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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 June 2015 (18.06.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/089448 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2014/070109

(22) International Filing Date:
12 December 2014 (12.12.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/915,673 13 December 2013 (13.12.2013) US

(71) Applicant: **UNIVERSITY OF NORTH DAKOTA** [US/US]; 264 Centennial Drive, Stop 7095, Twamley Hall, Room 102, Grand Forks, North Dakota 58202 (US).

(72) Inventors: **FARUQUE, Saleh**; 264 Centennial Drive, Stop 7095, Grand Forks, North Dakota 58202-7095 (US). **RANGANATHAN, Prakash**; 264 Centennial Drive, Stop 7095, Grand Forks, North Dakota 58202-7095 (US).

(74) Agents: **PERDOK, Monique M., Reg. No. 42,989** et al.; Schwegman, Lundberg & Woessner, P.A., P.O. Box 2938, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: SMART GRID SECURE COMMUNICATIONS METHOD AND APPARATUS

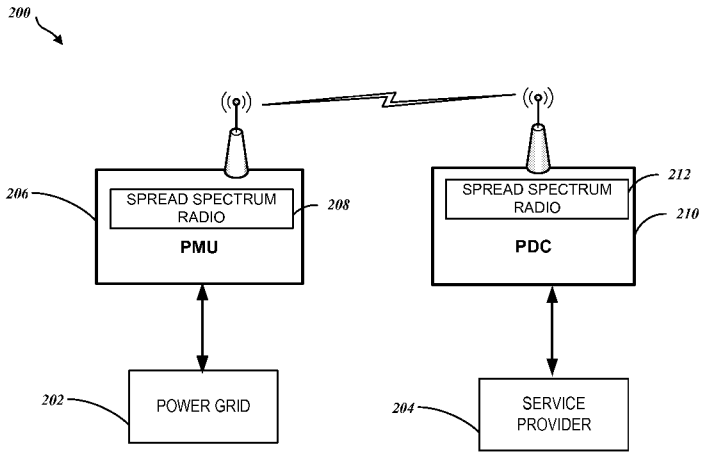

FIG. 2

(57) Abstract: Apparatus and methods performing secure communications in an energy delivery system. Energy delivery systems may include phasor measurement units (PMU), phasor data concentrators (PDC) along with power generation, transmission and consumption equipment. The PMU and PDC may communicate in a grid network over secured wired or wireless communication protocols. Embodiments may include utilizing spread spectrum communication between PMU devices and PDC devices to sustain energy delivery functionality during a communications attack. Communications security may include a cryptographic key management scheme for secure PMU and PDC communication and identification. Embodiments may include clustering of PMU and PDC data for analysis and real-time presentation to grid operators. Embodiments may include clustering of PMU devices in a hexagonal geometry to provide for frequency reuse among devices with directional antenna.

WO 2015/089448 A1

SMART GRID SECURE COMMUNICATIONS METHOD AND APPARATUS

CLAIM OF PRIORITY

This patent application claims the benefit of priority of U.S. Provisional Patent Application Serial Number 61/915,673, entitled "SMART GRID SECURE COMMUNICATIONS METHOD AND APPARATUS," filed on December 13, 2013 (Attorney Docket No. 3311.010PRV), which is hereby incorporated by reference herein in its entirety.

TECHNICAL FIELD

This document pertains generally, but not by way of limitation, to security for utility grid communications. More particularly, embodiments include a spread spectrum radio communication scheme for secure electric-grid network communications and monitoring.

BACKGROUND

The use of the Internet for communications has become inseparably intertwined with our modern lives, and its use for various purposes is rapidly increasing. Unfortunately, cyber-attacks or other malicious activities involving the Internet, commonly referred to as hacking, are also on the rise. As a result, the community of Internet users is becoming more and more vulnerable to malicious activities.

The electrical power grid that supplies electricity to homes, schools and businesses is no exception to these attacks and vulnerabilities. Electricity is an important component in nearly every aspect of modern life. Accordingly, there is an ongoing need to protect the electrical grid and its associated communications from being compromised by a cyber-attack.

Performance monitoring tools measure power system conditions in many locations in the electrical power grid. Conditions such as frequency, voltage phasors, current phasors and other valuable parameters can be used for state estimation, transient analysis, capacitor-bank performance monitoring, analysis

of load shedding schemes, inter-area oscillation control, and other analysis. The growth of the electrical power grid, and the high frequency at which measurements can be obtained, present a need to provide power grid operators with analytical and decision making tools that can aid them in gathering, classifying and analyzing the power system conditions as quickly as possible.

OVERVIEW

Systems and methods of secure communication utilizing spread spectrum communication between Phasor Measurement Unit (PMU) units and Phasor Data Concentrator (PDC) units. Spread Spectrum communication is a form of wireless communication in which the frequency of the transmitted signal is deliberately varied and spread over wide frequency band. Because the frequency of the transmitted PMU data signal is deliberately varied, spread spectrum communication may be utilized to optimize the efficiency of bandwidth within a frequency range, and also provides security benefits. A secure communication signal can be demodulated at the Phasor Data Concentrator (PDC) side for data recovery. This approach addresses various cyber threats such as denial of service (DoS) or flooded attacks in an electric power grid communication.

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

FIG. 1 is a block diagram of an example network based communication system, in accordance with some embodiments;

FIG. 2 is a block diagram of an example secure wireless communication system, in accordance with some embodiments;

FIG. 3 is a flow diagram illustrating an example method for generating MAC keys, in accordance with some embodiments;

FIG. 4 is a block diagram of an example communication flow, in accordance with some embodiments;

FIG. 5 is a flow diagram illustrating an example method for establishing secure communications in an electrical grid, in accordance with some embodiments;

FIG. 6 depicts a unit circle diagram, in accordance with some embodiments;

FIG. 7 depicts a display including four unit circle diagrams that represent the voltages from four individual buses in a multi-buss system, in accordance with some embodiments;

FIG. 8 depicts a three-dimensional scatter plot of data from an example electric utility system, in accordance with some embodiments;

FIG. 9 depicts a three-dimensional scatter plot of data from an example electric utility system, in accordance with some embodiments;

FIG. 10 depicts a graph 1000 of voltage data clusters, in accordance with some embodiments;

FIG. 11 depicts a graph 1100 of frequency data clusters, in accordance with some embodiments;

FIG. 12 depicts a graph 1200 of phase angle data clusters, in accordance with some embodiments;

FIG. 13 is a flow diagram depicting a scheme for performing PMU data analysis, in accordance with some embodiments;

FIG. 14A depicts cell clusters in a three-tier hexagonal geometry, in accordance with some embodiments;

FIG. 14B depicts the clusters of FIG. 14A nested together, in accordance with some embodiments;

FIG. 15 depicts a frequency reuse plan for a hexagonal geometry, in accordance with some embodiments;

FIG. 16 is a block diagram illustrating a wireless communication device in accordance with some embodiments; and

FIG. 17 is a diagrammatic representation of a machine in the example form of a computer system within which a set of instructions for causing the

machine to perform any one or more of the methodologies discussed herein may be executed.

DETAILED DESCRIPTION

Electric power infrastructure is undergoing changes that will unfold over a number of years. As the electric grid is modernized, it will become highly automated, leverage information technology more fully, and become more capable in managing energy from a variety of distributed sources. However, in this process of becoming increasingly smarter and more connected, the electric grid will expand to generate more data and contain more complex interconnections that may become portals for intrusions, error-caused disruptions, malicious attacks, and other threats. Effective strategies for monitoring electric distribution equipment and securing the computing and communication networks that will be central to the performance and availability of the envisioned electric power infrastructure, and protecting the privacy of Smart Grid-related data, are needed.

A synchrophasor, also referred to as a phasor measurement unit (PMU), is a sensor placed on a transmission line that tracks voltage, current, phase and frequency information of the transmission line. In order to have situational awareness of a smart electric grid, a utility operator must monitor the data delivered by the synchrophasor in real-time. Time-stamped synchronized data measurements provide for performance of event prediction and post-event analysis.

Multiple phasor measurement units (PMUs) can provide time-synchronized measurements of a power system such as frequency, voltage phasors, current phasors and other valuable parameters that can be used for state estimation, transient analysis, capacitor bank's performance, analysis of load shedding schemes, and inter-area oscillations. A basic PMU measurement can be obtained at a rate of at least thirty samples per second. With these multiple and frequent data samples, system and grid operators (SGO) can observe any anomalies in frequency, voltage or current in the grid to enhance the situational awareness of the grid. In an example, the use of data analytics to detect these anomalies may provide a tool for SGOs to reduce the frequently occurring brownouts/blackouts. Although, PMU can provide information on the system

conditions, the SGOs need visual analytical and decision tools that can aid them to gather, classify and analyze the data samples to make decisions in real-time.

Currently, the TCP/IP protocol (Transmission Control Protocol (TCP) / Internet Protocol (IP)) is commonly used to communicate between devices in an electric grid. Routable protocols, such as TCP/IP, use addresses that typically have at least two parts: a network address and a device address. Routable protocols allow devices to communicate between two different networks by forwarding packets between the two networks. Non-routable protocols typically only use a device address, and generally do not allow messages to be sent from one network to another, thus allowing communications to take place only on a single network. Routing takes place at a routing layer in the network devices, thus using a routing protocol, such as IP, to route data from one local area network to another. In general, the TCP/IP protocol has vulnerabilities that make it susceptible to a variety of attacks, such as denial-of-service (DOS) attacks, dictionary attacks, Sybil attacks, and message manipulation attacks.

The term Sybil attack denotes an attack where the attacker tries to forge multiple identifications in a certain device or in multiple devices within a region. For example, if a sufficient number of phasor measurement unit (PMU) nodes are infected with a Sybil-like virus, an attacker may be able to completely alter the aggregate reading of the phasor data concentrator (PDC). Depending on the number of nodes the attacker infects or controls, he or she may be able to determine the outcome of any vote, either claim a legitimate node is misbehaving or Sybil nodes can vouch for each other.

A denial-of-service attack includes attacks that flood the system with repeated attempts using the same bogus name. By flooding the system with too much traffic, the server(s) in the system cannot maintain an acceptable level of responsiveness causing the system to become or appear unavailable. A dictionary attack is a brute force attack that uses common words as possible passwords or decryption keys and provides a more efficient way of discovering a user's passcode. If a valid password or key is determined by an attacker, the system is then vulnerable to malicious behavior and at a greater risk of being sabotaged. For example, the loss of the integrity of sensitive PMU data may compromise the security of the power grid. This may include a physical impact of compromising the PMU and a corresponding situational awareness system. In

an example worst case scenario, a compromised PMU could lead to cascading failures of sub-systems or other equipment in the power grid. In response to these hazards, techniques are discussed herein to minimize or prevent the likelihood of a successful attack, and also to maintain authenticated communications between system components.

FIG. 1 is a block diagram of an example network based communication system 100. Power grid 102 may include a PMU (Phasor Measurement Unit) 104 that provides data communication to a PDC (Phasor Data Concentrator) 106. Multiple PMU and PDC may be distributed throughout the power grid 102. The PMU 104 and the PDC 106 may utilize an Internet protocol for data communication over a network 108, such as the Internet or a private network.

Each phasor measurement is time stamped to utilize a Global Positioning System (GPS) universal time; when a phasor measurement is time stamped. This allows measurements taken by PMUs in different locations or by different owners to be synchronized and time-aligned, then combined to provide a precise, comprehensive view of an entire region or interconnection. PMUs samples may be obtained very frequently, for example, at rates of thirty to one-hundred-twenty observations per second.

A power supply service provider 110 may be coupled directly to the PDC 106, or communicate with the PDC 106 over the network 108 via wired or wireless communication technologies. The PMU 104 and PDC 106 may provide data to service provider 110. The PMU 104 and PDC 106 may each be assigned unique identifiers to facilitate encrypted and authenticated communication over the network 108. The power supply service provider 110 may utilize system 100 to monitor electric power usage by consumers, detect cyber-attacks 112, and take appropriate measures in response to changes in power usage or attacks.

Wide area monitoring systems, such as system 100, may include installation of multiple phasor measurement units (PMUs) and substation phasor data concentrators (PDCs). PMUs and substation PDCs are networked appliances that use routable protocols to communicate. PMUs and substation PDCs may become the target of attacks against bulk electric power systems. Threats against these devices may include denial of service attacks, attacks against open ports and services intended to elevate privilege, attempts to change device settings, attempts to inject malicious device commands, attempts to hijack

device access credentials or other confidential information, and attempts to place a man-in-the-middle between devices.

In an example, a strong intrusion detection and prevention mechanism may be used to defend against cyber-attacks while sustaining energy delivery function carried by Phasor Measurement Units (PMU). The addition of security features to PMU devices that utilize attack resilient techniques to mitigate any cyber-attacks within acceptable duration set by the North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP) standards. The energy impact of such a method will yield increased security in the existing grid.

FIG. 2 is a block diagram of an example secure wireless communication system 200 in accordance with some embodiments. The system 200 may include a power grid 102 that is monitored by a service provider 204. The power grid 102 may utilize one or more PMU (Phasor Measurement Units) 206 that include a spread spectrum radio 208 to communicate with a PDC (Phasor Data Concentrator) 210 that also includes a compatible spread spectrum radio 212. The PMU 206 and the PDC 210 may utilize the spread spectrum radio 208 and the spread spectrum radio 212 to perform data communication that is encrypted. The spread spectrum radio 208 and the spread spectrum radio 212 may utilize a frequency-hopping protocol, or configured with a code or password that is periodically or continuously changed, to avoid jamming, interference, impersonation, interception, or other attacks on communications between the PMU 206 and the service provider 204.

In an example, a communication channel utilizing a routing protocol with a keying scheme may be utilized by the PMU 206 and the PDC 210 to further secure communication. Such a security measure may provide grid operators (e.g., service provider 204) with real-time grid conditions, and early evidence of changing threats or conditions and emerging grid problems, thereby allowing the grid operators to manually diagnose, implement and evaluate remedial actions to protect system security and reliability. The PMU 206, the PDC 210, or the power grid 202 may be configured to automatically diagnose, implement and evaluate remedial actions to protect system security and reliability. Although the system 200 is depicted with a single PMU 206 and single PDC 210 the techniques and

processes discussed herein are scalable to accommodate additional PMU units without impeding energy delivery functionality.

In an example, service provider 204 may include an Intrusion Detection System (IDS) configured to communicate with PDC 201 and PMU 206. The IDS may be configured to perform techniques that automate an intrusion detection process.

In an example, service provider 204 may include an intrusion prevention system (IPS) may be configured to include all the capabilities of the IDS, and can also be configured to attempt to stop possible attacks. IDS and IPS techniques may include many of the same capabilities, and administrators may configure one or more prevention features in an IPS module, thereby causing the IPS module to function as an IDS. Intrusion prevention may help to ensure the accuracy and integrity of system 200 capabilities including: billing data, market information, system measurement, and control information. By incorporating IPS functionality security threats may be combatted by blocking and preventing various cyber–attacks, such as Sybil, dictionary, denial-of-service and other similar cyber-attacks.

The availability of communication channels (e.g., access to individual devices such as PDC 201 and PMU 206) is also an important feature for utility delivery systems, including control applications. Confidentiality features may also be utilized in order to protect user consumption and financial data. Non-repudiation techniques may be utilized in inter-domain systems where applications, individuals or organization may be held responsible for any fraudulent actions. Additionally, authentication may be utilized to ensure that malicious individuals are not able to manipulate critical systems or information.

In an example, data gathered from PMU 206 may be protected through attack resilient control algorithms, such as cipher based message authentication (CMAC). A cipher based message authentication code (CMAC) may be used to test the communication among PMUs (e.g., PMU 206 of FIG. 2) and a PDC 210. The use of a CMAC algorithm may prevent inconsistencies and inter-operability in a smart grid environment. The CMAC algorithm may be determined based on the choice of an underlying symmetric key block cipher. The CMAC algorithm is thus a mode of operation (a mode, for short) of the block cipher. The CMAC

key is the block cipher key (the key, for short) that may be utilized as part of the security control in PMU units.

For any given key, the underlying block cipher of the mode consists of two functions that are inverses of each other. The choice of the block cipher includes the designation of one of the two functions of the block cipher as the forward function/transformation, and the other as the inverse function, as in the specifications of the Advanced Encryption Standard (AES) algorithm and Triple Data Encryption Algorithm (TDEA). The CMAC mode does not employ the inverse function.

The forward cipher function is a permutation on bit strings of a fixed length; the strings are called blocks. The bit length of a block is denoted b, and the length of a block is called the block size. For the AES algorithm, b = 128; for the Triple Data Encryption Algorithm (TDEA), b = 64. The key is denoted as K, and the resulting forward cipher function of the block cipher is denoted as CIPHK. The underlying block cipher shall be approved, and the key shall be generated uniformly at random, or close to uniformly at random so that each possible key is (nearly) equally likely to be generated. FIG. 3 is a flow diagram illustrating an example method 300 for generating MAC keys.

The notations M in FIG. 3 represent messages in blocks. The key may be secret and shall be used exclusively for the CMAC mode of the chosen block cipher. To fulfill the requirements of the key, the key should be assigned to the devices that will exchange information (e.g., PMU 206 and PDC 210 of FIG. 2) by a secure key management structure within system 200. Thus the combination of CMAC key management and RSSI approach will defend securely against the Sybil attack during PMU and PDC communication.

In addition, intra-cluster routing between PMU and PDC may be performed when each PMU sensor has one shared-key with every neighbor PMU sensor. For example, two neighbor PMU sensors u and v, and denote their shared-key as K_s. If node ID u < v. PMU sensors u and v may perform the following two-way handshake before exchanging any data:

1) The PMU sensor with smaller node ID (PMU u) sends a challenge message to (PMU v): $\{u, N_0\}K_s+MAC(K_s)$, where nonce N_0 is a one-time random number generated by u, and $MAC(K_s)$ denotes the Message Authentication Code (MAC) generated from message using key K_s.

2) PMU v then replies with a response message to u: {v, $K_{u,v}$, K_v^b, N_0 +1} K_s +MAC($K_{u,v}$, K_v^b), where $K_{u,v}$ and K_v^b are keys generated by v. $K_{u,v}$ is the new pairwise shared-key used for the later communication between u and v, and K_v^b is a broadcast key for v. These security features may be included during the transitioning stages by time-stamping and node-ID specifier.

A wireless Intrusion Detection and Prevention system may monitor phasor related wireless network traffic and analyzes traffic over wireless networking protocols to identify and stop suspicious activities involving the protocols themselves. A received signal strength indicator (RSSI) based solution for Sybil attacks is therefore provided in such a way that it does not burden the WSN with shared keys or require piggybacking of keys to messages. In an example, upon receiving a message, the receiver will associate the RSSI of the message with the sender-ID included in the message, and later if another message with same RSSI but with different sender-ID is received the receiver can detect a potential Sybil attack.

In a less computationally demanding example, a calculation of sender's position may be eliminated. For example, computation requirements may be related by avoiding calculation of fading through distance, for example a Sybil PMU node attempting to impersonate other PMU nodes by broadcasting messages with multiple node identifiers (ID). In contrast to existing solutions which are based on sharing encryption keys, a robust and lightweight solution for the Sybil attack problem based on the received signal strength indicator (RSSI) readings of messages is provided. This solution based on network simulation will yield robust results since it detects all Sybil attack cases and reduces the occurrences of false positives. This solution is lightweight in the sense that alongside the receiver, the collaboration of one other node (i.e., only one message communication) is needed for this protocol. It will be shown that even though RSSI is time-varying and unreliable in general and radio transmission is non-isotropic, using the ratio of RSSIs from multiple receivers it is feasible to overcome the stated problems.

FIG. 4 is a block diagram of an example communication flow 400 between multiple PMUs and a PDC. In a Sybil attack, a single PMU node may present multiple identities to other nodes, such as the PDC, in the network. Through the use of the authentication techniques discussed herein, one node

cannot pretend to be other nodes, i.e., when a sensor node u sends a packet to another node v, node u must present a MAC that is computed using the shared pair wise key K(u, v) between node u and node v. A CMAC algorithm to establish secure communication process between PMUs and PDCs can be thereby be provided both in a PMU and at an aggregator side PDC, as shown in FIG. 4.

FIG. 5 is a flow diagram illustrating an example method for establishing secure communications in an electrical grid. At 502, each PMU and PDC is provided with a key that is unique to each device. At 502, identifiers are established. For example, shared pair wise key may be computed for two adjacent devices. At 506, each PMU or PDC may connect to a peer-to-peer network. The connection may be established through the use of the keys and identifiers.

At 508, each device may monitor the network for attacks or intrusion attempts. For example, at 510, a device may check to determine whether any attempted communication is from an authentic identifier. The authenticity of the identifier may be determined by calculating the pair wise key that corresponds to the purported identity. At 512, in response to a determination that the identifier is authentic the communication may be allowed. At 514, in response to a determination that the identifier is inauthentic, or faked, an anomaly may be reported. The report may be broadcast to a supervisory unit or logged internally at the device.

FIG. 6 depicts a unit circle diagram 601 that depicts three phi (φ) voltage phasors (V1, V2, V3). The lengths of each arrow in the unit circle diagram 601 represent voltage magnitude and angular deviation that can be viewed. Due to the large amount of data generated by an electric grid of any useful size, it is not practical to monitor every data point, which may fluctuate depending on various conditions, nor is it desirable to leave any useful data that may warn of an impending event unmonitored. The unit circle diagram 601 can provide a visual representation of data that is intuitive and communicates the gathered data to an observer accurately and clearly.

FIG. 7 depicts a display 701 including four unit circle diagrams that represent the voltages from four individual buses in a multi-buss system. Each of the unit circle diagrams represents three-φ voltages (V1, V2, V3) that may be

depicted in different colors (e.g., red, blue and green, respectively) for easy or quick identification. Each unit circle diagram may depict the bus voltages at specified time periods. Data generated in the grid can be visually represented unit circle diagrams or other forms, so that the system operators can quickly understand the events as they are happening in real-time.

FIG. 8 depicts a three-dimensional scatter plot 800 of data from an example electric utility system. The nominal voltages at ideal conditions are one p.u. and three-hundred kilo-volts respectively. Under real conditions, the values are little off from actual values (e.g., approximately 0.98 p.u. and 299.5k volts).

Clustering is a process of grouping the data into clusters, so that objects within a cluster have high similarity in comparison to one another but are very dissimilar to objects in other clusters. The advantages of clustering schemes in high streaming data rate applications such as synchrophasors are useful to detect key features (e.g., bad vs. good data, faults, or cyber threats) that distinguish different groups of clusters.

A density based clustering technique based on the temporal data structure of synchrophasors can track parameters both in real-time and off-line analysis. For example, a DBSCAN (density-based spatial clustering of applications with noise) clustering algorithm can be utilized present a visualization of activities in an electric grid system. An example DBSCAN algorithm is discussed in "A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise," by M. Ester, H. Kriegel, J. Sander, and X. Xu, Kdd, 1996. The classification and clustering of data can be used to extract patterns describing important data classes, or to predict future data trends in the system. Clustering is a process of grouping the data into clusters, so that objects within a cluster have high similarity in comparison to one another but are very dissimilar to objects in other clusters. An advantage of utilizing clustering schemes in streaming data rate applications such as synchrophasors is the ability to detect events (e.g., bad vs good data, equipment faults, or cyber threats) that distinguish different groups of clusters. Such event detection can help provide SGOs with a better understanding of the data and the system in operation.

FIG. 9 depicts a three-dimensional scatter plot 900 of data from an example electric utility system. The use of density based clustering algorithms to analyze the temporal data structure of synchrophasors can be used to track

parameters both in real-time, and to perform historical or off-line analysis. The DBSCAN algorithm clusters the data into three types: core points (circle), border points (triangle) and noise points (diamond). All these points are clustered based on the two parameters called as ε (Eps) and Minpts. The noise (diamond) points are the unwanted points caused due to bad data that is further away in distance from the majority of the good core points (circle).

FIG. 10 depicts a graph 1000 of voltage data clusters, where each vertical cluster 1002 includes a centroid 1004. A k-means algorithm may be executed to group the individual data points in each cluster 1002 and plot the centroid 1004 for the cluster 1002. FIG. 11 depicts a graph 1100 of frequency data clusters, where each vertical cluster 1102 includes a centroid 1104. In a typical system, the frequency may typically be stable such that the sampled data does not deviate more than a few one-hundredths during stead state conditions. In the example depicted in FIG. 11 the clusters are grouped near 59.9 Hz. FIG. 12 depicts a graph 1200 of phase angle data clusters, where each vertical cluster 1202 includes a centroid 1204.

In FIGs. 10, 11 and 12, the X-axis presents the number of clusters that are formed. The Y-axis presents the parameter being clustered. An example clustering technique may be performed by using a k-means algorithm. For example:

```
Do {
        changed = false;
        // Empty out clusters
        foreach (List<double> cluster in clusters) {
                cluster.Clear;
                }
        // Distribute data points through
foreach (double datum in data) {
        closest = 0;
        // Find nearest centroid for each data point
        for (int i = 1; i < numOfClusters; i++) {
                if (Math.Abs(datum - centroids- centroids[closest] ) >
                        Math.Abs(datum - centroids[i])) {
                        closest = i;
                        }
                }
        clusters[closest].Add(datum);
        // Add data point to appropriate
        }
// Find the new centroids for each cluster
for (int i = 0; i < numOfClusters; i++) {
        if (clusters[i].Any() && clusters[i].Average() != centroids[i]) {
                clusters[i].Average();
                changed = true;
                }
        }
} while (changed);
```

FIG. 13 is a flow diagram depicting a scheme 1300 for performing PMU data analysis. The analysis may be performed by a PDC, or a subsequent computing device that receives data from the PDC. At 1302, a PDC may be flooded with one or more streams of data from one or more PMU devices. The data received contains all the parameters from various PMU units that are connected to the PDC. At 1304, the PMU data received is sorted out based on the originating PMU device. Once the data is sorted from a PMU, at 1306 the PMU sorted data is sorted based on the type of parameter.

The data of a particular parameter (e.g., frequency or voltage magnitude) may be selected and processed at 1308. The data processing at 1308 may include an analysis of device parameters such as location (e.g., latitude, longitude), in order to allow for subsequent analysis. For example, at 1310, a location based

heat map can be displayed with symbols or colors indicating the status of one or more grid equipment monitored by the PMU. Additionally, a graphical user interface may provide clustered data in any format requested by an operator. For example, the unit circle diagrams of FIG. 7, the three-dimensional scatter plot of FIGs. 8 or 9, or the graphs of FIGs. 10-12.

Additionally, and in parallel, at 1312, stored data can be extracted from archives, and at 1314 the newly received and stored data can be clustered by considering different parameters such as number of samples, a specific location, or a particular time frame. At 1316 the clustered data can be displayed, and also used to form future predictions based on a combination of the received and stored data.

In large electrical grid systems, where there are multiple PMUs involved, IP networks can be employed to transport sets of data from individual PMUs between substations and control centers. Substations may be linked to each other and control centers by leased lines, privately owned synchronous optical networks (SONETs), or wireless links. Small cells of PMUs may be utilized in electrical grid networks to provide additional data gathering coverage and capacity where macro networks are overburdened.

FIG. 14A depicts cells clustered in a three-tier hexagonal geometry. The synchrophasor or PMU includes an antenna embedded within the device that can communicate the phasor data information wirelessly to a data aggregator. At Tier-0 an individual cell 1402 includes three sectors. Directional antennas are used in each sector such that each antenna radiates into its respective 120-degree sector. This this antenna directivity may be used to assigning the same frequency to all three directions, such that co-channel isolation will be increased, interference will be reduced, and the channel capacity will be increased.

A directional frequency reuse pattern that can be superimposed on a hexagonal grid to yield a given frequency only at the three corners of the triangle in each tier to provide wireless communication between devices. This technique divides up the available frequency into L x L frequency groups arranged as an L x L matrix. These L x L matrices may then be reused horizontally and vertically according to the following rule:

[L x L] [L x L] . .

[L x L] [L x L] . .

:

where

$L = 1+3i$, $i = 1, 2, \ldots$

This methodology provides a frequency reuse plan where three adjacent reuses of a group form an apex of a triangle. Table 1 shows the number of frequencies needed to form an apex of a triangle.

i	L	Frequencies
1	4	16
2	7	49
3	10	100
4	13	169
5	16	256
6	19	361
7	22	484
8	25	625

TABLE 1

In every tier of hexagonal cellular geometry, there exists an apex of a triangle. FIG. 14B depicts the clusters of FIG. 14A nested together in a single hexagonal geometry 1400.

FIG. 15 depicts a frequency reuse plan 1500 for a hexagonal geometry, such as the tiers depicted in FIG. 14B, that forms an apex of a triangle. For example, a ten-by-ten array ($i = 3$, $L = 10$), as shown in TABLE 1, has 100 frequencies. Each frequency is assigned to a sector, which results in a back-to-back triangular formation of the same frequency throughout the entire hexagonal grid. The frequency plan as illustrated is then expanded as needed, in areas surrounding the first use, as required to cover a geographical area. For example, frequency group 1 radiates in a different direction, 120 degrees apart, almost back-to-back.

The frequency reuse of the proposed plan reduces interference in such a way that the effective number of interferers is reduced to less than two. The C/I of this plan may be determined as sown in FORMULA 1,

$$\frac{C}{I} \geq 10 \log\left[\frac{1}{2}\left(\sqrt{3N}\right)^{\gamma}\right] \approx 35\,dB$$

FORMULA 1

where N = (100 / 3) = 33.33 is the reuse factor, and $\gamma = 3.8$ is the path loss slope. The path loss slope, γ, also referred to in the art as the propagation constant, is the rate of decay of signal strength as a function of distance. The scheme described herein provides a C/I of 35dB.

FIG. 16 is a block diagram illustrating a wireless communication device 600, upon which any one or more of the techniques (e.g., methodologies) discussed herein may be performed. The wireless communication device 600 may include a processor 610. The processor 610 may be any of a variety of different types of commercially available processors suitable for mobile devices, for example, an XScale architecture microprocessor, a Microprocessor without Interlocked Pipeline Stages (MIPS) architecture processor, or another type of processor. A memory 620, such as a Random Access Memory (RAM), a Flash memory, or other type of memory, is typically accessible to the processor 610. The memory 620 may be adapted to store an operating system (OS) 630, as well as application programs 640 and a key 650. The OS 630 or application programs 640 may include instructions stored on a computer readable medium (e.g., memory 620) that may cause the processor 610 of the wireless communication device 600 to perform any one or more of the techniques discussed herein. The key 650 may be a cryptographic key that is private or shared with one or more other devices. The key 650 may be managed and utilized by the OS 630 or the application programs 640 to communicate securely with one or more other devices. The processor 610 may be coupled, either directly or via appropriate intermediary hardware, such as a display, or to one or more input/output (I/O) devices 660, such as a keypad, a touch panel sensor, a microphone, etc. Similarly, in an example embodiment, the processor 610 may be coupled to a

transceiver 670 that interfaces with an antenna 690. The transceiver 670 may be configured to both transmit and receive cellular network signals, wireless data signals, spread spectrum communication signals, encrypted communication signals, or other types of signals via the antenna 690, depending on the nature of the wireless communication device 600.

FIG. 17 illustrates a block diagram of an example machine 700 upon which any one or more of the techniques (e.g., methodologies) discussed herein may be performed. In alternative embodiments, the machine 700 may operate as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine 700 may operate in the capacity of a server machine, a client machine, or both in server-client network environments. In an example, the machine 700 may act as a peer machine in peer-to-peer (P2P) (or other distributed) network environment. The machine 700 may be a personal computer (PC), a tablet PC, a Personal Digital Assistant (PDA), a mobile telephone, a web appliance, or any machine capable of executing instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein, such as cloud computing, software as a service (SaaS), other computer cluster configurations.

Examples, as described herein, may include, or may operate on, logic or a number of components, modules, or mechanisms. Modules are tangible entities capable of performing specified operations and may be configured or arranged in a certain manner. In an example, circuits may be arranged (e.g., internally or with respect to external entities such as other circuits) in a specified manner as a module. In an example, the whole or part of one or more computer systems (e.g., a standalone, client or server computer system) or one or more hardware processors may be configured by firmware or software (e.g., instructions, an application portion, or an application) as a module that operates to perform specified operations. In an example, the software may reside (1) on a non-transitory machine-readable medium or (2) in a transmission signal. In an example, the software, when executed by the underlying hardware of the module, causes the hardware to perform the specified operations.

Accordingly, the term "module" is understood to encompass a tangible entity, be that an entity that is physically constructed, specifically configured (e.g., hardwired), or temporarily (e.g., transitorily) configured (e.g., programmed) to operate in a specified manner or to perform part or all of any operation described herein. Considering examples in which modules are temporarily configured, each of the modules need not be instantiated at any one moment in time. For example, where the modules comprise a general-purpose hardware processor configured using software, the general-purpose hardware processor may be configured as respective different modules at different times. Software may accordingly configure a hardware processor, for example, to constitute a particular module at one instance of time and to constitute a different module at a different instance of time.

Machine (e.g., computer system) 700 may include a hardware processor 702 (e.g., a processing unit, a graphics processing unit (GPU), a hardware processor core, or any combination thereof), a main memory 704, and a static memory 706, some or all of which may communicate with each other via a link 708 (e.g., a bus, link, interconnect, or the like). The machine 700 may further include a display device 710, an input device 712 (e.g., a keyboard), and a user interface (UI) navigation device 714 (e.g., a mouse). In an example, the display device 710, input device 712, and UI navigation device 714 may be a touch screen display. The machine 700 may additionally include a mass storage (e.g., drive unit) 716, a signal generation device 718 (e.g., a speaker), a network interface device 720, and one or more sensors 721, such as a global positioning system (GPS) sensor, camera, video recorder, compass, accelerometer, or other sensor. The machine 700 may include an output controller 728, such as a serial (e.g., universal serial bus (USB), parallel, or other wired or wireless (e.g., infrared (IR)) connection to communicate or control one or more peripheral devices (e.g., a printer, card reader, etc.).

The mass storage 716 may include a machine-readable medium 722 on which is stored one or more sets of data structures or instructions 724 (e.g., software) embodying or utilized by any one or more of the techniques or functions described herein. The instructions 724 may also reside, completely or at least partially, within the main memory 704, within static memory 706, or within the hardware processor 702 during execution thereof by the machine 700.

In an example, one or any combination of the hardware processor 702, the main memory 704, the static memory 706, or the mass storage 716 may constitute machine-readable media.

While the machine-readable medium 722 is illustrated as a single medium, the term "machine readable medium" may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that configured to store the one or more instructions 724.

The term “machine-readable medium” may include any tangible medium that is capable of storing, encoding, or carrying instructions for execution by the machine 700 and that cause the machine 700 to perform any one or more of the techniques of the present disclosure, or that is capable of storing, encoding or carrying data structures used by or associated with such instructions. Non-limiting machine-readable medium examples may include solid-state memories, and optical and magnetic media. Specific examples of machine-readable media may include: non-volatile memory, such as semiconductor memory devices (e.g., Electrically Programmable Read-Only Memory (EPROM), Electrically Erasable Programmable Read-Only Memory (EEPROM)) and flash memory devices; magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks.

The instructions 724 may further be transmitted or received over a communications network 726 using a transmission medium via the network interface device 720 utilizing any one of a number of transfer protocols (e.g., frame relay, internet protocol (IP), transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), etc.). The term “transmission medium” shall be taken to include any intangible medium that is capable of storing, encoding or carrying instructions for execution by the machine 700, and includes digital or analog communications signals or other intangible medium to facilitate communication of such software.

Embodiments may be implemented in one or a combination of hardware, firmware and software. Embodiments may also be implemented as instructions stored on a computer-readable storage device, which may be read and executed by at least one processor to perform the operations described herein. A computer-readable storage device may include any non-transitory mechanism for storing information in a form readable by a machine (e.g., a computer). For

example, a computer-readable storage device may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media.

The above detailed description includes references to the accompanying drawings, which form a part of the detailed description. The drawings show, by way of illustration, specific embodiments in which the invention can be practiced. These embodiments are also referred to herein as "examples." Such examples can include elements in addition to those shown or described. However, the present inventors also contemplate examples in which only those elements shown or described are provided. Moreover, the present inventors also contemplate examples using any combination or permutation of those elements shown or described (or one or more aspects thereof), either with respect to a particular example (or one or more aspects thereof), or with respect to other examples (or one or more aspects thereof) shown or described herein.

In the event of inconsistent usages between this document and any documents so incorporated by reference, the usage in this document controls.

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

Method examples described herein can be machine or computer-implemented at least in part. Some examples can include a computer-readable medium or machine-readable medium encoded with instructions operable to configure an electronic device to perform methods as described in the above examples. An implementation of such methods can include code, such as

microcode, assembly language code, a higher-level language code, or the like. Such code can include computer readable instructions for performing various methods. The code may form portions of computer program products. Further, in an example, the code can be tangibly stored on one or more volatile, non-transitory, or non-volatile tangible computer-readable media, such as during execution or at other times. Examples of these tangible computer-readable media can include, but are not limited to, hard disks, removable magnetic disks, removable optical disks (e.g., compact disks and digital video disks), magnetic cassettes, memory cards or sticks, random access memories (RAMs), read only memories (ROMs), and the like.

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

CLAIMS

1. A secure communication system comprising:

a phasor measurement unit (PMU) coupled to a power grid, the PMU being configured to collect a plurality of data parameters from the power grid;

a first radio coupled to the PMU;

a phasor data concentrator (PDC) configured to receive and analyze the plurality of data parameters; and

a second radio coupled to the PDC, the second radio being configured to receive the plurality of data parameters from the first radio and provide the plurality of data parameters to the PDC;

wherein the first radio and the second radio are spread spectrum radios configured to communicate over secure channels, the secure channels utilizing a passcode configured in the first radio and the second radio.

2. The secure communication system of claim 1, wherein the first radio and the second radio are anti-jam (AJ) and low probability of intercept (LPI) spread spectrum radios.

3. The secure communication system of claim 1, wherein the first radio and the second radio are frequency hopping radios.

4. The secure communication system of claim 1, wherein the PDU and the PDC both include a cipher based message authentication code, and exchange the cipher based message authentication code as part of a handshake protocol before providing or receiving the plurality of data parameters.

5. The secure communication system of claim 4, wherein the PDU and the PDC are configured to ignore communications that do not include the cipher based message authentication code.

6. A method comprising:

providing a unique key value to each one of a plurality of devices configured to access a peer-to-peer network;

establishing an identifier for each one of the plurality of devices based at least in part on the unique key value for each one of the plurality of devices;

generating a pairwise shared-key in response to one of a pair of the plurality of devices in the peer-to-peer network to a second of the pair of the plurality of devices in the peer-to-peer network in response to a request from the one of the pair of devices to connect to the second of the pair;

monitoring the peer-to-peer network for communications that lack an identifier that is determined to correspond to at least one pair of the plurality of devices.

7. The method of claim 6, wherein establishing the identifier includes generating a cipher based message authentication code.

8. The method of claim 7, further comprising:

performing a handshake protocol exchange of the cipher based message authentication code before providing or receiving data.

9. A machine readable storage medium comprising a plurality of instructions that when executed by a computing device cause the computing device to perform operations comprising:

providing a unique key value to each one of a plurality of devices configured to access a peer-to-peer network;

establishing an identifier for each one of the plurality of devices based at least in part on the unique key value for each one of the plurality of devices;

generating a pairwise shared-key in response to one of a pair of the plurality of devices in the peer-to-peer network to a second of the pair of the plurality of devices in the peer-to-peer network in response to a request from the one of the pair of devices to connect to the second of the pair;

monitoring the peer-to-peer network for communications that lack an identifier that is determined to correspond to at least one pair of the plurality of devices.

10. The machine readable storage medium of claim 9, wherein establishing the identifier includes generating a cipher based message authentication code.

11. The machine readable storage medium of claim 10, the operations comprising further comprising:

performing a handshake protocol exchange of the cipher based message authentication code before providing or receiving data.

12. An apparatus comprising means for performing any of the methods of claims 6-8.

13. A method comprising:

receiving, at a phasor data concentrator (PDC), sensor measurements from a plurality of phasor measurement units (PMUs) in a power grid, the PMUs each being configured to collect a plurality of data parameters from the power grid;

sorting the plurality of data parameters based on individual PMUs in the plurality of PMUs;

sorting the plurality of data parameters based on an individual parameter; and

displaying a status of one or more grid equipment monitored by the plurality of PMUs.

14. The method of claim 13, wherein, the PMUs each individually collect the plurality of data parameters from separate devices in the power grid.

15. The method of claim 13, wherein, the plurality of data parameters include at least one of: a voltage, a frequency, or a phase angle.

16. The method of claim 13, further comprising:

analyzing the plurality of data parameters based on location information of grid equipment monitored by an individual PMU.

17. The method of claim 13, further comprising:

determining an equipment status by of one or more grid equipment monitored by the plurality of PMUs based on a density based clustering analysis of the data parameters.

18. The method of claim 17, wherein the equipment status includes a unit circle diagram depicting three phi voltage phasors.

19. The method of claim 17, further comprising:

displaying a three-dimensional representation of the data parameters based on the density clustering analysis of the data parameters.

20. At least one machine readable storage medium comprising a plurality of instructions that when executed by a computing device cause the computing device to:

receive, at a phasor data concentrator (PDC), sensor measurements from a plurality of phasor measurement units (PMUs) in a power grid, the PMUs each being configured to collect a plurality of data parameters from the power grid;

sort the plurality of data parameters based on individual PMUs in the plurality of PMUs;

sort the plurality of data parameters based on an individual parameter; and

display a status of one or more grid equipment monitored by the plurality of PMUs.

21. The machine readable storage medium of claim 20, wherein, the PMUs each individually collect the plurality of data parameters from separate devices in the power grid.

22. The machine readable storage medium of claim 20, wherein, the plurality of data parameters include at least one of: a voltage, a frequency, or a phase angle.

23. The machine readable storage medium of claim 20, further comprising instructions that when executed by the computing device cause the computing device to:

analyze the plurality of data parameters based on location information of grid equipment monitored by an individual PMU.

24. The machine readable storage medium of claim 20, further comprising instructions that when executed by the computing device cause the computing device to:

determine an equipment status by of one or more grid equipment monitored by the plurality of PMUs based on a density based spatial clustering analysis of the data parameters.

25. The machine readable storage medium of claim 20, wherein the equipment status includes a unit circle diagram depicting three phi voltage phasors.

26. The machine readable storage medium of claim 20, further comprising instructions that when executed by the computing device cause the computing device to:

display a three-dimensional representation of the data parameters based on the density clustering analysis of the data parameters.

27. An electrical power grid monitoring system comprising:

a plurality of phasor measurement units (PMUs) each being configured to collect a plurality of data parameters from equipment in the electrical power grid;

a phasor data concentrator (PDC) wirelessly coupled to the plurality of PMUs by a secure network connection, such that the PDC receives the plurality of data parameters from the PMUs over the secure network connection, the PDC configured to:

collect the plurality of data parameters from each PMU;

sort the plurality of data parameters based on individual PMUs in the plurality of PMUs;

sort the plurality of data parameters based on an individual parameter;

monitor the secure network connection for communications that lack an identifier that is determined to correspond to at least one of the plurality of PMUs;

perform a density based spatial clustering of the data parameters.

28. The system of claim 27, wherein the plurality of data parameters include at least one of: a voltage, a frequency, or a phase angle.

29. The system of claim 27, wherein the PDC is further configured to:

determine an equipment status based on the density based spatial clustering analysis of the data parameters.

30. The system of claim 27, wherein the PMU devices include a direction antenna and are organized in a hexagonal geometry to provide for frequency reuse among the PMU devices.

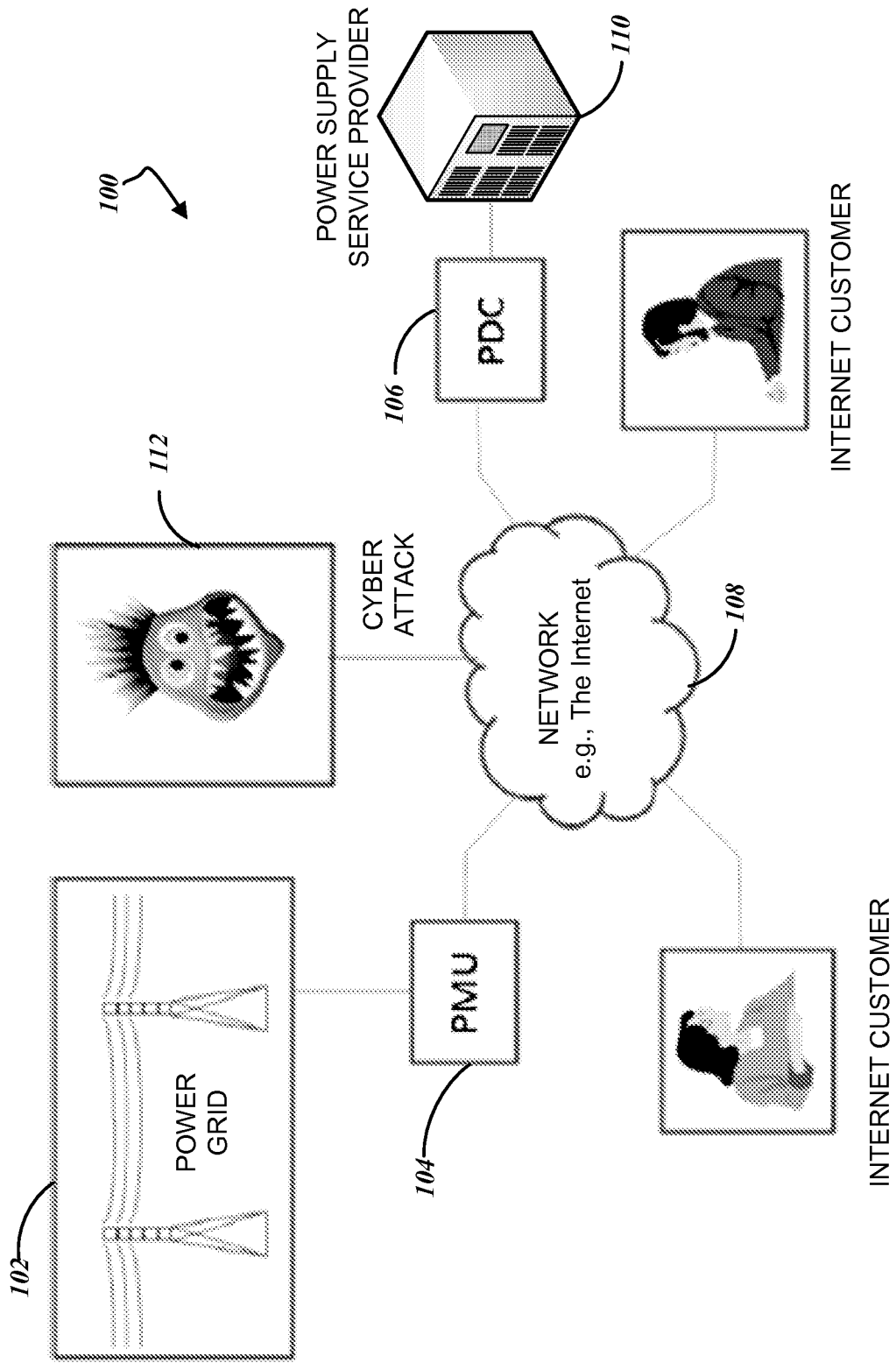
100
POWER SUPPLY
SERVICE PROVIDER
110
PDC
106
INTERNET CUSTOMER
112
CYBER
ATTACK
NETWORK
e.g., The Internet
108
POWER
GRID
102
PMU
104
INTERNET CUSTOMER

FIG. 1

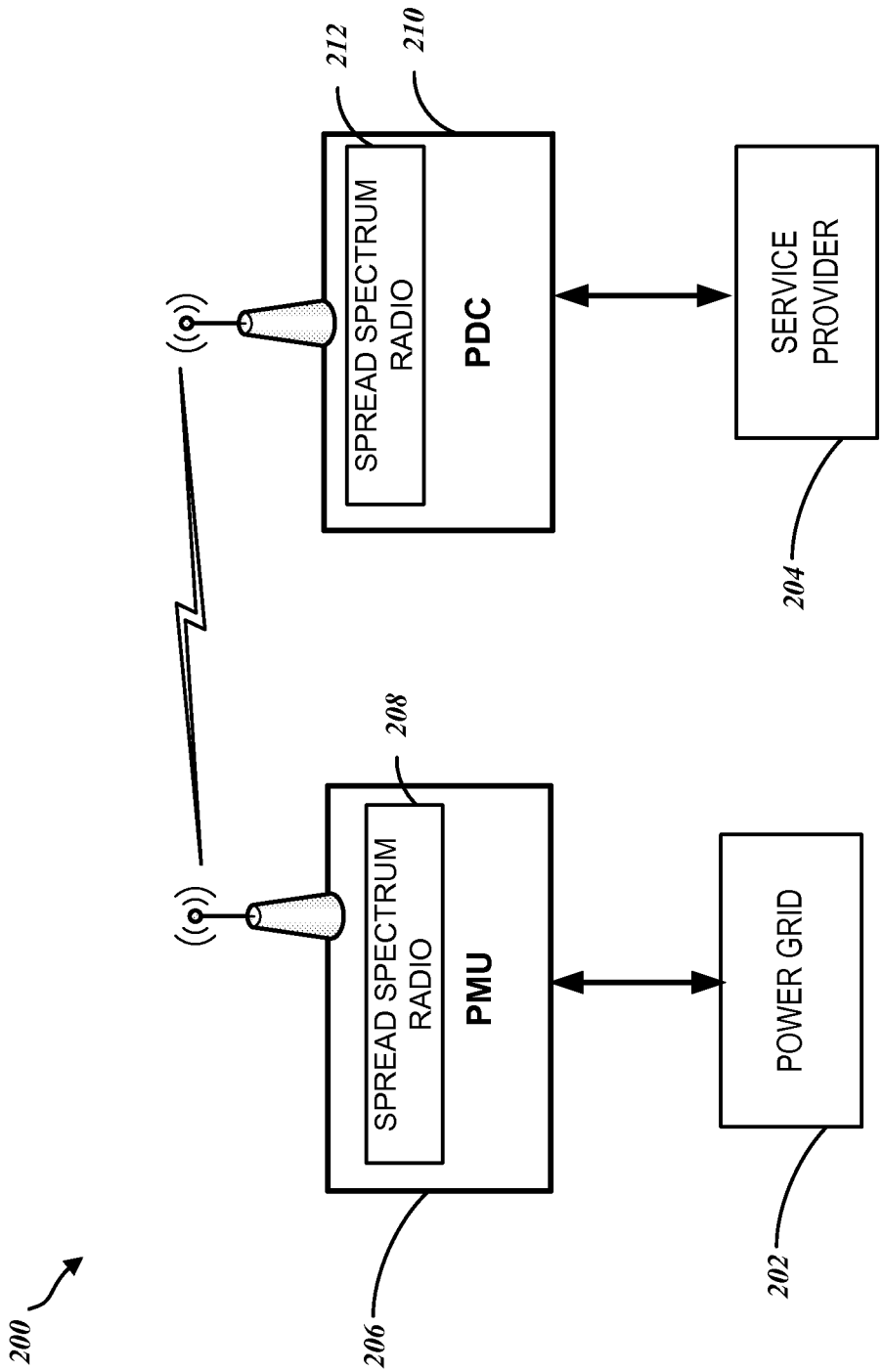
200
206
PMU
SPREAD SPECTRUM RADIO
208
202
POWER GRID
204
SERVICE PROVIDER
PDC
SPREAD SPECTRUM RADIO
210
212

FIG. 2

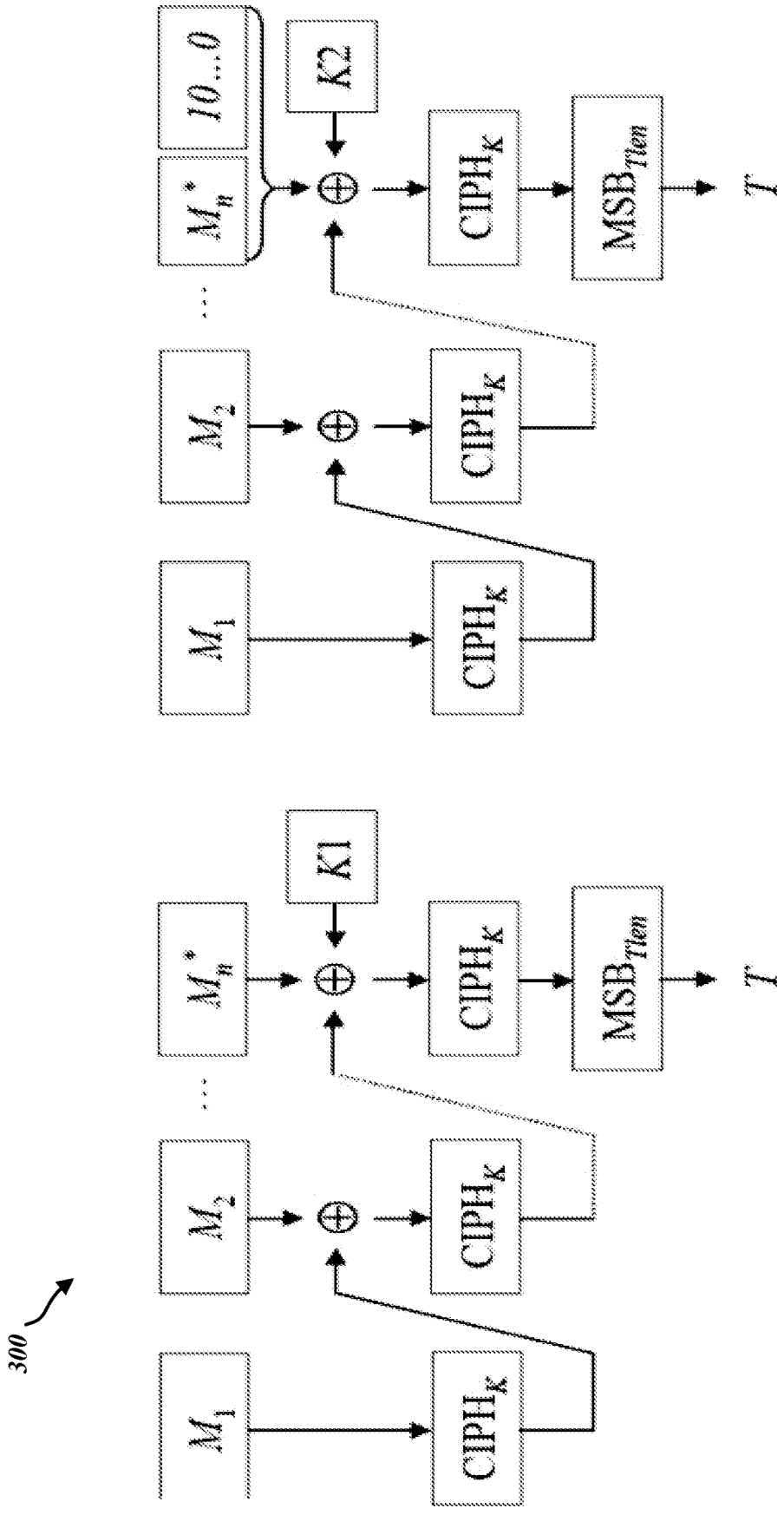

FIG. 3

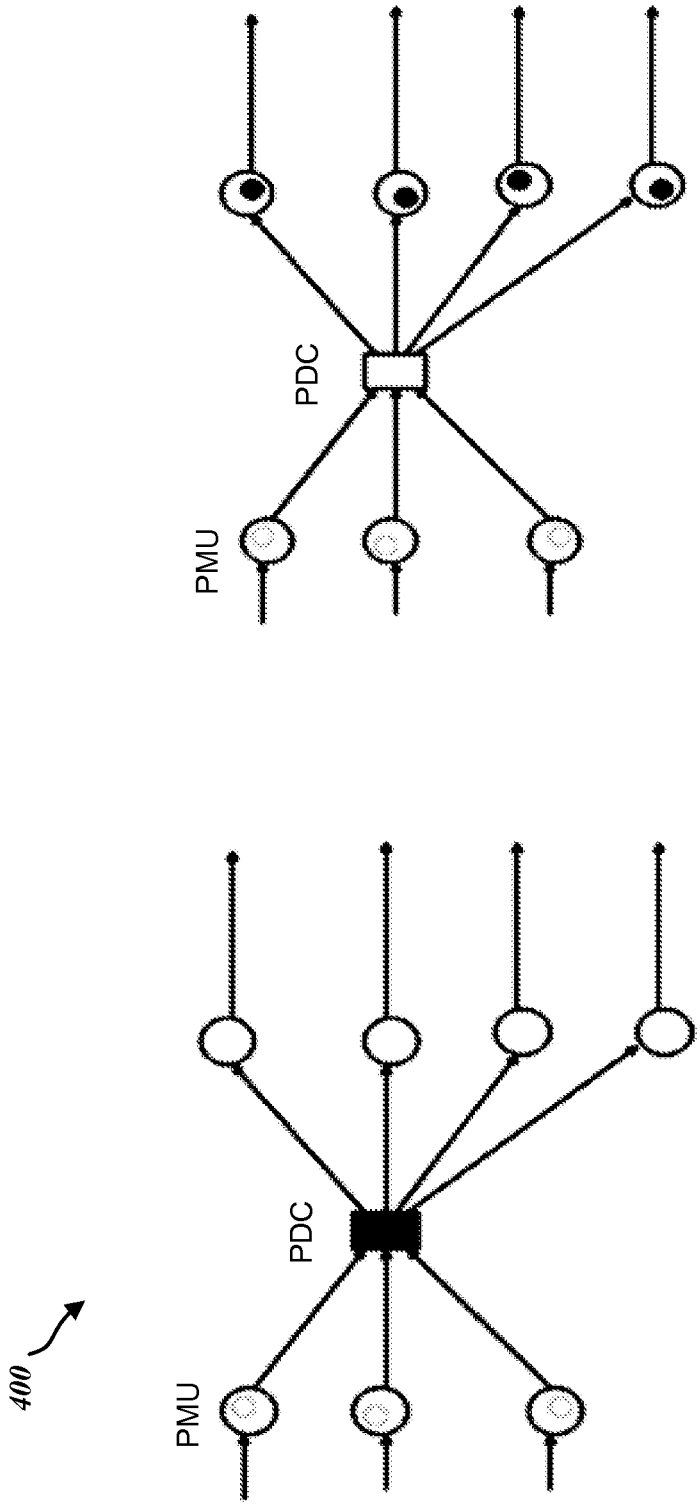

FIG. 4

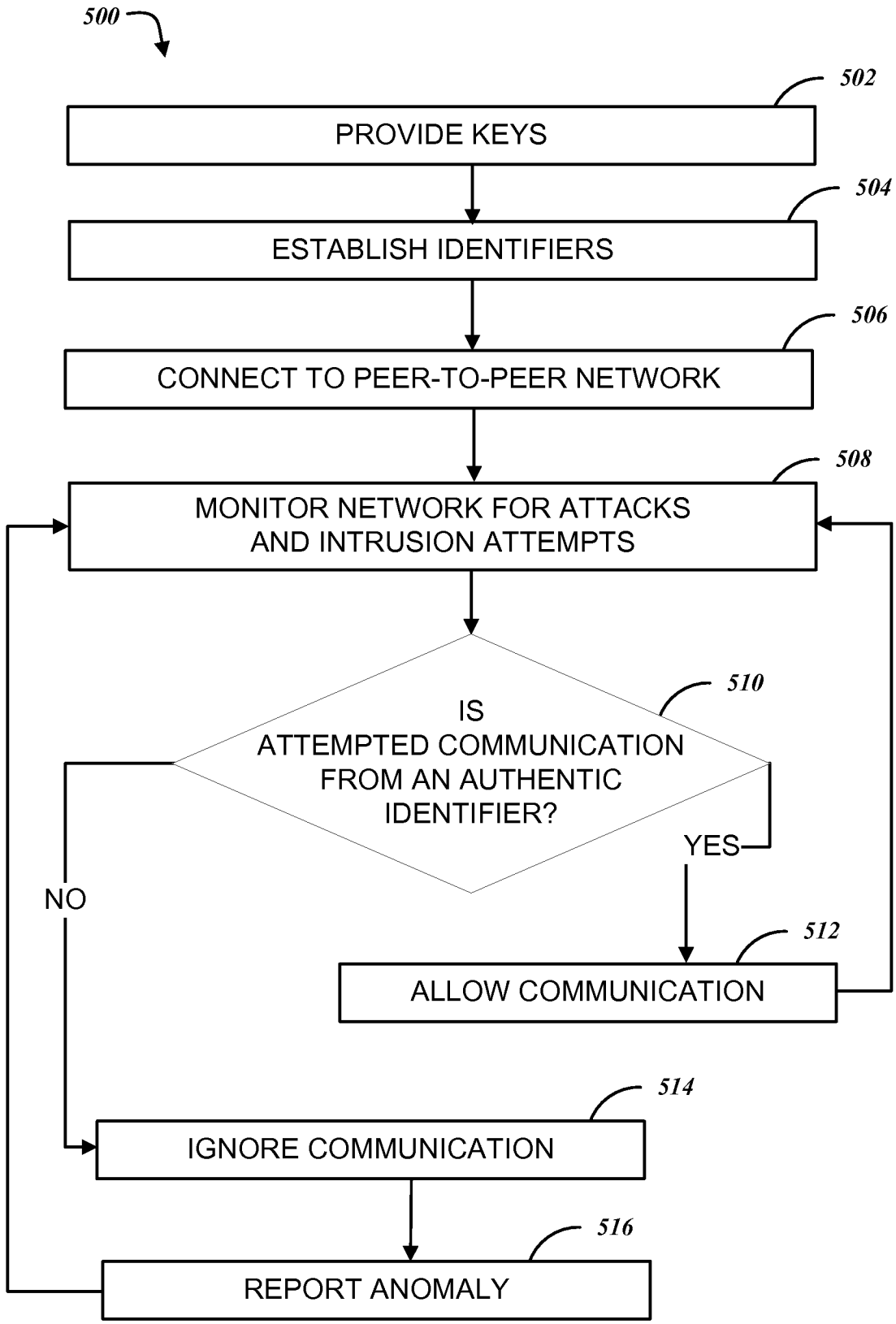
500
502
PROVIDE KEYS
504
ESTABLISH IDENTIFIERS
506
CONNECT TO PEER-TO-PEER NETWORK
508
MONITOR NETWORK FOR ATTACKS AND INTRUSION ATTEMPTS
510
IS ATTEMPTED COMMUNICATION FROM AN AUTHENTIC IDENTIFIER?
YES
NO
512
ALLOW COMMUNICATION
514
IGNORE COMMUNICATION
516
REPORT ANOMALY

FIG. 5

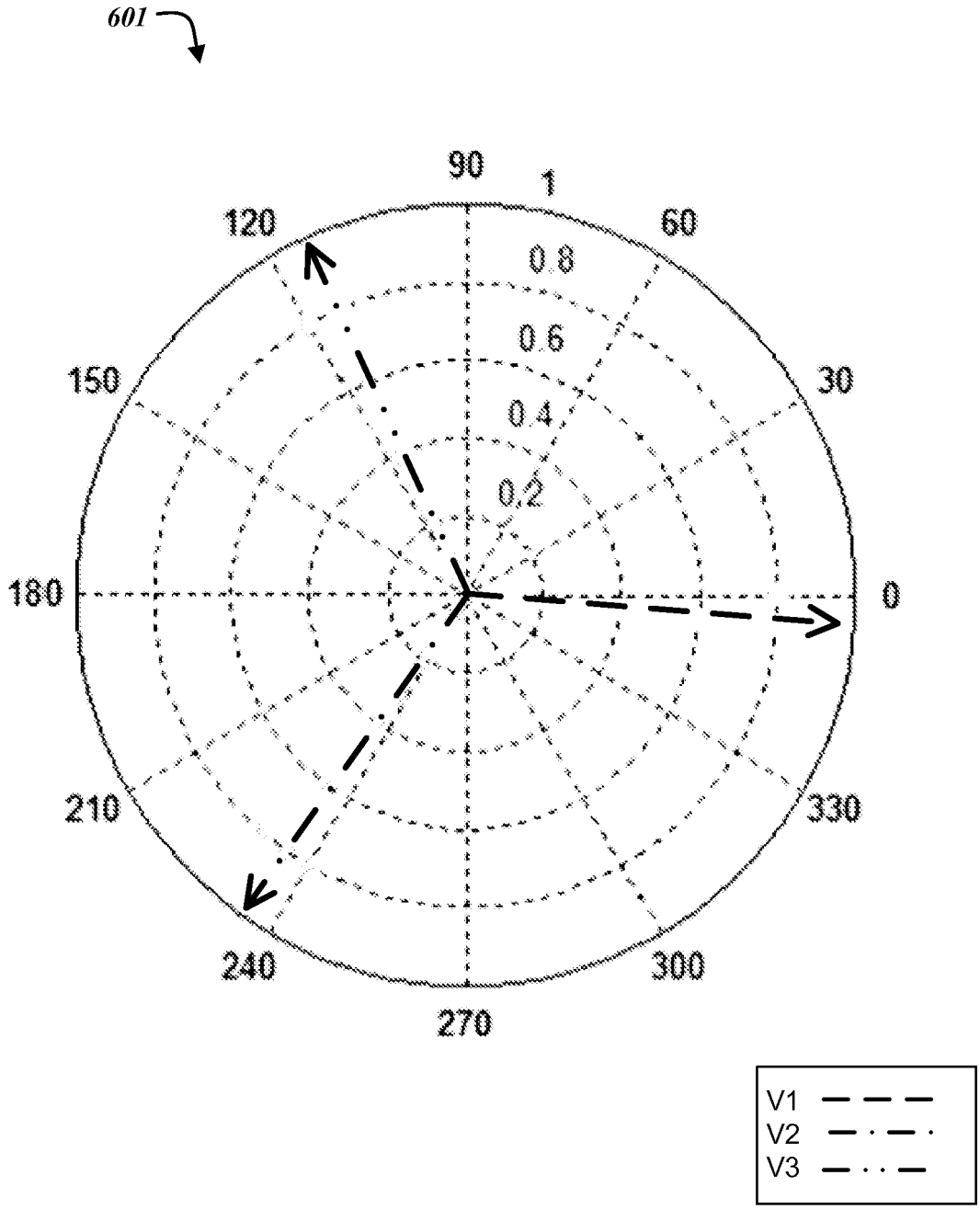

FIG. 6

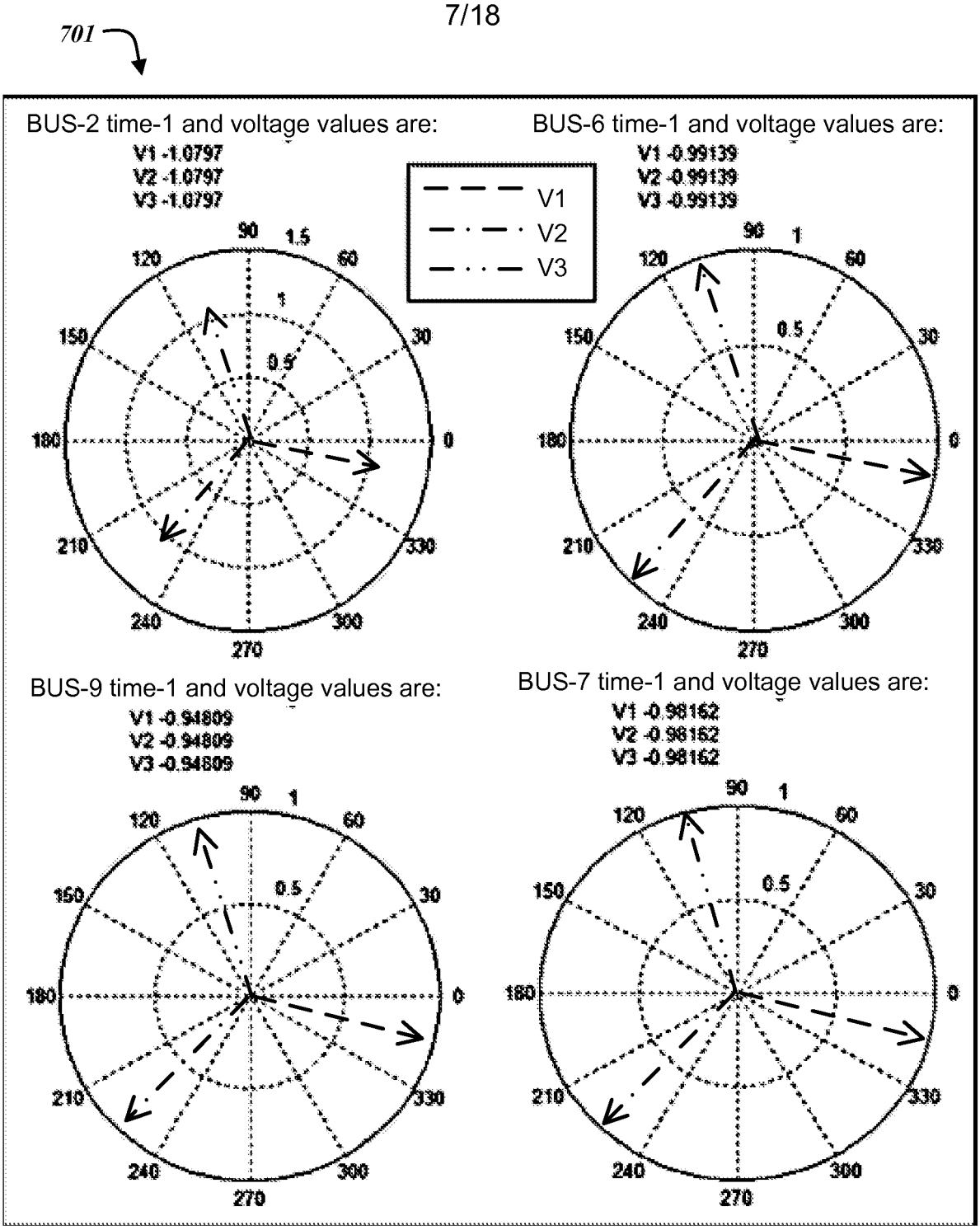
701
BUS-2 time-1 and voltage values are:
V1 -1.0797
V2 -1.0797
V3 -1.0797
BUS-6 time-1 and voltage values are:
V1 -0.99139
V2 -0.99139
V3 -0.99139
V1
V2
V3
BUS-9 time-1 and voltage values are:
V1 -0.94809
V2 -0.94809
V3 -0.94809
BUS-7 time-1 and voltage values are:
V1 -0.98162
V2 -0.98162
V3 -0.98162
90
120
60
150
30
180
0
210
330
240
300
270

FIG. 7

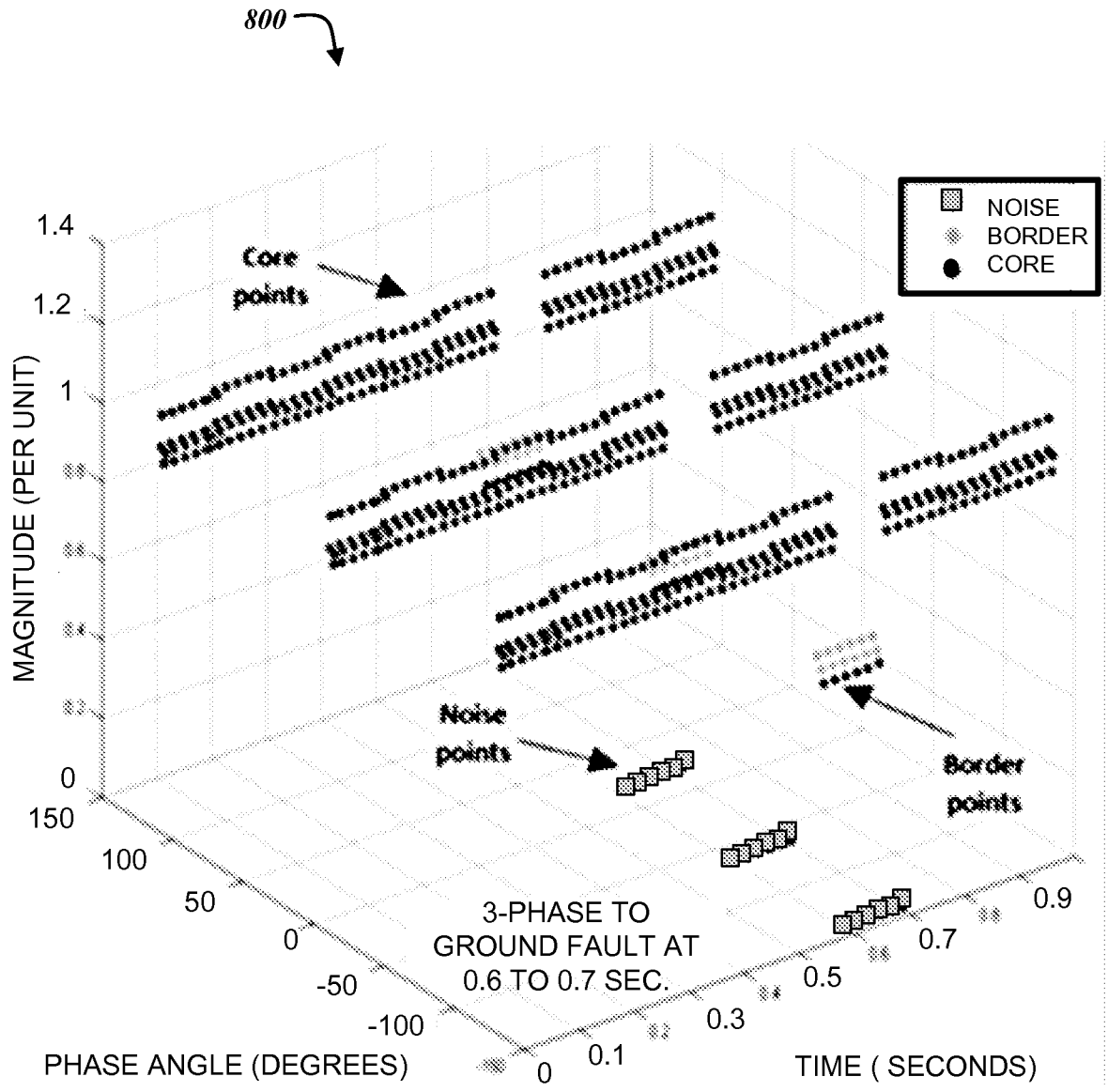
800
NOISE
BORDER
CORE
Core points
Noise points
Border points
MAGNITUDE (PER UNIT)
1.4
1.2
1
0
150
100
50
0
-50
-100
PHASE ANGLE (DEGREES)
3-PHASE TO GROUND FAULT AT 0.6 TO 0.7 SEC.
0
0.1
0.3
0.5
0.7
0.9
TIME (SECONDS)

FIG. 8

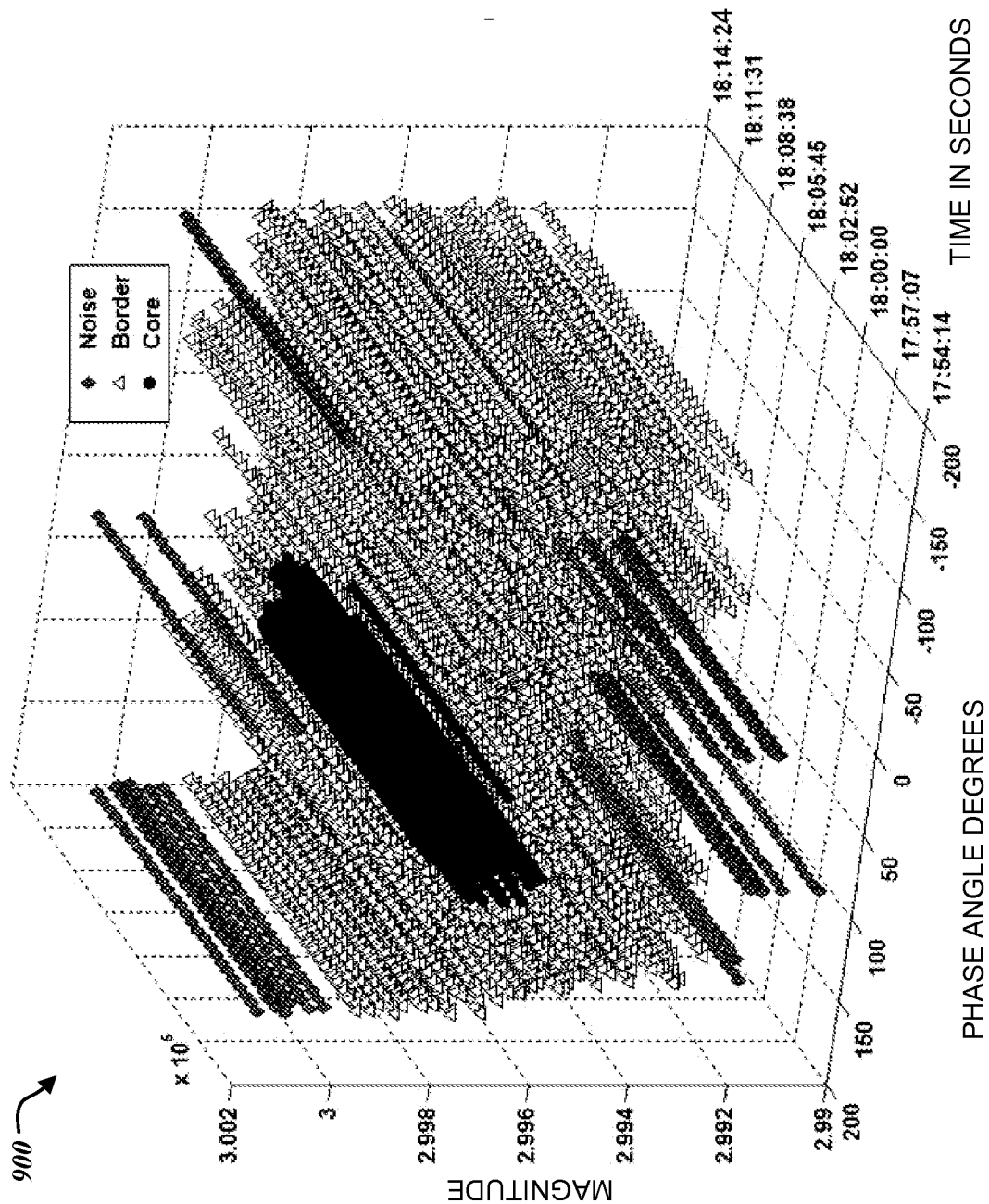
900
Noise
Border
Core
x 10^5
3.002
3
2.998
2.996
2.994
2.992
2.99
MAGNITUDE
200
150
100
50
0
-50
-100
-150
-200
PHASE ANGLE DEGREES
18:14:24
18:11:31
18:08:38
18:05:45
18:02:52
18:00:00
17:57:07
17:54:14
TIME IN SECONDS

FIG. 9

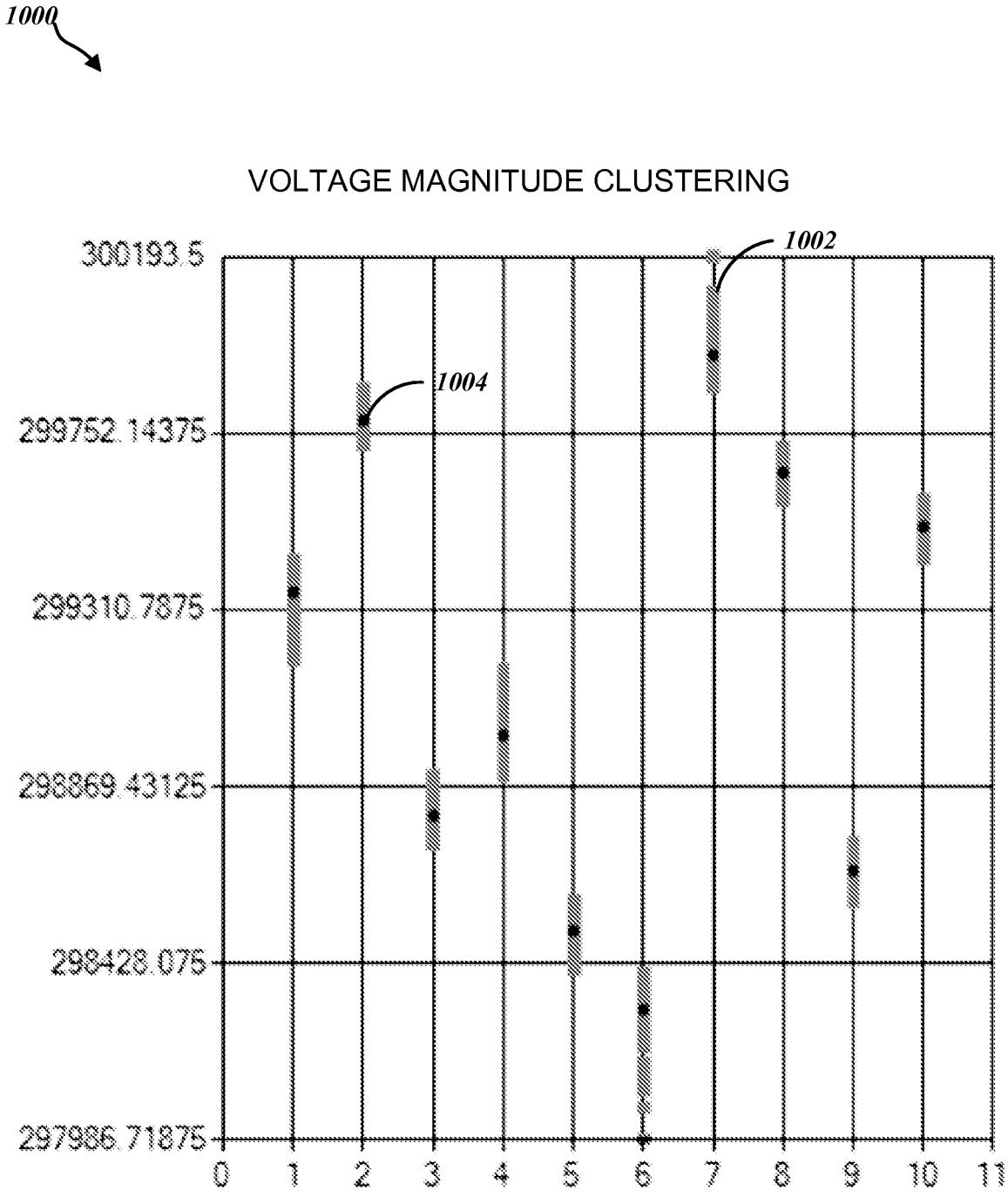
1000
VOLTAGE MAGNITUDE CLUSTERING
300193.5
299752.14375
299310.7875
298869.43125
298428.075
297986.71875
0
1
2
3
4
5
6
7
8
9
10
11
1002
1004

FIG. 10

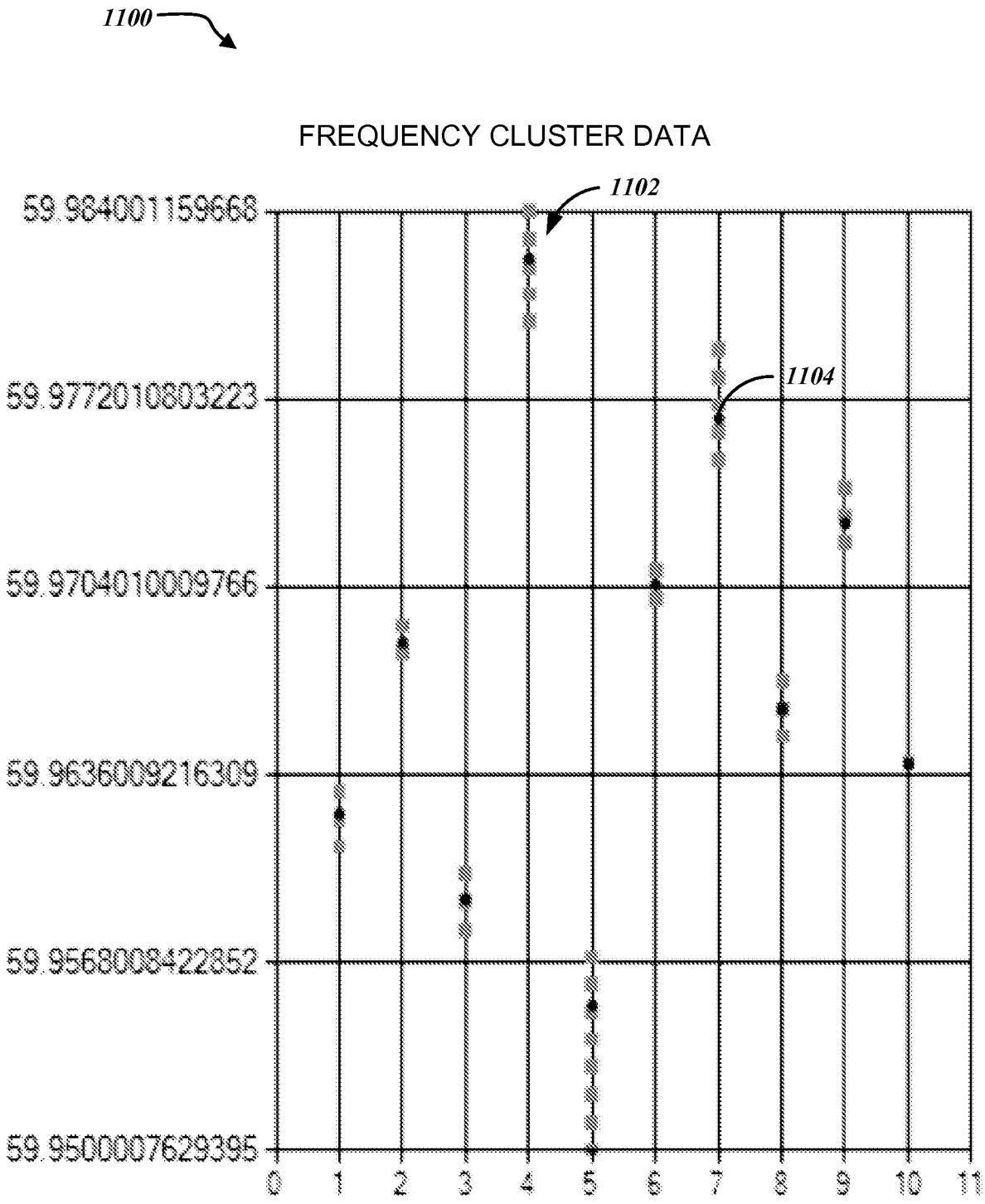
1100
FREQUENCY CLUSTER DATA
1102
1104
59.984001159668
59.9772010803223
59.9704010009766
59.9636009216309
59.9568008422852
59.9500007629395
0
1
2
3
4
5
6
7
8
9
10
11

FIG. 11

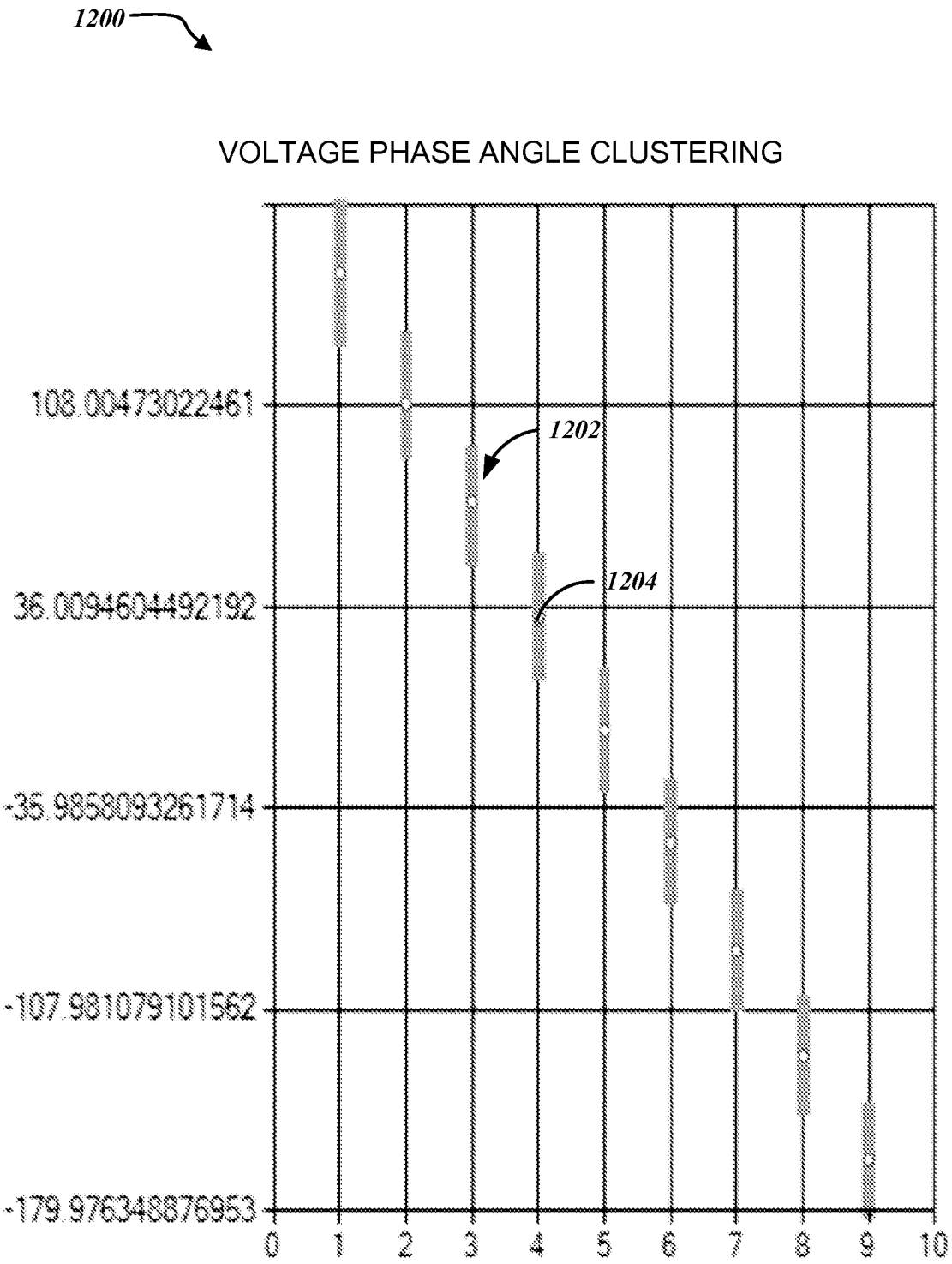
1200
VOLTAGE PHASE ANGLE CLUSTERING
108.00473022461
36.0094604492192
-35.9858093261714
-107.981079101562
-179.976348876953
1202
1204
0
1
2
3
4
5
6
7
8
9
10

FIG. 12

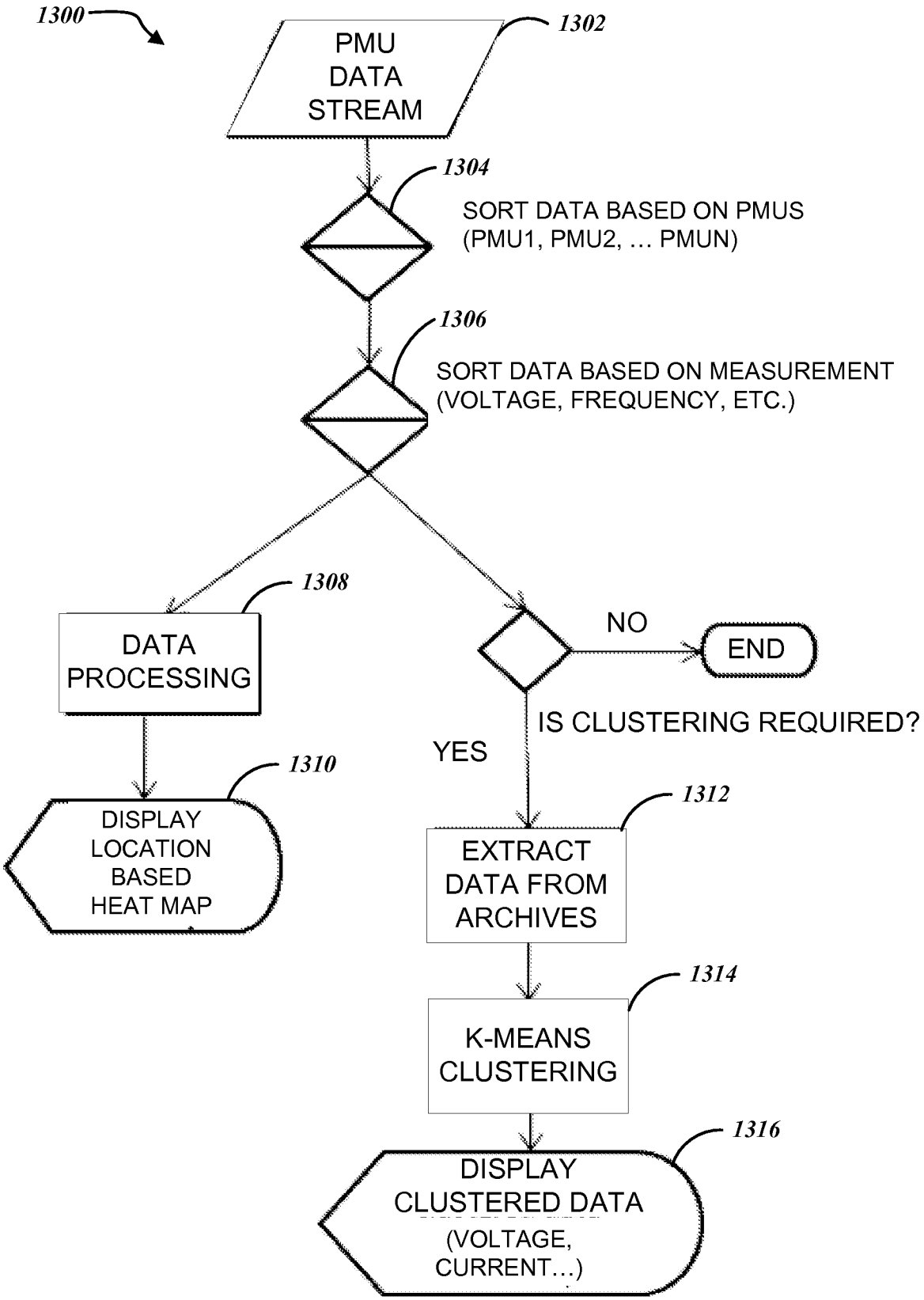
1300
PMU DATA STREAM
1302
1304
SORT DATA BASED ON PMUS (PMU1, PMU2, … PMUN)
1306
SORT DATA BASED ON MEASUREMENT (VOLTAGE, FREQUENCY, ETC.)
1308
DATA PROCESSING
NO
END
IS CLUSTERING REQUIRED?
YES
1310
DISPLAY LOCATION BASED HEAT MAP
1312
EXTRACT DATA FROM ARCHIVES
1314
K-MEANS CLUSTERING
1316
DISPLAY CLUSTERED DATA (VOLTAGE, CURRENT…)

FIG. 13

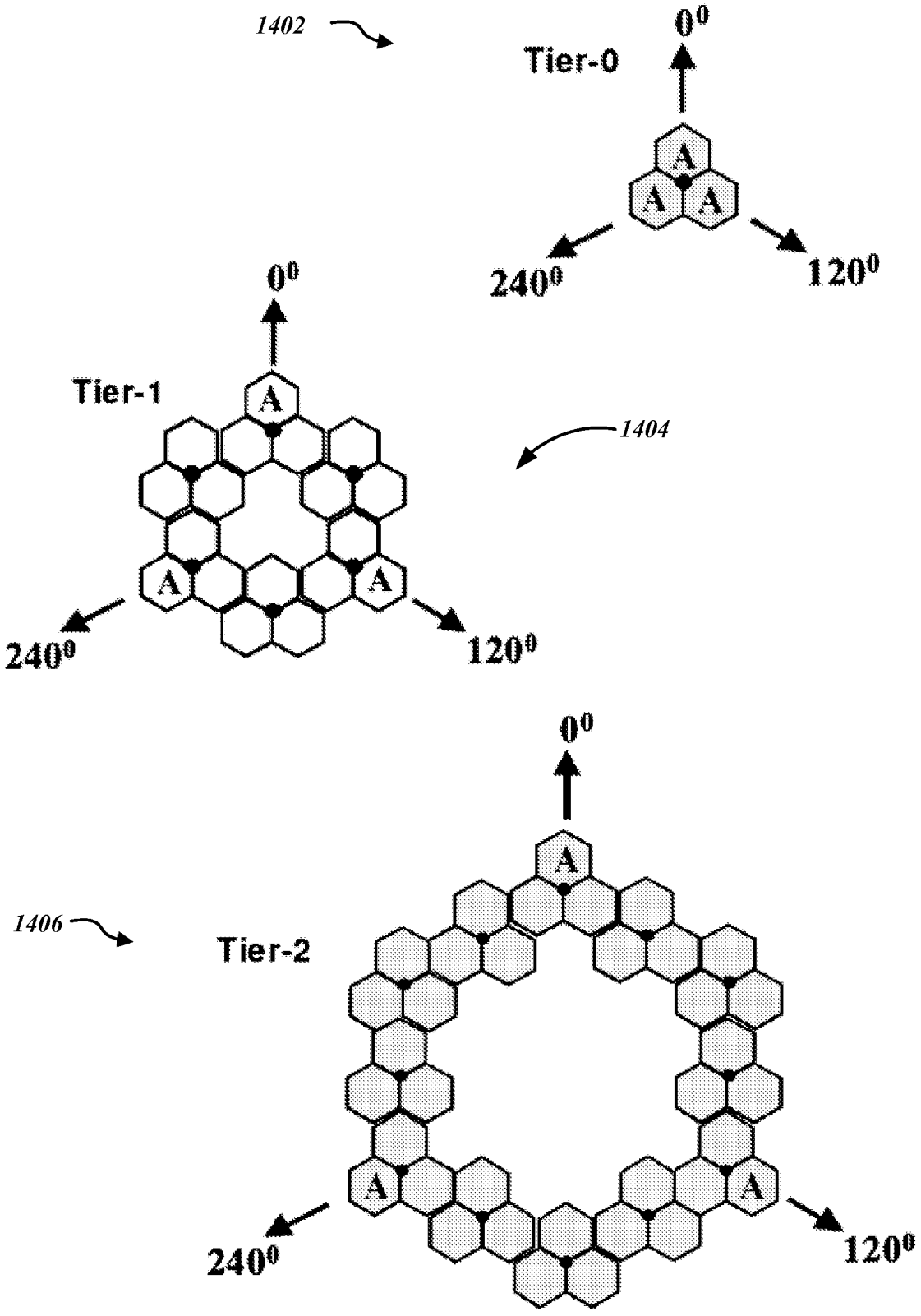
1402
Tier-0
0⁰
A
A A
240⁰
120⁰
Tier-1
0⁰
A
A A
240⁰
120⁰
1404
1406
Tier-2
0⁰
A
A A
240⁰
120⁰

FIG. 14A

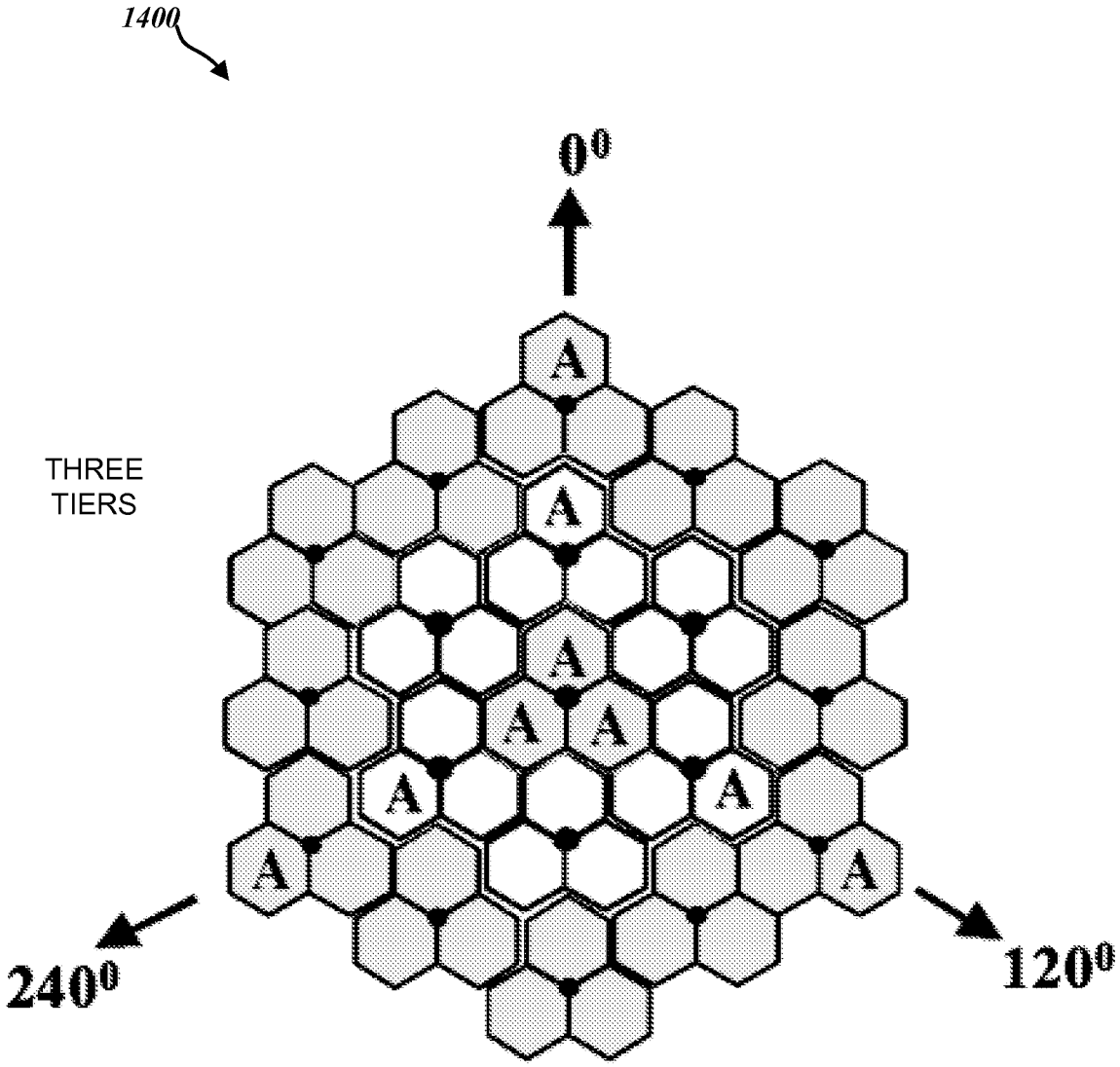

FIG. 14B

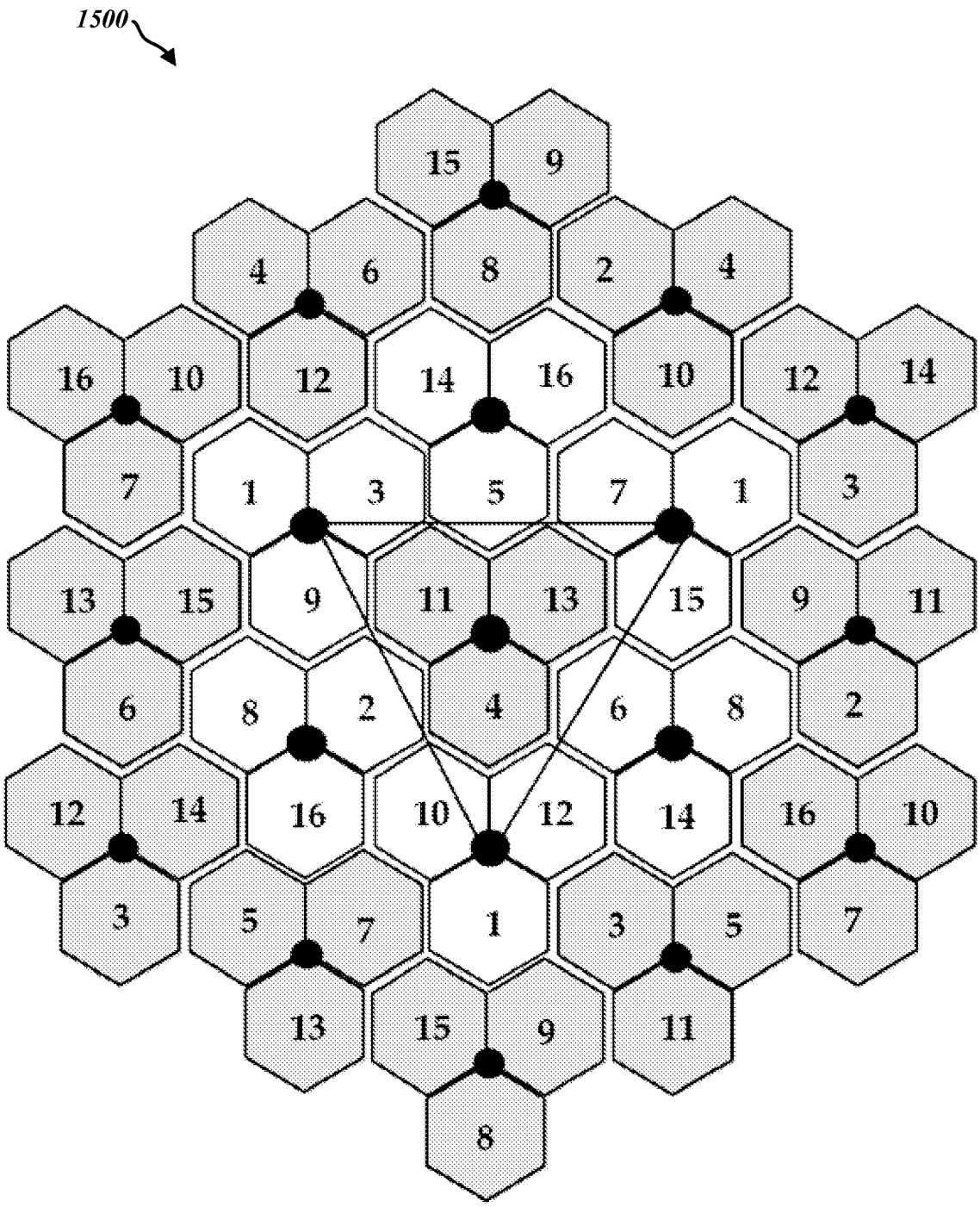
1500
15 9
4 6 8 2 4
16 10 12 14 16 10 12 14
7 1 3 5 7 1 3
13 15 9 11 13 15 9 11
6 8 2 4 6 8 2
12 14 16 10 12 14 16 10
3 5 7 1 3 5 7
13 15 9 11
8

FIG. 15

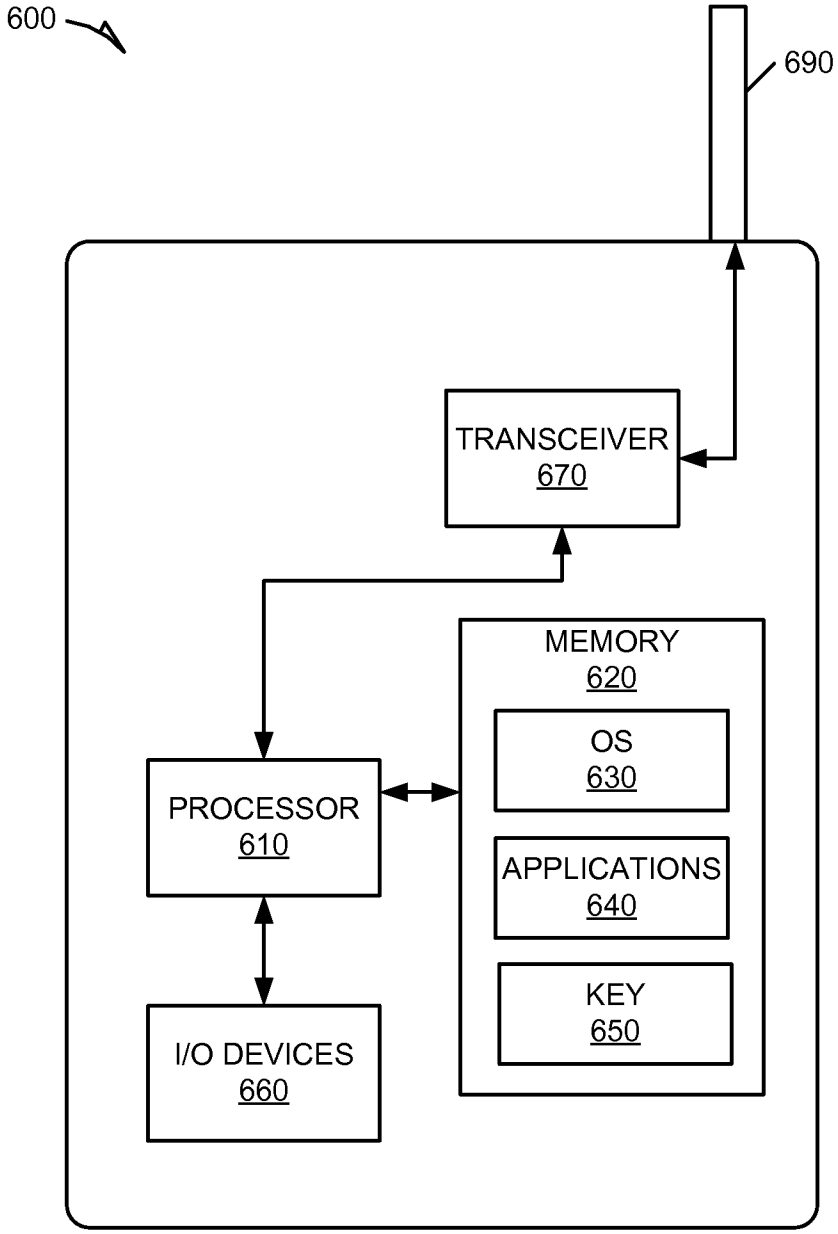
600
690
TRANSCEIVER
670
MEMORY
620
OS
630
PROCESSOR
610
APPLICATIONS
640
KEY
650
I/O DEVICES
660

FIG. 16

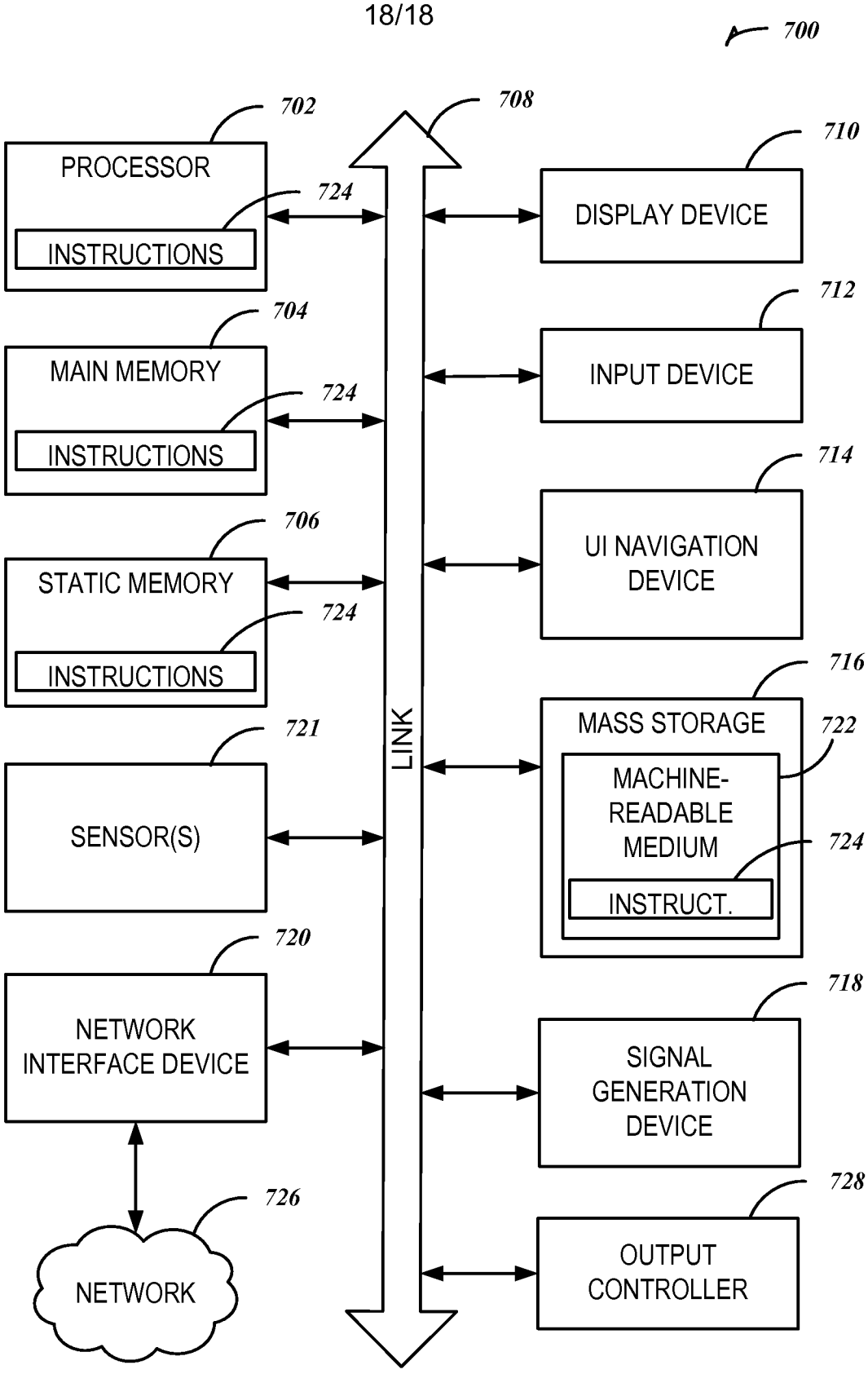
700
702
PROCESSOR
724
INSTRUCTIONS
704
MAIN MEMORY
724
INSTRUCTIONS
706
STATIC MEMORY
724
INSTRUCTIONS
721
SENSOR(S)
720
NETWORK INTERFACE DEVICE
726
NETWORK
708
LINK
710
DISPLAY DEVICE
712
INPUT DEVICE
714
UI NAVIGATION DEVICE
716
MASS STORAGE
722
MACHINE-READABLE MEDIUM
724
INSTRUCT.
718
SIGNAL GENERATION DEVICE
728
OUTPUT CONTROLLER

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/070109

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 9/32 (2015.01)
CPC - H04L 9/32 (2014.12)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC(8) - G01R 23/02; G06F 15/16, 19/00; H04L 9/32 (2015.01)
USPC - 324/76.11, 76.39; 702/64

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC - G01R 23/02; G06F 15/16, 19/00; H04L 9/32 (2014.12) (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Google, Orbit, Google Patents
Search terms used:phasor measurement unit, phasor data concentrator, power grid, wireless, radio

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/0220856 A1 (KRUYS et al) 02 September 2010 (02.09.2010) entire document	6, 9, 12
---		----
Y	US 2011/0138182 A1 (MURRAY et al) 09 June 2011 (09.06.2011) entire document	5,7,8,10-11,27-30
Y	US 2013/0193951 A1 (KOROVIN et al) 01 August 2013 (01.08.2013) entire document	5, 7, 8, 10, 11
Y	US 2013/0301688 A1 (KHANDANI) 14 November 2013 (14.11.2013) entire document	1-5, 27-30
Y	US 7,289,460 B1 (THACKER et al) 30 October 2007 (30.10.2007) entire document	1-5
Y	US 2005/0141562 A1 (CHEN et al) 30 June 2005 (30.06.2005) entire document	2
Y	US 2013/0166910 A1 (WILKINSON et al) 27 June 2013 (27.06.2013) entire document	3
Y	US 2006/0259255 A1 (ANDERSON et al) 16 November 2006 (16.11.2006) entire document	4, 5
Y	US 2011/0282508 A1 (GOUTARD et al) 17 November 2011 (17.11.2011) entire document	13-30
Y	US 2013/0207980 A1 (ANKISETTIPALLI et al) 15 August 2013 (15.09.2013) entire document	13-26
Y	US 2012/0020316 A1 (DONG et al) 26 January 2012 (26.01.2012) entire document	17-19, 24, 26-30
Y	US 2010/0253504 A1 (LLITERAS et al) 07 October 2010 (07.10.2010) entire document	18, 25, 30
A		1-30

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 April 2015	30 APR 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/070109

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See Extra Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/070109

Continuation of Box III:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claims 1-5, drawn to a secure communication system.
Group II, claims 6-12, drawn to a method and medium for monitoring the peer-to-peer network.
Group III, claims 13-30, drawn to a method, medium, and system comprising sorting the plurality of data parameters.

The inventions listed as Groups I, II and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: the special technical feature of the Group I invention: wherein the first radio and the second radio are spread spectrum radios configured to communicate over secure channels, the secure channels utilizing a passcode configured in the first radio and the second radio as claimed therein is not present in the invention of Groups II and III. The special technical feature of the Group II invention: monitoring the peer-to-peer network for communications that lack an identifier that is determined to correspond to at least one pair of the plurality of devices as claimed therein is not present in the invention of Groups I or III. The special technical feature of the Group III invention: sort the plurality of data parameters based on an individual parameter as claimed therein is not present in the invention of Groups I or II.

Groups I, II and III lack unity of invention because even though the inventions of these groups require the technical feature of a phasor measurement unit (PMU) coupled to a power grid, the PMU being configured to collect a plurality of data parameters from the power grid; a phasor data concentrator (PDC) configured to receive and analyze the plurality of data parameters, this technical feature is not a special technical feature as it does not make a contribution over the prior art.

Specifically, US 2006/0259255 A1 (ANDERSON et al) 16 November 2006 (16.11.2006) teaches a phasor measurement unit (PMU) coupled to a power grid (each of the phasor measurement units are associated with different power system grids, Para. 25), the PMU being configured to collect a plurality of data parameters from the power grid (phasors may be obtained using any phasor measurement unit (PMU), Para. 64); a phasor data concentrator (PDC) configured to receive and analyze the plurality of data parameters (the power system data concentrator 154 may be adapted to aggregate among other power system data, phasor data, and be therefore referred to as a phasor data concentrator (PDC), Para. 75).

Since none of the special technical features of the Group I, II or III inventions are found in more than one of the inventions, unity of invention is lacking.