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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 November 2015 (19.11.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/172657 A1

(51) International Patent Classification:
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/CN2015/077810

(22) International Filing Date:
29 April 2015 (29.04.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14278854 15 May 2014 (15.05.2014) US

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventors: **GOPALAKRISHNAN, Nandu**; 380 Main St #20, Chatham, NJ New Jersey 07928 (US). **SHEEN, Baoling**; 1767 Denison Rd, Naperville, IL Illinois 60565 (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).

Declarations under Rule 4.17:

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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

WO 2015/172657 A1

(54) Title: SYSTEM AND METHOD FOR ANOMALY DETECTION

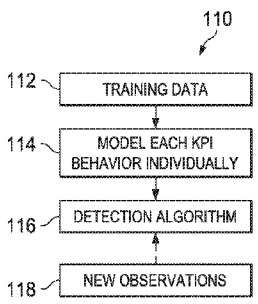


FIG. 2

(57) Abstract: In one embodiment, a method of detecting an anomaly includes receiving a data point and determining a metric in accordance with the data point and a center value. The method also includes determining whether the metric is below a lower threshold, between the lower threshold and an upper threshold, or above the upper threshold and determining that the data point is not the anomaly when the metric is below the lower threshold. Additionally, the method includes determining that the data point is the anomaly when the metric is above the upper threshold and determining that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

SYSTEM AND METHOD FOR ANOMALY DETECTION

TECHNICAL FIELD

[0001] The present invention claims priority to U.S. non-provisional patent application Serial No. 14/278,854, filed on May 15, 2014 and entitled " System and Method for Anomaly Detection," which is incorporated herein by reference as if reproduced in its entirety.

[0002] The present invention relates to a system and method for wireless communications, and, in particular, to a system and method for anomaly detection.

BACKGROUND

[0003] In network elements of a radio access network, such as base stations (or NodeBs or eNodeBs or cells) or radio network controllers (RNCs) of a cellular system, anomalies occur every now and then. Examples of anomalies include cell outage (e.g., sleeping cell), which may be indicated by key performance indicators (KPIs) with unusually poor (low or high) values. Anomalies may also occur in the form of unusual or broken relationships or correlations observed between sets of variables. It is desirable for anomalies to be rapidly detected while minimizing false alarms.

[0004] An anomaly has a root cause, such as malfunctioning user equipment (UE) or network element, interference, resource congestion from heavy traffic, in particular the bottleneck may be the downlink bandwidth, uplink received total wideband power, downlink bandwidth (codes or resource blocks), uplink bandwidth (resource blocks), backhaul bandwidth, channel elements (CE), control channel resources, etc. It is desirable to determine the root cause of an anomaly.

SUMMARY

[0005] An embodiment method of detecting an anomaly includes receiving a data point and determining a metric in accordance with the data point and a center value. The method also includes determining whether the metric is below a lower threshold, between the lower threshold and an upper threshold, or above the upper threshold and determining that the data point is not the anomaly when the metric is below the lower threshold. Additionally, the method includes determining that the data point is the anomaly when the metric is above the upper threshold and determining that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

[0006] An embodiment method of root cause analysis includes traversing a soft decision tree, where the soft decision tree includes a plurality of decision nodes and a plurality of root cause nodes. Traversing the soft decision tree includes determining a first plurality of probabilities that the plurality of decision nodes indicate an event which is an anomaly and determining a second plurality of probabilities of the plurality of root causes in accordance with the first plurality of probabilities.

[0007] An embodiment computer for detecting an anomaly includes a processor and a computer readable storage medium storing programming for execution by the processor. The programming includes instructions to receive a data point and determine a metric in accordance with the data point and a center value. The programming also includes instructions to determine whether the metric is less than a lower threshold, between the lower threshold and an upper threshold, or greater than the upper threshold and determine that the data point is not the anomaly when the metric is less than the lower threshold. Additionally, the programming includes instructions to determine that the data point is the anomaly when the metric is greater than the upper threshold and determine that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

[0008] An embodiment of an anomaly detecting system, comprising a receiving means configured to receive a data point; and a determining means configured to determine a metric in accordance with the data point and a center value; determine whether the metric is below a lower threshold, between the lower threshold and an upper threshold, or above the upper threshold; determine that the data point is not the anomaly when the metric is below the lower threshold; determine that the data point is the anomaly when the metric is above the upper threshold; and

determine that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

[0009] The foregoing has outlined rather broadly the features of an embodiment of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of embodiments of the invention will be described hereinafter, which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiments disclosed may be readily utilized as a basis for modifying or designing other structures or processes for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

[0011] Figure 1 illustrates an embodiment wireless network for communicating data;

[0012] Figure 2 illustrates a flowchart for an embodiment method of anomaly detection;

[0013] Figures 3A-B illustrate example probability density functions;

[0014] Figure 4 illustrates a probability density function with example data points;

[0015] Figure 5 illustrates a flowchart for another embodiment method of anomaly detection;

[0016] Figures 6A-B illustrate an example probability density function;

[0017] Figure 7 illustrates example data;

[0018] Figure 8 illustrates an example histogram with inner, middle, and outer bands;

[0019] Figure 9 illustrates example inner, middle, and outer bands;

[0020] Figure 10 illustrates a graph of example data samples over time;

[0021] Figure 11 illustrates a flowchart of an additional embodiment method of anomaly detection;

[0022] Figure 12 illustrates an example of a hard decision tree;

[0023] Figure 13 illustrates an example of a soft decision tree;

[0024] Figure 14 illustrates an example probability function;

[0025] Figure 15 illustrates a flowchart for an embodiment method of root cause analysis; and

[0026] Figure 16 illustrates a block diagram of an embodiment general-purpose computer system.

[0027] Corresponding numerals and symbols in the different figures generally refer to corresponding parts unless otherwise indicated. The figures are drawn to clearly illustrate the relevant aspects of the embodiments and are not necessarily drawn to scale.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0028] It should be understood at the outset that although an illustrative implementation of one or more embodiments are provided below, the disclosed systems and/or methods may be implemented using any number of techniques, whether currently known or in existence. The disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, including the exemplary designs and implementations illustrated and described herein, but may be modified within the scope of the appended claims along with their full scope of equivalents.

[0029] An embodiment method detects anomalies and the root causes of the anomalies. Examples of root causes of anomalies include malfunctioning user equipment (UE) or network elements, interference, resource congestion from heavy traffic. In particular, the bottleneck may be a downlink power, uplink received total wideband power, downlink bandwidth (codes or resource blocks), uplink bandwidth (resource blocks), backhaul bandwidth, channel elements, (CE), control channel resources, etc. It is desirable to detect and determine the root cause of an anomaly.

[0030] Some anomaly detection methods select thresholds on variables or distance metrics yielding a decision boundary based on the structure of training data to determine that outliers are represent anomalies. However, selection of the threshold often trades off false alarms with missed anomalies and detection time. An embodiment method uses two thresholds levels to detect anomalies. When the data point is below the lower threshold, it is determined to not indicate an anomaly. When the data point is above the higher threshold, it is determined to indicate an anomaly. When the data point is between the thresholds, the history is used to determine whether the data point indicates an anomaly.

[0031] The root cause of a detected anomaly is determined in an embodiment method. A hard decision tree may be used. The decision tree may be created by an expert or learned from the data. However, hard detection trees may lead to an unknown diagnosis of the root cause or to a misdiagnosis. An embodiment method uses a soft decision tree to one or more likely root causes of an anomaly by mapping metric into a probability via the logistic function. Then, the probabilities are multiplied together invoking the naive Bayes assumption of independent attributes. As a result, the most likely root cause or top few likely root causes are determined, along with a probability or confidence measure for each cause.

[0032] Figure 1 illustrates wireless network 100 for wireless communications. Network 100 includes radio network controllers (RNCs) 108 which communicate with each other. RNCs 108 are coupled to communications controllers 102. A plurality of user equipments (UEs) 104 are coupled to communications controllers 102. Communications controllers 102 may be any components capable of providing wireless access by, inter alia, establishing uplink and/or downlink connections with UEs 104, such as base stations, an enhanced base stations (eNBs), access points, picocells, femtocells, and other wirelessly enabled devices. UEs 104 may be any component capable of establishing a wireless connection with communications controllers 102, such as cell phones, smart phones, tablets, sensors, etc. In some embodiments, the network 100 may include various other wireless devices, such as relays, femtocells, etc. Embodiments may detect anomalies on a network, such as network 100. Also, the network may determine the root cause of a detected anomaly.

[0033] Figure 2 illustrates flowchart 110 for a method of detecting anomalies. Training data is stored in block 112. The training data is historical data. In block 114 individual features are modeled. For example, a key performance index (KPI) is examined for each feature.

[0034] Probability density functions may be used to determine whether a data point is likely to be an anomaly. Data points close to the center are likely to not indicate anomalies, while data points in the tails are likely to indicate anomalies. The center may be the mean, median, or another value indicating the center of the expected values. Figures 3A-B illustrate probability density functions 120 and 130, respectively. Probability density function 120 has a narrow peak and a low variance, while probability density function 130 has a wider peak and a larger variance. The mean of a probability density function is given by:

$$\mu_j = \frac{1}{m}\sum_{i=1}^{m} x_j^{(i)},$$

and the variance is given by:

$$\sigma_j^2 = \frac{1}{m}\sum_{i=1}^{m}\left(x_j^{(i)} - \mu_j\right)^2.$$

[0035] In block 116, a detection algorithm detects anomalies based on new observations 118 using the modeled data. Figure 4 illustrates probability density function 142 with data points 144 in the normal range of probability density function 142, and data points 146 in the tail of probability density function 142, which are likely anomalies. The probability to determine that new observations are not anomalies is given by:

$$p(x) = \prod_{j=1}^{n} p\left(x_j; \mu_j, \sigma_j^2\right) = \prod_{j=1}^{n} \frac{1}{\sqrt{2\pi}\sigma_j} e^{\frac{-(x_j-\mu_j)^2}{2\sigma_j^2}}.$$

Abnormal validation data points determine the probability of the data being normal. A new input x_i, is predicted to be anomalous if:

$$p(x_i) < \varepsilon,$$

where ε is a threshold learned, for example, from historical data.

[0036] Figure 5 illustrates flowchart 160 for a method of detecting anomalies with multiple variables. Multiple KPI behaviors at the same time are modeled in block 164 using training data from block 162. Figures 6A-B illustrates graphs 170 and 180 of a two dimensional probability density function. The variables x_1 and x_2 are independent variables. The relationships among KPIs are learned. The mean is given by:

$$\mu = \frac{1}{m}\sum_{i=1}^{m} x^{(i)}.$$

Also, the variance is given by:

$$\Sigma = \frac{1}{m}\sum_{i=1}^{m}\left(x^{(i)} - \mu\right)\left(x^{(i)} - \mu\right)^T.$$

[0037] A detection algorithm in block 166 detects anomalies from new observations from block 168 using modeled data. Figure 7 illustrates a graph of existing data points 192 and new data points x_A, x_B, x_C, and x_D. These new data points are on the outskirts of the training data and are likely anomalies, especially x_1. In this example, one variable is central processing unit (CPU) load and the other variable is memory use. The Mahalanobis distance and probability are calculated. The probability to determine that the new observation is not an anomaly is given by:

$$p(x;\mu,\Sigma) = \frac{1}{(2\pi)^{n/2}|\Sigma|^{1/2}} e^{\left(-\frac{1}{2}(x-\mu)^T\Sigma^{-1}(x-\mu)\right)}.$$

The covariance matrix and the shape of the angle are used. Abnormal validation datasets are used to determine ε, the threshold. A new input x_i is predicted to be anomalous when:

$$p(x_i) < \varepsilon.$$

[0038] An embodiment uses an inner band, a middle band, and an outer band of a probability density function to detect an anomaly. Figure 8 illustrates graph 200 with inner band 206, middle band 208, and outer band 210 for probability density histogram 202, a one dimensional probability density. Curve 204 illustrates an example of a single threshold which may be used to detect anomalies. Data points corresponding to a frequency above the threshold are determined to not be anomalies, and values below the threshold are determined to be anomalies. Data points in the inner band are determined to not be anomalies, while data points in the outer band are

determined to be anomalies. Data points in the middle band may or may not be determined to be anomalies. There is a lower threshold between the inner and middle bands and an upper threshold between the middle and outer bands.

[0039] Figure 9 illustrates graph 220 with inner band 226, middle or donut band 224, and outer band 222 for a bivariate two dimensional metric space Gaussian example. Three dimensional or *n* dimensional examples may be used. As in the one dimensional case, there is a lower threshold between the inner band and the middle band, and an upper threshold between the middle band and the outer band. The inner threshold and the outer threshold are points of equal distance elliptical contours. The Mahalanobis distance may be used as a metric for the multi-dimensional case. Prior weighted average Mahalanobis distances may be used when the data is structured as a mixture of Gaussian clusters. The parameters of each cluster mode are learned.

[0040] The lower and upper thresholds are derived from historical or training data for the KPI sets. Highly fluctuating KPIs, for example high variance or heavy tail KPIs, such as packet switching (PS) throughput, have a wider distance between the lower and upper threshold. The lower and upper thresholds are closer together for more stable KPIs, such as security mode command failures. In one example, a user selects the sensitivity. When the user increases the sensitivity, more anomalies will be detected at the expense of more false positives. With a higher sensitivity, the donut region shrinks. A user may also select a sacrosanct KPI expectation. When a KPI passes above this absolute threshold, regardless of the degree of deviation from normal, an alarm is raised. Thus, the user selects the upper threshold.

[0041] When a metric, for example the Mahalanobis distance of a vector of metrics passes beyond the upper threshold to the outer band, an alarm is raised. When the metric passes within the lower threshold to the inner band no alarm is raised, and the alarm is turned off if it were previously on. Also, the delay window timer is reset. When the observed metric enters the middle band or donut region between the lower and upper thresholds, the delay window timer is set. If the observed metric is still in the middle band when the delay window timer expires, an alarm is raised. In one example, the delay window is a fixed value. Alternatively, the delay window depends on the trend of the observed metric. If the value continues to get worse, the alarm is raised earlier.

[0042] Figure 10 illustrates graph 230 of metric 232 over time. Initially, metric 232 is in the inner band, and there is a low probability of an anomaly. Metric 232 enters the donut region, and

delay window timer 234 is set. The metric does not reach the upper threshold. However, because the metric is still in the donut band when the delay window timer expires, an alarm is raised. If the metric returned to the inner band before the delay window timer expires, no alarm is raised, and the delay window timer is reset. If the metric again enters the donut band from the inner band, the delay window timer is set again. Operation is similar for two or more variables.

[0043] To minimize false alarms and missed detection of anomalies, a wider range between the lower and upper threshold, yielding a larger middle band, may be used. The observations are more likely to stay between these bounds, serving as safety guards. The alarm may be triggered based on the consistency and trend over the delay window. This takes more time, but produces fewer false alarms. Alarms may be more obvious, for example, at the cell level than the RNC level. At the RNC level the aggregate of cells is more stable.

[0044] Figure 11 illustrates flowchart 240 for a method of detecting anomalies. Initially, in step 242, upper threshold and lower threshold are determined. This is done based on historical or training data. Values which are well within the normal region are below the lower threshold, values which are well outside the normal region are outside the upper threshold, and intermediate values are between the lower threshold and the upper threshold. In one example, a user hard sets the upper threshold. The span between the lower threshold and the upper threshold are set to trade off the sensitivity and false alarm rate with detection time. A larger distance between the lower threshold and upper threshold increases the sensitivity and decreases the false alarm rate at the expense of detection time. The size of the delay window may also be set in step 242. In one example, these values are initially set before receiving data. In another example, these values are periodically updated based on performance.

[0045] Next, in step 244, a data point is received. The data point may be a value in a cellular system, or another system.

[0046] Then, in step 246, the system determines whether the data point is in the inner band, the middle band or the outer band. When the data point is in the outer band, the system proceeds to step 246 and an alarm is raised. The alarm may trigger root cause analysis. The system may also return to step 244 to receive the next data point.

[0047] When the data point is in the inner band, the system proceeds to step 250. No alarm is raised, and the alarm is reset if it were previously raised. Also, the delay window timer is reset if it were previously set. The system then proceeds to step 244 to receive the next data point.

[0048] When the data point is in the middle band, the system proceeds to step 254. In step 254, the system determines whether the delay window timer has previously been set. When the delay window timer has not previously been set, the system is just entering the middle band, and proceeds to step 256.

[0049] In step 256, the system sets the delay window timer. Then, it proceeds to step 244 to receive the next data point.

[0050] When the delay window timer has been previously set, the system proceeds to step 258, where it determines whether the delay window timer has expired. When the delay window timer has not expired, the system proceeds to step 244 to receive the next data point. When the delay window timer has expired, the system proceeds to step 246 to raise an alarm. The system may also consider other factors in deciding to set the alarm, such as the trend. When the data point is trending closer to the upper threshold, an alarm may be raised earlier.

[0051] After an anomaly is detected, it is desirable to determine the root cause of the anomaly. Figure 12 illustrates decision tree 290 for determining a root cause of an anomaly. Some examples of root causes are that the UE is in a coverage hole, there is a big truck blocking coverage of a UE, or that there is a software bug in a UE operating system or in the cellular network. The decision tree is generated from engineering experience or mined from labeled historic data, and may be modified when new causes of anomalies are detected. Decision tree 290 is a hard decision tree, where a path is chosen at each node. Also, decision tree 290 is hierarchical, with drilling down to lower levels performed by special metric sets and/or network nodes. There are three decision levels of decision tree 290: first RNC level 400, the root level, second RNC level 402, and cell level 404. Causes level 406 contains the leaves. A tree node for event E_{ij} acts on a set of test metrics S_{ij} by computing a learned non-linear function, such as a Mahalanobis distance. The tree node compares the output of the function against a threshold to determine a yes or no hard decision.

[0052] Initially, in node 292, the system determines whether anomaly event E_1 occurred. General metric set S_1 is determined, and is compared to a threshold. For example, when the metric is greater than the threshold, anomaly event E_1 occurred, and the system proceeds to node 296, and when the metric is less than or equal to the threshold τ_1, anomaly event E_1 did not occur, and the system proceeds to node 294.

[0053] In node 296, the system determines whether anomaly event E_{22} occurred. Specific metric S_{22} is determined. Then, specific metric S_{22} is compared to a threshold τ_{22}. When the metric is less than the threshold, anomaly event E22 did not occur, and the system proceeds to node 302, where it determines that the anomaly is an unknown problem. This may happen, for example, the first time this anomaly occurs. When the metric is greater than the threshold, anomaly event E_{22} occurred, and the system proceeds to node 304.

[0054] In node 304, the system determines whether anomaly event E_{33} occurred. Metric S_{33} is determined, and compared to a threshold τ_{33}. When the metric is less than the threshold, anomaly event E_{33} has not occurred, and the system looks for other anomaly events to determine the root cause in node 314. On the other hand, when the metric is greater than the threshold, it is determined that anomaly event E_{33} has occurred. Then, in node 316, the root cause is determined to be RNC and cell problem type Z.

[0055] In node 294, the system determines whether anomaly event E_{21} occurred. Metric S_{21} is determined, and compared to a threshold τ_{21}. When metric S_{21} is less than the threshold, it is determined that anomaly event E_{21} did not occur, and the system proceeds to node 298. On the other hand, when metric S_{21} is greater than or equal to the threshold, the system proceeds to node 300, determining that anomaly event E_{21} did occur.

[0056] In node 298, the system determines whether anomaly event E_{31} occurred. Metric S_{31} is determined, and compared to a threshold τ_{31}. When metric S_{31} is less than the threshold, it is determined that anomaly event E_{31} did not occur, and the anomaly is not a problem of type X in node 306. When metric S_{31} is greater than or equal to the threshold, it is determined that the problem is a cell only problem of type X in node 308.

[0057] In node 300, the system determines whether anomaly event E_{32} occurred. Metric S_{32} is determined, and compared to a threshold τ_{32}. When metric S_{32} is less than the threshold, it is determined that anomaly event E_{32} did not occur, and, in node 310, it is determined to look at other anomaly events for the root cause. When metric S_{32} is greater than or equal to the threshold, it is determined that the problem is an RNC and cell problem of type Y in node 312.

[0058] Decision tree 290 is a binary tree, but a non-binary tree may be used. For example, there may be joint analysis of two events A and B with four mutually exclusive leaves: A and B, A and not B, not A and B, and not A and not B. If A and B arise from different components, then the

respective probabilities are multiplied. Likewise, there may be eight leaves for 3 potential events, and so on.

[0059] Figure 13 illustrates soft decision tree 320, which is used to determine the cause of an anomaly. Using a soft decision tree, the probability that a particular problem caused the anomaly may be determined. One or more likely root cause(s) may be determined. The probability that a given node is yes, P_{ij}, is the logistic function operating on the learned function value threshold difference for the output probability of anomaly event E_{ij}. The probability is determined form the distance from the mean. The probability is given by:

$$P_{ij} = \frac{1}{1+e^{-(f(\mathbf{x_{ij}})-\tau_{ij})}},$$

where $f(\mathbf{x}_{ij})$ is the learned function, for example the mahalanobus distance, its argument $\mathbf{x}$ is the test vector, and τ_{ij} is the threshold. Figure 14 illustrates graph 360, an example logistic function. The probability of a no is $1\text{-}P_{ij}$. This is because of the mutual exclusivity of events and their complements at the nodes in the tree, which implies that a set of leaves or root causes are mutually exclusive.

[0060] Given nodes ij and kl, corresponding to events E_{ij} and E_{kl}, respectively, the edge weight between the nodes, if it exists on the decision tree, is denoted by (ij, kl). The probabilities are converted to a distance via a transform, so that the edge weight is given by:

$$D_{ij,kl} = \ln(P_{ij})$$

when (ij, kl) exists on a yes branch, and by:

$$D_{ij,kl} = \ln(1 - P_{ij})$$

when (ij, kl) exists on a no branch. The edge weight is ∞ otherwise. $D_{ij,kl}$ decreases as P_{ij} increases for a yes edge and as $(1\text{-}P_{ij})$ increases for a no edge. To find the final likelihood of a root cause in a node, $D_{ij,kl}$ is summed along the path to that leaf from the root. The shortest distance path from the root node to one of the leaf nodes is the most likely root cause. Several likely root causes may be considered, along with their likelihood. For example, all root causes with a distance below a threshold may be considered. Alternatively, the two, three, or more of the smallest edge distances are considered. The most likely path or set of events is the argument of the minimum (arg min) path from the root to the leaves, that is:

$$\Sigma_{(ij,kl)\in path} D_{ij,kl}.$$

In the naïve Bayes assumption, the additive distances along edges of a candidate path leads to multiplicative probabilities for independent events E_{ij} along the path.

[0061] Soft decision tree 320 has root level of first RNC level 346, two intermediate levels, second RNC level 348 and cell level 350, and a root cause level, leaves 352. Initially, in node 322, the system determines the probability P_{11} that anomaly event E_{11} occurred. This probability is given by:

$$P_{11} = \frac{1}{1+e^{-(f(\mathbf{x_{11}})-\tau_{11})}},$$

where $f(\mathbf{x_{11}})$ is the learned for the measurement for anomaly event E_{11}, and τ_{11} is the threshold for event E_{11}. The probability that anomaly event E_{11} did not occur is given by $(1-P_{11})$.

[0062] Then, the probabilities are determined for second RNC level 348. The probability P_{21} that anomaly event E_{21} occurred is determined in node 324. This probability is given by:

$$P_{21} = \frac{1}{1+e^{-(f(\mathbf{x_{21}})-\tau_{21})}},$$

where $f(\mathbf{x_{21}})$ is the learned for the measurement for anomaly event E_{21}, and τ_{21} is the threshold for event E_{21}. The probability that anomaly event E_{21} did not occur is given by $(1-P_{21})$. Similarly, in node 326, the probability P_{22} that anomaly event E_{22} occurred is determined by:

$$P_{22} = \frac{1}{1+e^{-(f(\mathbf{x_{22}})-\tau_{22})}},$$

where $f(\mathbf{x_{22}})$ is the learned for the measurement for anomaly event E_{22}, and τ_{22} is the threshold for event E_{22}. The probability that anomaly event E_{22} did not occur is given by $(1-P_{22})$.

[0063] Likewise, the probabilities for the cell level anomalies are determined. The probability P_{31} that anomaly event E_{31} occurred is determined in node 328. This probability is given by:

$$P_{31} = \frac{1}{1+e^{-(f(\mathbf{x_{31}})-\tau_{31})}},$$

where $f(\mathbf{x_{31}})$ is the learned for the measurement for anomaly event E_{31}, and τ_{31} is the threshold for event E_{31}. The probability that anomaly event E_{31} did not occur is given by $(1-P_{31})$. Additionally, in node 330, the probability P_{32} that anomaly event E_{32} occurred is determined by:

$$P_{32} = \frac{1}{1+e^{-(f(\mathbf{x_{32}})-\tau_{32})}},$$

where $f(\mathbf{x}_{32})$ is the learned for the measurement for anomaly event E_{32}, and τ_{32} is the threshold for event E_{32}. The probability that anomaly event E_{32} did not occur is given by $(1-P_{32})$. Also, in node 334, the probability P_{33} that anomaly event E_{33} occurred is determined by:

$$P_{33} = \frac{1}{1+e^{-(f(\mathbf{x}_{33})-\tau_{33})}},$$

where $f(\mathbf{x}_{33})$ is the learned for the measurement for anomaly event E_{33}, and τ_{33} is the threshold for event E_{33}. The probability that anomaly event E_{33} did not occur is given by $(1-P_{33})$.

[0064] When the probabilities are calculated, the edge weight distance is determined for the leaves. For example, the edge weight distance for node 336, not a problem of type X, is given by:

$$-\ln(1-P_{11}) - \ln(1-P_{21}) - \ln(1-P_{31}).$$

Also, the edge weight distance for node 338, a cell only problem of type X, is given by:

$$-\ln(1-P_{11}) - \ln(1-P_{21}) - \ln(P_{31}).$$

Similarly, the edge weight distance for node 340, look at other anomaly events for the root cause, is given by:

$$-\ln(1-P_{11}) - \ln(P_{21}) - \ln(1-P_{32}).$$

Additionally, the edge weight distance for node 342, an RNC and cell problem of type Y, is given by:

$$-\ln(1-P_{11}) - \ln(P_{21}) - \ln(P_{32}).$$

The edge weight distance for node 332, an unknown problem, is given by:

$$-\ln(P_{11}) - \ln(1-P_{22}).$$

Also, the edge weight distance for node 344, look for other anomaly events for the root cause, is given by:

$$-\ln(P_{11}) - \ln(P_{22}) - \ln(1-P_{33}).$$

The edge weight distance for node 344, an RNC and cell problem of type Z, is given by:

$$-\ln(P_{11}) - \ln(P_{22}) - \ln(P_{33}).$$

[0065] Correlated events along a path may clarify path discovery by strengthening correlated events and suppressing anti-correlated events when conditional probabilities are used. This is tantamount to joint analysis. As an edge strengthens, and the probability approaches one, its

complementary edge weakens, with a probability approaches zero. The multiplication of path edge probabilities causes paths with weak edges to disappear quickly. Spurious path outcomes are still possible with noisy signals. To prevent this, leaves may be removed upfront that are uninteresting for anomaly detection. A few shortest paths, or all the paths that are short enough may be retained for reporting and analysis. Several root causes may be likely from an ambiguous ancestor in the tree.

[0066] Figure 15 illustrates flowchart 370 for a method of determining the root cause of an anomaly. Initially, in step 372, a soft decision tree is created. In one example, the soft decision is created based on engineering experience and previous anomalies. The soft decision tree may be modified as new root causes of anomalies are observed. This may be done automatically or based on user input.

[0067] Next, in step 374, an anomaly is detected. For example, anomalies may be detected using a lower threshold and an upper threshold. An anomaly is detected when a metric is above the upper threshold. Also, an anomaly is detected when the metric stays between the lower threshold and the upper threshold for a delay length of time.

[0068] Then, in step 376, the probability that an anomaly has occurred. Initially, the probability that the root anomaly occurred is determined. The probability that anomaly E_{ij} occurred is given by:

$$P_{ij} = \frac{1}{1+e^{-(f(x_{ij})-\tau_{ij})}}.$$

[0069] Next, in step 378, the system proceeds to the next level. The nodes at the next level are examined.

[0070] In step 380, the system determines whether the first node is a leaf. When the first node is not a leaf, the system proceeds to step 382, and when the first node is not a leaf, the system proceeds to step 386. Also, when the first node is not a leaf, the system proceeds to step 376 to determine the probabilities for the first node.

[0071] In step 386, the system determines whether the second node is a leaf. When the second node is a leaf, the system proceeds to step 376 to determine the probabilities for the second node. When the second node is a leaf, the edge distances of root causes are determined in step 384.

[0072] In step 382, the system determines whether the second node is a leaf. When the second node is not a leaf, the system proceeds to step 376 to determine the probability for the second node. When the second branch is a leaf, the system determines the edge distances for the leaf in step 384. The edge distances for the root causes are calculated in step 384. The edge distance for a node representing a root cause is given by the sum of the logs of the probabilities along that path. The edge distances of all the paths are calculated. The root cause with the shortest edge distance, or several root causes, may be selected for further examination.

[0073] Figure 16 illustrates a block diagram of processing system 270 that may be used for implementing the devices and methods disclosed herein. Specific devices may utilize all of the components shown, or only a subset of the components, and levels of integration may vary from device to device. Furthermore, a device may contain multiple instances of a component, such as multiple processing units, processors, memories, transmitters, receivers, etc. The processing system may comprise a processing unit equipped with one or more input devices, such as a microphone, mouse, touchscreen, keypad, keyboard, and the like. Also, processing system 270 may be equipped with one or more output devices, such as a speaker, a printer, a display, and the like. The processing unit may include central processing unit (CPU) 274, memory 276, mass storage device 278, video adapter 280, and I/O interface 288 connected to a bus.

[0074] The bus may be one or more of any type of several bus architectures including a memory bus or memory controller, a peripheral bus, video bus, or the like. CPU 274 may comprise any type of electronic data processor. Memory 276 may comprise any type of system memory such as static random access memory (SRAM), dynamic random access memory (DRAM), synchronous DRAM (SDRAM), read-only memory (ROM), a combination thereof, or the like. In an embodiment, the memory may include ROM for use at boot-up, and DRAM for program and data storage for use while executing programs.

[0075] Mass storage device 278 may comprise any type of storage device configured to store data, programs, and other information and to make the data, programs, and other information accessible via the bus. Mass storage device 278 may comprise, for example, one or more of a solid state drive, hard disk drive, a magnetic disk drive, an optical disk drive, or the like.

[0076] Video adaptor 280 and I/O interface 288 provide interfaces to couple external input and output devices to the processing unit. As illustrated, examples of input and output devices include the display coupled to the video adapter and the mouse/keyboard/printer coupled to the

I/O interface. Other devices may be coupled to the processing unit, and additional or fewer interface cards may be utilized. For example, a serial interface card (not pictured) may be used to provide a serial interface for a printer.

[0077] The processing unit also includes one or more network interface 284, which may comprise wired links, such as an Ethernet cable or the like, and/or wireless links to access nodes or different networks. Network interface 284 allows the processing unit to communicate with remote units via the networks. For example, the network interface may provide wireless communication via one or more transmitters/transmit antennas and one or more receivers/receive antennas. In an embodiment, the processing unit is coupled to a local-area network or a wide-area network for data processing and communications with remote devices, such as other processing units, the Internet, remote storage facilities, or the like.

[0078] While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods might be embodied in many other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted, or not implemented.

[0079] In addition, techniques, systems, subsystems, and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as coupled or directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

WHAT IS CLAIMED IS:

1. A method of detecting an anomaly, the method comprising:

receiving a data point;

determining a metric in accordance with the data point and a center value;

determining whether the metric is below a lower threshold, between the lower threshold and an upper threshold, or above the upper threshold;

determining that the data point is not the anomaly when the metric is below the lower threshold;

determining that the data point is the anomaly when the metric is above the upper threshold; and

determining that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

2. The method of claim 1, wherein determining that the data point might be the anomaly comprises:

determining a first length of time that a plurality of data points comprising the data point have been between the lower threshold and the upper threshold;

comparing the first length of time to a second length of time of a delay window; and

determining that the data point is the anomaly when the first length of time is greater than or equal to the second length of time of the delay window.

3. The method of claim 2, wherein determining that the data point might be the anomaly further comprises:

determining whether a delay window timer has been set; and

setting the delay window timer when the delay window timer has not been set.

4. The method of claim 2, further comprising releasing a delay window timer when the metric is less than the lower threshold.

5. The method of claim 1, wherein determining the metric comprises determining a Mahalanobis distance between the data point and the center value.

6. The method of claim 1, further comprising:

determining the lower threshold; and

determining the upper threshold.

7. The method of claim 6, further comprising receiving a sensitivity level, wherein determining the lower threshold comprises determining the lower threshold in accordance with the sensitivity level, and wherein determining the upper threshold comprises determining the upper threshold in accordance with the sensitivity level.

8. The method of claim 6, wherein determining the upper threshold comprises:

receiving a user input; and

setting the upper threshold to the user input.

9. The method of claim 1, further comprising determining a probabilistic root cause of the anomaly when the data point is determined to be the anomaly.

10. The method of claim 9, wherein determining the root cause of the anomaly comprises traversing a soft decision tree.

11. A method of root cause analysis, the method comprising traversing a soft decision tree, wherein the soft decision tree comprises a plurality of decision nodes and a plurality of root cause nodes, wherein traversing the soft decision tree comprises:

determining a first plurality of probabilities that the plurality of decision nodes indicate an event which is an anomaly; and

determining a second plurality of probabilities of the plurality of root causes in accordance with the first plurality of probabilities.

12. The method of claim 11, wherein determining a first probability of the first plurality of probabilities comprises calculating the first probability to be

$$\frac{1}{1-e^{-(f-\tau)}},$$

wherein f is a Mahalonobis distance between a test vector and a center value, and wherein τ is a threshold.

13. The method of claim 11, wherein determining the second plurality of probabilities comprises determining a plurality of edge weights in accordance with first plurality of probabilities.

14. The method of claim 13, wherein determining the plurality of edge weights comprises calculating negatives of the natural logarithm of the first plurality of probabilities and negatives of the natural logarithm of one minus the first plurality of probabilities.

15. The method of claim 13, wherein determining the plurality of edge weight distances comprises determining a plurality of path distances in accordance with the plurality of edge weights.

16. The method of claim 15, further comprising:

determining the minimum of the plurality of path distances to produce a most likely root cause; and

transmitting the most likely root cause.

17. The method of claim 15, further comprising:

determining which of the plurality of path distances are below a path threshold to produce a group of likely causes; and

transmitting the group of likely causes.

18. The method of claim 11, further comprising constructing the soft decision tree.

19. The method of claim 18, wherein constructing the soft decision tree comprises constructing the soft decision tree in accordance with user input.

20. The method of claim 18, wherein constructing the soft decision tree comprises performing a machine learning algorithm on a plurality of labels.

21. The method of claim 11, further comprising detecting an initial anomaly.

22. The method of claim 11, wherein determining the second plurality of probabilities of the plurality of root causes comprises determining a probability of a first root cause comprises multiplying a subset of the first plurality of probabilities to determine the probability of the first root cause, wherein the plurality of root causes comprises the first root cause, wherein the subset of the first plurality of probabilities are on a path along the soft decision tree from a root level of the soft decision tree to the first root cause.

23. A computer for detecting an anomaly comprising:

a processor; and

a computer readable storage medium storing programming for execution by the processor,

the programming including instructions to

receive a data point,

determine a metric in accordance with the data point and a center value,

determine whether the metric is less than a lower threshold, between the lower threshold and an upper threshold, or greater than the upper threshold,

determine that the data point is not the anomaly when the metric is less than the lower threshold,

determine that the data point is the anomaly when the metric is greater than the upper threshold, and

determine that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

24. An anomaly detecting system, comprising:

a receiving means configured to receive a data point; and

a determining means configured to:

determine a metric in accordance with the data point and a center value;

determine whether the metric is below a lower threshold, between the lower threshold and an upper threshold, or above the upper threshold;

determine that the data point is not the anomaly when the metric is below the lower threshold;

determine that the data point is the anomaly when the metric is above the upper threshold; and

determine that the data point might be the anomaly when the metric is between the lower threshold and the upper threshold.

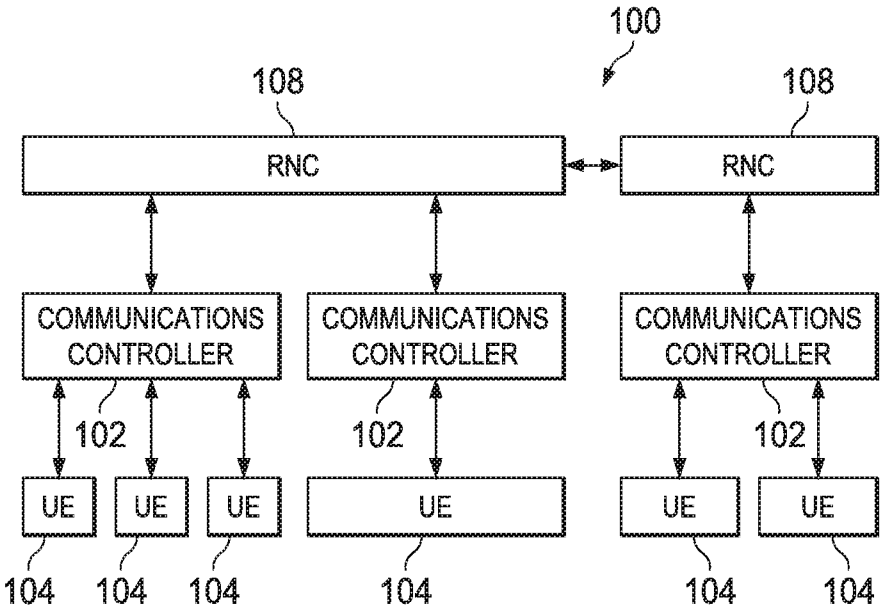

100
108
108
RNC
RNC
COMMUNICATIONS CONTROLLER
COMMUNICATIONS CONTROLLER
COMMUNICATIONS CONTROLLER
102
102
102
UE
UE
UE
UE
UE
UE
104
104
104
104
104
104

FIG. 1

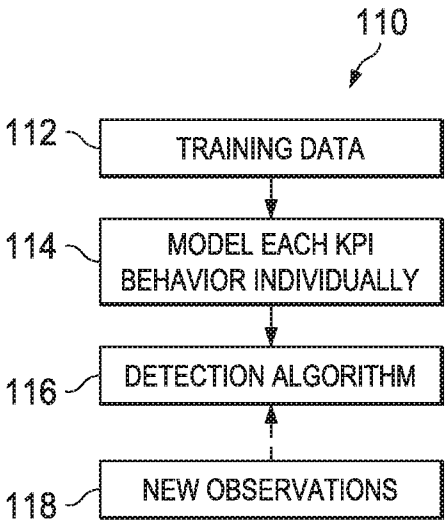

110
112
TRAINING DATA
114
MODEL EACH KPI BEHAVIOR INDIVIDUALLY
116
DETECTION ALGORITHM
118
NEW OBSERVATIONS

FIG. 2

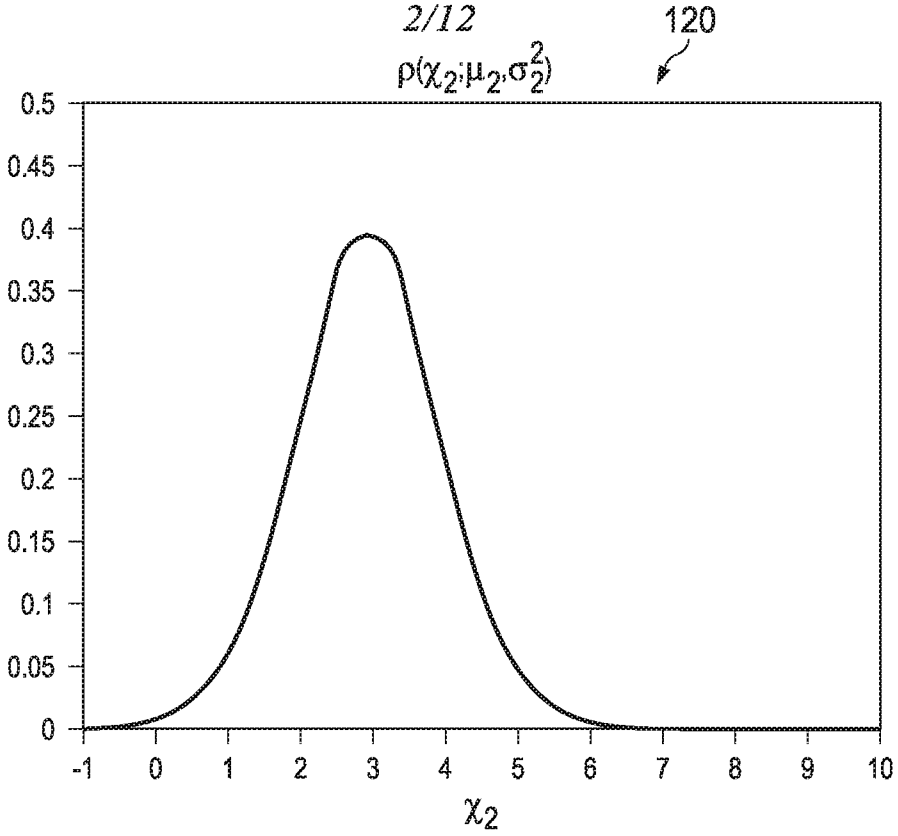

120
$\rho(\chi_2;\mu_2,\sigma_2^2)$
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
-1 0 1 2 3 4 5 6 7 8 9 10
χ_2

FIG. 3A

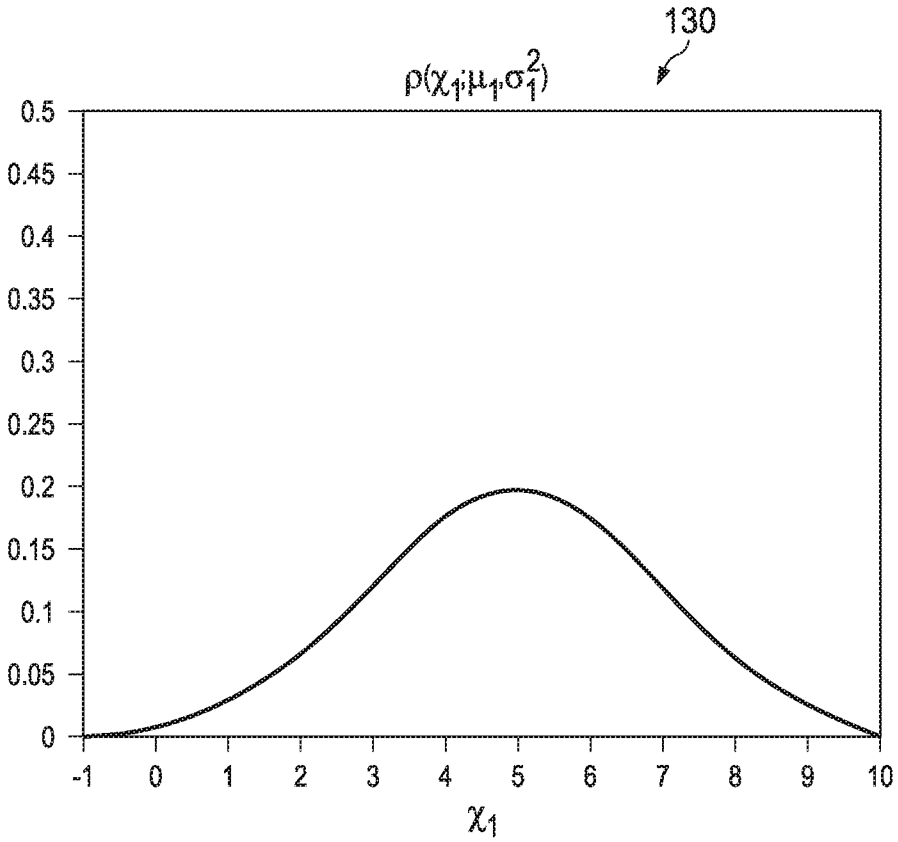

130
$\rho(\chi_1;\mu_1,\sigma_1^2)$
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
-1 0 1 2 3 4 5 6 7 8 9 10
χ_1

FIG. 3B

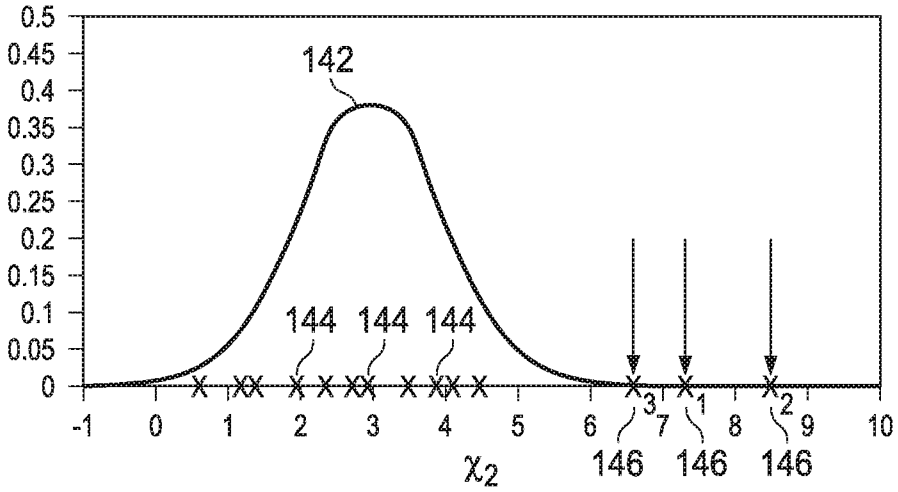

0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
142
144
144
144
-1
0
1
2
3
4
5
6
7
8
9
10
χ_2
146
146
146

FIG. 4

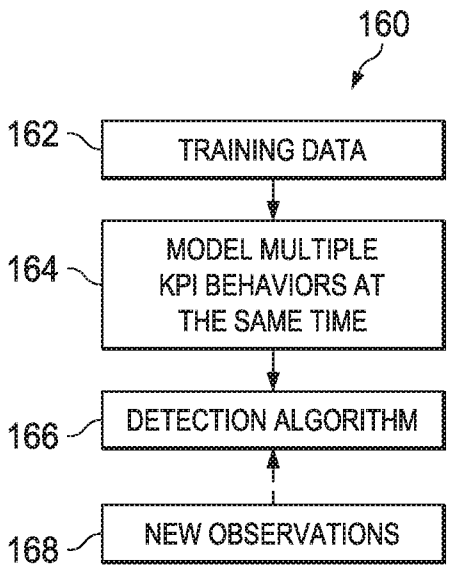

160
162
TRAINING DATA
164
MODEL MULTIPLE KPI BEHAVIORS AT THE SAME TIME
166
DETECTION ALGORITHM
168
NEW OBSERVATIONS

FIG. 5

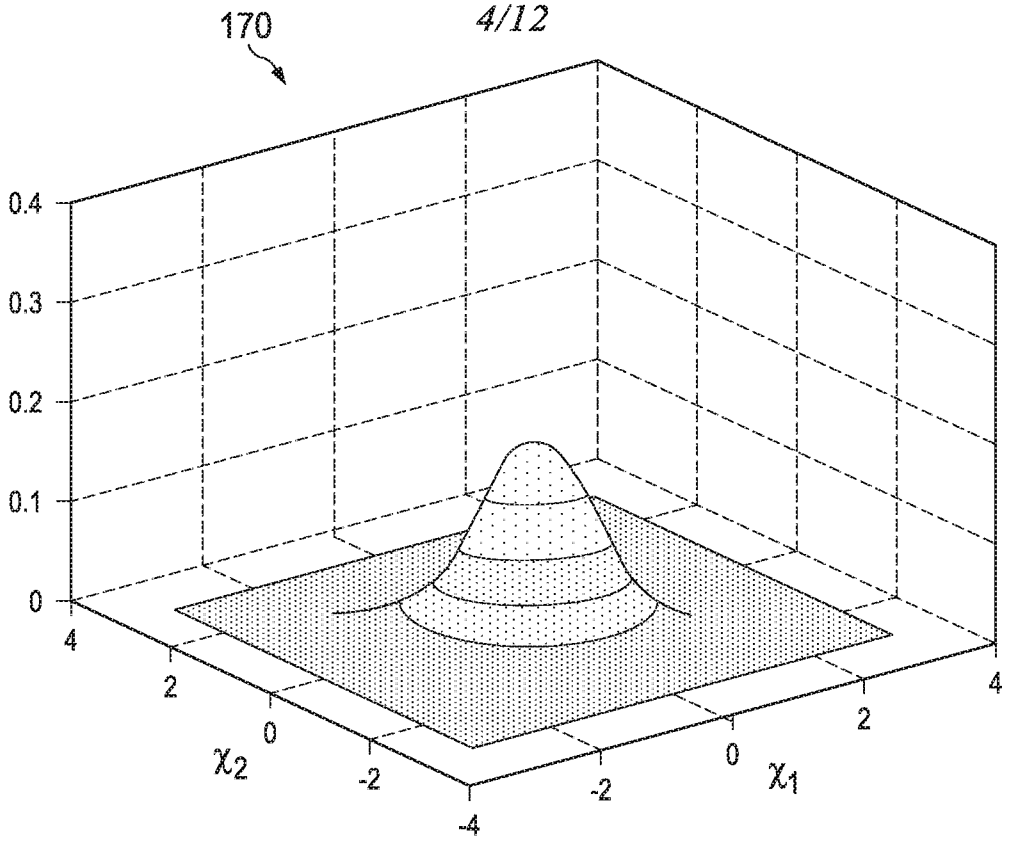

170
0.4
0.3
0.2
0.1
0
4
2
0
-2
-4
χ_2
-4
-2
0
2
4
χ_1

FIG. 6A

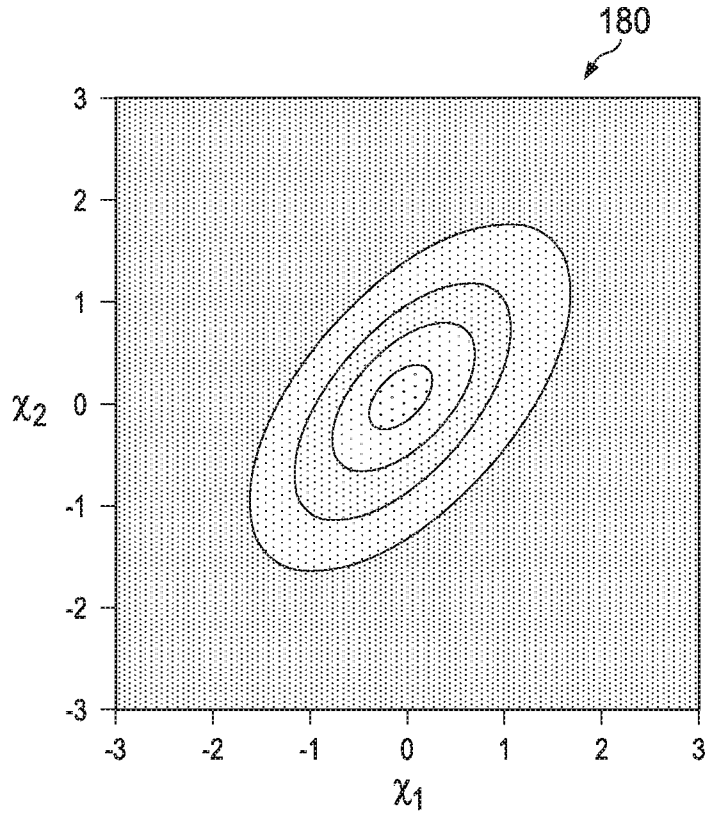

180
3
2
1
0
-1
-2
-3
χ_2
-3
-2
-1
0
1
2
3
χ_1

FIG. 6B

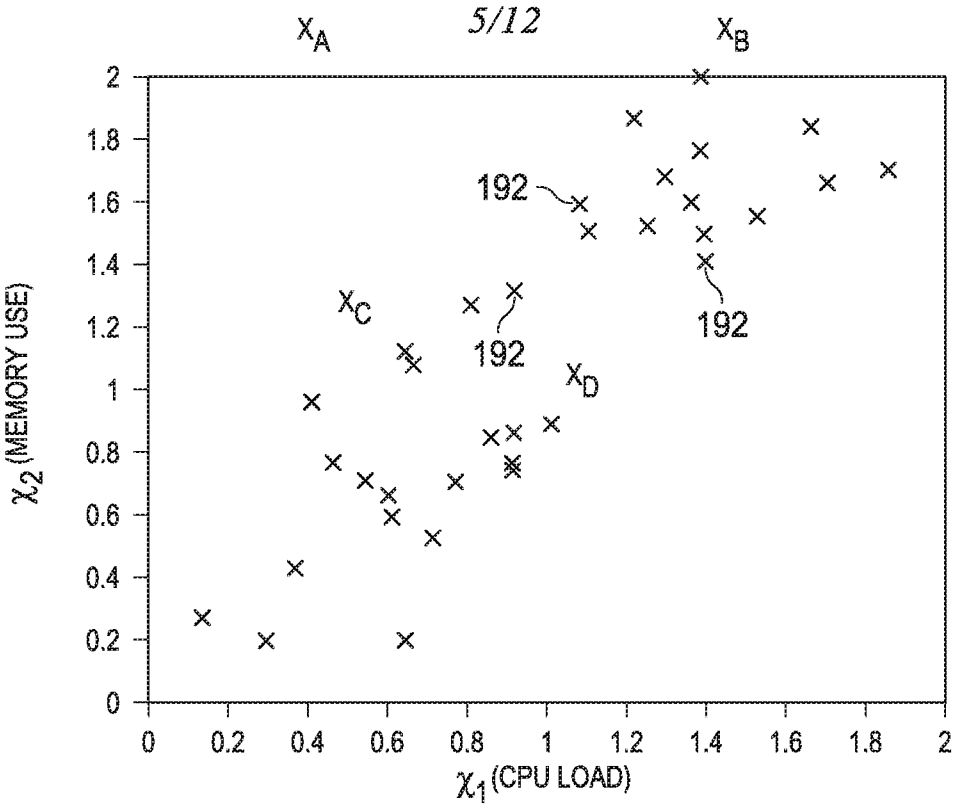

X_A
X_B
X_C
X_D
192
192
192
χ_2 (MEMORY USE)
χ_1 (CPU LOAD)
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

FIG. 7

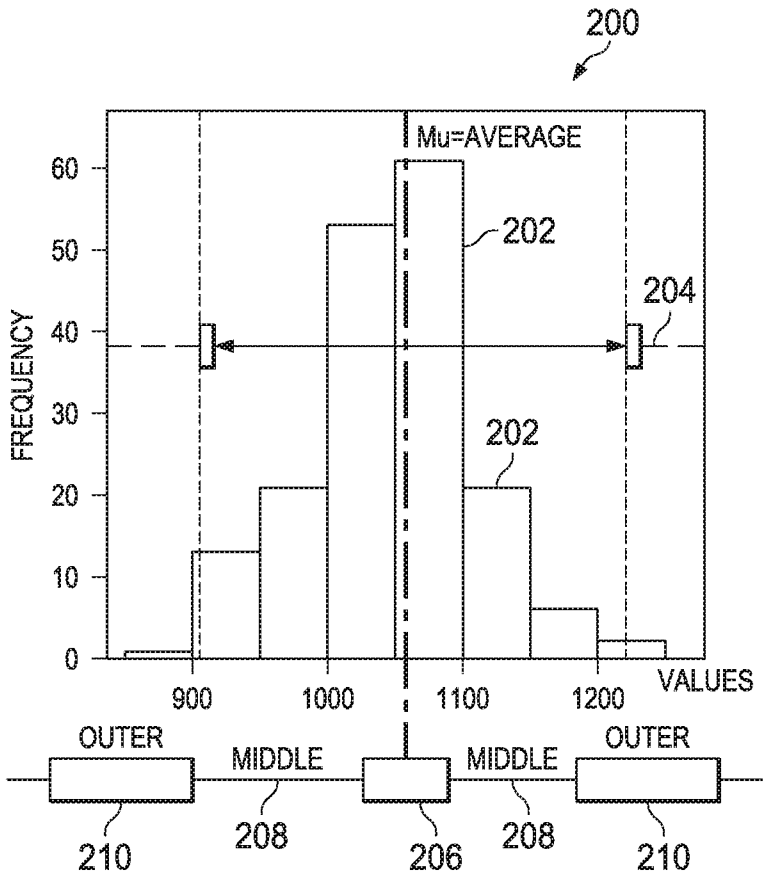

200
Mu=AVERAGE
202
202
204
FREQUENCY
0
10
20
30
40
50
60
900
1000
1100
1200
VALUES
OUTER
MIDDLE
MIDDLE
OUTER
210
208
206
208
210

FIG. 8

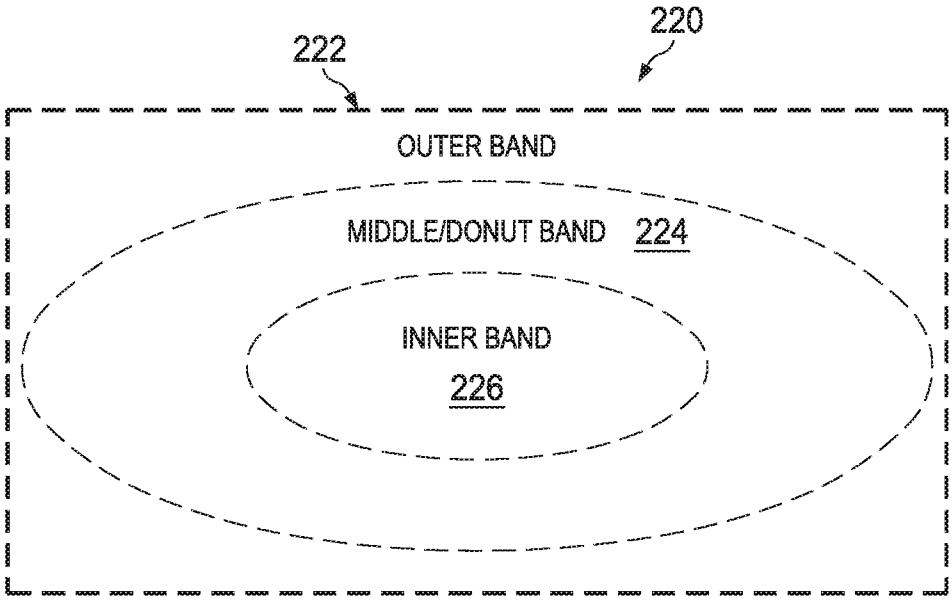

220
222
OUTER BAND
MIDDLE/DONUT BAND 224
INNER BAND
226

FIG. 9

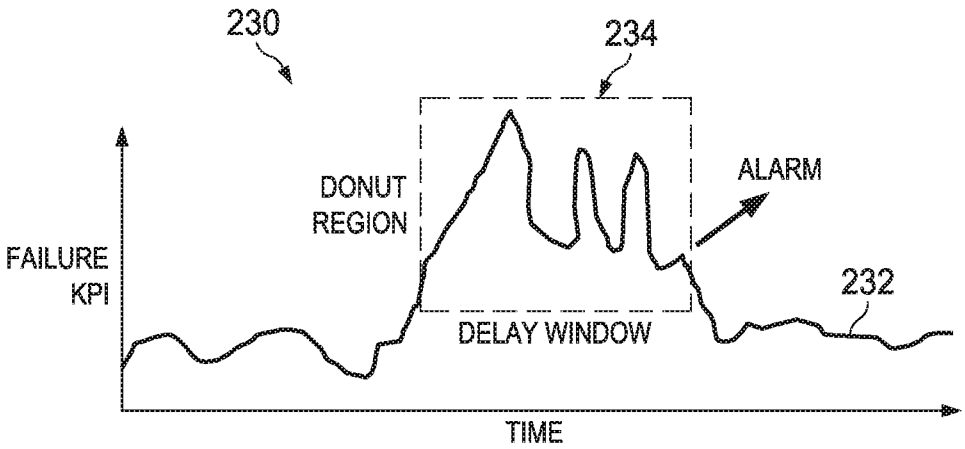

230
234
DONUT
REGION
ALARM
FAILURE
KPI
232
DELAY WINDOW
TIME

FIG. 10

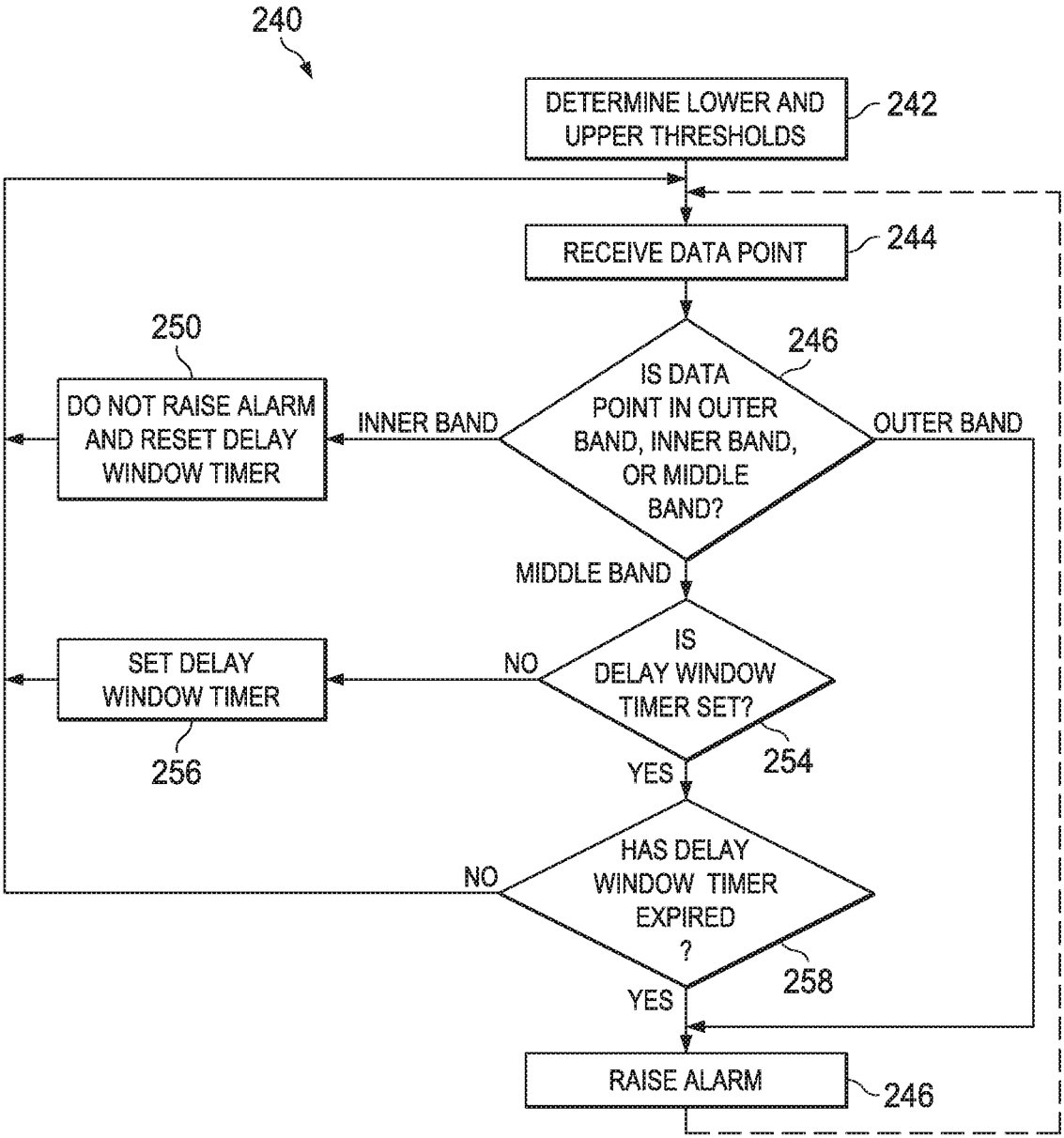

240
DETERMINE LOWER AND UPPER THRESHOLDS
242
RECEIVE DATA POINT
244
IS DATA POINT IN OUTER BAND, INNER BAND, OR MIDDLE BAND?
246
INNER BAND
OUTER BAND
MIDDLE BAND
250
DO NOT RAISE ALARM AND RESET DELAY WINDOW TIMER
IS DELAY WINDOW TIMER SET?
254
NO
YES
SET DELAY WINDOW TIMER
256
HAS DELAY WINDOW TIMER EXPIRED ?
258
NO
YES
RAISE ALARM
246

FIG. 11

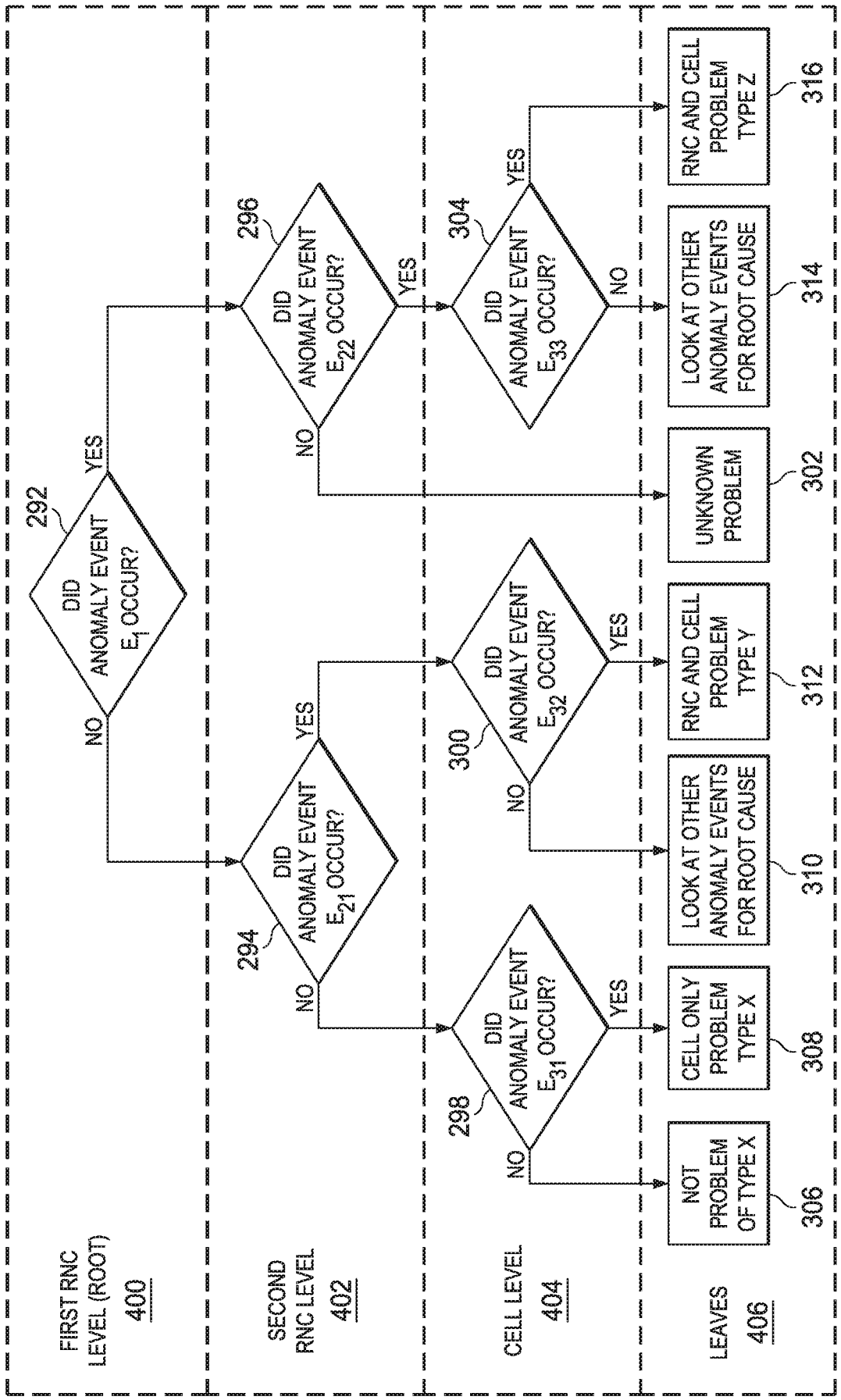

290
FIRST RNC LEVEL (ROOT) 400
SECOND RNC LEVEL 402
CELL LEVEL 404
LEAVES 406
292
DID ANOMALY EVENT E_1 OCCUR?
YES
NO
296
DID ANOMALY EVENT E_{22} OCCUR?
YES
NO
304
DID ANOMALY EVENT E_{33} OCCUR?
YES
NO
294
DID ANOMALY EVENT E_{21} OCCUR?
YES
NO
300
DID ANOMALY EVENT E_{32} OCCUR?
YES
NO
298
DID ANOMALY EVENT E_{31} OCCUR?
YES
NO
UNKNOWN PROBLEM
302
LOOK AT OTHER ANOMALY EVENTS FOR ROOT CAUSE
314
RNC AND CELL PROBLEM TYPE Z
316
RNC AND CELL PROBLEM TYPE Y
312
LOOK AT OTHER ANOMALY EVENTS FOR ROOT CAUSE
310
CELL ONLY PROBLEM TYPE X
308
NOT PROBLEM OF TYPE X
306

FIG. 12

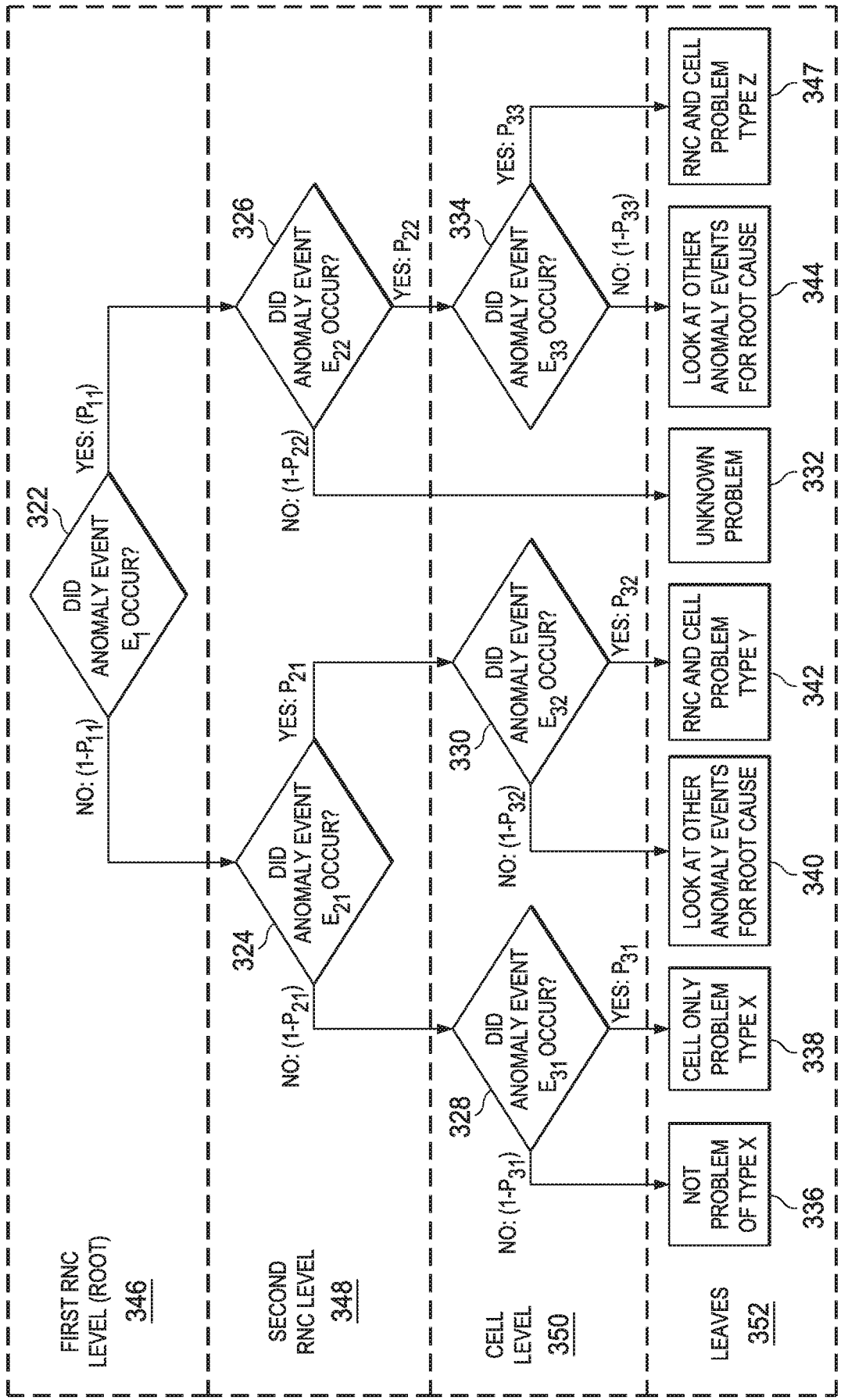

320
FIRST RNC LEVEL (ROOT) 346
SECOND RNC LEVEL 348
CELL LEVEL 350
LEAVES 352
322
DID ANOMALY EVENT E_1 OCCUR?
YES: (P_{11})
NO: $(1-P_{11})$
324
DID ANOMALY EVENT E_{21} OCCUR?
YES: P_{21}
NO: $(1-P_{21})$
326
DID ANOMALY EVENT E_{22} OCCUR?
YES: P_{22}
NO: $(1-P_{22})$
328
DID ANOMALY EVENT E_{31} OCCUR?
YES: P_{31}
NO: $(1-P_{31})$
330
DID ANOMALY EVENT E_{32} OCCUR?
YES: P_{32}
NO: $(1-P_{32})$
334
DID ANOMALY EVENT E_{33} OCCUR?
YES: P_{33}
NO: $(1-P_{33})$
336 NOT PROBLEM OF TYPE X
338 CELL ONLY PROBLEM TYPE X
340 LOOK AT OTHER ANOMALY EVENTS FOR ROOT CAUSE
342 RNC AND CELL PROBLEM TYPE Y
332 UNKNOWN PROBLEM
344 LOOK AT OTHER ANOMALY EVENTS FOR ROOT CAUSE
347 RNC AND CELL PROBLEM TYPE Z

FIG. 13

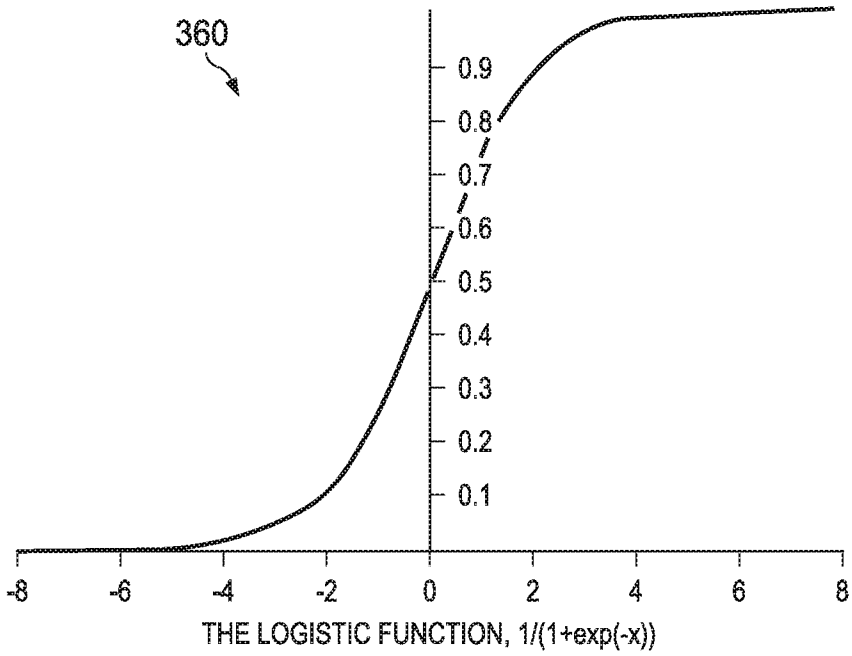

360
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
-8
-6
-4
-2
0
2
4
6
8
THE LOGISTIC FUNCTION, 1/(1+exp(-x))

FIG. 14

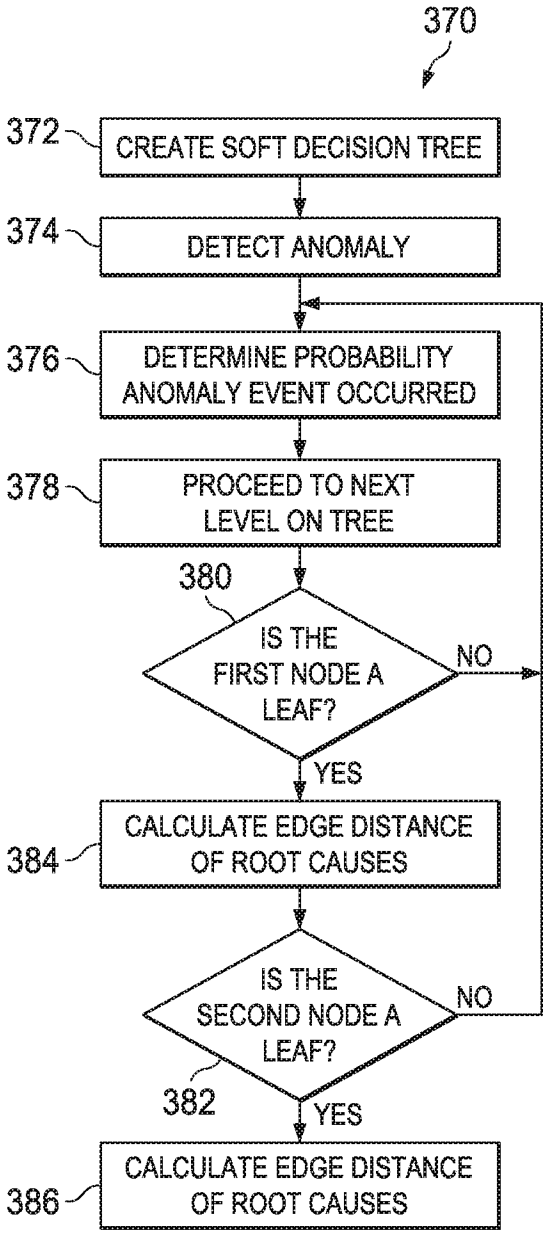

370
372
CREATE SOFT DECISION TREE
374
DETECT ANOMALY
376
DETERMINE PROBABILITY ANOMALY EVENT OCCURRED
378
PROCEED TO NEXT LEVEL ON TREE
380
IS THE FIRST NODE A LEAF?
NO
YES
384
CALCULATE EDGE DISTANCE OF ROOT CAUSES
IS THE SECOND NODE A LEAF?
NO
382
YES
386
CALCULATE EDGE DISTANCE OF ROOT CAUSES

FIG. 15

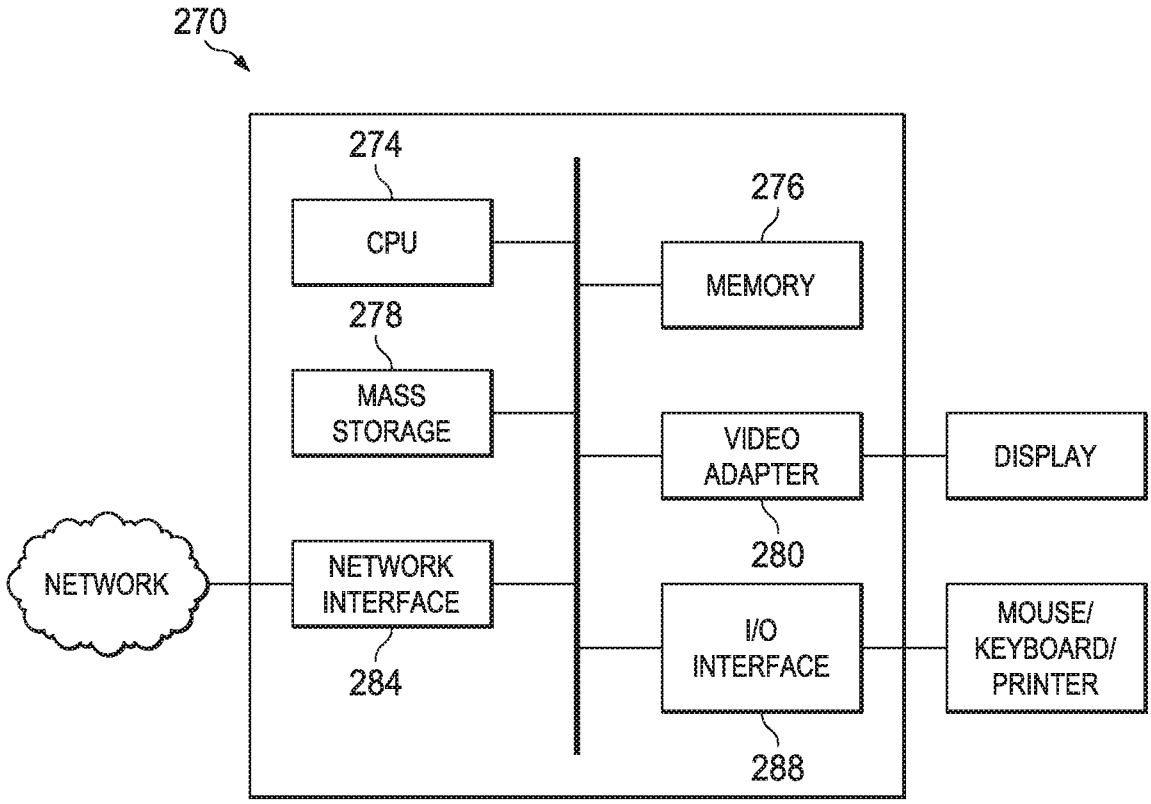

270
274
CPU
276
MEMORY
278
MASS STORAGE
VIDEO ADAPTER
DISPLAY
280
NETWORK
NETWORK INTERFACE
I/O INTERFACE
MOUSE/ KEYBOARD/ PRINTER
284
288

FIG. 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/077810

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i

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)

H04L G06F H04W H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

CNPAT,EPODOC,WPI:anomaly,abnormal,detect,threshold,limit,upper,lower,larger,between,less,metric,distance,probability, root,cause,analysis,decision,tree,data,point

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 1770885 A (HUAWEI TECHNOLOGIES CO., LTD.) 10 May 2006 (2006-05-10) description page 6 line 9 to page 8 line 24, abstract	1-24
A	WO 2013044974 A1 (TELEFONAKTIEBOLAGET L M ERICSSON PUBL) 04 April 2013 (2013-04-04) description page 9 lines 10-12, claim 1	1-24
A	US 2013339515 A1 (INTERNATIONAL BUSINESS MECHINES CORPORATION) 19 December 2013 (2013-12-19) the whole document	1-24
A	US 7444263 B2 (OPNET TECHNOLOGIES, INC.) 28 October 2008 (2008-10-28) the whole document	1-24
A	CN 1996888 A (HUAWEI TECHNOLOGIES CO., LTD. ET AL.) 11 July 2007 (2007-07-11) the whole document	1-24

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* 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
11 July 2015	**04 August 2015**
Name and mailing address of the ISA/CN **STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer **YAN,Yan** Telephone No. **(86-10)62413415**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/077810

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	1770885	A	10 May 2006	None			
WO	2013044974	A1	04 April 2013	CN	103947156	A	23 July 2014
				US	2014321311	A1	30 October 2014
				EP	2742646	A1	18 June 2014
				KR	20140054397	A	08 May 2014
				JP	2014534661	A	18 December 2014
US	2013339515	A1	19 December 2013	None			
US	7444263	B2	28 October 2008	US	2008016412	A1	17 January 2008
CN	1996888	A	11 July 2007	None			