allows determination  
5 of one or more child nodes that are immediately connected to the given node.

**[0011]** Generally, the system may be triggered to determine or select a node for which topology information is desired. The system may be triggered by occurrence of an event or condition (event-driven) or upon request of a user (user-driven). As an example of an event-driven trigger, the system may detect abnormal activities (such as significant  
10 changes in consumption of a utility service associated with the distribution network, etc.) in a node of the distribution network and may select that node for which topology information is to be determined. As an example of a user-driven trigger, the system may allow a user to select a node for which topology information is desired. Additionally or alternatively, the system may receive a request to determine a topology of a given node.  
15 Additionally or alternatively, the system may select a node for which topology information is to be determined on a regular basis, for example, every one week, every one month, etc. In one implementation, the selected node may be used as a root node for which the topology information is determined. In other implementations, the selected or given node may include an intermediate node of a distribution network  
20 through which a utility service (e.g., electricity, gas or water, etc.) is transmitted from a utility station of a service provider to a node where the utility service is consumed (e.g.,

a customer node). By way of example and not limitation, the selected node may include, a junction node, such as a transformer node or a substation node for electricity service, for example.

**[0012]** In response to receiving a selected or given node, the system may explore utility usage information received from metering devices associated with (or included in) a plurality of other nodes, and determine which one or more nodes are immediately connected to the selected node, or which one or more nodes to which the selected node delivers the utility service. In one implementation, the system may determine a topology associated with the selected node by comparing the utility usage information received from the plurality of nodes (or the metering devices associated therewith) with utility usage information recorded at the selected node.

**[0013]** In one implementation, the utility usage information of a node may include changes in usage values of the utility service recorded at a metering device associated with (or included in) the node at a regular time interval or at respective times of change in electricity usage, for example. Additionally or alternatively, the utility usage information of a node may include only, for example, changes in usage values (that are greater than or equal to a predetermined threshold or percentage) of the utility service recorded at a metering device associated with (or included in) the node at a regular time interval or at respective times of change of electricity usage, for example, etc. In one implementation, the utility usage information of a node may further include respective

time stamps of the changes in usage values of the utility service recorded at a metering device associated with (or included in) the node.

**[0014]** In one implementation, the system may compare the utility usage information received from the plurality of nodes with the utility usage information recorded at the selected node by computing correlations between the utility usage information of the plurality of nodes and the utility usage information of the selected node. Additionally or alternatively, in one implementation, the system may determine whether a correlation between the utility usage information of a node of the plurality of nodes and the utility usage information of the selected node is greater than or equal to a predetermined correlation threshold. If the correlation between the utility usage information of the node and the utility usage information of the selected node is greater than or equal to the predetermined correlation threshold, the system may determine that the node is connected to the selected node, or in other words, the node is a component or part of the topology of a network associated with the selected node. By determining that a plurality of nodes are connected to the selected node, the system therefore successfully determines the topology of the network associated with the selected node, i.e., the topology of the network including the selected node and the plurality of determined nodes with the selected node being a root node of the network.

**[0015]** In some implementations, given a determined topology or a previously known topology of a network having a given node as a root node, the system may further monitor and determine whether a discrepancy exists in utility usage data among

one or more nodes in the network including the given node and a plurality of child nodes. In one implementation, the discrepancy may include, but is not limited to, a discrepancy due to fraud (e.g., by tampering with or bypassing a metering device associated with a child node) and/or leakage associated with the utility service in the network. In one implementation, the system may determine whether a change in the utility usage recorded at the given node is unattributable by any combination of changes of one or more utility usages of the plurality of child nodes. Additionally or alternatively, the system may determine whether a value of utility usage recorded at the given node is different from a sum of values of the utility usages received from the plurality of child nodes at a particular time or over a particular period of time.

**[0016]** In one implementation, the system may detect that fraud and/or leakage exists in the network. By way of example and not limitation, the system may detect that a change in a utility usage of a child node is unattributable by (or unable to be correlated with) any change in the utility usage recorded at the given node. Additionally or alternatively, the system may detect that a change in the utility usage recorded at the given node is unattributable by (or unable to be correlated with) any combination of utility usages of one or more of the plurality of child nodes. Additionally or alternatively, the system may detect that a difference exists between a sum of the utility usages of the plurality of child nodes and the utility usage recorded at the given node, and each change in the utility usages of the plurality of child nodes are attributable by (or able to

be correlated with) a change in the utility usage recorded at the given node over one or more periods of time.

**[0017]** In response to detecting a fraud and/or a leakage, the system may report the detection of the fraud and/or the leakage in the network to a management system for subsequent processing, such as reporting the detection to a relevant person to follow up on the situation, locating the fraud and/or the leakage in the network, etc.

**[0018]** The described system allows determining a topology of a network having a given node as a root node based on determining relationships or correlations between utility usages of a plurality of nodes and utility usage recorded at the given node. The described system further enables detecting fraud and leakage in the network by comparing the utility usages associated with the plurality of nodes and the utility consumption recorded at the given node based on the determined topology and/or a previously known topology of the network. Through the described system, a utility service provider can easily detect potential fraud and leakage in a network automatically.

**[0019]** In the examples described herein, the system computes correlations between utility usage recorded at a given node and utility usages of a plurality of nodes, determines a topology of a network including the given node and some of the plurality of nodes (with the given node as a root node), monitors and detects frauds and/or leakages in the network. However, in other implementations, one or more other devices or services may perform some or all of these functions. For example, in one

implementation, a device or service may compute correlations between utility usage recorded at a given node and utility usages of a plurality of nodes, while another device or service may determine a topology of a network based on the computed correlations, and yet another device or service may monitor and detect frauds and/or leakages in the network based on the determined topology.

**[0020]** The application describes multiple and varied embodiments and implementations. The following section describes an example environment that is suitable for practicing various implementations. Next, the application describes example systems, devices, and processes for implementing network topology detection and fraud detection.

#### **Example Architecture**

**[0021]** FIG. 1 is a schematic diagram of an example architecture 100 usable to implement a network topology detection and fraud detection system 102. The architecture 100 includes a plurality of nodes 104-1, 104-2, 104-3, 104-4, 104-5, ... , 104-N (collectively referred to as nodes 104). In this example, N represents a number of nodes arranged in a network. In one implementation, the network may include a distribution network of utility services including, but not limited to, electricity, gas, water, etc. The plurality of nodes 104 are coupled to each other via utility service paths, such as electrical wiring paths, gas pipes, or water pipes, for example. In one implementation, these utility service paths may not be known (or may be partially known) to the network topology detection and fraud detection system 102 and/or a

utility service provider of the distribution network due to dynamics and evolution of the distribution network over time. The plurality of nodes 104 may include, for example, nodes of customers of the utility service, nodes of junctions facilitating routing of the utility service to the customers, nodes of substations serving the utility service for a particular area, etc.

**[0022]** In some implementations, the plurality of nodes 104 may include or be associated with a plurality of devices 106-1, 106-2, 106-3, 106-4, 106-5, ... , 106-M (collectively referred to as devices 106) communicatively coupled to each other via direct communication paths or “links.” In this example, M represents a number of devices arranged in a communication network. In one implementation, the number of devices, M, may be the same as the number of nodes, N. In some implementations, the number of devices, M, may be greater or less than the number of nodes.

**[0023]** In one implementation, the communication network may include an autonomous routing area (ARA), such as a wide area network (WAN), metropolitan area network (MAN), local area network (LAN), neighborhood area network (NAN), personal area network (PAN), or the like. While only one ARA is shown in FIG. 1, in practice, multiple ARAs may exist and may collectively define a larger network, such as an advanced metering infrastructure (AMI) network.

**[0024]** As discussed above, the term “link” refers to a direct communication path between two devices (without passing through or being propagated by another device). The link may be over a wired or wireless communication path. Each link may represent

a plurality of channels over which a device is able to transmit or receive data. Each of the plurality of channels may be defined by a frequency range which is the same or different for each of the plurality of channels. In some instances, the plurality of channels comprises radio frequency (RF) channels.

5   **[0025]**     In one implementation, some or all of the devices 106 may be implemented as any of a variety of conventional computing devices such as, for example, smart utility meters (e.g., electric, gas, and/or water meters), sensors (e.g., temperature sensors, weather stations, frequency sensors, etc.), control devices, transformers, routers, servers, relays (e.g., cellular relays), switches, valves, combinations of the foregoing, or  
10 any device couplable to a communication network and capable of sending and/or receiving data.

**[0026]**     In some implementations, some or all of the devices 106 may additionally or alternatively be implemented as any of a variety of conventional computing devices including, for example, a notebook or portable computer, a handheld device, a netbook,  
15 an Internet appliance, a portable reading device, an electronic book reader device, a tablet or slate computer, a game console, a mobile device (e.g., a mobile phone, a personal digital assistant, a smart phone, etc.), a media player, etc. or a combination thereof.

**[0027]**     In this example, the devices 106 may further be configured to communicate  
20 with a central office 108 via an edge device (e.g., cellular relay, cellular router, edge router, DODAG root, etc.) which serves as a connection point of the ARA to a backhaul

network(s) 110, such as the Internet. In this illustrated example, the device 106-1 serves as a cellular relay to relay communications from the other devices 106-2 – 106-M of the ARA to and from the central office 108 via the network(s) 110.

**[0028]** In one implementation, some or all of the devices 106 may include a processing unit 112. The processing unit 112 may include one or more processor(s) 114 communicatively coupled to memory 116. The memory 116 may be configured to store one or more software and/or firmware modules, which are executable on the processor(s) 114 to implement various functions. While the modules are described herein as being software and/or firmware stored in memory and executable on a processor, in other implementations, any or all of the modules may be implemented in whole or in part by hardware (e.g., as an ASIC, a specialized processing unit, etc.) to execute the described functions.

**[0029]** The memory 116 may comprise computer-readable media and may take the form of volatile memory, such as random access memory (RAM) and/or non-volatile memory, such as read only memory (ROM) or flash RAM. Computer-readable media includes volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer-readable instructions, data structures, program modules, or other data for execution by one or more processors of a computing device. Examples of computer-readable media include, but are not limited to, phase change memory (PRAM), static random-access memory (SRAM), dynamic random-access memory (DRAM), other types of random access

memory (RAM), read-only memory (ROM), electrically erasable programmable read-only memory (EEPROM), flash memory or other memory technology, compact disk read-only memory (CD-ROM), digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or  
5 any other non-transmission medium that can be used to store information for access by a computing device. As defined herein, computer-readable media does not include communication media, such as modulated data signals and carrier waves.

**[0030]** In one implementation, some or all of the devices 106 may additionally include a radio 118. The radio 118 comprises a radio frequency (RF) transceiver  
10 configured to transmit and/or receive RF signals via one or more of a plurality of channels/frequencies.

**[0031]** Additionally or alternatively, in some implementations, some or all of the devices 106 may include a network interface 120, and/or an input/output interface 122. The processing unit 112 may further be configured to receive and act on data from the  
15 network interface 120, received from the input/output interface 122, and/or stored in the memory 116. In some implementations, the memory 116 may also include a metrology module 124 configured to collect consumption data of one or more resources (e.g., electricity, water, natural gas, etc.), which may then be transmitted to one or more other devices 106 for eventual propagation to the central office 108 or other  
20 destination.

**[0032]** The network(s) 110, meanwhile, represents a backhaul network, which may itself comprise a wireless or a wired network, or a combination thereof. The network(s) 110 may be a collection of individual networks interconnected with each other and functioning as a single large network (e.g., the Internet or an intranet). Further, the  
5 individual networks may be wireless or wired networks, or a combination thereof.

**[0033]** The central office 108 may be implemented by one or more computing devices, such as servers, personal computers, laptop computers, routers, switches, etc. The one or more computing devices may be equipped with one or more processor(s) communicatively coupled to memory. In some examples, the central office 108 includes  
10 a centralized meter data management system that performs processing, analysis, storage, and/or management of data received from one or more of the devices 106. For instance, the central office 108 may process, analyze, store, and/or manage data obtained from a smart utility meter, sensor, control device, router, regulator, server, relay, switch, valve, and/or other devices. The central office 108 may additionally or  
15 alternatively include a network management system (NMS) for maintaining a registry of devices of the AMI network, device configuration settings, version information, and the like. Although the example of FIG. 1 illustrates the central office 108 in a single location, in some examples the central office may be distributed amongst multiple locations and/or may be eliminated entirely (e.g., in the case of a highly decentralized distributed  
20 computing platform).

**[0034]** In FIG. 1, the network topology detection and fraud detection system 102 is described to be separate from the central office 108 and the plurality of nodes 104 (or devices 106), and to communicate with the central office 108 and the plurality of devices 106 through the network(s) 110. In some implementations, the network topology detection and fraud detection system 102 may be included in the central office 108 and/or the plurality of nodes 104 (or devices 106). For example, the network topology detection and fraud detection system 102 may be included in the central office 108. In some implementations, a node 104 (such as a junction node or a substation node, for example) of the distribution network or a device 106 of the communication network may include the network topology detection and fraud detection system 102. In alternative implementations, functions of the network topology detection and fraud detection system 102 may be distributed amongst a plurality of nodes 104 (or devices 106) and/or the central office 108. In some implementations, the network topology detection and fraud detection system 102 may be included in servers 126 other than the central office 108.

**[0035]** In one implementation, the network topology detection and fraud detection system 102 is usable to determine a topology associated with part or all of the distribution network, and to detect fraud and leakage in the distribution network based on the determined (or previously known) topology of the distribution network or part of the distribution network.

### **Example Network Topology Detection**

[0036] FIG. 2 illustrates the example network topology detection and fraud detection system 102 in more detail. In one implementation, the network topology detection and fraud detection system 102 may include, but is not limited to, a processing unit 202. The processing unit 202 may include one or more processor(s) 204 communicatively coupled to memory 206. The memory 206 may be configured to store one or more software and/or firmware modules, which are executable on the processor(s) 204 to implement various functions. While the modules are described herein as being software and/or firmware stored in memory and executable on a processor, in other implementations, any or all of the modules may be implemented in whole or in part by hardware (e.g., as an ASIC, a specialized processing unit, etc.) to execute the described functions. The memory 206 may comprise computer-readable media as defined in the foregoing description.

[0037] In one implementation, the network topology detection and fraud detection system 102 may include an input module 208 that receives an instruction or request from the central office 108 or a management or query system associated with the utility service, for example, to determine a network topology associated with a node 104 (such as the node 104-4, for example). Additionally or alternatively, the input module 208 may receive an instruction or request from the node 104 (or the device 106 associated with the node 104) to determine a network topology associated with the node 104.

**[0038]** In one implementation, the node 104 may include, for example, a junction node (such as a transformer node for electricity service), a substation node of the distribution network, etc. In some implementations, the network topology associated with the node 104 may include, but is not limited to, a downstream topology of a part of the utility service distribution network having the node 104 as a root node and including one or more immediate child nodes of the node 104 to which the utility service is delivered via the node 104. In one implementation, an immediate child node of a given node may include a node that is immediately connected to the given node and is a child node of the given node in the distribution network.

10 **[0039]** By way of example and not limitation, the node 104-4 in FIG. 1 may be used as a node given in the received instruction or request to illustrate operations of the network topology detection and fraud detection system 102. In one implementation, the network topology detection and fraud detection system 102 may include a determination module 210 to determine one or more nodes 104 of the distribution network of the utility service that may be considered as potential components of the network topology associated with the given node 104-4 that is to be determined.

**[0040]** In one implementation, the network topology detection and fraud detection system 102 may obtain location information of the nodes 104 of the distribution network to narrow down the number of nodes 104 to be considered for determining the network topology associated with the node 104-4, for example. By way of example and not limitation, the network topology detection and fraud detection system 102 may

determine that nodes 104 having associated devices 106 belonging to a same and/or neighboring communication network(s) (e.g., a same and/or neighboring ARA network(s)) of the given node 104-4 are potential components of the network topology of the part of the distribution network that is associated with the node 104-4 to be  
5 determined.

**[0041]** Additionally or alternatively, in some implementations, the network topology detection and fraud detection system 102 may obtain information about respective physical areas (such as city, district, street, building, etc.) of the plurality of nodes 104 from a database 212 of the network topology detection and fraud detection system 102  
10 or a database outside the network topology detection and fraud detection system 102. The network topology detection and fraud detection system 102 may determine that nodes 104 which belong to physical area(s) that is/are the same as or neighboring to a physical area of the node 104-4 are potential components of the network topology to be determined. In some implementations, the physical area of the node 104-4 may include  
15 one or more junction nodes and a plurality of customer nodes of the distribution network.

**[0042]** Additionally or alternatively, in one implementation, the distribution network may be divided into a number of grids. The network topology detection and fraud detection system 102 may obtain information of respective grids of the plurality of  
20 nodes 104 from the database 212 or a database outside the network topology detection and fraud detection system 102. In one implementation, the network topology

detection and fraud detection system 102 may determine that nodes 104 which belong to grid(s) that is/are the same as and/or neighboring to a grid of the node 104-4 are potential components of the network topology to be determined. In some implementations, the grid of the node 104-4 may include one or more junction nodes and a plurality of customer nodes of the distribution network.

**[0043]** In one implementation, the input module 208 of the network topology detection and fraud detection system 102 may further receive utility service related information from the given node 104-4 and the plurality of considered nodes 104 (e.g., the nodes 104-1, 104-2, and 104-5, etc.) of the distribution network. Additionally or alternatively, the input module 208 of the network topology detection and fraud detection system 102 may receive the utility service related information from device 106-4 associated with (or included in) the given node 104-4 and devices 106 (e.g., the devices 106-1, 106-2, and 106-5, etc.) of the communication network that are associated with the plurality of considered nodes 104.

**[0044]** In one implementation, the utility service related information of a node 104 may include, but is not limited to, information of utility usage of the node 104 (e.g., a customer node), utility usage (or delivery) information through the node 104 (e.g., a junction node, a substation node, etc.), etc. The utility usage of the node 104 may be measured in terms of a physical quantity. Depending on the type of utility service considered, the physical quantity may include, but is not limited to, an electrical current

usage, an electrical voltage usage or an electrical power usage (for electricity service), a volume of gas usage (for gas service) or a volume of water usage (for water service), etc.

**[0045]** In some implementations, the utility usage information of a node 104 (or a device 106 associated therewith) may include, but is not limited to, changes in usage values of the utility service recorded at the device 106 associated with (or included in) the node 104 at a regular time interval or at respective times of change. Additionally or alternatively, the utility usage of a node 104 (or a device 106 associated therewith) may include only, for example, changes (which are greater than or equal to a predetermined threshold or percentage) in usage values of the utility service recorded at the device 106 associated with (or included in) the node 104 at a regular time interval or at respective times of change, etc. Additionally or alternatively, the utility usage information of a node 104 (or a device 106 associated therewith) may include usage values of the utility service recorded at the device 106 associated with (or included in) the node 104 at a regular time interval. In one implementation, the utility usage information of a node 104 (or a device 106 associated therewith) may further include respective time stamps of the usage values and/or the changes in usage values of the utility service recorded at the device 106 associated with (or included in) the node 104.

**[0046]** In one implementation, the network topology detection and fraud detection system 102 may include a topology module 214 to determine which one(s) of the plurality of considered nodes 104 is/are part(s) of the topology of the part of the distribution network associated with the given node 104-4 that is to be determined. In

one implementation, the topology module 214 may compare utility usage information of the plurality of considered nodes 104 with utility usage (or delivery) information of the given node 104-4 to determine which one(s) of the plurality of considered nodes 104 is/are part(s) of the network topology associated with the given node 104-4 to be  
5 determined.

**[0047]** By way of example and not limitation, the topology module 214 may apply a correlation function to compute correlations between respective utility usages of the plurality of considered nodes 104 and the utility usage of the given node 104-4. For example, the topology module 214 may employ a correlation function, such as a cross  
10 correlation function, to compute correlations between respective patterns of utility usages of the plurality of considered nodes 104 and a pattern of the utility usage of the given node 104-4 over one or more predetermined periods of time. In one implementation, the topology module 214 may compute correlations between respective changes (or patterns of changes) in usage values of the utility service of the  
15 plurality of considered nodes 104 and changes (or pattern(s) of changes) in usage values of the utility service of the given node 104-4 over one or more predetermined periods of time. Additionally or alternatively, in some implementations, the topology module 214 may compute correlations between respective usage values (or patterns of usage values) of the utility service of the plurality of considered nodes 104 and usage values (or  
20 pattern(s) of usage values) of the utility service of the over node 104-4 over one or more predetermined periods of time.

**[0048]** In one implementation, in response to computing the correlations between the utility usages of the plurality of considered nodes 104 and the utility usage of the given node 104-4, the network topology detection and fraud detection system 102 may compare the computed correlations with a predetermined correlation threshold. In one  
5 implementation, the network topology detection and fraud detection system 102 may determine that a considered node 104 is a component or part of the topology of the network associated with the given node 104-4 if a computed correlation between the considered node 104 (e.g., 104-1) and the given node 104-4 is greater than or equal to the predetermined correlation threshold.

10 **[0049]** In response to determining one or more considered nodes (e.g., the customer nodes 104-1 and 104-2) to be components or parts of the topology of the network associated with the given node 104-4, the network topology detection and fraud detection system 102 may successfully determine the topology of the network associated with the given node 104-4 to include the customer nodes 104-1 and 104-2,  
15 for example.

**[0050]** Alternatively, in some implementations, upon finding or determining one or more considered nodes 104 (e.g., the customer nodes 104-1 and 104-2) to be components or parts of the network topology associated with the given node 104-4, the network topology detection and fraud detection system 102 may further include a  
20 checking module 216 to check whether the network topology found or determined for the given node 104-4 is complete. For example, the checking module 216 may

determine whether one or more customer nodes 104 that belong to the network topology associated with the given node 104-4 have not been considered by the network topology detection and fraud detection system 102. In one implementation, the checking module 216 may determine whether one or more customer nodes 104  
5 have not previously been considered by comparing the utility usage information of the one or more found nodes 104 with the utility usage information of the given node 104-4.

**[0051]** By way of example and not limitation, the checking module 216 may compare a sum (or combination) of the utility usages (usage values or usage value  
10 changes) of the one or more nodes 104 (e.g., the customer nodes 104-1 and 104-2) found or determined by the topology module 214 with the utility usage of the given node 104-4 at one or more instants of time (or over one or more periods of time), and determine if they are the same. If they are the same, the checking module 216 may determine that the determined network topology is complete. If they are different, e.g.,  
15 the sum of the utility usages of the one or more found nodes is less than the utility usage of the given node 104-4, the checking module 216 may determine that some nodes that belong to the network topology are missing.

**[0052]** In one implementation, in response to determining that some nodes that belong to the network topology are missing, the network topology detection and fraud  
20 detection system 102 may expand a scope of consideration. By way of example and not limitation, the checking module 216 may obtain information about one or more adjacent

communication networks that have not been considered previously from, for example, the database 212 or other database outside the network topology detection and fraud detection system 102. The checking module 216 may consider nodes of these one or more adjacent communication networks for determining or finding missing nodes in this

5 network topology detection associated with the given node 104-4. Additionally or alternatively, the checking module 216 may obtain information about one or more adjacent physical areas and/or grids that have not been considered previously from, for example, the database 212 or other database outside the network topology detection and fraud detection system 102.

10 **[0053]** In one implementation, the network topology detection and fraud detection system 102 may then repeat the foregoing operations of determining the network topology associated with the given node 104-4 until a complete topology is found. Additionally or alternatively, the network topology detection and fraud detection system 102 may then repeat the foregoing operations of determining the network topology

15 associated with the given node 104-4 until a predetermined number of iterations for searching missing nodes is reached. Additionally or alternatively, the network topology detection and fraud detection system 102 may then repeat the foregoing operations of determining the network topology associated with the given node 104-4 until a current scope of consideration is greater than or equal to a reasonable scope associated with

20 the given node. Additionally or alternatively, the network topology detection and fraud detection system 102 may then repeat the foregoing operations of determining the

network topology associated with the given node 104-4 until an administrator temporarily terminates the operations to adjust values of parameters such as the predetermined correlation threshold, for example.

**[0054]** In one implementation, if the sum of the utility usages (e.g., values or value  
5 changes) of the one or more found nodes is different from the utility usage of the given node 104-4 and no missing node is found after a predetermined number of iterations, for example, the checking module 216 may determine that a fraud or leakage may exist in the network. In one implementation, the checking module 216 may notify a relevant person such as a system administrator or personnel of the central office 108, for  
10 example, to follow up on this observation of possible fraud and/or leakage in the network.

#### **Example Fraud Detection**

**[0055]** Given a successfully determined or previously known network topology associated with a node 104 (e.g., the junction node 104-4), the network topology  
15 detection and fraud detection system 102 may further be configured to detect fraud and leakage in (the part of) the distribution network associated with the node 104-4. In one implementation, the network topology detection and fraud detection system 102 may include a monitoring module 218 to monitor the distribution network and determine whether a fraud and/or a leakage occur(s) in the distribution network. In one  
20 implementation, the monitoring module 218 may determine whether a discrepancy exists in utility usage information among one or more nodes in the distribution network.

The discrepancy may include, for example, a discrepancy due to a fraud and/or a leakage in the distribution network.

**[0056]** Continuing with the above example of using the junction node 104-4, in one implementation, the monitoring module 218 may determine whether a change in utility usage value of the junction node 104-4, for example, is unattributable by any combination of one or more changes in utility usage values of the nodes 104 included in the topology. Additionally or alternatively, the monitoring module 218 may determine whether a change in usage value of a node (e.g., the node 104-1) included in the topology is unattributable by any change in the usage value of the junction node 104-4. Additionally or alternatively, the monitoring module 218 may determine whether a difference exists between a value (such as utility usage value) associated the junction node 104-4 (or a metering device associated therewith) and a sum of values (e.g., a sum of utility usage values) associated with the nodes (or metering devices associated therewith) included in the topology at a particular time or over a predetermined period of time. If no change in the utility usage of the junction node 104-4 or any node included in the topology is unattributable or no difference exists, the monitoring module 218 may determine that no fraud or leakage occur in the network.

**[0057]** Alternatively, in response to detecting or determining that a usage value change in a node (e.g., the node 104-1) of the nodes included in the topology is unattributable by any usage value change of the junction node 104-4, the monitoring module 218 may determine that a fraud associated with that particular node 104-1 (e.g.,

tampering a metering device 106-1 associated with the node 104-1) is committed. Additionally or alternatively, the monitoring module 218 may determine that a fraud (e.g., bypassing the metering device 106-1 associated with the node 104-1) and/or a leakage between the node 104-1 and the junction node 104-4 occurs.

5   **[0058]**     In some implementations, in response to determining that one or more changes in the usage value of the junction node 104-4 are unattributable by any combination of one or more changes in utility usage values of the nodes 104 included in the topology, the monitoring module 218 may determine that a fraud (e.g., bypassing a metering device 106-1 associated with a node 104-1 included in the topology) may exist  
10   in the part of the distribution network associated with the junction node 104-4. Additionally or alternatively, the monitoring module 218 may determine that a leakage between the node 104-1 and the junction node 104-4 occurs.

**[0059]**     Additionally or alternatively, in one implementation, in response to determining that each change in the usage value of the nodes 104 included in the  
15   topology is attributable by changes in the usage value of the junction node 104-4 and one or more changes in the usage value of the junction node 104-4 are unattributable by any combination of one or more changes in utility usage values of the nodes 104 included in the topology, the monitoring module 218 may determine that a fraud (e.g., bypassing a metering device 106-1 associated with a node 104-1 included in the  
20   topology) may exist in the part of the distribution network associated with the junction

node 104-4. Additionally or alternatively, the monitoring module 218 may determine that a leakage between the node 104-1 and the junction node 104-4 occurs.

**[0060]** Additionally or alternatively, in some implementations, in response to determining that detecting that each change in the usage value associated with the junction node 104-4 is attributable by a combination of one or more changes in the usage values associated with one or more of the nodes 104 included in the topology and a difference exists between a usage value associated with the junction device 104-4 and a sum of usage values associated with the nodes 104 included in the topology at a particular time or over a predetermined period of time, the monitoring module 218 may determine that a leakage between a node (e.g., the node 104-1) and the junction node 104-4 occurs.

**[0061]** In response to detecting a fraud and/or a leakage in the distribution network, the network topology detection and fraud detection system 102 may include an output module 220 to notify a relevant person such as a system administrator or personnel of the central office 108, for example, to follow up on this detection of the fraud and/or the leakage, and fix the fraud and/or the leakage in the distribution network.

#### **Alternative Implementations**

**[0062]** Although the foregoing implementations describe determining a topology of a part or subset of a distribution network having a given node as a root node of the part or subset of the distribution network, the present disclosure is not limited thereto. In one implementation, a topology of a network including a given node (e.g., the customer

node 104-2, etc.) to be determined may alternatively include an upstream topology associated with the given node 104-2 that includes a network of the given node 104-2 and a junction node (e.g., the junction node 104-4) through which the utility service is delivered to the given node 104-2.

5   **[0063]**     In some implementations, a topology of a network including a given node (e.g., the customer node 104-2, etc.) to be determined may alternatively include a coverage topology that includes a part of the distribution network of the utility service including the given node 104-2, a junction node (e.g., the junction node 104-4) through which the utility service is delivered to the given node 104-2 and other nodes of the  
10   distribution network to which the utility service is delivered via the junction node 104-4, for example.

**[0064]**     In one implementation, the network topology detection and fraud detection system 102 may determine which type of topology an instruction or a request is interested in based on, for example, a type of node of the distribution network for  
15   which the topology is to be determined. By way of example and not limitation, the network topology detection and fraud detection system 102 may determine that a downstream topology is to be determined for a node, such as a junction node or substation node, that includes child nodes in the distribution network of the utility service. In some implementations, the network topology detection and fraud detection  
20   system 102 may determine that an upstream or coverage topology is to be determined

for a node, such as a customer node, that includes no child node in the distribution network of the utility service.

**[0065]** Additionally or alternatively, the network topology detection and fraud detection system 102 may determine which type of topology an instruction or a request is interested in based on, for example, information in the instruction or the request received. For example, the instruction or the request may be received from the central office 108 (or other management or query system), and include information about which type of the topologies the central office 108 (or other management or query system) is interested in. Additionally or alternatively, in some implementations, the network topology detection and fraud detection system 102 may determine a topology of part or all of the distribution network based on an instruction or request from the central office 108 (or other management or query system).

**[0066]** In some implementations, in order to accommodate latencies between nodes with respect to utility usage information (e.g., a change in water usage at node 104-1 may not be instantaneously reflected at node 104-4, etc.), the network topology detection and fraud detection system 102 may employ a sliding window in computing correlations of usage values or changes in usage values between two nodes (e.g., a given node and a considered node, etc.) over one or more periods of time. By using a sliding window, the network topology detection and fraud detection system 102 may tolerate mismatching of utility usage values or value changes between two nodes due to latency

(e.g., because of a distance between the two nodes, etc.), and therefore reduce the likelihood of obtaining false negatives in network topology detection.

### **Exemplary methods**

**[0067]** FIG 3 is a flow chart depicting an example method 300 of network topology  
5 detection. FIG. 4 is a flow chart depicting an example method 400 of fraud detection. The methods of FIG. 3 and FIG. 4 may, but need not, be implemented in the environment of FIG. 1 and using the system of FIG. 2. For ease of explanation, methods 300 and 400 are described with reference to FIGS. 1-2. However, the methods 300 and 400 may alternatively be implemented in other environments and/or using other  
10 systems.

**[0068]** Methods 300 and 400 are described in the general context of computer-executable instructions. Generally, computer-executable instructions can include routines, programs, objects, components, data structures, procedures, modules, functions, and the like that perform particular functions or implement particular  
15 abstract data types. The methods can also be practiced in a distributed computing environment where functions are performed by remote processing devices that are linked through a communication network. In a distributed computing environment, computer-executable instructions may be located in local and/or remote computer storage media, including memory storage devices.

20 **[0069]** The exemplary methods are illustrated as a collection of blocks in a logical flow graph representing a sequence of operations that can be implemented in hardware,

software, firmware, or a combination thereof. The order in which the methods are described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method, or alternate methods. Additionally, individual blocks may be omitted from the method  
5 without departing from the spirit and scope of the subject matter described herein. In the context of software, the blocks represent computer instructions that, when executed by one or more processors, perform the recited operations.

**[0070]** Referring back to FIG. 3, at block 302, the network topology detection and fraud detection system 102 may be triggered to determine a topology of a part of a  
10 utility service distribution network including a given node as a root node. In one implementation, the network topology detection and fraud detection system 102 may receive an instruction or a request to determine a topology of a part of a utility service distribution network including a given node as a root node. Additionally or alternatively, the network topology detection and fraud detection system 102 may determine a  
15 topology of a part of a utility service distribution network including a given node as a root node on a regular basis. Additionally or alternatively, the network topology detection and fraud detection system 102 may be triggered by an event to determine a topology of a part of a utility service distribution network. For example, the network topology detection and fraud detection system 102 may detect abnormal activities or  
20 readings (such as significant changes in utility service consumption, for example) in a given node and may be triggered to determine a topology of a part of a utility service

distribution network including the given node as a root node of the topology to be determined.

**[0071]** At block 304, in response to receiving a given node, the network topology detection and fraud detection system 102 may determine a plurality of nodes of the utility service distribution network that are potentially parts of the topology associated with the given node to be determined. The network topology detection and fraud detection system 102 may determine the plurality of potential nodes based on information such as associated physical locations, associated communication networks, and/or associated grids of the distribution network, for example.

**[0072]** At block 306, upon determining a plurality of potential nodes to be considered, the network topology detection and fraud detection system 102 may determine which one or more potential nodes belong to the topology to be determined based on correlations between utility usages (or changes in the utility usages) of respective potential nodes and utility usage (or changes in the utility usage) of the given node.

**[0073]** At block 308, the network topology detection and fraud detection system 102 may compare the correlations between the plurality of potential nodes and the given node to a predetermined correlation threshold. In one implementation, if a correlation between a potential node and the given node is greater than or equal to a predetermined correlation threshold, the network topology detection and fraud

detection system 102 may render the potential node to be a part of the topology to be determined.

**[0074]** At block 310, upon determining one or more potential nodes to be parts of the topology to be determined, the network topology detection and fraud detection system 102 may determine whether the topology determined so far is complete. The network topology detection and fraud detection system 102 may determine whether the topology is determined so far complete based on, for example, whether a difference exists between the utility usage (or changes in the utility usage) of the given node and a sum of the utility usages (or changes in the utility usages) of the one or more determined nodes. If a difference exists, the network topology detection and fraud detection system 102 may determine that the topology determined so far is incomplete. The network topology detection and fraud detection system 102 may then repeat the operations of topology determination with a larger scope of consideration, for example, by considering additional nodes in other communication networks, physical locations and/or grids of the distribution network that have not been considered previously.

**[0075]** At block 312, if no difference exists, the network topology detection and fraud detection system 102 may determine that the topology determined so far is complete. The network topology detection and fraud detection system 102 may make available of the determined topology associated with the given node for subsequent use such as fraud detection.

**[0076]** Referring back to FIG. 4, at block 402, given a previously determined or known topology of a network associated with a given node (with the given node being a root node of the network), the network topology detection and fraud detection system 102 may monitor and/or detect frauds and/or leakages in the network on a regular basis and/or upon request, for example, by the central office 108 or a maintenance personnel.

**[0077]** At block 404, the network topology detection and fraud detection system 102 may determine whether a fraud and/or a leakage may exist in the network by determining whether a discrepancy exists between utility usage information, such as changes in utility usage values, for example, of the given nodes and a plurality of nodes branching from the given node in the network.

**[0078]** At block 406, if no discrepancy exists, the network topology detection and fraud detection system 102 may determine that no fraud and leakage exist in the network. The network topology detection and fraud detection system 102 may wait for a next scheduled monitoring time for this given node. Additionally or alternatively, the network topology detection and fraud detection system 102 may shift to another node of the distribution network and determine whether a fraud and/or a leakage exists in a topology of a network associated with another node.

**[0079]** At block 408, if a discrepancy exists, the network topology detection and fraud detection system 102 may determine that a fraud and/or a leakage exist(s) in the network. In response to determining or detecting a fraud and/or a leakage exist(s) in the network, the network topology detection and fraud detection system 102 may send a

warning or alert to the central office 108 or the maintenance personnel for follow-up or field investigation to fix the fraud and/or the leakage in the network.

**[0080]** Any of the acts of any of the methods described herein may be implemented at least partially by a processor or other electronic device based on instructions stored on one or more computer-readable media. By way of example and not limitation, any of the acts of any of the methods described herein may be implemented under control of one or more processors configured with executable instructions that may be stored on one or more computer-readable media such as one or more computer storage media.

## 10 **Conclusion**

**[0081]** Although the invention has been described in language specific to structural features and/or methodological acts, it is to be understood that the invention is not necessarily limited to the specific features or acts described. Rather, the specific features and acts are disclosed as exemplary forms of implementing the invention.

15

**WHAT IS CLAIMED IS:**

1. A method comprising:

under control of a processing unit:

correlating, for a given node, value changes associated with the given node and

5 value changes associated with a plurality of nodes with respect to a physical quantity;

and

determining, for the given node, a topology of a network comprising the given

node and at least some nodes of the plurality of nodes with the given node as a root

node based at least on the correlating.

10

2. The method as recited in claim 1, wherein the plurality of nodes

comprises electricity meters, and the physical quantity comprises a usage of an

electrical current, an electrical voltage or an electrical power.

15

3. The method as recited in claim 1, wherein the plurality of nodes

comprises gas meters, and the physical quantity comprises a volume of gas usage.

4. The method as recited in claim 1, wherein the plurality of nodes

comprises water meters, and the physical quantity comprises a volume of water usage.

20

5. The method as recited in claim 1, further comprising receiving records of respective value changes from the plurality of nodes.

6. The method as recited in claim 1, further comprising determining  
5 whether a discrepancy exists in value information among one or more nodes in the network based on the determined topology, the discrepancy comprising a discrepancy due to a fraud and/or a leakage in the network.

7. The method as recited in claim 6, wherein the determining comprises  
10 determining whether a value change associated with the given node is attributable by a combination of one or more value changes associated with one or more of the at least some nodes.

8. The method as recited in claim 6, wherein the determining comprises  
15 determining whether a difference exists between a value associated with the given node and a sum of values associated with the at least some nodes with respect to the physical quantity at a particular time.

9. The method as recited in claim 6, further comprising detecting that a  
20 discrepancy exists in the value information among the one or more nodes in the network based on the determined topology.

10. The method as recited in claim 9, wherein the determining comprises:  
detecting that a value change associated with a node of the at least some nodes  
is unattributable by any value change associated with the given node; and  
5 determining that a fraud associated with the node of the at least some nodes  
has been committed.

11. The method as recited in claim 9, wherein the detecting comprises:  
detecting that each value change associated with the at least some nodes is  
10 attributable by a value change associated with the given node; and  
determining that a fraud bypassing a node of the at least some nodes and/or a  
leakage exist(s) in the network.

12. The method as recited in claim 9, wherein the detecting further  
15 comprises:  
detecting that one or more value changes associated with the given node are  
unattributable by any combination of one or more value change associated with the at  
least some nodes; and  
determining that a fraud bypassing a node of the at least some nodes exists in  
20 the network.

13. The method as recited in claim 9, wherein the detecting further comprises:

detecting that each value change associated with the given node is attributable by a combination of one or more value changes associated with one or more of the at

5 least some nodes; and

determining that a leakage exists in the network.

14. The method as recited in claim 13, wherein the detecting further comprises detecting that a difference exists between a value associated with the given

10 node and a sum of values associated with the at least some nodes with respect to the physical quantity at a particular time.

15. A system comprising:

a processing unit configured to perform acts comprising:

15 determining whether a value change associated with at least one junction node with respect to a physical quantity is unattributable by a combination of one or more value changes associated with one or more of a plurality of nodes; and

detecting whether a discrepancy exists in a network comprising the at least one junction node and the plurality of nodes based on the determining, the discrepancy

20 comprising a discrepancy due to a fraud and/or a leakage in the network.

16. The system as recited in claim 15, wherein the plurality of nodes comprise electricity meters, gas meters or water meters, and wherein the physical quantity comprises an electrical current, an electrical voltage, an electrical power, a volume of gas usage or a volume of water usage.

5

17. The system as recited in claim 15, wherein the determining further comprises determining whether a difference exists between a value associated with the at least one junction node and a sum of values associated with the plurality of nodes with respect to the physical quantity at a particular time.

10

18. The system as recited in claim 17, wherein the determining further comprises determining whether a value change associated with a node of the plurality of nodes is unattributable by any value change associated with the at least one junction node within a sliding time window of a time associated with the value change associated with the node of the plurality of nodes.

15

19. The system as recited in claim 15, the acts further comprising:

detecting that one or more value changes associated with the at least one junction node are unattributable by any combination of one or more value change associated with the plurality of nodes; and

20

determining that a fraud bypassing the plurality of nodes and/or a leakage exists  
in the network.

20. One or more computer-readable media storing executable instructions  
that, when executed by a processing unit, configure the processing unit to perform acts  
comprising:

determining, for a given node, a topology of a network comprising a plurality of  
nodes with the given node as a root node, based at least on correlating respective value  
changes associated with the plurality of nodes to value changes associated with the  
given node with respect to a physical quantity; and

determining whether a discrepancy exists in the network based on the  
determined topology, the discrepancy comprising a discrepancy due to a fraud and/or a  
leakage in the network, the determining comprising:

determining whether a difference exists between a value associated with  
the given node and a sum of values associated with the plurality of nodes with  
respect to the physical quantity at a particular time, and

determining whether a value change associated with the given node is  
unattributable by a combination of one or more value changes associated with  
one or more of the plurality of nodes.

20