(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年7 月23 日 (23.07.2009)

PCT

(10) 国際公開番号
WO 2009/090939 A1

(51) 国際特許分類:
H04L 12/56 (2006.01) *G06F 13/00* (2006.01)
G06F 11/30 (2006.01) *H04L 12/24* (2006.01)
G06F 11/34 (2006.01) *H04L 12/26* (2006.01)

(21) 国際出願番号: PCT/JP2009/050318

(22) 国際出願日: 2009 年1 月13 日 (13.01.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2008-005603 2008 年1 月15 日 (15.01.2008) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 広瀬 俊亮 (HIROSE, Shunsuke) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 山西 健司 (YAMANISHI, Kenji) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 宮崎 昭夫, 外(MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂１丁目９番２０号 第１６興和ビル８階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

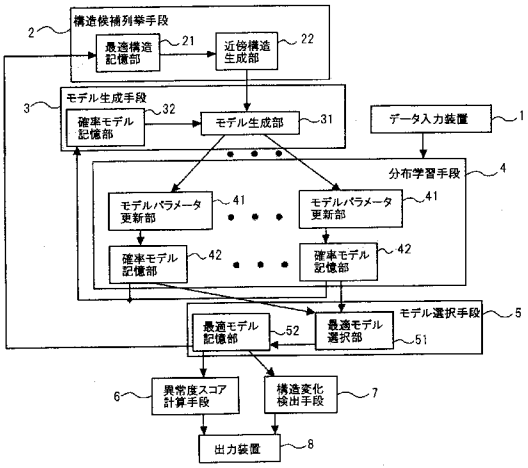
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[続葉有]

(54) **Title:** APPARATUS AND METHOD FOR DETECTING NETWORK ABNORMALITY

(54) **発明の名称:** ネットワーク異常検出装置及び方法

[図1]



2 STRUCTURE CANDIDATE ENUMERATION MEANS
21 OPTIMUM STRUCTURE STORAGE UNIT
22 NEIGHBORHOOD STRUCTURE GENERATION UNIT
3 MODEL GENERATION MEANS
32 PROBABILITY MODEL STORAGE UNIT
31 MODEL GENERATION UNIT
1 DATA INPUT DEVICE
4 DISTRIBUTION LEARNING MEANS
41 MODEL PARAMETER UPDATING UNIT
42 PROBABILITY MODEL STORAGE UNIT
5 MODEL SELECTION MEANS
52 OPTIMUM MODEL STORAGE UNIT
51 OPTIMUM MODEL SELECTION UNIT
6 ABNORMALITY SCORE CALCULATION MEANS
7 STRUCTURAL CHANGE DETECTION MEANS
8 OUTPUT DEVICE

(57) Abstract: A network abnormality detection apparatus comprises a data distribution learning unit (2, 3, 4, 5) and an abnormality detection unit (6, 7). The data distribution learning unit receives data that describes a network state by means of matrix variables having a hierarchical structure, and learns the network state as a probability distribution of the matrix variables. Based on the learning result by the data distribution learning unit, the abnormality detection unit detects, as an abnormality of the network, a state in which the probability distribution has been transferred from a distribution representing a normal state of the network to a distribution representing other state.

(57) 要約: ネットワーク異常検出装置は、ネットワークの状態を階層構造の行列変数で表したデータを入力とし、上記ネットワークの状態を上記行列変数の確率分布として学習するデータ分布学習部（２、３、４、５）と、上記データ分布学習部による学習の結果に基づいて、上記確率分布が上記ネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態を上記ネットワークの異常として検出する異常検出部（６、７）と、を有する。

WO 2009/090939 A1

SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

ネットワーク異常検出装置及び方法

技術分野

[0001] 本発明は、ネットワークの異常を検出する技術に関する。

背景技術

[0002] ネットワークの異常を検出する上で考慮すべき点として、以下のようなネットワークの性質がある。

[0003] 第一の性質は、ネットワーク上では頂点毎に相互作用がある点である。この相互作用の下でネットワークがどのような状態にあるか、もしくは、どのように働いているか、といった、ネットワークの全体的な構造(グラフ構造)を考慮する必要がある。ここでいう全体的な構造とは、例えば、どの頂点も均一に働いていること、重点的に稼動している重要な頂点が少数存在することなどを示す構造である。

[0004] この第一の性質があるため、個別の要素を調べるだけでは、ネットワークの異常を検出することは難しい。例えば、ネットワークの或る部分のトラフィック量が多くなるだけでは、ネットワークの異常とは言えないが、他のある部分のトラフィック量と同時に多くなる場合は、ネットワークの異常であると言える。ネットワークの全体的な構造を考慮することで、例えば、ネットワークが通常の状態にあり、トラフィック量が均一であったものが、全体的にウィルスに感染してあるサーバを攻撃し始めたために、トラフィック量が一極集中するようになる、といったネットワークの異常を検出することができる。

[0005] 第二の性質は、ネットワーク上のトラフィック量は時刻と共に変化し、どの頂点とどの頂点が繋がっているかというネットワークの構造も時間と共に変化する点である。この第二の性質があるため、ネットワークの異常を検出するためには、ネットワークの通常の状態がどういう状態であるかを学習する必要がある。例えば、深夜の時間帯においては、トラフィック量が異常に多くなったとしても、昼の時間帯においては、トラフィック量は通常の量となる、といったような状況が、第二の性質に対応する。

[0006] 上記の性質を考慮したネットワークの異常検出方法として、特開2005－216066号公報(以下、特許文献1と記す。)に記載の方法がある。特許文献1に記載の方法

では、ネットワークの特徴量を成分に持つ行列の最大固有ベクトルを入力として、ベクトルの通常の状態を学習し、通常のベクトルと大きく異なる場合を異常として検出する。

[0007] ネットワークの持つ特徴的な構造としては、以下の非特許文献1乃至3に記載のものがある。

[0008] 1. A. L. Barabasi, and R. Albert, 'Emergence of Scaling in Random Networks ', Science vol. 286, pp509-512 (1999).)

2. (C. Song, S. Havlin and H. Makse, 'Self-similarity of complex networks', Nature vol. 433, pp.392-395 (2005).)

3. (Jure Leskovec and Christos Faloutsos, 'Scalable Modeling of Real Graphs using Kronecker Multiplication', ICML2007

非特許文献1には、ネットワークの構造について、多くの現実のネットワークがスケールフリー性を持つことが示されている。ここで、スケールフリー性とは、ネットワークの多くの頂点が少ないリンク数を持つ一方、膨大なリンクを持つ頂点も少数ながら存在するという性質のことをいう。Webページを例に挙げると、人気のページは、膨大な数のページから参照されるが、他の大多数のページは、少数の参照元しか持たない。このような性質をスケールフリー性と呼ぶ。

[0009] 非特許文献2には、スケールフリー性を持つネットワークが自己相似性を持つことが報告されている。自己相似性とは、全体を相似的に縮小した際に、元と同じ形が現れるという性質である。具体的には、遠くからぼんやりと眺めた場合も、近くに寄って細かい構造を見た場合も、同じ形に見えるという性質を、自己相似性という。

[0010] スケールフリー性を持つネットワークを、行列を用いて表現する方法として、非特許文献3には、行列を行列の直積として表すという方法が示されている。n×m行列Uとp×q行列Vとの直積は、以下のpn×qm行列で定義される。

[0011] [数1]

$$U \otimes V = \begin{pmatrix} U_{11}V & U_{12}V & \cdots & U_{1m}V \\ U_{21}V & U_{22}V & \cdots & U_{2m}V \\ \vdots & \vdots & & \vdots \\ U_{n1}V & U_{n2}V & \cdots & U_{nm}V \end{pmatrix}$$

特開2005－141601号公報（以下、特許文献2と記す。）には、ネットワークの構造についての技術ではないが、複数の構造があった場合に、その中から最適な構造を選択する技術が記載されている。この技術によれば、予め用意された構造の中から情報量規準を最小にするものを最適な構造として逐次的に選択することで、構造の時間的な変化に対応する。

発明の開示

[0012] ネットワーク上のトラフィックにおいて、ある区域において重要な働きをするハブがあり、更に広い区域で見ると、それらをまとめるハブがある、というような階層構造が、各所で現れる場合がある。このような階層構造を有するネットワークにおいて、ワームの発生等の異常が発生した場合、全体が同じようなトラフィックになったり、一部だけがおかしくなったりする。このような異常を検出するためには、ネットワークの階層構造を考慮する必要がある。

[0013] 特許文献1に記載の手法では、入力を固有ベクトルに変換するため、ネットワークの構造に関する情報が出力に含まれない。このため、どのような変化が起こったために(全体的な構造がどのように変化したために)、ネットワークの異常と判断されたのかを知ることはできない。

[0014] 非特許文献1、2には、現実のネットワークの特徴的な構造としてスケールフリー構造や自己相似構造があることが開示されている。しかし、自己相似性やスケールフリー性といった階層構造の変化をどのようにして検出するかについては、これら非特許文献1、2には示されていない。

[0015] 特許文献2には、入力データの確率分布の構造の変化を捉える異常検出手法が記載されている。しかし、特許文献2に記載の手法は、候補となる構造を全て用意し、その中から最適な構造を選択するという手法である。階層構造を考慮したネットワー

クの異常検出に関する技術思想については、特許文献2には何も開示されていない。

[0016] 本発明の目的は、上記の課題を解決し、ネットワークの全体的な構造を考慮して異常の検出を行うことのできる、ネットワーク異常検出装置および方法を提供することにある。

[0017] 上記の目的を達成するため、本発明のネットワーク異常検出装置は、ネットワークの状態を階層構造の行列変数で表したデータを入力とし、前記ネットワークの状態を前記行列変数の確率分布として学習するデータ分布学習部と、前記データ分布学習部による学習の結果に基づいて、前記確率分布が前記ネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態を前記ネットワークの異常として検出する異常検出部と、を有する。

[0018] また、本発明のネットワーク異常検出方法は、ネットワークの状態を階層構造の行列変数で表したデータを入力するコンピュータシステムにおいて行われるネットワーク異常検出方法であって、データ分布学習部が、入力される前記データに基づいて、前記ネットワークの状態を前記行列変数の確率分布として学習し、異常検出部が、前記データ分布学習部による学習の結果に基づいて、前記確率分布が前記ネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態を前記ネットワークの異常として検出する。

図面の簡単な説明

[0019] [図1]図1は、本発明の一実施形態であるネットワーク異常検出装置の構成を示すブロック図である。

[図2]図2は、図1に示すネットワーク異常検出装置において行われる異常検出処理を説明するためのフローチャートである。

符号の説明

[0020] 1 データ入力装置

2 構造候補列挙手段

3 モデル生成手段

4 分布学習手段

5 モデル選択手段

6 異常スコア計算手段

7 構造変化検出手段

8 出力装置

発明を実施するための最良の形態

[0021] 以下、本発明における一実施形態を、図面を参照して説明する。

[0022] 次に、本発明の実施形態について図面を参照して説明する。

[0023] 図1は、本発明の一実施形態であるネットワーク異常検出装置の構成を示すブロック図である。図1を参照すると、ネットワーク異常検出装置は、データ入力装置1、構造候補列挙手段2、モデル生成手段3、分布学習手段4、モデル選択手段5、異常度スコア計算手段6、構造変化検出手段7および出力装置8を有する。

[0024] データ入力装置1は、ネットワークの状態を階層構造のパラメータで表したデータ、より具体的には、ネットワークの特徴量を成分に持つテンソル型データを入力するためのものである。入力データは、時刻と共に逐次的に入力される、もしくは、そのデータが発生した時刻に関する情報が付与されている。ここで、ネットワークの特徴量とは、例えば、ノード間のトラフィック量(もしくはその関数)や、ノード間の接続の有無を0、1の2値の情報で表したものである。入力データは、一般の階数のテンソル型であってもよく、また、行列型であってもよい。

[0025] 行列型データは、例えばD(i, j)のような、データを指定する自由度が二つ(iとj)あるデータを表す。例えば、Webページ間のリンクを表すデータD(i, j)の場合、D(i, j)はページ間のリンクの有無を表し、i、jはそれぞれ一つのWebページを表す。ページiからページjへリンクが張られている場合は、D(i, j)＝1となる。ページiからページjへリンクが張られていない場合は、D(i, j)＝0となる。

[0026] テンソル型データは、E(i, j, k)やF(i, j, k, l)のように、データを指定する自由度が二つ以上あるデータである。E(i, j, k)のように自由度が3つあるものは、三階のテンソルと言う。F(i, j, k, l)のように自由度が4つあるものは、四階のテンソルと言う。行列型は、二階のテンソルと言うことができる。

[0027] 例えば、ネットワークの通信の種類と容量を記録したデータE(i, j, k)において、i, j

はそれぞれ一つのサーバを表し、kは通信の種類(ftp,smtp,ssh…)を表す。E(i, j, k)はネットワーク上の通信量を表す。この通信量は、サーバiからサーバjへの通信における、通信の種類がkであったものがどれくらいの量あったかを示す。

[0028] 以下では、行列型の入力データを例にとって、本実施形態のネットワーク異常検出装置の各部の動作を説明する。

[0029] 構造候補列挙手段2は、現時点で最適な構造として選ばれている階層構造の近傍の構造を列挙する。ただし、計算量を節約しなくても良い場合は、構造候補列挙手段2は、可能な全ての構造を列挙しても良い。

[0030] 構造候補列挙手段2の主要部は、最適構造記憶部21および近傍構造生成部22からなる。最適構造記憶部21には、現時点で最適な構造として選ばれている階層構造の情報が格納される。近傍構造生成部22は、最適構造記憶部21に記憶されている最適な構造をもとに、最適な構造の近傍の構造を列挙し、その情報をモデル生成手段3に供給する。

[0031] なお、最適な構造が決まっていない場合、すなわち初めてデータが入力された場合は、近傍構造生成部22は、可能な構造のうちの一つをランダムに選び、それを最適な構造とする。ここで、階層構造とは、一般のグラフ的な階層構造を指すものであり、例えば、ツリー構造、自己相似構造、スケールフリー構造などを含む。

[0032] 構造は、例えば行列の直積構造である。行列の直積構造は、一般に、

[0033] [数2]

$$\Sigma = \sigma 1 \times \sigma 2 \times \sigma 3 \cdots \times \sigma d$$

で示されるものであり、各要素(σ)が階層構造に対応する。可能な構造とは、このΣを分割してつくることが可能な階層構造である。可能な階層構造は、Σを幾つのσの掛け算で表すか、および、各σの次元が幾つであるか、といったことにより決まる。例えば、

[0034] [数3]

$$\Sigma = \sigma 1 \times \sigma 2 \quad (\sigma 1 = 2\text{次元}、\ \sigma 2 = 15\text{次元})$$

で表される構造の場合、Σは30次元(入力データの次元に対応する)となる。入力データの次元が分かれば、可能な構造を列挙することができる。ネットワーク異常検出装置の起動時には、入力データの次元に関する情報がデータ入力装置1から近傍構造生成部22に供給される。

[0035] 以下では、データ入力装置1からの入力データ(ネットワークの特徴量)が直積構造を持つ場合を例にとって説明する。

[0036] 入力データをTとするとき、Tが直積構造を持つとは、以下の式のように、Tが二つ以上の行列または二つ以上の一般の階数のテンソルの直積で表されることを指す。

[0037] [数4]

$$T = U \otimes V$$

この式によれば、Uという階層の値とVという階層の値の積で入力データTが表される、という階層構造をTが持っている。非特許文献3に記載されているとおり、直積構造は、スケールフリー構造と対応しており、現実のネットワークが持つ構造の一つである。

[0038] 以下、近傍の構造の列挙の方法について説明する。

[0039] K番目のモデルのパラメータ行列MKが、

[0040] [数5]

$$M_k = \mu_{k1} \otimes \cdots \otimes \mu_{kd_k}$$

で表される直積構造の場合は、階層構造は、幾つの行列の直積で書かれているかを示す(dk)と、それぞれの階層の行列μ1～μdkの各次元とで表される。各階層の行列の次元を並べた

[0041] [数6]

$$(s_1, s_2, s_3, \cdots, s_{dk})$$

といったもので構造を表すことができる。

[0042] 最適な構造の近傍の構造とは、最適な階層構造と類似する構造のことである。直積構造を考える場合、最適な構造と類似する直積構造を持つ構造が近傍の構造とされる。例えば、最適な構造が(s_1,s_2,…,s_d)のように表されるとき、その近傍の構造とは、以下のような構造である。

(1)隣接する二つの階層の次元を交換した構造

[0043] [数7]

$$(s_2, s_1, s_3, \cdots, s_d)$$

(2)隣接する二つの階層を一つにまとめた構造

[0044] [数8]

$$(s'_1, s_3, \cdots, s_d)$$

(3)一つの階層を二つに分割した構造

[0045] [数9]

$$(s_1, s'_2, s''_2, s_3, \cdots, s_d)$$

モデル生成手段3は、入力データの確率分布のモデルを複数生成する。入力データをXと表す。データの分布のモデルとして、直積構造を持つ行列型パラメータを持つ行列変数の確率分布を用いる。分布として、例えば、行列変数の正規分布を用いることができる。

[0046] [数10]

$$p(X \mid \Sigma, \Psi, M) = \frac{1}{(2\pi)^{\frac{n^2}{2}} (\det \Sigma)^{\frac{n}{2}} (\det \Psi)^{\frac{n}{2}}} \exp\left[-\frac{1}{2} tr\left[\Sigma^{-1}(X-M)\Psi^{-1}(X-M)^{\dagger}\right]\right]$$

データの分布のモデルは、階層構造を持つ行列型パラメータを持つ行列変数の確率分布であれば良い。ここでは、データ分布モデルを、パラメータ行列が直積構造を持った行列変数の正規分布とする。

[0047] 生成された複数のモデルのうち、k番目のモデルは、

[0048] [数11]

$$p_k(X|\Sigma_k,\Psi_k,M_k)$$

で与えられる。

[0049] 各モデルのパラメータに、構造候補列挙手段2にて列挙された構造と対応する直積構造を持たせる。k番目のモデルの階層の深さをdkとする。この深さdkは、幾つの直積でパラメータを表すかを示す。

[0050] [数12]

$$\Sigma_k = \sigma_{k1} \otimes \cdots \otimes \sigma_{kd_k}$$
$$M_k = \mu_{k1} \otimes \cdots \otimes \mu_{kd_k}$$
$$\Psi_k = \psi_{k1} \otimes \cdots \otimes \psi_{kd_k}$$

モデル生成手段3は、モデル生成部31および確率モデル記憶部32からなる。分布学習手段4は、複数のモデルパラメータ更新部41および複数の確率モデル記憶部42からなる。

[0051] モデル生成部31は、一段階前のモデルのパラメータと構造の情報を確率モデル記憶部32から取得し、新たに生成されたモデルの構造の情報を近傍構造生成部22から受け取り、複数のモデルのパラメータと構造の情報を各モデルパラメータ更新部41に供給する。

[0052] 近傍構造生成部22から得られた構造が、確率モデル記憶部32から送られた一段階前の時刻における複数のモデルの中に含まれる場合は、一段階前の時刻のパラメータをそのまま引き継ぐ。近傍構造生成部22から得られた構造が、一段階前の時刻における複数のモデルの中に含まれない場合、すなわち、最適な構造の変化によって構造候補列挙手段2で新たに生成された構造に対応したモデルである場合は、最

適な構造に対応するモデルのパラメータに近くなるようにパラメータを決める。例えば、最適なモデルのパラメータがσであって、新たに生成した構造に対応するモデルのパラメータがσ'1×σ'2という形である場合、フロベニウスノルム

[0053] [数13]

$$\left\|\sigma-\sigma'_1\otimes\sigma'_2\right\|_F$$

を最小にするσ'1とσ'2を求め、それを新たなモデルのパラメータの値とする。

[0054] モデル学習手段4は、モデル生成手段3で用意された複数のモデルのパラメータを更新する。モデルパラメータ更新部41は、一段階前の時刻におけるモデルの情報をモデル生成部31から受け取り、入力データを入力装置1から受け取り、モデルのパラメータの更新を行う。時刻tでのパラメータの算出方法としては、時刻jの入力データをXjとして、例えば以下の式で与えられる対数尤度が最大になるようにパラメータを決める、という方法がある。

[0055] [数14]

$$\sum_{j=0}^{t}\log p\left(X_j\mid\Sigma_k,\Psi_k,M_k\right)$$

また、以下の式で与えられる時間幅Lの中での対数尤度が最大になるようにパラメータを決めてもよい。

[0056] [数15]

$$\sum_{J=t-L+1}^{t}\log p\left(X_j\mid\Sigma_k,\Psi_k,M_k\right)$$

また、過去のものの重みを小さくした以下の対数尤度が最大になるようにパラメータを決めてもよい。ただし、0<r<1である。このパラメータの決定方法は、一般に、忘却型学習と呼ばれる。

[0057] [数16]

$$\sum_{j=0}^{t} r(1-r)^{t-j} \log p\left(X_j \mid \Sigma_k, \Psi_k, M_k\right)$$

上記の例のような、パラメータを決める方式を、学習方式と呼ぶ。

[0058] 更新されたパラメータと構造の情報は確率モデル記憶部42に格納される。確率モデル記憶部42に格納されている情報は、情報が更新される度に、確率モデル記憶部32に送られる。

[0059] モデル選択手段5は、モデル学習手段4にて学習された各モデルについて情報量規準を計算し、その値が最小になるモデルを最適なモデルとして選択する。モデル選択手段5は、最適モデル選択部51および最適モデル記憶部52からなる。最適モデル選択部51は、各確率モデル記憶部42から供給された複数のモデルの情報から、最適なモデルを一つ選択する。最適なモデルの選択方法について、以下に説明する。

[0060] 時刻jでのk番目のモデルのパラメータをまとめて

[0061] [数17]

$$\theta_k^{(j)}$$

と表し、時刻jでのk番目のモデルの直積構造を

[0062] [数18]

$$s_k^{(j)} = \left(\left(s_k^{(j)}\right)_1, \left(s_k^{(j)}\right)_2, \cdots, \left(s_k^{(j)}\right)_{d_k^{(j)}}\right)$$

と表す。

[0063] 時刻jでの最適なモデルを

[0064] [数19]

$$k_j^*$$

と表す。

[0065] 情報量規準を用いて最適なモデルを選択する方法の例として、以下のものが挙げられる。

[0066] 学習方式として忘却型学習を用いている場合に、以下の予測的確率的コンプレキシティとして知られる量(Universal coding, information, prediction, and estimation, IEEE Transactions on Information Theory, 30, pp:629-636, 1984)をモデル選択の為の情報量規準として用い、この値を最小にするモデルkを最適なモデルとして選択するという方法を用いることが出来る。

[0067] [数20]

$$\sum_{j=0}^{t-1} -\log p\left(X_j \mid \theta_k^{(j-1)}\right)$$

学習方式に依らず、ある範囲のモデルの推移を一括して求める場合には、時刻j－1までのモデルの系列

[0068] [数21]

$$k^{j-1} = (k_0, k_1, \cdots, k_{j-1})$$

とモデルの遷移確率

[0069] [数22]

$$p\left(k_j \mid k^{j-1}\right)$$

とを用いて表される、以下の一括型動的モデル選択基準(特許文献2参照)

[0070] [数23]

$$-\sum_{j=1}^{t} \log p\left(X_j \mid \theta_{k_j}^{(j-1)}\right) - \sum_{j=1}^{t} \log p\left(k_j \mid k^{j-1}\right)$$

を最小にするように最適なモデルの系列

[0071] [数24]

$$(k_1^*, k_2^*, \cdots, k_t^*)$$

を決めるという方法を用いることが出来る。

[0072] また、忘却型でない学習方式を用いる場合や、計算量を小さくしたい場合には、ある時間幅Wの中で、パラメータの数とデータの数とデータの尤度等を引数とする関数の値を計算して、それを最小にするモデルを最適なモデルとして選択するという方法を用いることができる。

[0073] パラメータの数とデータの数とデータの尤度等を引数とする関数としては、MDL，AIC，BIC等の情報量規準を用いることができる。例えば、情報量規準としてMDLを用いる場合には、以下の量を最小にするモデルを最適なモデルとして選択すればよい。

[0074] [数25]

$$-\sum_{j=t-W+1}^{t} \log p\left(X_j \mid \theta_k^{(t)}\right) + \frac{1}{2}\sum_{t=1}^{d_k}\left((s_k)_t\right)^2 \log W$$

異常度スコア計算手段6は、モデル選択手段5にて選択された最適なモデルを用いて、データの異常度スコアを算出する。異常度スコアは、入力データが通常のデータとどれだけ異なっているかを表す量で、値が大きい程、通常は、現れない異常なデータであることに対応する。異常度スコアが突然高くなったところを調べることで、突発的な異常を検出することができる。

[0075] 異常度スコアとして、例えば以下の量を用いることが出来る。

[0076] [数26]

$$-\log p\left(X_t \mid \theta_{k_j^*}^{(t)}\right)$$

例えば、入力をネットワークのノード間の通信量とする場合、異常度スコアが高いことは、通常同時に通信量が多くならない二箇所で同時通信量が多くなる場合や、通常の通信量よりも全体的に通信量が多くなる場合など、通常の状態とは異なった状態にネットワークが置かれていることに対応する。したがって、この例では、異常度スコアを監視することで、ネットワーク上の通信の状態の異常を検出することが出来る。計算された異常度スコアは、出力装置8に送られる。

[0077] スコアに対して予め閾値を設定できる場合は、スコアがその値を超えたか否か(異常か否か)の情報を出力装置8に送っても良い。

[0078] 構造変化検出手段7では、データの背後にある階層構造の変化を検出する。最適なモデルのパラメータが持つ階層構造

[0079] [数27]

$$s_{k_t^*}^{(t)} = \left(\left(s_{k_t^*}^{(t)}\right)_1, \left(s_{k_t^*}^{(t)}\right)_2, \cdots, \left(s_{k_t^*}^{(t)}\right)_{d_{k_t^*}^{(t)}}\right)$$

が変化した場合、これを階層構造の変化として検出する。構造の変化として、階層構造そのものは変化していないが、何れかの階層の中の構造が変化している、という変化も検出する。このような何れかの階層の中の構造変化の検出方法として、各階層のパラメータ行列の一時刻前からの変化量を計算し、その量の急激な変化を検出する、という方法を用いることが出来る。

[0080] パラメータ行列の一時刻前からの変化量として、以下のような量を用いることが出来る。

[0081] [数28]

$$d(\mu_{k^*_{t-1}i}, \mu_{k^*_t i}) = \mathrm{tr}\left[(\mu_{k^*_{t-1}i} - \mu_{k^*_t i})^2\right]$$

例えば、入力がネットワーク上の通信量である場合に、構造の変化が起こるということは、ある区域において重要な働きをするハブがあり、更に、広い区域で見た場合に、それらをまとめるハブがある、といった、似たような構造を持つネットワークにおいて、ワームの発生等の異常が発生して、全体が同じようなトラフィックになったり、一部だけがおかしくなったりする、といった一時的ではない通信の全体的な異常が発生していることに対応する。したがって、この例では、構造の変化を監視することで、一時的ではない全体的な通信の構造の異常を検出することが出来る。

[0082] 上記の二つの変化が検出されたか否かを出力装置8に送る。

[0083] その他、最適な構造に関する情報なども出力装置8に送っても良い。

[0084] 出力装置8は、異常度スコア計算手段6と構造変化検出手段7で得られた結果を受け取り、それを出力または表示する。

[0085] 図2は、図1に示すネットワーク異常検出装置において行われる異常検出処理を説明するためのフローチャートである。

[0086] 図2を参照すると、異常検出処理は、ネットワークの状態を階層構造の行列変数で表したデータを入力とし、該入力データの分布を行列変数の確率分布として学習するステップS10と、その確率分布が通常の状態から他の状態に遷移した場合にネットワークの異常と判定するステップS20とを含む。

[0087] ステップS10の処理では、まず、近傍構造生成部22が、最適構造記憶部21に最適な構造の情報が格納されているか否かを確認する(ステップS11)。最適構造記憶部21に最適な構造の情報が格納されていない場合(起動直後の状態)、近傍構造生成部22は、入力装置1から予め与えられた入力データの次元に関する情報に基づいて、候補として可能な構造を列挙し、その中からランダムに選択した構造を最適な構造として用いる(ステップS12)。

[0088] ステップS12の後、または、最適構造記憶部21に最適な構造の情報が格納されると、近傍構造生成部22が、最適な構造に類似の構造(近傍の構造)を列挙する。次に、モデル生成部31が、近傍構造生成部22にて列挙した近傍の構造のそれぞれに

ついて、近傍の構造に対応する直積構造のパラメータよりなるモデルを生成する(ステップS14)。このモデル生成において、モデル生成部31は、生成するモデルのパラメータとして、最適な構造におけるパラメータおよび確率モデル記憶部32に格納されたモデルのパラメータを参照する。モデル生成部31にて生成された各モデルは、各モデルパレメータ更新部41に供給される。

[0089] 次に、モデルパレメータ更新部41のそれぞれが、学習方式により、モデル生成部31から供給されたモデルのパラメータを更新する(ステップS15)。各モデルパレメータ更新部41でパラメータの更新がなされたモデルはそれぞれ、対応する確率モデル記憶部42に格納される。確率モデル記憶部42に格納された、パラメータの更新がなされたモデルの情報は、モデル生成主だ3の確率モデル記憶部に供給される。

[0090] 次に、最適モデル選択部51が、各確率モデル記憶部42に格納されたモデルについて、情報量規準の値を計算し、この値が最も小さなモデルを最適モデルとする(ステップS16)。最適モデルは、最適モデル記憶部52に格納される。最適モデル記憶部52に格納された最適モデルの情報は、構造候補列挙手段2の最適構造記憶部21に供給される。

[0091] 上述のステップS11～S16が、データ入力装置1からデータが供給される度に繰り返し実行される。

[0092] ステップS20では、ステップS11～S16の繰り返しの処理において、ステップS16で得られる最適モデルの分布(行列変数の確率分布)を監視し、その分布が通常の状態から他の状態に遷移した場合にネットワークの異常と判定する。この異常判定の処理は、異常度スコア計算手段6による計算結果に基づく第1の異常判定処理と、構造変化検出手段7による検出結果に基づく第2の異常判定処理とを含む。ステップS20において、第1および第2の異常判定処理のいずれかが一方が行われるようにしてもよい。

[0093] 以上説明したネットワーク異常検出装置は、本発明の一例であり、その構成および動作は発明の趣旨を逸脱しない範囲で適宜に変更することができる。例えば、図1に示した構成において、異常度スコア計算手段6および構造変化検出手段7の一方のみを有するように構成してもよい。

[0094] また、ネットワーク異常検出装置は、プログラムより動作するコンピュータシステムにより構成することができる。コンピュータシステムの主要部は、プログラムやデータなどを蓄積する記憶装置、キーボードやマウスなどの入力装置、CRTやLCDなどの表示装置、外部との通信を行うモデムなどの通信装置、プリンタなどの出力装置および入力装置からの入力を受け付けて通信装置、出力装置、表示装置の動作を制御する制御装置から構成される。

[0095] 上記のコンピュータシステムにおいて、制御部が、記憶部に格納されたプログラムを実行することで実現される機能ブロックとして、ネットワークの状態を階層構造の行列変数で表したデータを入力とし、上記ネットワークの状態を上記行列変数の確率分布として学習するデータ分布学習部と、該データ分布学習部による学習の結果に基づいて、上記確率分布が上記ネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態を上記ネットワークの異常として検出する異常検出部と、を有していてもよい。

[0096] 上記の構成において、上記データ分布学習部が、入力される上記データの階層構造に対応する候補として複数の異なる構造を列挙する構造候補列挙手段と、上記構造候補列挙手段にて列挙された構造のそれぞれについて、当該構造と同じ階層構造の行列変数を持つ確率モデルを生成するモデル生成手段と、上記モデル生成手段で生成した確率モデルのそれぞれについて、該確率モデルの行列変数として与えられているパラメータを、入力される上記データに基づいて更新する分布学習手段と、上記分布学習手段にてパラメータの更新がなされた確率モデルのそれぞれについて、モデル選択の指標である情報量規準の値を計算し、該情報量規準の値が最も小さな確率モデルを最適なモデルとして選択するモデル選択手段と、を有し、上記異常検出部が、上記モデル選択手段にて選択した最適なモデルの行列変数の確率分布に関する学習の結果に基づいて上記ネットワークの異常の判定を行うように構成してもよい。この場合、上記構造候補列挙手段は、上記モデル選択手段にて最適なモデルの選択がなされると、該選択された最適なモデルの階層構造に類似した複数の異なる構造を上記候補として列挙してもよい。

[0097] また、図1に示した構成において、上記のデータ分布学習部は、近傍構造生成部2

2、モデル生成部31、モデルパラメータ更新部31および最適モデル選択部51に対応する機能ブロックにより構成され、異常検出部は、異常度スコア計算手段6および構造変化検出手段に対応する機能ブロックにより構成される。

[0098] 以上説明した本発明によれば、以下のような効果を奏する。

[0099] 例えば、ネットワーク上のトラフィックにおいて、ある区域において重要な働きをするハブがあり、更に広い区域で見ると、それらをまとめるハブがある、というような階層構造が、各所で現れる場合がある。このような構造のネットワークにおいて、ワームの発生等の異常が発生した場合、全体が同じようなトラフィックになったり、一部だけがおかしくなったりする。

[0100] 本発明では、ネットワークの状態を階層構造(一般のグラフ的な階層構造、例えば、ツリー構造や自己相似構造などを含む)の行列変数で表したデータを入力とし、ネットワークの状態をその行列変数の確率分布として学習し、その学習の結果に基づいて、その確率分布がネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態をネットワークの異常として検出する。これにより、ネットワークの構造の変化を監視することができ、ワームの発生等の異常の発生を検出することができる。このようにネットワークの構造を考慮して異常の検出を行うことで、異常検出の精度を向上させることができる。

[0101] また、ネットワークの状態を表す階層構造を持つ行列をパラメータとして持つ確率分布を学習し、そのパラメータ行列のどの階層が激しく変化するかを検出することができる。したがって、ネットワークの構造の変化を見る際に、部分的な構造の変化についても検出することができる。加えて、どのような構造の変化から異常が発生したのかということも提示することができ、その結果、検出結果の可読性を向上することができる。

[0102] 非特許文献1、2で示されているように、現実のネットワークに特徴的な構造としてスケールフリー構造や自己相似構造が存在する。スケールフリー構造は、多数の頂点が繋がっているハブとなる少数の頂点があり、それら少数のハブが繋がっている更に少数のハブがある、という構造になっているので、階層構造の一種であると言える。また、自己相似構造も、どの階層も同じ形をしているという階層構造である。本発明によ

れば、ネットワークの階層構造を考慮した異常検出を行うようになっているので、現実のネットワークへの適用を容易に行うことができる。

[0103] 以上説明した本発明のネットワーク異常検出装置は、要素同士が相関を持つネットワーク全般に適用することができる。

[0104] 以上、実施形態を参照して本発明を説明したが、本発明は上述した実施形態に限定されるものではない。本発明の構成および動作については、本発明の趣旨を逸脱しない範囲において、当業者が理解し得る様々な変更を行うことができる。

[0105] この出願は、2008年1月15日に出願された日本出願特願2008－5603を基礎とする優先権を主張し、その開示の全てをここに取り込む。

請求の範囲

[1] ネットワークの状態を階層構造の行列変数で表したデータを入力とし、前記ネットワークの状態を前記行列変数の確率分布として学習するデータ分布学習部と、

前記データ分布学習部による学習の結果に基づいて、前記確率分布が前記ネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態を前記ネットワークの異常として検出する異常検出部と、を有する、ネットワーク異常検出装置。

[2] 前記データ分布学習部は、

入力される前記データの階層構造に対応する候補として複数の異なる構造を列挙する構造候補列挙手段と、

前記構造候補列挙手段にて列挙された構造のそれぞれについて、当該構造と同じ階層構造の行列変数を持つ確率モデルを生成するモデル生成手段と、

前記モデル生成手段で生成した確率モデルのそれぞれについて、該確率モデルの行列変数として与えられているパラメータを、入力される前記データに基づいて更新する分布学習手段と、

前記分布学習手段にてパラメータの更新がなされた確率モデルのそれぞれについて、モデル選択の指標である情報量規準の値を計算し、該情報量規準の値が最も小さな確率モデルを最適なモデルとして選択するモデル選択手段と、を有し、

前記異常検出部は、前記モデル選択手段にて選択した最適なモデルの行列変数の確率分布に関する学習の結果に基づいて前記ネットワークの異常を検出する、請求の範囲第1項に記載のネットワーク異常検出装置。

[3] 前記構造候補列挙手段は、前記モデル選択手段にて最適なモデルの選択がなされると、該選択された最適なモデルの階層構造に類似した複数の異なる構造を前記候補として列挙する、請求の範囲第2項に記載のネットワーク異常検出装置。

[4] 前記異常検出部は、前記モデル選択手段にて選択された最適なモデルにより与えられる入力データの、前記ネットワークが通常の状態における入力データとの差を示す異常度スコアを計算する異常度スコア計算手段を有する、請求の範囲第2項または第3項に記載のネットワーク異常検出装置。

[5] 前記異常度スコア計算手段は、前記異常度スコアが閾値を越えるか否かを判定し

、その判定結果を出力する、請求の範囲第4項に記載のネットワーク異常検出装置。

[6] 前記異常検出部は、前記モデル選択手段にて選択された最適なモデルに基づいて前記ネットワークの階層構造の変化を検出する構造変化検出手段を有する、請求の範囲第2項または第3項に記載のネットワーク異常検出装置。

[7] ネットワークの状態を階層構造の行列変数で表したデータを入力するコンピュータシステムにおいて行われるネットワーク異常検出方法であって、

データ分布学習部が、入力される前記データに基づいて、前記ネットワークの状態を前記行列変数の確率分布として学習し、

異常検出部が、前記データ分布学習部による学習の結果に基づいて、前記確率分布が前記ネットワークの通常の状態を示す分布から他の状態を示す分布に遷移した状態を前記ネットワークの異常として検出する、ネットワーク異常検出方法。

[8] 前記データ分布学習部による学習のステップは、

入力される前記データの階層構造に対応する候補として複数の異なる構造を列挙する第1のステップと、

前記第1のステップで列挙された構造のそれぞれについて、当該構造と同じ階層構造の行列変数を持つ確率モデルを生成する第2のステップと、

前記第2のステップで生成した確率モデルのそれぞれについて、該確率モデルの行列変数として与えられているパラメータを、入力される前記データに基づいて更新する第3のステップと、

前記第3のステップでパラメータの更新がなされた確率モデルのそれぞれについて、モデル選択の指標である情報量規準の値を計算し、該情報量規準の値が最も小さな確率モデルを最適なモデルとして選択する第4のステップを含み、

前記異常検出部による異常検出のステップは、前記第4のステップで選択した前記最適なモデルの行列変数の確率分布に関する学習の結果に基づいて前記ネットワークの異常を検出するステップである、請求の範囲第7項に記載のネットワーク異常検出方法。

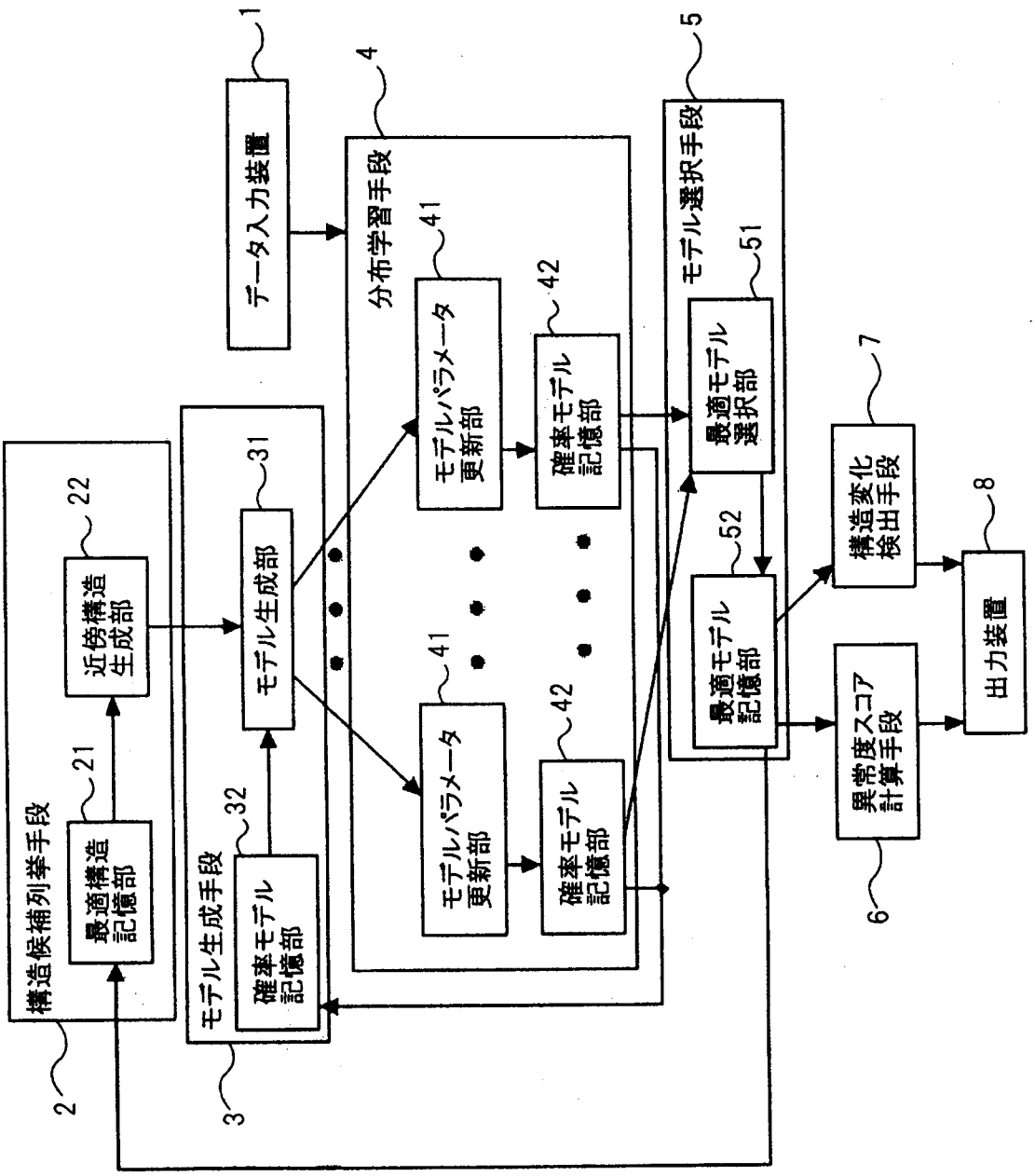
[9] 前記第1のステップは、前記第4のステップで選択された最適なモデルの階層構造に類似した複数の異なる構造を前記候補として列挙するステップである、請求の範囲

第8項に記載のネットワーク異常検出方法。

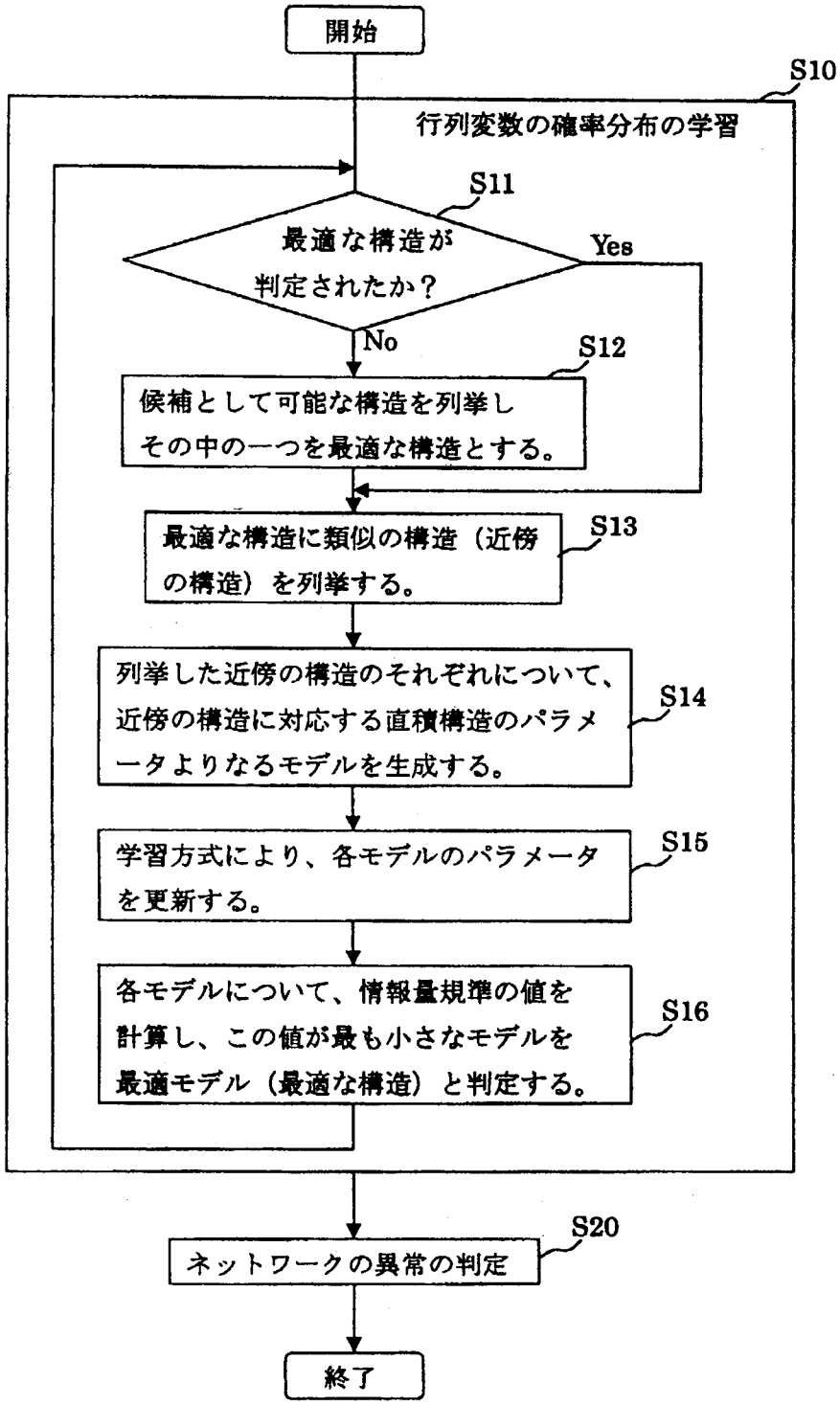
[10] 前記異常検出部による異常検出のステップは、前記第4のステップで選択された最適なモデルにより与えられる入力データの、前記ネットワークが通常の状態における入力データとの差を示す異常度スコアを計算し、該異常度スコアの計算結果に基づいて前記ネットワークの異常を検出するステップを含む、請求の範囲第8項または第9項に記載のネットワーク異常検出方法。

[11] 前記異常検出部による異常検出のステップは、前記第4のステップで選択された最適なモデルに基づいて前記ネットワークの階層構造の変化を検出し、該構造変化の検出結果に基づいて前記ネットワークの異常を検出するステップを含む、請求の範囲第8項または第9項に記載のネットワーク異常検出方法。

[図1]


1
データ入力装置
4
分布学習手段
41
モデルパラメータ更新部
42
確率モデル記憶部
5
モデル選択手段
51
最適モデル選択部
52
最適モデル記憶部
7
構造変化検出手段
8
出力装置
6
異常度スコア計算手段
2
構造候補列挙手段
21
最適構造記憶部
22
近傍構造生成部
3
モデル生成手段
31
モデル生成部
32
確率モデル記憶部

[図2]


開始
S10
行列変数の確率分布の学習
S11
最適な構造が判定されたか？
Yes
No
S12
候補として可能な構造を列挙しその中の一つを最適な構造とする。
最適な構造に類似の構造（近傍の構造）を列挙する。
S13
列挙した近傍の構造のそれぞれについて、近傍の構造に対応する直積構造のパラメータよりなるモデルを生成する。
S14
学習方式により、各モデルのパラメータを更新する。
S15
各モデルについて、情報量規準の値を計算し、この値が最も小さなモデルを最適モデル（最適な構造）と判定する。
S16
S20
ネットワークの異常の判定
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/050318

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/56(2006.01)i, *G06F11/30*(2006.01)i, *G06F11/34*(2006.01)i, *G06F13/00*(2006.01)i, *H04L12/24*(2006.01)i, *H04L12/26*(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)
H04L12/56, G06F11/30, G06F11/34, G06F13/00, H04L12/24, H04L12/26

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009
Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2005-216066 A (International Business Machines Corp.), 11 August, 2005 (11.08.05), Par. Nos. [0022] to [0127]; Figs. 1 to 10 & US 2005/0193281 A1	1-11
Y	Akira YAMADA, "Characterization and Anomaly Detection for Network Log Using Attribute Oriented Induction", Transactions of Information Processing Society of Japan, Vol.47, No.8, IPSJ Journal, 15 August, 2006 (15.08.06), Vol.47, pages 2488 to 2498	1-11
Y	JP 2005-141601 A (NEC Corp.), 02 June, 2005 (02.06.05), Par. Nos. [0064] to [0206]; all drawings & US 2005/0102122 A1 & EP 1530149 A2	2-6,8-11

☒ 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
30 January, 2009 (30.01.09)	10 February, 2009 (10.02.09)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/050318

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 06-037782 A (Hitachi Cable, Ltd.), 10 February, 1994 (10.02.94), Par. Nos. [0010] to [0023]; Figs. 1 to 3 (Family: none)	1-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０５０３１８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/56(2006.01)i, G06F11/30(2006.01)i, G06F11/34(2006.01)i, G06F13/00(2006.01)i, H04L12/24(2006.01)i, H04L12/26(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/56, G06F11/30, G06F11/34, G06F13/00, H04L12/24, H04L12/26

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００９年
日本国実用新案登録公報	１９９６－２００９年
日本国登録実用新案公報	１９９４－２００９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2005-216066 A（インターナショナル・ビジネス・マシーンズ・コーポレーション）2005.08.11, 【0022】－【0127】、【図1】－【図10】 & US 2005/0193281 A1	1-11

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
３０．０１．２００９	１０．０２．２００９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｘ　３８６２
齋藤　浩兵
電話番号　０３－３５８１－１１０１　内線　３５９６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	山田　明　AKIRA　YAMADA, 属性指向帰納によるネットワークログの特徴抽出と異常検知　Characterization and Anomaly Detection for Network Log Using Attribute Oriented Induction, 情報処理学会論文誌　第４７巻　第８号　IPSJ Journal, 2006.08.15, 第47巻, 第2488-2498頁	1-11
Y	JP 2005-141601 A（日本電気株式会社）2005.06.02, 【0064】－【0206】、全図 ＆ US　2005/0102122 A1 ＆ EP　1530149 A2	2-6,8-11
A	JP 06-037782 A（日立電線株式会社）1994.02.10, 【0010】－【0023】、【図1】－【図3】（ファミリーなし）	1-11