

(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
2023年1月19日(19.01.2023)



(10) 国際公開番号

WO 2023/286172 A1

(51) 国際特許分類:

H04L 12/70 (2013.01)

(21) 国際出願番号: PCT/JP2021/026340

(22) 国際出願日: 2021年7月13日(13.07.2021)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

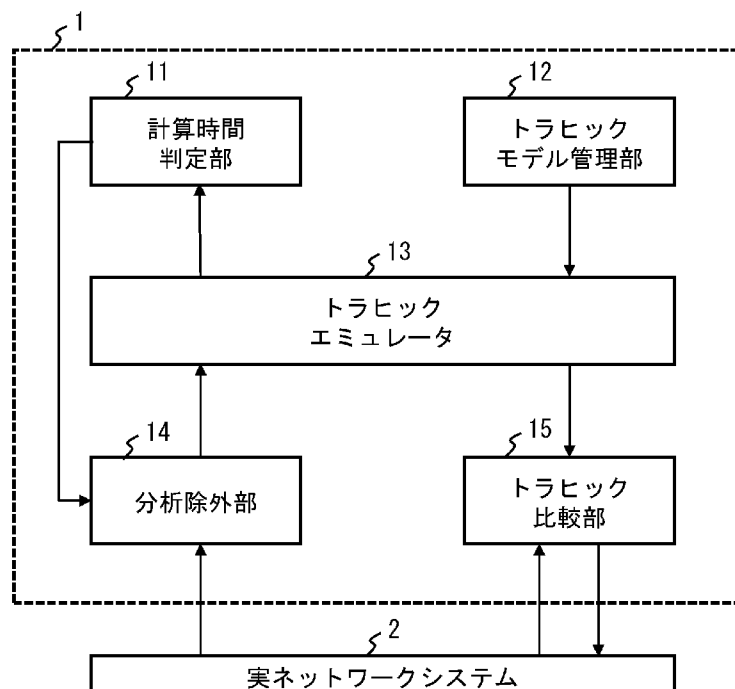
(72) 発明者: 服部 恭太 (HATTORI, Kyota); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP). 郡川 智洋(KORIKAWA, Tomohiro); 〒1808585

東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP). 大和田 英成(OWADA, Hidenari); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP). 清水 雅史(SHIMIZU, Masafumi); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP). 高谷 直樹(TAKAYA, Naoki); 〒1808585 東京都武蔵野市緑町3丁目9-1 1 N T T 知的財産センタ内 Tokyo (JP).

(74) 代理人: 特許業務法人磯野国際特許商標事務所(ISONO INTERNATIONAL PATENT OFFICE, P.C.); 〒1050001 東京都港区虎ノ門一丁目1番18号 ヒューリック虎ノ門ビル Tokyo (JP).

(54) Title: TRAFFIC ANALYSIS DEVICE, TRAFFIC ANALYSIS METHOD, AND TRAFFIC ANALYSIS PROGRAM

(54) 発明の名称: トラヒック分析装置、トラヒック分析方法、および、トラヒック分析プログラム



- 2 Real network system
11 Calculation time assessment unit
12 Traffic model management unit
13 Traffic emulator
14 Analysis exclusion unit
15 Traffic comparison unit

(57) Abstract: This traffic analysis device (1) comprises: a traffic emulator (13) for mirroring each element of traffic in a real network system (2) at the present time of day into a virtual space and executing protocol control of each element of the traffic in the virtual space to thereby calculate the status of the traffic in the real network system (2) at the next time of day; and an analysis exclusion unit (14) for excluding, from the calculation object of the traffic emulator (13) with respect to each element of mirrored traffic, any traffic for which the calculation result of the traffic emulator (13) is predicted not to be obtainable by the next time of day.

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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).

添付公開書類:

一 国際調査報告(条約第21条(3))

(57) 要約: トラヒック分析装置(1)は、現時刻における実ネットワークシステム(2)上の各トラヒックを仮想空間上にミラーリングし、各トラヒックのプロトコル制御を仮想空間上で実行することで、次時刻における実ネットワークシステム(2)上のトラヒックの状態を計算するトラヒックエミュレータ(13)と、ミラーリングされた各トラヒックについて、トラヒックエミュレータ(13)の計算結果が次時刻までに得られないと予測されるトラヒックを、トラヒックエミュレータ(13)の計算対象から除外する分析除外部(14)と、を有する。

明 細 書

発明の名称：

トラヒック分析装置、トラヒック分析方法、および、トラヒック分析プログラム

技術分野

[0001] 本発明は、トラヒック分析装置、トラヒック分析方法、および、トラヒック分析プログラムに関する。

背景技術

[0002] 将来のトラヒック量を予測する技術が提案されている。例えば、特許文献 1 には、将来のユーザトラヒック量を予測し、通信サービスに必要な帯域設備量を算出する通信帯域算出装置が記載されている。これにより、過不足のない通信リソースの設備量を算出することで、通信サービスの供給者の経済性を向上させる。

先行技術文献

特許文献

[0003] 特許文献1：特開 2 0 2 0 - 1 5 0 5 2 4 号公報

発明の概要

発明が解決しようとする課題

[0004] 将来のトラヒック量を予測する技術を、不正通信の検知に応用する場合を検討する。不正通信の検知には、特許文献 1 のようなトラヒック量という大まかな予測値よりも、個々のトラヒックをフロー単位で細かく予測するトラヒックエミュレーションが有効である。

トラヒックエミュレータは、現時刻 (t) の実網を流れる各トラヒックを仮想空間上に模擬 (ミラーリング) し、現時刻 (t) の各トラヒックを起点として、次時刻 (t+1) の仮想空間上のプロトコル規約に適合した (理想的な) トラヒック状態を予測する。

[0005] なお、現時刻 (t) とは実網を観測するターゲット時刻であり、次時刻 ($t+1$) とは現時刻の次のタイミングで実網を観測するターゲット時刻である。そして、トラヒックエミュレータは、次時刻の理想的なトラヒック状態と、次時刻の実空間上のユーザトラヒック状態とを比較することで、プロトコル規約に違反したユーザトラヒックを検出できる。

[0006] しかし、大容量の基幹ネットワーク上を流れるトラヒック量は、1波長あたり10[Gbps], 100[Gbps]など大量であるため、トラヒックエミュレータが計算対象とするトラヒックのフロー数も膨大である。そのため、現時刻 (t) から次時刻 ($t+1$) までの計算間隔を短縮化するほど（例えば10秒ごと）、トラヒックエミュレータには非常に高い（リアルタイムな）計算能力が求められる。

[0007] よって、いくらトラヒックエミュレータが膨大なトラヒックを正しく計算できたとしても、計算完了時刻が次時刻 ($t+1$) に間に合わなければ、その計算結果を不正通信の検知には応用できなくなってしまう。

なお、特許文献1のような従来のトラヒック量を予測する技術では、このような厳しい計算時間の制約が存在しなかったため、そもそも計算結果が次時刻までに得られないトラヒックに対する計算コストを低減することは検討されてこなかった。

[0008] そこで、本発明は、現時刻 (t) のトラヒック状態から次時刻 ($t+1$) のトラヒック状態を予測するときに、適切に計算コストを低減させることを主な課題とする。

課題を解決するための手段

[0009] 前記課題を解決するために、本発明のトラヒック分析装置は、以下の特徴を有する。

本発明は、現時刻における実ネットワークシステム上の各トラヒックを仮想空間上にミラーリングし、各トラヒックのプロトコル制御を仮想空間上で実行することで、次時刻における前記実ネットワークシステム上のトラヒックの状態を計算するトラヒックエミュレータと、

ミラーリングされた各トラヒックについて、前記トラヒックエミュレータの計算結果が次時刻までに得られないと予測されるトラヒックを、前記トラヒックエミュレータの計算対象から除外する計算除外部と、を有することを特徴とする。

発明の効果

[0010] 本発明によれば、現時刻（ t ）のトラヒック状態から次時刻（ $t+1$ ）のトラヒック状態を予測するときに、適切に計算コストを低減させることができる。

図面の簡単な説明

[0011] [図1]本実施形態に係わるトラヒック分析装置の構成図である。

[図2]本実施形態に係わるトラヒック分析装置のハードウェア構成図である。

[図3]本実施形態に係わるトラヒック分析装置の処理の概要を示す説明図である。

[図4]本実施形態に係わるトラヒック分析装置の処理を示すシーケンス図である。

[図5]本実施形態に係わるトラヒック分析装置の効果を主張するための比較テーブルである。

発明を実施するための形態

[0012] 以下、本発明の一実施形態について、図面を参照して詳細に説明する。

[0013] 図1は、トラヒック分析装置1の構成図である。

トラヒック分析装置1は、計算時間判定部11と、トラヒックモデル管理部12と、トラヒックエミュレータ13と、分析除外部14と、トラヒック比較部15と有する。

実ネットワークシステム2は、トラヒック分析装置1の分析対象となる実際のネットワークシステムである。

[0014] トラヒックエミュレータ13は、現時刻（ t ）における実ネットワークシステム2上の各トラヒックを仮想空間上にミラーリングし、各トラヒックのプロトコル制御を仮想空間上で実行することで、次時刻（ $t+1$ ）における実ネッ

トワークシステム 2 上のトラヒックの状態を計算する。

[0015] 計算時間判定部 1 1（計算除外部）は、現時刻でミラーリングしたトラヒックをトラヒックエミュレータ 1 3 に入力してから、次時刻のトラヒックの状態を出力するまでのトラヒックエミュレータ 1 3 の計算時間をもとに、計算結果が次時刻までに得られるか否かを判定する。計算時間判定部 1 1 は、判定結果を分析除外部 1 4 に出力する。

分析除外部 1 4（計算除外部）は、実ネットワークシステム 2 からミラーリングする各トラヒックについて、トラヒックエミュレータ 1 3 の計算結果が次時刻までに得られないと予測されるトラヒックを、トラヒックエミュレータ 1 3 の計算対象から除外する。

[0016] 分析除外部 1 4 は、例えば、以下のいずれかの手法により、計算対象から除外するトラヒックを決定する。

（手法 1：事前見積もり）各トラヒックのプロトコル制御を仮想空間上で実行する処理量と、トラヒックエミュレータ 1 3 が動作する計算機の処理能力とを参照して、トラヒックエミュレータ 1 3 の計算に要する予想時間を見積もり、現時刻から予想時間分だけ将来の時刻が次時刻を超過したトラヒックを、トラヒックエミュレータ 1 3 の計算対象から除外する。

（手法 2：計算中の進捗度合い確認）現在までにトラヒックエミュレータ 1 3 が計算したトラヒックの状態の進捗度合いと、現在から次時刻までの残り時間とをもとに、トラヒックエミュレータ 1 3 の計算結果が次時刻までに得られないと予測されるトラヒックを、トラヒックエミュレータ 1 3 の計算対象から除外する。

[0017] トラヒックモデル管理部 1 2 には、トラヒックエミュレータ 1 3 が各トラヒックのプロトコル制御を仮想空間上で実行するための、プロトコルに規定された制御の情報が、トラヒックモデルとして管理されている。トラヒックエミュレータ 1 3 はトラヒックモデル管理部 1 2 からトラヒックのプロトコルごとにトラヒックモデルを読み出して、トラヒックの状態を計算するために使用する。

トラヒック比較部 15 は、次時刻における実ネットワークシステム 2 上のトラヒックの状態が、そのトラヒックのプロトコルで規定された動作を満たさない場合に、その満たさないトラヒックを異常なトラヒックとして実ネットワークシステム 2 に通知する。

[0018] 図 2 は、トラヒック分析装置 1 のハードウェア構成図である。

トラヒック分析装置 1 は、CPU 901 と、RAM 902 と、ROM 903 と、HDD 904 と、通信 I/F 905 と、入出力 I/F 906 と、メディア I/F 907 とを有するコンピュータ 900 として構成される。

通信 I/F 905 は、外部の通信装置 915 と接続される。入出力 I/F 906 は、入出力装置 916 と接続される。メディア I/F 907 は、記録媒体 917 からデータを読み書きする。さらに、CPU 901 は、RAM 902 に読み込んだプログラム（アプリケーションや、その略のアプリとも呼ばれる）を実行することにより、各処理部を制御する。そして、このプログラムは、通信回線を介して配布したり、CD-ROM 等の記録媒体 917 に記録して配布したりすることも可能である。

[0019] 図 3 は、トラヒック分析装置 1 の処理の概要を示す説明図である。

状態 101 は、現時刻 (t) の時点でトラヒックエミュレータ 13 がミラーリングした 4 つのトラヒック VA, VB, VC, VD それぞれの計算に要する予想時間を、棒グラフ表示したものである。

トラヒック VA, VB は次時刻 (t+1) までに計算が間に合うが、トラヒック VC, VD は次時刻 (t+1) までに計算が間に合わないことが、現時刻 (t) の時点で予想された。

[0020] 状態 102 は、トラヒック VA, VB, VC の計算時間を、棒グラフ表示したものである。

ここで、計算時間判定部 11 は、状態 101 において計算が間に合わないトラヒック VC, VD を今後の計算対象から除外する候補とした。分析除外部 14 は、優先度の高いトラヒック VC を計算対象として残しつつ、優先度の低いトラヒック VD を計算対象から除外した。

よって、状態102では、トラヒックVDの計算を中断して得られる計算能力の余力を、トラヒックVCに割り当てることで、トラヒックVCは予想時間よりも早く計算が完了した（波線縦線の時点）。

このように、トラヒック分析装置1は、ミラーリングしたトラヒックの一部を計算対象から早期に除外することで、次時刻（ $t+1$ ）までに計算が間に合うトラヒックを増やすことができる。

[0021] 図4は、トラヒック分析装置1の処理を示すシーケンス図である。

S101として、トラヒックエミュレータ13は、現時刻における実トラヒック（またはその状態を示す情報）を実ネットワークシステム2から受信すると、その実トラヒックをS106の除外処理の候補として、分析除外部14に通知する。

[0022] S102aとして、トラヒックエミュレータ13は、S101で受信した現時刻における実トラヒックの Protokol 情報を検索キーとして、そのトラヒックの次時刻の Protokol 動作内容を、トラヒックモデル管理部12から取得する。

S102bとして、トラヒック比較部15は、S102aで取得された Protokol 動作内容を規定するための情報（Protokol 規定情報）を、S112の異常判定処理のためにトラヒックモデル管理部12から取得する。

[0023] トラヒックエミュレータ13は、実ネットワークシステム2上のトラヒックのフローごとの Protokol 動作を仮想空間上で模擬実行することで、現時刻のトラヒック状態から、次時刻のトラヒック状態を計算する。この計算過程は、S103aの計算開始→S103bの計算中→S103cの計算完了の順に遷移する。

S103aの計算開始時点では、トラヒックエミュレータ13は、S101で通知された現時刻における実トラヒックを、仮想空間上にミラーリングする。その後、トラヒックエミュレータ13は、仮想空間上の各トラヒックについて、S102aで取得した Protokol 動作内容を反映させることで、仮想空間のネットワーク条件が変更された次時刻のトラヒック状態に遷移さ

せる計算を開始する。

[0024] また、S 1 0 3 a の計算開始時点では、トラヒックエミュレータ 1 3 は、トラヒックごとの次時刻のトラヒック状態を計算するための予想時間をトラヒックごとに見積もる。この見積処理は、例えば、(予想時間) = (現時刻から次時刻までプロトコル動作内容を反映させるための計算量) ÷ (トラヒックエミュレータ 1 3 が動作する計算機の計算能力) であり、計算機の計算能力は、CPUのコア数やクロック数などから求める。

予想時間の終点は、S 1 0 3 c の計算完了時刻である。予想時間の起点は、S 1 0 1 で現時刻における実トラヒックを受信した時刻としてもよい、S 1 0 3 a の計算開始時刻としてもよい。

[0025] S 1 0 4 として、トラヒックエミュレータ 1 3 は、見積もったトラヒックごとの予想時間を、計算時間判定部 1 1 に通知する。

S 1 0 5 a として、計算時間判定部 1 1 は、判定式「現時刻 (t) + 予想時間 < 次時刻 (t+1)」により、現時刻 (t) から S 1 0 4 の予想時間分だけ将来の時刻が、次時刻 (t+1) を超過したか否かを判定する。

つまり、次時刻 (t+1) を超過したと S 1 0 5 a で判定されたトラヒックは、次時刻 (t+1) までにトラヒックエミュレータ 1 3 の計算が間に合わないことが事前に予測される。

[0026] S 1 0 5 b として、計算時間判定部 1 1 は、計算が間に合わない (S 1 0 5 a でYesの) トラヒックをトラヒックエミュレータ 1 3 の計算対象から除外する候補となる除外候補トラヒックとして、分析除外部 1 4 に通知する。

[0027] S 1 0 6 として、分析除外部 1 4 は、S 1 0 5 b で通知された除外候補トラヒックの一部または全部を、トラヒックエミュレータ 1 3 の計算対象から除外することを決定する。ここで、分析除外部 1 4 は、実際にトラヒックを計算対象から除外するか否か、および、どの順序で除外したトラヒックの計算を中断させるかについて、以下に示す方法を用いてもよい。

(除外方法 1) トラヒックを送受信する端末ごとに次時刻における優先度を事前に決めておき、その優先度が低い端末のトラヒックほど、計算対象か

ら除外されやすくする、または、早い順序でトラヒックの計算を中断させる。

[0028] (除外方法2) 現在までに計算されたトラヒック状態と、S102bのプロトコル規定情報とを照合し、プロトコル規定情報に合致しない(プロトコル規定に従った動作をしていない、または、プロトコル規定に従っていない動作をする)トラヒックが発見された場合、計算対象から除外されやすくする、または、早い順序でトラヒックの計算を中断させる。

[0029] (除外方法3) 現在までに計算されたトラヒック状態の進捗度合いが少ないトラヒックほど、計算対象から除外されやすくする、または、早い順序でトラヒックの計算を中断させる。例えば、次時刻まで計算できた状態を100%とすると、20%計算済のトラヒックAを先に除外し、60%計算済のトラヒックAを後に除外する。

[0030] S107として、分析除外部14は、S106で決定したトラヒックを計算対象から除外する旨の指示をトラヒックエミュレータ13に通知する。トラヒックエミュレータ13は、S103bで計算中のトラヒックから、S107の除外指示を受けたトラヒックの計算を中断(または強制終了)する。

これにより、トラヒックエミュレータ13が動作する計算機の計算能力に生まれた余力を、除外しなかった他のトラヒックの計算に活用できるので、結果として、次時刻までに計算完了(S103c)となるトラヒックのフロ一数を増やすことができる。

[0031] なお、計算時間判定部11は、S105aとして、トラヒックの計算前に見積もった予想時間をもとに、次時刻までの時間超過を判定していた。一方、計算時間判定部11は、S105aの代わりに、現在までに計算されたトラヒック状態の進捗度合いと、次時刻までの残り時間とを比較することで、次時刻までの時間超過を判定してもよい。

[0032] 例えば、現時刻(t)=10時0分、次時刻(t+1)=10時10分、計算中の現在時刻=10時5分(50%経過)とする。

トラヒックAの計算は進捗度合い=75%とする。現在時刻(50%経過)より

も速いペースで計算ができており、このまま計算を継続しても次時刻＝10時10分までに間に合うと予想され、計算時間判定部11は、トラヒックAの計算を除外しない（S105aでNo）と判断する。

トラヒックBの計算は進捗度合い＝25%とする。現在時刻（50%経過）よりも遅いペースで計算が遅れている。よって、このまま計算を継続しても次時刻＝10時10分までに間に合わないと予想され、計算時間判定部11は、トラヒックBの計算を除外する（S105aでYes）と判断する。

[0033] S108として、トラヒックエミュレータ13は、計算が完了した（S103cでYes）次時刻における仮想空間上の仮想トラヒックをトラヒック比較部15に通知する。

以上、S101～S108までの各処理が、現時刻（t）から次時刻（t+1）までの期間に実行される。以下、S111以降は次時刻（t+1）以降に実行される処理である。

[0034] S111として、トラヒック比較部15は、次時刻（t+1）における実トラヒックを実ネットワークシステム2から受信すると、その実トラヒックと、S108で受信した次時刻における仮想トラヒックとを比較する。なお、比較結果が不一致なら、トラヒック比較部15は、次時刻（t+1）における実トラヒックは異常なトラヒックであるとみなす。

[0035] S112として、トラヒック比較部15は、S111の両トラヒックの比較結果として、以下の異常が存在するか否かを判定する。以下、TCP（Transmission Control Protocol）のプロトコル規定情報を例示する。TCPでは、ノードAからノードBに所定のシーケンス番号を含むデータ信号が送信された後、同じシーケンス番号を含む確認応答信号（Ack）がノードBからノードAに返信される動作を規定している。

[0036] （異常1）仮想トラヒックは存在するが、対応する実トラヒックが存在しない場合。例えば、仮想トラヒックにはデータ信号とAckとの組み合わせが存在するが、実トラヒックにはデータ信号だけが存在してAckが存在しない場合。この場合、ノードBがプロトコルの規定違反（Ackの返信義務の不履行）で

ある旨の異常を検出する。

- [0037] (異常2) 実トラヒックは存在するが、対応する仮想トラヒックが存在しない場合。例えば、データパケットの中に記載されたシーケンス番号とは全く関係のないACK番号(確認応答番号)を含んだACKを受信した場合。

なお、途中で欠落したデータパケットがあることを送信側に伝えるために、正しいACK番号は「最初のシーケンス番号+連続して正常に受信できたバイト数」として計算される。よって、シーケンス番号とは全く関係のないACK番号のACKは、不正なトラヒックである旨の異常を検出する。

- [0038] (異常3) 実トラヒックと仮想トラヒックとが互いにフローとしては対応するが、実トラヒックの状態と仮想トラヒックの状態とが不一致であり、かつ、実トラヒックの状態がS102bのプロトコル規定情報(シーケンス番号の一致ルール)に合致しない場合。

例えば、仮想トラヒックにはシーケンス番号=101のデータ信号とAckとの組み合わせが存在するが、実トラヒックにはシーケンス番号=101のデータ信号と、シーケンス番号=109のAckが存在する場合。この場合、実トラヒックの動作がプロトコルの規定違反(シーケンス番号の不一致)である旨の異常を検出する。

- [0039] S113として、トラヒック比較部15は、S111の比較結果や、S112の(異常1)～(異常3)で発見した実トラヒックに異常の旨(異常が存在するか否か、異常の原因は何かなど)を示す異常フラグを付与する。

S114として、トラヒック比較部15は、異常フラグを付与した次時刻の実トラヒックを実ネットワークシステム2に返信する。これにより、実ネットワークシステム2の各装置は、異常フラグが付与された実トラヒックを廃棄したり、異常フラグの内容を管理者の画面に表示したりするなどの異常対策を実行できる。

- [0040] 図5は、トラヒック分析装置1の効果を主張するための比較テーブルである。

比較テーブルの第1列(時刻)は、計算中の各状態の時刻を示す。

比較テーブルの第2列（実ネットワーク）は、実ネットワークシステム2上に存在する実トラヒックのリストである。実トラヒックの識別子（例えば「RTa(t)」）の1文字目は、実トラヒックのR(Real)または仮想トラヒックのV(Virtual)を付し、2文字目はトラヒックを示すT (Traffic) を付す。

また、実トラヒックの識別子の3文字目はフローの識別子 (a, b, c, d) を示し、その後には (t) など第1列の時刻の情報をカッコつきで示す。

[0041] 比較テーブルの第3列（仮想1）は、トラヒック分析装置1の計算能力が十分に供給される計算機環境（スーパーコンピュータなど）により、すべてのトラヒックが次時刻までに計算完了する場合の仮想トラヒックを示す。

比較テーブルの第4, 5列（仮想2, 3）は、トラヒック分析装置1の計算能力が限定的な計算機環境（一般のパソコンなど）により、一部のトラヒックが次時刻までに計算完了しない場合の仮想トラヒックを示す。第4列（仮想2）と第5列（仮想3）との違いは、図3に示した一部のトラヒックを計算対象から除外する処理を適用しない場合（仮想2）か、適用した場合（仮想3）かである。

[0042] 比較テーブルの第1行は、現時刻 (t) の実ネットワークシステム2上に存在する実トラヒックが、（仮想1, 2, 3）それぞれにミラーリングされている旨を示す。つまり、RTa(t)→VTa(t)、RTb(t)→VTb(t)、RTc(t)→VTc(t)、RTd(t)→VTd(t)という4組のミラーリングが行われる。

[0043] 比較テーブルの第2行は、次時刻 (t+1) のトラヒック状態を示す。実ネットワークシステム2からは、RTa(t+1), RTb(t+1), RTc(t+1)という正常トラヒックが残るが、異常トラヒックとして、RTd(t+1)が消え、RTe(t+1)が追加されたとする。

次時刻 (t+1) での（仮想1）は十分な計算能力により、VTa(t)→VTa(t+1)、VTb(t)→VTb(t+1)、VTc(t)→VTc(t+1)、VTd(t)→VTd(t+1)という4組のトラヒック状態を次時刻までに計算できる。よって、次時刻 (t+1) の第2列と第3列との比較により、以下のように異常トラヒックを検出できる。

・ RTa(t+1)=VTa(t+1) →正常トラヒック

- ・ $RTb(t+1)=VTb(t+1)$ →正常トラヒック
- ・ $RTc(t+1)=VTc(t+1)$ →正常トラヒック
- ・ $VTd(t+1)$ の不一致 →異常トラヒック
- ・ $RTe(t+1)$ の不一致 →異常トラヒック

[0044] 次時刻 (t+1) での (仮想 2) は不十分な計算能力により、 $VTa(t) \rightarrow VTa(t+1)$ 、 $VTb(t) \rightarrow VTb(t+1)$ という 2 組のトラヒック状態だけ次時刻までに計算した。よって、次時刻 (t+1) の第 2 列と第 4 列との比較により、以下のように異常トラヒックを検出できる。

- ・ $RTa(t+1)=VTa(t+1)$ →正常トラヒック
- ・ $RTb(t+1)=VTb(t+1)$ →正常トラヒック
- ・ $RTc(t+1)$ の不一致 →異常トラヒックであると誤検出
- ・ ($VTd(t+1)$ の不一致は検出できず)
- ・ $RTe(t+1)$ の不一致 →異常トラヒック

[0045] 次時刻 (t+1) での (仮想 3) は不十分な計算能力ではあるが、トラヒックを計算対象から除外する処理を適用した結果、 $VTa(t) \rightarrow VTa(t+1)$ 、 $VTb(t) \rightarrow VTb(t+1)$ 、 $VTc(t) \rightarrow VTc(t+1)$ という 3 組のトラヒック状態を次時刻までに計算できる。よって、次時刻 (t+1) の第 2 列と第 5 列との比較により、以下のように異常トラヒックを検出できる。

- ・ $RTa(t+1)=VTa(t+1)$ →正常トラヒック
- ・ $RTb(t+1)=VTb(t+1)$ →正常トラヒック
- ・ $RTc(t+1)=VTc(t+1)$ →正常トラヒック
- ・ ($VTd(t+1)$ の不一致は検出できず)
- ・ $RTe(t+1)$ の不一致 →異常トラヒック

つまり、(仮想 2) の誤検出は (仮想 3) では予防できている。

[0046] [効果]

本発明のトラヒック分析装置 1 は、現時刻における実ネットワークシステム 2 上の各トラヒックを仮想空間上にミラーリングし、各トラヒックのプロトコル制御を仮想空間上で実行することで、次時刻における実ネットワーク

システム2上のトラヒックの状態を計算するトラヒックエミュレータ13と、

ミラーリングされた各トラヒックについて、トラヒックエミュレータ13の計算結果が次時刻までに得られないと予測されるトラヒックを、トラヒックエミュレータ13の計算対象から除外する分析除外部14と、を有することを特徴とする。

[0047] これにより、現時刻(t)のトラヒック状態から次時刻(t+1)のトラヒック状態を予測するときに、計算結果が次時刻までに得られないと予測される無駄なトラヒックを計算から除外する。よって、無駄なトラヒックの分については、適切に計算コストを低減できるので、無駄に消費されていた計算リソースを、次時刻までに計算可能な別のトラヒックに効率的に割り当て可能となる。よって、次時刻までに計算できるトラヒックを増加できる。

[0048] 本発明は、分析除外部14が、各トラヒックのプロトコル制御を仮想空間上で実行する処理量と、トラヒックエミュレータ13が動作する計算機の処理能力とを参照して、トラヒックエミュレータ13の計算に要する予想時間を見積もり、現時刻から予想時間分だけ将来の時刻が次時刻を超過したトラヒックを、トラヒックエミュレータ13の計算対象から除外することを特徴とする。

[0049] これにより、計算対象から除外するトラヒックを事前に見積もることで、早期に無駄なトラヒックを計算から除外できる。

[0050] 本発明は、分析除外部14が、現在までにトラヒックエミュレータ13が計算したトラヒックの状態の進捗度合いと、現在から次時刻までの残り時間とをもとに、トラヒックエミュレータ13の計算結果が次時刻までに得られないと予測されるトラヒックを、トラヒックエミュレータ13の計算対象から除外することを特徴とする。

[0051] これにより、計算対象から除外するトラヒックを計算途中で検出することで、高精度に無駄なトラヒックを計算から除外できる。

[0052] 本発明は、トラヒック分析装置1が、さらに、トラヒック比較部15を有

しており、

トラヒック比較部 1 5 が、トラヒックエミュレータ 1 3 が算出した次時刻におけるトラヒックの状態と、次時刻における実ネットワークシステム 2 上のトラヒックの状態とを比較し、不一致のトラヒックを異常なトラヒックとして実ネットワークシステム 2 に通知することを特徴とする。

[0053] これにより、次時刻における実ネットワークシステム 2 上のトラヒックから、不正通信を検出できる。

[0054] 本発明は、トラヒック比較部 1 5 が、次時刻における実ネットワークシステム 2 上のトラヒックの状態が、そのトラヒックのプロトコルで規定された動作を満たさない場合に、その満たさないトラヒックを異常なトラヒックとして実ネットワークシステム 2 に通知することを特徴とする。

[0055] これにより、所定の制御メッセージの送信を省略できるなど、プロトコルで規定された動作に解釈の幅がある場合でも、適切に不正通信を検出できる。

符号の説明

- [0056]
- | | |
|-----|----------------|
| 1 | トラヒック分析装置 |
| 2 | 実ネットワークシステム |
| 1 1 | 計算時間判定部（計算除外部） |
| 1 2 | トラヒックモデル管理部 |
| 1 3 | トラヒックエミュレータ |
| 1 4 | 分析除外部（計算除外部） |
| 1 5 | トラヒック比較部 |

請求の範囲

- [請求項1] 現時刻における実ネットワークシステム上の各トラヒックを仮想空間上にミラーリングし、各トラヒックのプロトコル制御を仮想空間上で実行することで、次時刻における前記実ネットワークシステム上のトラヒックの状態を計算するトラヒックエミュレータと、
- ミラーリングされた各トラヒックについて、前記トラヒックエミュレータの計算結果が次時刻までに得られないと予測されるトラヒックを、前記トラヒックエミュレータの計算対象から除外する計算除外部と、を有することを特徴とする
- トラヒック分析装置。
- [請求項2] 前記計算除外部は、各トラヒックのプロトコル制御を仮想空間上で実行する処理量と、前記トラヒックエミュレータが動作する計算機の処理能力とを参照して、前記トラヒックエミュレータの計算に要する予想時間を見積もり、現時刻から予想時間分だけ将来の時刻が次時刻を超過したトラヒックを、前記トラヒックエミュレータの計算対象から除外することを特徴とする
- 請求項1に記載のトラヒック分析装置。
- [請求項3] 前記計算除外部は、現在までに前記トラヒックエミュレータが計算したトラヒックの状態の進捗度合いと、現在から次時刻までの残り時間とをもとに、前記トラヒックエミュレータの計算結果が次時刻までに得られないと予測されるトラヒックを、前記トラヒックエミュレータの計算対象から除外することを特徴とする
- 請求項1に記載のトラヒック分析装置。
- [請求項4] 前記トラヒック分析装置は、さらに、トラヒック比較部を有しており、
- 前記トラヒック比較部は、前記トラヒックエミュレータが算出した次時刻におけるトラヒックの状態と、次時刻における前記実ネットワークシステム上のトラヒックの状態とを比較し、不一致のトラヒック

を異常なトラヒックとして前記実ネットワークシステムに通知することを特徴とする

請求項 1 ないし請求項 3 のいずれか 1 項に記載のトラヒック分析装置。

[請求項 5] 前記トラヒック比較部は、次時刻における前記実ネットワークシステム上のトラヒックの状態が、そのトラヒックのプロトコルで規定された動作を満たさない場合に、その満たさないトラヒックを異常なトラヒックとして前記実ネットワークシステムに通知することを特徴とする

請求項 4 に記載のトラヒック分析装置。

[請求項 6] トラヒック分析装置は、トラヒックエミュレータと、計算除外部と、を有しており、

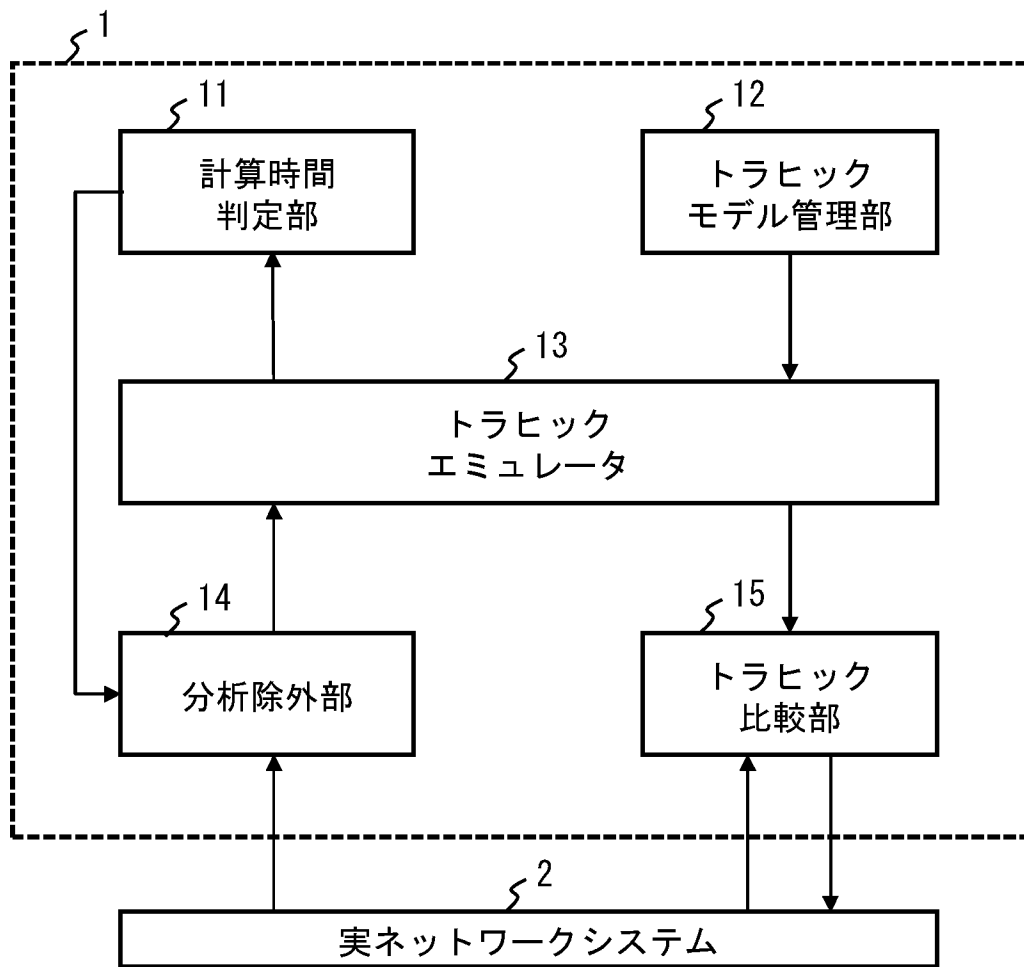
前記トラヒックエミュレータは、現時刻における実ネットワークシステム上の各トラヒックを仮想空間上にミラーリングし、各トラヒックのプロトコル制御を仮想空間上で実行することで、次時刻における前記実ネットワークシステム上のトラヒックの状態を計算し、

前記計算除外部は、ミラーリングされた各トラヒックについて、前記トラヒックエミュレータの計算結果が次時刻までに得られないと予測されるトラヒックを、前記トラヒックエミュレータの計算対象から除外することを特徴とする

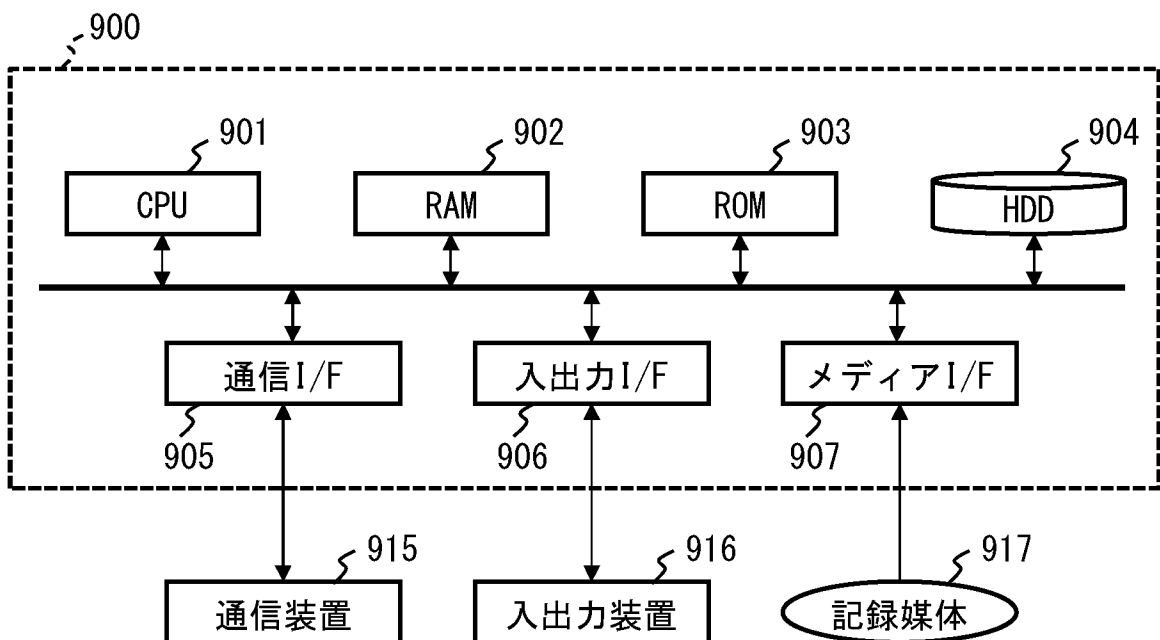
トラヒック分析方法。

[請求項 7] コンピュータを、請求項 1 ないし請求項 5 のいずれか 1 項に記載のトラヒック分析装置として機能させるためのトラヒック分析プログラム。

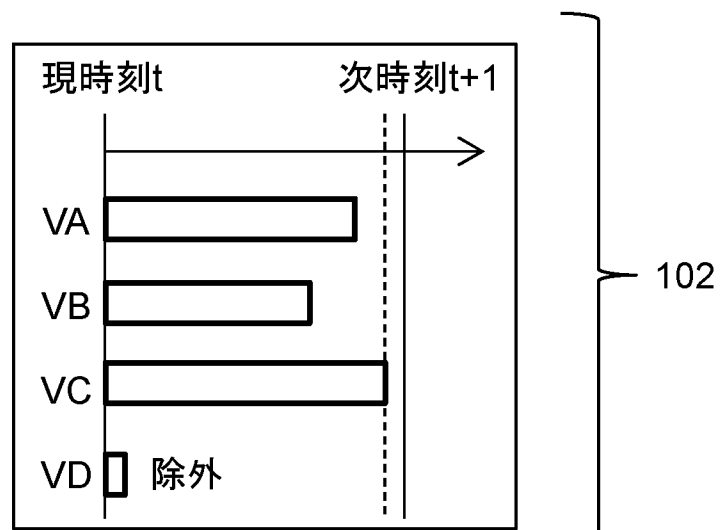
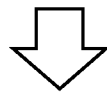
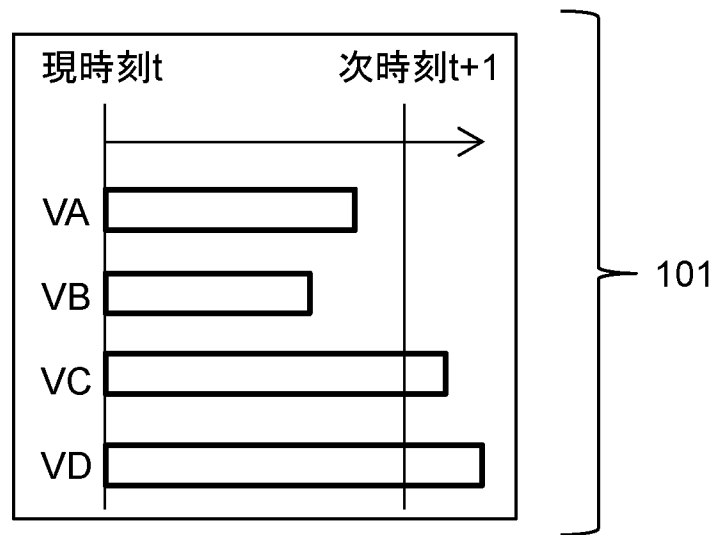
[図1]



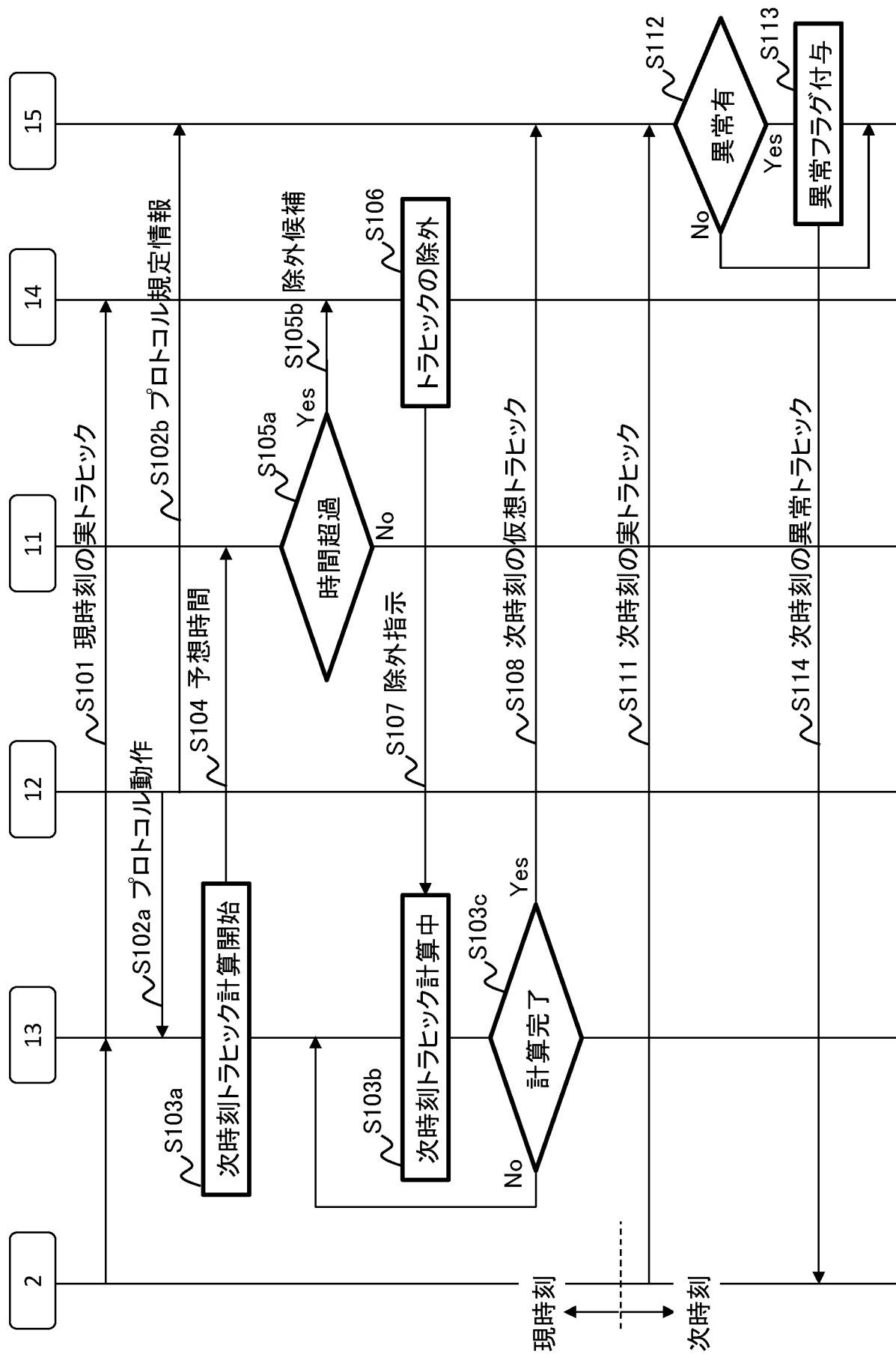
[図2]



[図3]



[図4]



[図5]

時刻	実ネットワーク	仮想ネットワーク		
		仮想 1	仮想 2	仮想 3
現時刻 (t)	RTa (t) RTb (t) RTc (t) RTd (t)	VTa (t) VTb (t) VTc (t) VTd (t)	VTa (t) VTb (t) VTc (t) VTd (t)	VTa (t) VTb (t) VTc (t) VTd (t)
次時刻 (t+1)	RTa (t+1) RTb (t+1) RTc (t+1) RTe (t+1)	VTa (t+1) VTb (t+1) VTc (t+1) VTd (t+1)	VTa (t+1) VTb (t+1)	VTa (t+1) VTb (t+1) VTc (t+1)
:	:	:	:	:
時刻 (t+n)		VTa (t+n) VTb (t+n) VTc (t+n) VTd (t+n)	VTa (t+n) VTb (t+n) VTc (t+1) VTd (t+1)	VTa (t+n) VTb (t+n) VTc (t+n) VTd (t+n)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/026340

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/70(2013.01)i

FI: H04L12/70 100Z

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)

H04L12/70

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

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

IEEE Xplore

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-200773 A (NTT DOCOMO INC) 15 July 2004 (2004-07-15) paragraphs [0014]-[0021], fig. 1	1-7
A	和久井拓 ほか, LSTM-RNN を用いたインターネットバックボーン汎用異常検知手法 GAMPAL の改良, 情報処理学会 コンピュータセキュリティシンポジウム 2020 論文集, 19 October 2020, pp. 891-898, section 3, (WAKUI, Taku et al. Improvement of GAMPAL: A General-Purpose Anomaly Detection Mechanism for Internet Backbone Using LSTM-RNN.), non-official translation (Proceedings of Computer Security Symposium 2020 of Information Processing Society of Japan)	1-7
A	US 2006/0109793 A1 (KIM, H. K. et al.) 25 May 2006 (2006-05-25) paragraphs [0027]-[0032], fig. 2	1-7



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
02 September 2021 (02.09.2021)

Date of mailing of the international search report
14 September 2021 (14.09.2021)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/026340

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2004-200773 A	15 Jul. 2004	US 2004/0170129 A1 paragraphs [0030]- [0043], fig. 1 EP 1432205 A2 CN 1514623 A	
US 2006/0109793 A1	25 May 2006	KR 10-2006-0058788 A page 3, line 38 to page 4, line 12, fig. 2	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 12/70(2013.01)i FI: H04L12/70 100Z		
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）） H04L12/70		
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 1971-2021年 日本国実用新案登録公報 1996-2021年 日本国登録実用新案公報 1994-2021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） IEEE Xplore		
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 請求項の番号
A	JP 2004-200773 A（株式会社エヌ・ティ・ティ・ドコモ）15.07.2004（2004-07-15） 段落 [0014] - [0021]，図1	1-7
A	和久井拓 ほか，LSTM-RNNを用いたインターネットバックボーン汎用異常検知手法GAMPALの改良，情報処理学会 コンピュータセキュリティシンポジウム2020 論文集，2020.10.19，pp. 891-898 第3節	1-7
A	US 2006/0109793 A1 (KIM, H.K. et al.) 25.05.2006（2006-05-25） 段落 [0027] - [0032]，図2	1-7
☐ 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、一般的な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抵触するものではなく、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 02.09.2021		国際調査報告の発送日 14.09.2021
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 平井 嗣人 5X 1160 電話番号 03-3581-1101 内線 3596

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2021/026340

引用文献			公表日	パテントファミリー文献	公表日
JP	2004-200773	A	15.07.2004	US 2004/0170129 A1 段落 [0 0 3 0] - [0 0 4 3] , 図 1 EP 1432205 A2 CN 1514623 A	
US	2006/0109793	A1	25.05.2006	KR 10-2006-0058788 A 第 3 ページ第 3 8 行 - 第 4 ページ第 1 2 行, 図 2	