

(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
2020年4月30日(30.04.2020)



(10) 国際公開番号

WO 2020/084908 A1

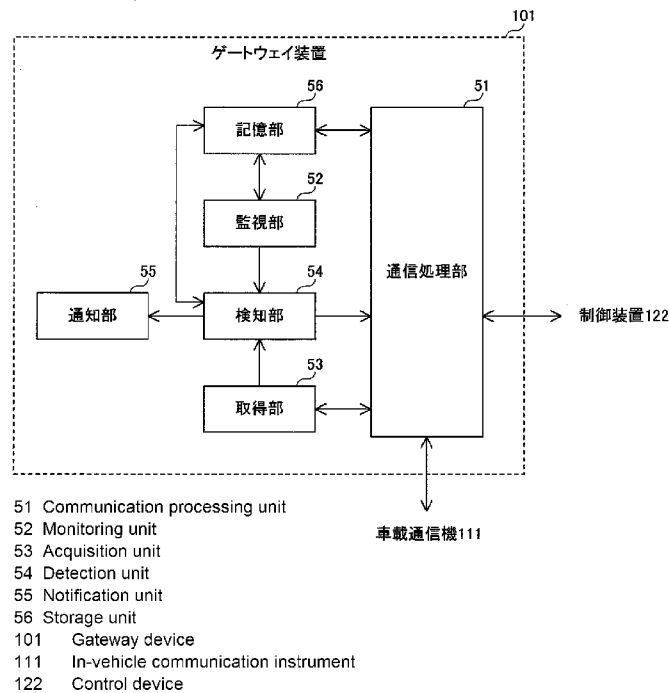
- (51) 国際特許分類:
H04L 12/28 (2006.01) H04L 12/46 (2006.01)
B60R 16/023 (2006.01)
- (21) 国際出願番号: PCT/JP2019/034553
- (22) 国際出願日: 2019年9月3日(03.09.2019)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2018-201835 2018年10月26日(26.10.2018) JP
- (71) 出願人: 住友電気工業株式会社
(SUMITOMO ELECTRIC INDUSTRIES, LTD.)
[JP/JP]; 〒5410041 大阪府大阪市中央区北
浜四丁目5番33号 Osaka (JP). 住友電

装株式会社(SUMITOMO WIRING SYSTEMS,
LTD.) [JP/JP]; 〒5108503 三重県四日市市西末
広町1番14号 Mie (JP). 株式会社オート
ネットワーク技術研究所(AUTONETWORKS
TECHNOLOGIES, LTD.) [JP/JP]; 〒5108503 三
重県四日市市西末広町1番14号 Mie (JP).

- (72) 発明者: 吉田圭吾(YOSHIDA, Keigo); 〒5410041
大阪府大阪市中央区北浜四丁目5番33号住
友電気工業株式会社内 Osaka (JP). 濱田芳博
(HAMADA, Yoshihiro); 〒5410041 大阪府大阪
市中央区北浜四丁目5番33号住友電気工業株
式会社内 Osaka (JP). 上田浩史(UEDA, Hiroshi);
〒5108503 三重県四日市市西末広町1番14号
株式会社オートネットワーク技術研究所内 Mie
(JP). 足立直樹(ADACHI, Naoki); 〒5108503 三

(54) Title: DETECTION DEVICE, GATEWAY DEVICE, DETECTION METHOD, AND DETECTION PROGRAM

(54) 発明の名称: 検知装置、ゲートウェイ装置、検知方法および検知プログラム



(57) Abstract: [Problem] To accurately detect an abnormality in an in-vehicle network by simple processing. [Solution] This detection device detects an abnormality in an in-vehicle network including a plurality of in-vehicle devices, and is provided with: a monitoring unit that monitors transmission messages in the in-vehicle network and acquires a communication load in the in-vehicle network; an acquisition unit that acquires the history of a communication load in the in-vehicle network thereof or another in-vehicle network; and a detection unit that detects an abnormality in the in-vehicle network

重県四日市市西末広町 1 番 1 4 号株式会社オートネットワーク技術研究所内 Mie (JP). 相羽慎一(AIBA,Shinichi); 〒5108503 三重県四日市市西末広町 1 番 1 4 号株式会社オートネットワーク技術研究所内 Mie (JP).

(74) 代理人: 特許業務法人ワンディー I P パートナーズ(ONEDEE IP PARTNERS); 〒5320003 大阪府大阪市淀川区宮原四丁目 1 番 4 号 KDX 新大阪ビル Osaka (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, 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, 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, SM, ST, SV, SY, TH, 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, 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))

on the basis of the history acquired by the acquisition unit, and the communication load acquired by the monitoring unit at a first timing after the history.

(57) 要約: 【課題】簡易な処理によって車載ネットワークにおける異常を正しく検知する。【解決手段】検知装置は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

明 細 書

発明の名称：

検知装置、ゲートウェイ装置、検知方法および検知プログラム

技術分野

[0001] 本発明は、検知装置、ゲートウェイ装置、検知方法および検知プログラムに関する。

この出願は、2018年10月26日に出願された日本出願特願2018-201835号を基礎とする優先権を主張し、その開示のすべてをここに取り込む。

背景技術

[0002] 特許文献1（特開2017-126978号公報）には、以下のような異常検知装置が開示されている。すなわち、異常検知装置は、CAN（Controller Area Network）プロトコルに従って車両内のバスを介してメッセージの授受を行う複数の電子制御ユニットを備える車載ネットワークシステムにおいて、前記バスに接続されて異常を検知する異常検知装置であって、前記バスからメッセージを受信する受信部と、単位時間を決定する決定部と、前記決定部により決定された単位時間内に前記受信部により受信されたメッセージの数に基づく特徴情報を特定する特定部と、前記特定部で特定された前記特徴情報とメッセージの出現頻度に係る基準を表す所定モデルとを用いた演算処理の結果に応じて、異常か否かを判定する判定部とを備える。

[0003] また、たとえば、特許文献2（特開2017-85663号公報）には、以下のようなセキュリティ装置が開示されている。すなわち、セキュリティ装置は、1つ又は複数のバスを介してCANプロトコルに従ってフレームの授受を行う複数の電子制御ユニットと接続されるセキュリティ装置であって、前記フレームは、IDを格納するIDフィールド、DLC（Data Length Code）及びデータフィールドを含むデータフレームであ

り、1つの前記バスからフレームを受信する受信部と、フレームについての検査内容として、前記データフィールドに格納されたデータの値の検査に係るデータ検査パラメータを保持する保持部と、前記受信部により受信されたフレームに関し、前記IDが同値の2つのフレームが送信される時間間隔である送信周期について判定を行い、前記IDが同値の2つのフレームの受信間隔が所定の許容範囲から外れる場合に、前記受信部により受信されたフレームの条件が成立したと判定して前記保持部が保持する前記データ検査パラメータを更新する更新部と、前記保持部が保持する前記データ検査パラメータに基づいて、前記受信部により受信されたフレームが攻撃フレームか否かの判定に係る検査を行う検査部とを備える。

先行技術文献

特許文献

[0004] 特許文献1：特開2017-126978号公報

特許文献2：特開2017-85663号公報

発明の概要

課題を解決するための手段

[0005] (1) 本開示の検知装置は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

[0006] (6) 本開示の検知装置は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

視部と、前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

[0007] (7) 本開示の検知方法は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置における検知方法であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、自己または他の車載ネットワークにおける通信負荷の履歴を取得するステップと、取得した前記履歴、および前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む。

[0008] (8) 本開示の検知方法は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置における検知方法であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、過去に取得した前記通信負荷に基づいて、前記通信負荷の推定値を算出するステップと、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得するステップと、取得した前記履歴、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む。

[0009] (9) 本開示の検知プログラムは、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置において用いられる検知プログラムであって、コンピュータを、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己ま

たは他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部、として機能させるためのプログラムである。

[0010] (10) 本開示の検知プログラムは、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置において用いられる検知プログラムであって、コンピュータを、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部、として機能させるためのプログラムである。

[0011] 本開示の一態様は、このような特徴的な処理部を備える検知装置として実現され得るだけでなく、検知装置を備える車載通信システムとして実現され得る。また、本開示の一態様は、検知装置の一部または全部を実現する半導体集積回路として実現され得る。

[0012] 本開示の一態様は、このような特徴的な処理部を備えるゲートウェイ装置として実現され得るだけでなく、ゲートウェイ装置を備える車載通信システムとして実現され得る。また、本開示の一態様は、ゲートウェイ装置の一部または全部を実現する半導体集積回路として実現され得る。

図面の簡単な説明

[0013] [図1]図1は、本発明の第1の実施の形態に係る車載通信システムの構成を示

す図である。

[図2]図2は、本発明の第1の実施の形態に係るバス接続装置群の構成を示す図である。

[図3]図3は、本発明の第1の実施の形態に係る車載通信システムにおけるゲートウェイ装置の構成を示す図である。

[図4]図4は、本発明の第1の実施の形態に係る車載通信システムにおける通信負荷の度数分布の一例を示す図である。

[図5]図5は、本発明の第1の実施の形態に係るゲートウェイ装置における検知部によるトラフィック異常の検知例を示す図である。

[図6]図6は、本発明の第1の実施の形態に係るゲートウェイ装置が検知対象バスにおけるトラフィック異常の検知を行う際の動作手順を定めたフローチャートである。

[図7]図7は、本発明の第1の実施の形態に係る車載ネットワークの接続トポロジの一例を示す図である。

[図8]図8は、本発明の第2の実施の形態に係るゲートウェイ装置の構成を示す図である。

[図9]図9は、本発明の第2の実施の形態に係るゲートウェイ装置が検知対象バスにおけるトラフィック異常の検知を行う際の動作手順を定めたフローチャートである。

[図10]図10は、本発明の第2の実施の形態に係る車載通信システムにおける通信負荷の時間変化の一例を示す図である。

[図11]図11は、本発明の第3の実施の形態に係るゲートウェイ装置の構成を示す図である。

[図12]図12は、本発明の第3の実施の形態に係る車載通信システムにおける通信負荷の時間変化の一例を示す図である。

[図13]図13は、本発明の第3の実施の形態に係る車載通信システムにおける通信負荷の誤差の度数分布の一例を示す図である。

[図14]図14は、本発明の第3の実施の形態に係るゲートウェイ装置におけ

る検知部による不正メッセージの発生の推定例を示す図である。

[図15]図15は、本発明の第3の実施の形態に係るゲートウェイ装置が検知対象バスにおけるトラフィック異常の検知および不正メッセージの発生の推定を行う際の動作手順を定めたフローチャートである。

[図16]図16は、本発明の第3の実施の形態の変形例に係るゲートウェイ装置が検知対象バスにおける不正メッセージの発生の推定を行う際の動作手順を定めたフローチャートである。

[図17]図17は、本発明の第3の実施の形態に係る車載通信システムにおける通信負荷の時間変化の一例を示す図である。

発明を実施するための形態

[0014] 従来、車載ネットワークにおけるセキュリティを向上させるための車載ネットワークシステムが開発されている。

[0015] [本開示が解決しようとする課題]

特許文献1に記載の異常検知装置は、特定部が、受信されたメッセージID毎のフレームの数を成分とする特徴ベクトルである特徴情報を生成し、特徴情報と所定モデルとを用いた演算処理を行い、演算処理の結果に応じて、所定モデルが表す基準を特徴情報が逸脱しているか否かを判定することにより、異常を検知する構成である。

[0016] しかしながら、特許文献1に記載の異常検知装置では、特徴ベクトルが基準を逸脱しているか否かを判定するために、たとえば、特徴ベクトルの、kd木等のデータ構造で表された所定モデルが示す基準に対する最近傍距離を計算して閾値と比較するという複雑な処理が必要であり、CPU（Central Processing Unit）等における負荷が大きい。

[0017] また、特許文献2に記載のセキュリティ装置では、IDが同値の2つのフレームの受信間隔が所定の許容範囲から外れるか否かを判断するために、各フレームの送信時刻を取得する必要があることから、CPU等における負荷が大きい。

[0018] 本開示は、上述の課題を解決するためになされたもので、その目的は、簡

易な処理によって車載ネットワークにおける異常を正しく検知することが可能な検知装置、ゲートウェイ装置、検知方法および検知プログラムを提供することである。

[0019] [本開示の効果]

本開示によれば、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0020] [本願発明の実施形態の説明]

最初に、本発明の実施形態の内容を列記して説明する。

[0021] (1) 本発明の実施の形態に係る検知装置は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

[0022] たとえば、車載ネットワークにおいて異常が発生している場合、監視部によって取得された第1のタイミングにおける通信負荷は大きい値となる。上記のように、通信負荷に着目し、通信負荷の履歴、および第1のタイミングにおける通信負荷に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0023] (2) 好ましくは、前記検知装置は、さらに、前記監視部によって取得された、前記第1のタイミングより前のタイミングにおける前記通信負荷に基づいて、前記第1のタイミングにおける前記通信負荷の推定値を算出する推定部を備え、前記検知部は、前記監視部によって取得された前記第1のタイミングにおける前記通信負荷と、前記推定部によって算出された前記第1のタイミングにおける前記推定値とを比較し、比較結果に基づいて、前記車載

ネットワークにおける不正メッセージの発生を推定する。

[0024] このような構成により、第1のタイミングにおける通信負荷からは車載ネットワークにおける異常が検知されない状況であっても、第1のタイミングより前のタイミングにおける通信負荷から推定される推定値と通信負荷との比較結果に基づいて、車載ネットワークにおける不正メッセージの発生を推定することができる。これにより、通信負荷によって車載ネットワークにおける異常を検知できるタイミングよりも早く、車載ネットワークにおける不正メッセージの発生を推定することができる。

[0025] (3) より好ましくは、前記推定部は、前記検知部によって前記不正メッセージの発生が推定された場合、前記第1のタイミングより後のタイミングである第2のタイミングにおける前記推定値を、前記第1のタイミング以降のタイミングにおける前記通信負荷に基づいて算出する。

[0026] このような構成により、通信負荷が大幅に増大したタイミング以降の通信負荷に基づいて、新たな推定値をより正確に算出することができる。これにより、たとえば、通信負荷のさらなる変化が生じた場合であっても、新たに算出した推定値に基づいて車載ネットワークにおける不正メッセージの発生を正確に推定することができる。

[0027] (4) より好ましくは、前記検知装置は、さらに、前記検知部によって前記車載ネットワークにおける異常が検知された場合、第1の警報情報を出力し、前記検知部によって前記車載ネットワークにおける不正メッセージの発生が推定された場合、前記第1の警報情報とは異なる第2の警報情報を出力する通知部を備える。

[0028] このように、車載ネットワークにおける異常が検知された場合と、車載ネットワークにおける不正メッセージの発生が推定された場合とで、通知部が互いに異なる警報情報を送信する構成により、たとえば、状況に応じて緊急度合いが異なる警告をユーザに通知することができる。

[0029] (5) より好ましくは、前記監視部は、前記第1のタイミングにおける前記通信負荷として、前記通信負荷の時系列データの移動平均を算出する。

[0030] このような構成により、通信負荷よりもばらつきが小さい移動平均を、車載ネットワークにおける異常の検知に用いることができる。これにより、車載ネットワークにおける異常をより正しくかつ安定して検知することができる。

[0031] (6) 本発明の実施の形態に係る検知装置は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

[0032] たとえば、車載ネットワークにおいて異常が発生すると、監視部によって取得された第1のタイミングにおける通信負荷と推定部によって算出された第1のタイミングにおける通信負荷の推定値との差分は大きい値となる。上記のように、通信負荷と推定値との差分に着目し、通信負荷と推定値との差分の履歴、第1のタイミングにおける通信負荷、および第1のタイミングにおける通信負荷の推定値に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0033] 本発明の実施の形態に係るゲートウェイ装置は、車載ネットワークにおける車載装置間のメッセージを中継するゲートウェイ装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記

履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

[0034] たとえば、車載ネットワークにおいて異常が発生している場合、監視部によって取得された第1のタイミングにおける通信負荷は大きい値となる。上記のように、通信負荷に着目し、通信負荷の履歴、および第1のタイミングにおける通信負荷に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0035] 本発明の実施の形態に係るゲートウェイ装置は、車載ネットワークにおける車載装置間のメッセージを中継するゲートウェイ装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える。

[0036] たとえば、車載ネットワークにおいて異常が発生すると、監視部によって取得された第1のタイミングにおける通信負荷と推定部によって算出された第1のタイミングにおける通信負荷の推定値との差分は大きい値となる。上記のように、通信負荷と推定値との差分に着目し、通信負荷と推定値との差分の履歴、第1のタイミングにおける通信負荷、および第1のタイミングにおける通信負荷の推定値に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0037] (7) 本発明の実施の形態に係る検知方法は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置における検知方法であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、自己または他の車載ネットワークにおける通信負荷の履歴を取得するステップと、取得した前記履歴、および前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む。

[0038] たとえば、車載ネットワークにおいて異常が発生している場合、第1のタイミングにおける通信負荷は大きい値となる。上記のように、通信負荷に着目し、通信負荷の履歴、および第1のタイミングにおける通信負荷に基づいて車載ネットワークにおける異常を検知する方法により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0039] (8) 本発明の実施の形態に係る検知方法は、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置における検知方法であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、過去に取得した前記通信負荷に基づいて、前記通信負荷の推定値を算出するステップと、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得するステップと、取得した前記履歴、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む。

[0040] たとえば、車載ネットワークにおいて異常が発生すると、第1のタイミングにおける通信負荷と推定値との差分は大きい値となる。上記のように、通信負荷と推定値との差分に着目し、通信負荷と推定値との差分の履歴、第1のタイミングにおける通信負荷、および第1のタイミングにおける通信負荷の推定値に基づいて車載ネットワークにおける異常を検知する方法により、簡易な処理によって車載ネットワークにおける異常を正しく検知することが

できる。

[0041] 本発明の実施の形態に係る検知方法は、車載ネットワークにおける車載装置間のメッセージを中継するゲートウェイ装置における検知方法であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、自己または他の車載ネットワークにおける通信負荷の履歴を取得するステップと、取得した前記履歴、および前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む。

[0042] たとえば、車載ネットワークにおいて異常が発生している場合、監視部によって取得された第1のタイミングにおける通信負荷は大きい値となる。上記のように、通信負荷に着目し、通信負荷の履歴、および第1のタイミングにおける通信負荷に基づいて車載ネットワークにおける異常を検知する方法により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0043] 本発明の実施の形態に係る検知方法は、車載ネットワークにおける車載装置間のメッセージを中継するゲートウェイ装置における検知方法であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、過去に取得した前記通信負荷に基づいて、前記通信負荷の推定値を算出するステップと、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得するステップと、取得した前記履歴、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む。

[0044] たとえば、車載ネットワークにおいて異常が発生すると、第1のタイミングにおける通信負荷と推定値との差分は大きい値となる。上記のように、通信負荷と推定値との差分に着目し、通信負荷と推定値との差分の履歴、第1のタイミングにおける通信負荷、および第1のタイミングにおける通信負荷

の推定値に基づいて車載ネットワークにおける異常を検知する方法により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0045] (9) 本発明の実施の形態に係る検知プログラムは、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置において用いられる検知プログラムであって、コンピュータを、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部、として機能させるためのプログラムである。

[0046] たとえば、車載ネットワークにおいて異常が発生している場合、監視部によって取得された第1のタイミングにおける通信負荷は大きい値となる。上記のように、通信負荷に着目し、通信負荷の履歴、および第1のタイミングにおける通信負荷に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0047] (10) 本発明の実施の形態に係る検知プログラムは、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置において用いられる検知プログラムであって、コンピュータを、複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにお

ける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部、として機能させるためのプログラムである。

[0048] たとえば、車載ネットワークにおいて異常が発生すると、監視部によって取得された第1のタイミングにおける通信負荷と推定部によって算出された第1のタイミングにおける通信負荷の推定値との差分は大きい値となる。上記のように、通信負荷と推定値との差分に着目し、通信負荷と推定値との差分の履歴、第1のタイミングにおける通信負荷、および第1のタイミングにおける通信負荷の推定値に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0049] 本発明の実施の形態に係る検知プログラムは、車載ネットワークにおける車載装置間のメッセージを中継するゲートウェイ装置において用いられる検知プログラムであって、コンピュータを、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部、として機能させるためのプログラムである。

[0050] たとえば、車載ネットワークにおいて異常が発生している場合、監視部によって取得された第1のタイミングにおける通信負荷は大きい値となる。上記のように、通信負荷に着目し、通信負荷の履歴、および第1のタイミングにおける通信負荷に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0051] 本発明の実施の形態に係る検知プログラムは、車載ネットワークにおける

車載装置間のメッセージを中継するゲートウェイ装置において用いられる検知プログラムであって、コンピュータを、前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部、として機能させるためのプログラムである。

[0052] たとえば、車載ネットワークにおいて異常が発生すると、監視部によって取得された第1のタイミングにおける通信負荷と推定部によって算出された第1のタイミングにおける通信負荷の推定値との差分は大きい値となる。上記のように、通信負荷と推定値との差分に着目し、通信負荷と推定値との差分の履歴、第1のタイミングにおける通信負荷、および第1のタイミングにおける通信負荷の推定値に基づいて車載ネットワークにおける異常を検知する構成により、簡易な処理によって車載ネットワークにおける異常を正しく検知することができる。

[0053] 以下、本発明の実施の形態について図面を用いて説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰り返さない。また、以下に記載する実施の形態の少なくとも一部を任意に組み合わせてもよい。

[0054] ＜第1の実施の形態＞

 [構成および基本動作]

 図1は、本発明の第1の実施の形態に係る車載通信システムの構成を示す図である。

[0055] 図1を参照して、車載通信システム301は、ゲートウェイ装置（検知装置）101と、複数の車載通信機111と、複数のバス接続装置群121と

を備える。

[0056] 図2は、本発明の第1の実施の形態に係るバス接続装置群の構成を示す図である。

[0057] 図2を参照して、バス接続装置群121は、複数の制御装置122を含む。なお、バス接続装置群121は、複数の制御装置122を備える構成に限らず、1つの制御装置122を含む構成であってもよい。

[0058] 車載通信システム301は、道路を走行する車両（以下、対象車両とも称する。）に搭載される。車載ネットワーク12は、車両の内部における装置である車載装置を複数含む。具体的には、車載ネットワーク12は、車載装置の一例である、複数の車載通信機111および複数の制御装置122を含む。なお、車載ネットワーク12は、複数の車載装置を含む構成であれば、複数の車載通信機111を含みかつ制御装置122を含まない構成であってもよいし、車載通信機111を含まずかつ複数の制御装置122を含む構成であってもよいし、1つの車載通信機111および1つの制御装置122を含む構成であってもよい。

[0059] 車載ネットワーク12において、車載通信機111は、たとえば、対象車両の外部における装置と通信する。具体的には、車載通信機111は、たとえば、TCU（Telematics Communication Unit）、近距離無線端末装置、およびITS（Intelligent Transport Systems）無線機である。

[0060] TCUは、たとえば、LTE（Long Term Evolution）または3G等の通信規格に従って、無線基地局装置と無線通信を行うことが可能であり、かつゲートウェイ装置101と通信を行うことが可能である。TCUは、たとえば、ナビゲーション、車両盗難防止、リモートメンテナンスおよびFOTA（Firmware Over The Air）等のサービスに用いる情報を中継する。

[0061] 近距離無線端末装置は、たとえば、Wi-Fi（登録商標）およびBluetooth（登録商標）等の通信規格に従って、対象車両に乗車している

人間（以下、搭乗者とも称する。）の保持するスマートホン等の無線端末装置と無線通信を行うことが可能であり、かつゲートウェイ装置１０１と通信を行うことが可能である。当該近距離無線端末装置は、たとえば、エンターテインメント等のサービスに用いる情報を中継する。

[0062] また、近距離無線端末装置は、たとえば、所定の通信規格に従って、搭乗者の保持するスマートキー等の無線端末装置、およびタイヤに設けられた無線端末装置とＬＦ（Low Frequency）帯またはＵＨＦ（Ultra High Frequency）帯の電波を用いて無線通信を行うことが可能であり、かつゲートウェイ装置１０１と通信を行うことが可能である。当該近距離無線端末装置は、たとえば、スマートエン트리およびＴＰＭＳ（Tire Pressure Monitoring System）等のサービスに用いる情報を中継する。

[0063] ＩＴＳ無線機は、たとえば、道路の近傍に設けられた光ビーコン、電波ビーコンおよびＩＴＳスポット等の路側機と路車間通信を行うことが可能であり、他の車両に搭載された車載端末と車車間通信を行うことが可能であり、かつゲートウェイ装置１０１と通信を行うことが可能である。ＩＴＳ無線機は、たとえば、渋滞緩和、安全運転支援およびルートガイダンス等のサービスに用いる情報を中継する。

[0064] ゲートウェイ装置１０１は、たとえば、ファームウェアのアップデート等のデータ、およびゲートウェイ装置１０１により蓄積されたデータ等を対象車両の外部における整備用端末装置とポート１１２を介して送受信することが可能である。

[0065] ゲートウェイ装置１０１は、たとえばバス１３，１４を介して車載装置と接続する。具体的には、バス１３，１４は、たとえば、ＣＡＮ（Controller Area Network）（登録商標）、FlexRay（登録商標）、MOST（Media Oriented Systems Transport）（登録商標）、イーサネット（登録商標）、およびＬＩＮ（Local Interconnect Network）等の規格

に従うバスである。

[0066] この例では、車載通信機 1 1 1 は、イーサネットの規格に従う対応のバス 1 4 を介してゲートウェイ装置 1 0 1 と接続されている。また、バス接続装置群 1 2 1 における各制御装置 1 2 2 は、CAN の規格に従う対応のバス 1 3 を介してゲートウェイ装置 1 0 1 と接続されている。制御装置 1 2 2 は、たとえば、対象車両における機能部を制御可能である。

[0067] バス 1 3 は、たとえば系統別に設けられる。具体的には、バス 1 3 は、たとえば、駆動系バス、シャーシ／安全系バス、ボディ／電装系バスおよび AV／情報系バスである。

[0068] 駆動系バスには、制御装置 1 2 2 の一例であるエンジン制御装置、AT (Automatic Transmission) 制御装置および HEV (Hybrid Electric Vehicle) 制御装置が接続されている。エンジン制御装置、AT 制御装置および HEV 制御装置は、エンジン、AT、およびエンジンとモータとの切替をそれぞれ制御する。

[0069] シャーシ／安全系バスには、制御装置 1 2 2 の一例であるブレーキ制御装置、シャーシ制御装置およびステアリング制御装置が接続されている。ブレーキ制御装置、シャーシ制御装置およびステアリング制御装置は、ブレーキ、シャーシおよびステアリングをそれぞれ制御する。

[0070] ボディ／電装系バスには、制御装置 1 2 2 の一例である計器表示制御装置、エアコン制御装置、盗難防止制御装置、エアバック制御装置およびスマートエントリ制御装置が接続されている。計器表示制御装置、エアコン制御装置、盗難防止制御装置、エアバック制御装置およびスマートエントリ制御装置は、計器、エアコン、盗難防止機構、エアバック機構およびスマートエントリをそれぞれ制御する。

[0071] AV／情報系バスには、制御装置 1 2 2 の一例であるナビゲーション制御装置、オーディオ制御装置、ETC (Electronic Toll Collection System) (登録商標) 制御装置および電話制御装置が接続されている。ナビゲーション制御装置、オーディオ制御装置、E

TC制御装置および電話制御装置は、ナビゲーション装置、オーディオ装置、ETC装置および携帯電話をそれぞれ制御する。

[0072] また、バス13には、制御装置122が接続される構成に限らず、制御装置122以外の装置が接続されてもよい。

[0073] ゲートウェイ装置101は、たとえば、セントラルゲートウェイ (Central Gateway: CGW) であり、車載装置と通信を行うことが可能である。

[0074] ゲートウェイ装置101は、たとえば、対象車両において異なるバス13に接続された制御装置122間でやり取りされる情報、各車載通信機111間でやり取りされる情報、制御装置122および車載通信機111間でやり取りされる情報を中継する中継処理を行う。

[0075] より詳細には、車載ネットワーク12では、ある車載装置から他の車載装置へ周期的にまたは不定期にメッセージが送信される。メッセージの送信は、ブロードキャストによって行われてもよいし、ユニキャストによって行われてもよい。

[0076] なお、以下では、ある制御装置122から他の制御装置122へ送信されるメッセージについて説明するが、制御装置122および車載通信機111間において送信されるメッセージ、ならびに各車載通信機111間において送信されるメッセージについても同様である。

[0077] [ゲートウェイ装置の構成]

図3は、本発明の第1の実施の形態に係る車載通信システムにおけるゲートウェイ装置の構成を示す図である。

[0078] 図3を参照して、ゲートウェイ装置101は、通信処理部51と、監視部52と、取得部53と、検知部54と、通知部55と、記憶部56とを備える。記憶部56は、たとえば、不揮発性メモリである。

[0079] ゲートウェイ装置101は、検知装置として機能し、車載ネットワーク12における異常を検知する検知処理を行う。

[0080] より詳細には、ゲートウェイ装置101は、車載ネットワーク12におけ

る異常を検知する処理として、各バス１３のうち検知対象となるバス（以下、検知対象バスとも称する。）における、不正メッセージによる通信トラフィックの異常（以下、トラフィック異常とも称する）を検知する。

[0081] [通信処理部]

通信処理部５１は、中継処理を行う。より詳細には、通信処理部５１は、ある制御装置１２２から対応のバス１３経由でメッセージを受信すると、受信したメッセージを記憶部５６に保存する。そして、通信処理部５１は、メッセージを記憶部５６から取得し、取得したメッセージを対応のバス１３経由で送信先の制御装置１２２へ送信する。

[0082] より詳細には、たとえば、記憶部５６には、メッセージの送信先である各バス接続装置群１２１に対応する複数のキューが設けられている。言い換えると、記憶部５６には、メッセージの送信時に経由する各バス１３に対応する複数のキューが設けられている。

[0083] 通信処理部５１は、たとえば、メッセージを受信すると、送信先のバス接続装置群１２１ごとに対応のキューに振り分けて保存する。そして、通信処理部５１は、メッセージを記憶部５６のキューから取得し、取得したメッセージを送信先のバス接続装置群１２１へ対応のバス１３経由で送信する。

[0084] [監視部]

監視部５２は、車載ネットワーク１２における送信メッセージを監視し、車載ネットワーク１２における通信負荷を取得する。たとえば、監視部５２は、記憶部５６におけるメッセージを監視することにより、検知対象バスの通信負荷を取得する。

[0085] たとえば、記憶部５６は、各バス１３において単位時間あたりに伝送可能なデータ量の上限値（以下、最大通信量とも称する。）を記憶している。監視部５２は、記憶部５６から検知対象バスの最大通信量を取得する。

[0086] 監視部５２は、記憶部５６における各キューのうち検知対象バスに対応するキューにおけるメッセージを監視することにより、単位時間あたりに検知対象バスを介して伝送されるメッセージの総データ量を取得する。

[0087] 監視部 5 2 は、取得した総データ量を検知対象バスの最大通信量で除した値を、検知対象バスの通信負荷 L として算出する。

[0088] 一例として、監視部 5 2 は、記憶部 5 6 における対応のキューに保存されたメッセージの数を取得し、取得したメッセージの数に基づいて、単位時間あたりに検知対象バスを介して伝送されるメッセージの総データ量を算出する。

[0089] また、他の例として、監視部 5 2 は、記憶部 5 6 における対応のキューに保存された各メッセージに含まれる DLC (Data Length Code) を参照することにより、当該メッセージのデータフィールドのデータ量を取得し、取得したデータ量の総和に基づいて、単位時間あたりに検知対象バスを介して伝送されるメッセージの総データ量を算出する。なお、DLC は、4 bit で構成され、データフィールドの長さを示す値である。

[0090] たとえば、記憶部 5 6 は、通信負荷 L の取得周期 C 1 などを示す設定情報を記憶している。監視部 5 2 は、記憶部 5 6 から設定情報を取得し、取得した設定情報に従って、取得周期 C 1 に従う取得タイミングにおいて検知対象バスの通信負荷 L を取得し、取得した通信負荷 L を検知部 5 4 へ出力する。

[取得部]

取得部 5 3 は、自己または他の車載ネットワークにおける通信負荷 L の履歴を取得する。たとえば、取得部 5 3 は、監視部 5 2 によって取得された検知対象バスの通信負荷 L の履歴を取得する。

[0091] 取得部 5 3 は、たとえば、検知対象バスの通信負荷 L の履歴として、サーバ等の他の装置によって予め作成された、検知対象バスの通信負荷 L の度数分布を示す分布情報 F 1 を取得する。

[0092] 図 4 は、本発明の第 1 の実施の形態に係る車載通信システムにおける通信負荷の度数分布の一例を示す図である。なお、図 4 において、縦軸は度数を示し、横軸は通信負荷 L を示す。

[0093] 図 4 を参照して、サーバは、監視部 5 2 によって一定期間にわたって取得されたバス 1 3 ごとの通信負荷 L に基づいて、通信負荷 L の度数分布 D 1 を

バス 13 ごとに作成する。この通信負荷 L は、たとえば、対象車両と同じ種類のテスト車両すなわち他の車載ネットワークにおいて取得される。なお、サーバは、対象車両すなわち自己の車載ネットワークにおいて取得された通信負荷 L に基づいて度数分布 D1 を作成してもよい。

[0094] サーバは、作成した度数分布 D1 に基づいて、通信負荷 L の標本平均および標本標準偏差などを算出する。サーバは、取得部 53 から分布情報 F1 の送信要求を受けると、通信負荷 L の標本平均および標本標準偏差などを含む分布情報 F1 を要求元の対象車両へ送信する。

[0095] 再び図 3 を参照して、取得部 53 は、検知対象バスの分布情報 F1 の送信要求をサーバへ送信することにより、分布情報 F1 を取得する。取得部 53 は、車載通信機 111 および通信処理部 51 経由でサーバから分布情報 F1 を受信すると、受信した分布情報 F1 を検知部 54 へ出力する。

[0096] なお、ゲートウェイ装置 101 では、取得部 53 が、車載通信機 111 および通信処理部 51 経由でサーバから分布情報 F1 を受信する構成であるとしたが、これに限定するものではない。たとえば、サーバまたは整備用端末装置によって記憶部 56 に各バス 13 の分布情報 F1 が保存されており、取得部 53 が記憶部 56 から検知対象バスの分布情報 F1 を取得する構成であってもよい。

[0097] [検知部]

検知部 54 は、取得部 53 によって取得された通信負荷 L の履歴、および、監視部 52 によって取得された、当該履歴よりも後の第 1 のタイミングにおける通信負荷 L に基づいて、車載ネットワーク 12 における異常を検知する。より詳細には、検知部 54 は、上記履歴、および、当該履歴に含まれる各通信負荷 L の取得タイミングよりも後の取得タイミング t において取得された通信負荷 L に基づいて、検知対象バスにおけるトラフィック異常を検知する。以下では、監視部 52 によって取得タイミング t において取得された通信負荷 L を通信負荷 Lt と称する。

[0098] たとえば、検知部 54 は、取得部 53 から受けた分布情報 F1、および監

監視部52から受けた通信負荷 L_t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0099] より詳細には、サーバが作成した度数分布 D_1 は、検知対象バスにおいてトラフィック異常が発生していないときの通信負荷 L の度数分布であると仮定することができる。検知部54は、度数分布 D_1 に対応する分布情報 F_1 と、監視部52から受けた通信負荷 L_t とに基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0100] たとえば、検知部54は、取得部53から受けた分布情報 F_1 に基づいて、通信負荷 L の度数分布 D_1 を正規分布で近似した確率密度関数をモデルとして作成し、作成したモデルと、監視部52から受けた通信負荷 L_t とに基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0101] 図5は、本発明の第1の実施の形態に係るゲートウェイ装置における検知部によるトラフィック異常の検知例を示す図である。なお、図5において、横軸は通信負荷を示す。図5の破線は、通信負荷 L の度数分布 D_1 を正規分布で近似した確率密度関数を示す。

[0102] 図3および図5を参照して、検知部54は、取得部53から分布情報 F_1 を受けると、分布情報 F_1 に基づいて、通信トラフィックが正常である場合における通信負荷 L の平均値の信頼区間の下限値 A_1 および上限値 B_1 を算出し、算出した上限値 B_1 をしきい値 ThA_1 として設定する。

[0103] 検知部54は、監視部52から通信負荷 L_t を受けると、受けた通信負荷 L_t としきい値 ThA_1 とを比較する。

[0104] たとえば、検知部54は、監視部52によって取得タイミング t_1 において取得された通信負荷 L_{t_1} がしきい値 ThA_1 以下である場合、検知対象バスにおけるトラフィック異常は発生していないと判断する。

[0105] これは、たとえば、取得タイミング t_1 において、検知対象バスにおけるトラフィック異常が発生していない場合、通信負荷 L_t は図5に示す確率密度関数の中心の近傍に位置する可能性が高く、しきい値 ThA_1 を超える可能性は低いからである。

[0106] 一方、検知部54は、監視部52によって取得タイミング t_2 において取得された通信負荷 L_{t_2} がしきい値 ThA_1 より大きい場合、検知対象バスにおけるトラフィック異常が発生していると判断する。

[0107] これは、たとえば、取得タイミング t_2 において、検知対象バスにおけるトラフィック異常が発生している場合、通信負荷 L_{t_2} は大きい値となり、しきい値 ThA_1 を超える可能性が高いからである。

[0108] 検知部54は、通信負荷 L_{t_2} およびしきい値 ThA_1 に基づく判断結果を示す判断情報を、通信処理部51および通知部55へ出力する。

[0109] 通信処理部51は、検知部54から受けた判断情報が、検知対象バスにおけるトラフィック異常が発生していないことを示す場合、当該検知対象バスを介した中継処理を通常通り行う。具体的には、通信処理部51は、当該検知対象バスを介してメッセージを送信先の制御装置122へ送信する。

[0110] 一方、通信処理部51は、検知部54から受けた判断情報が、検知対象バスにおけるトラフィック異常が発生していることを示す場合、たとえば、当該検知対象バスを介した中継処理を停止する。そして、通信処理部51は、当該判断情報が示すメッセージおよび検知対象バスをログとして記憶部56に記録する。

[0111] 通知部55は、検知部54から受けた判断情報が、検知対象バスにおけるトラフィック異常が発生していることを示す場合、検知対象バスにおけるトラフィック異常が発生していることを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する。

[0112] [動作]

車載通信システム301における各装置は、メモリを含むコンピュータを備え、当該コンピュータにおけるCPU等の演算処理部は、以下のフローチャートの各ステップの一部または全部を含むプログラムを当該メモリからそれぞれ読み出して実行する。これら複数の装置のプログラムは、それぞれ、外部からインストールすることができる。これら複数の装置のプログラムは、それぞれ、記録媒体に格納された状態で流通する。

[0113] 図6は、本発明の第1の実施の形態に係るゲートウェイ装置が検知対象バスにおけるトラフィック異常の検知を行う際の動作手順を定めたフローチャートである。

[0114] 図6を参照して、まず、ゲートウェイ装置101は、検知対象バスの通信負荷 L の度数分布 $D1$ を示す分布情報 $F1$ を取得する（ステップS102）。

[0115] 次に、ゲートウェイ装置101は、分布情報 $F1$ に基づいて、しきい値 $ThA1$ を設定する（ステップS104）。

[0116] 次に、ゲートウェイ装置101は、取得タイミング t における検知対象バスの通信負荷 L_t を取得する（ステップS106）。

[0117] 次に、ゲートウェイ装置101は、設定したしきい値 $ThA1$ と取得した通信負荷 L_t とを比較する（ステップS108）。

[0118] 次に、ゲートウェイ装置101は、通信負荷 L_t がしきい値 $ThA1$ 以下である場合（ステップS110でNO）、検知対象バスにおけるトラフィック異常が発生しておらず、通信トラフィックは正常であると判断する（ステップS112）。

[0119] 次に、ゲートウェイ装置101は、次の取得タイミング $t+1$ における検知対象バスの通信負荷 L_{t+1} を取得する処理（ステップS106）、および通信負荷 L_{t+1} としきい値 $ThA1$ とを比較する処理（ステップS108）等を行う。

[0120] 一方、ゲートウェイ装置101は、通信負荷 L_t がしきい値 $ThA1$ より大きい場合（ステップS110でYES）、検知対象バスにおけるトラフィック異常が発生していると判断する（ステップS114）。

[0121] 次に、ゲートウェイ装置101は、検知対象バスにおけるトラフィック異常が発生していることを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する（ステップS116）。

[0122] 次に、ゲートウェイ装置101は、次の取得タイミング $t+1$ における検知対象バスの通信負荷 L_{t+1} を取得する処理（ステップS106）、およ

び通信負荷 $L_t + 1$ としきい値 $ThA1$ とを比較する処理（ステップS108）等を行う。

[0123] なお、本発明の第1の実施の形態に係る車載通信システム301では、ゲートウェイ装置101が、検知対象バスにおけるトラフィック異常を検知する構成であるとしたが、これに限定するものではない。車載通信システム301では、ゲートウェイ装置101とは別の検知装置が、検知対象バスにおけるトラフィック異常を検知する構成であってもよい。

[0124] また、本発明の第1の施の形態に係る車載通信システムでは、検知装置として機能するゲートウェイ装置101がバス13に直接接続される構成であるとしたが、これに限定するものではない。

[0125] 図7は、本発明の第1の実施の形態に係る車載ネットワークの接続トポロジの一例を示す図である。

[0126] 図7を参照して、検知装置131が、車載装置たとえば制御装置122を介してバス13に接続される構成であってもよい。この場合、検知装置131は、たとえば、当該車載装置が送受信するメッセージを監視することにより、当該車載装置を介して接続されるバス13におけるトラフィック異常を検知する構成であってもよい。

[0127] 図7に示す例では、たとえば、検知装置131の監視部52は、制御装置122がバス13を介して単位時間あたりに伝送するメッセージの総データ量を取得し、取得した総データ量を当該バス13の最大通信量で除した値を、当該バスの通信負荷 L として算出する。

[0128] また、本発明の第1の実施の形態に係るゲートウェイ装置101では、検知部54は、制御装置122間を接続するバス13を検知対象バスとして検知処理を行う構成であるとしたが、これに限定するものではない。検知部54は、制御装置122および車載通信機111間を接続するバス13, 14を検知対象バスとして検知処理を行う構成であってもよいし、車載通信機111間を接続するバス14を検知対象バスとして検知処理を行う構成であってもよい。

- [0129] さらに、検知部54は、車載ネットワーク12におけるすべてのバス13，14を並行して検知対象として検知処理を行う構成であってもよいし、各バス13，14を時分割で検知対象として検知処理を行う構成であってもよい。
- [0130] また、本発明の第1の実施の形態に係るゲートウェイ装置101では、検知部54は、車載ネットワーク12における異常を検知する処理として、検知対象バスにおけるトラフィック異常の有無を判断する構成であるとしたが、これに限定するものではない。検知部54は、車載ネットワーク12における異常を検知する処理として、検知対象バスにおける通信トラフィックが異常である確率を算出する構成であってもよい。
- [0131] また、本発明の第1の実施の形態に係るゲートウェイ装置101では、検知部54は、取得タイミング t において取得された通信負荷 L_t と、しきい値 T_{hA1} とに基づいてトラフィック異常を検知する構成であるとしたが、これに限定するものではない。検知部54は、通信負荷 L_t と、2つ以上のしきい値とに基づいてトラフィック異常を検知する構成であってもよい。たとえば、図5を参照して、検知部54は、通信トラフィックが正常である場合における通信負荷 L の平均値の信頼区間の下限値 $A1$ をしきい値として設定する構成であってもよいし、異なる信頼区間の上限値をしきい値として設定する構成であってもよい。
- [0132] また、本発明の第1の実施の形態に係るゲートウェイ装置101における検知部54は、たとえば、ユーザから検知処理を停止すべき旨を示す命令情報を受けた場合には、検知処理を行わない構成であってもよい。
- [0133] このような構成により、ゲートウェイ装置101がファームウェアの更新プログラムを受信する場合などにおいて、検知処理を停止することができるため、CPU等の処理負荷を軽減することができる。
- [0134] また、本発明の第1の実施の形態に係るゲートウェイ装置101では、記憶部56は不揮発性メモリであるとしたが、これに限定するものではない。記憶部56は、揮発性メモリであってもよいし、揮発性記憶領域と不揮発性

記憶領域とを有する構成であってもよい。

[0135] ところで、特許文献１に記載の異常検知装置では、特徴ベクトルが基準を逸脱しているか否かを判定するために、たとえば、特徴ベクトルの、 k 次元等のデータ構造で表された所定モデルが示す基準に対する最近傍距離を計算して閾値と比較するという複雑な処理が必要であり、CPU等における負荷が大きい。また、特許文献２に記載のセキュリティ装置では、IDが同値の２つのフレームの受信間隔が所定の許容範囲から外れるか否かを判断するために、各フレームの送信時刻を取得する必要があることから、CPU等における負荷が大きい。

[0136] これに対して、本発明の第１の実施の形態に係る検知装置は、複数の車載装置を含む車載ネットワーク１２における異常を検知する。監視部５２は、車載ネットワーク１２における送信メッセージを監視し、車載ネットワーク１２における検知対象バスの通信負荷 L を取得する。取得部５３は、自己または他の車載ネットワークにおける検知対象バスの通信負荷 L の履歴を取得する。検知部５４は、取得部５３によって取得された通信負荷 L の履歴、および監視部５２によって取得された、通信負荷 L の履歴よりも後の取得タイミング t における通信負荷 L_t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0137] たとえば、検知対象バスにおけるトラフィック異常が発生している場合、取得タイミング t における通信負荷 L_t は大きい値となる。本発明の第１の実施の形態に係る検知装置は、通信負荷 L に着目し、通信負荷 L の履歴、および取得タイミング t における通信負荷 L_t に基づいて検知対象バスにおけるトラフィック異常を検知する構成により、たとえば特許文献１に記載の異常検知装置および特許文献２に記載のセキュリティ装置と比べて、簡易な処理によって検知対象バスにおけるトラフィック異常を検知することができる。

[0138] したがって、本発明の第１の実施の形態に係る検知装置では、簡易な処理によって車載ネットワーク１２における異常を正しく検知することができる。

。

[0139] 本発明の第1の実施の形態に係るゲートウェイ装置101は、車載ネットワーク12における車載装置間のメッセージを中継する。監視部52は、車載ネットワーク12における送信メッセージを監視し、車載ネットワーク12における検知対象バスの通信負荷 L を取得する。取得部53は、自己または他の車載ネットワークにおける検知対象バスの通信負荷 L の履歴を取得する。検知部54は、取得部53によって取得された通信負荷 L の履歴、および監視部52によって取得された、通信負荷 L の履歴よりも後の取得タイミング t における通信負荷 L_t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0140] たとえば、検知対象バスにおけるトラフィック異常が発生している場合、取得タイミング t における通信負荷 L_t は大きい値となる。本発明の第1の実施の形態に係る検知装置は、通信負荷 L に着目し、通信負荷 L の履歴、および取得タイミング t における通信負荷 L_t に基づいて検知対象バスにおけるトラフィック異常を検知する構成により、たとえば特許文献1に記載の異常検知装置および特許文献2に記載のセキュリティ装置と比べて、簡易な処理によって検知対象バスにおけるトラフィック異常を検知することができる。

。

[0141] したがって、本発明の第1の実施の形態に係るゲートウェイ装置101では、簡易な処理によって車載ネットワーク12における異常を正しく検知することができる。

[0142] 本発明の第1の実施の形態に係る検知方法では、まず、検知装置が、車載ネットワークにおける送信メッセージを監視し、車載ネットワーク12における検知対象バスの通信負荷 L を取得する。次に、検知装置が、自己または他の車載ネットワークにおける検知対象バスの通信負荷 L の履歴を取得する。次に、検知装置が、取得した通信負荷 L の履歴、および通信負荷 L の履歴よりも後の取得タイミング t における通信負荷 L_t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0143] たとえば、検知対象バスにおけるトラフィック異常が発生している場合、取得タイミング t における通信負荷 L_t は大きい値となる。本発明の第1の実施の形態に係る検知装置は、通信負荷 L に着目し、通信負荷 L の履歴、および取得タイミング t における通信負荷 L_t に基づいて検知対象バスにおけるトラフィック異常を検知する構成により、たとえば特許文献1に記載の異常検知装置および特許文献2に記載のセキュリティ装置と比べて、簡易な処理によって検知対象バスにおけるトラフィック異常を検知することができる。

[0144] したがって、本発明の第1の実施の形態に係る検知方法では、簡易な処理によって車載ネットワーク12における異常を正しく検知することができる。

[0145] 本発明の第1の実施の形態に係る検知方法では、まず、ゲートウェイ装置101が、車載ネットワークにおける送信メッセージを監視し、車載ネットワーク12における検知対象バスの通信負荷 L を取得する。次に、ゲートウェイ装置101が、自己または他の車載ネットワークにおける検知対象バスの通信負荷 L の履歴を取得する。次に、ゲートウェイ装置101が、取得した通信負荷 L の履歴、および通信負荷 L の履歴よりも後の取得タイミング t における通信負荷 L_t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0146] たとえば、検知対象バスにおけるトラフィック異常が発生している場合、取得タイミング t における通信負荷 L_t は大きい値となる。本発明の第1の実施の形態に係る検知装置は、通信負荷 L に着目し、通信負荷 L の履歴、および取得タイミング t における通信負荷 L_t に基づいて検知対象バスにおけるトラフィック異常を検知する構成により、たとえば特許文献1に記載の異常検知装置および特許文献2に記載のセキュリティ装置と比べて、簡易な処理によって検知対象バスにおけるトラフィック異常を検知することができる。

[0147] したがって、本発明の第1の実施の形態に係る検知方法では、簡易な処理

によって車載ネットワーク 12 における異常を正しく検知することができる。
。

[0148] 次に、本発明の他の実施の形態について図面を用いて説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰り返さない。

[0149] <第 2 の実施の形態>

本実施の形態は、第 1 の実施の形態に係るゲートウェイ装置と比べて、通信負荷 L の時系列データの移動平均を用いて、車載ネットワーク 12 における異常を検知するゲートウェイ装置に関する。以下で説明する内容以外は第 1 の実施の形態に係るゲートウェイ装置と同様である。

[0150] 図 8 は、本発明の第 2 の実施の形態に係るゲートウェイ装置の構成を示す図である。

[0151] 図 8 を参照して、ゲートウェイ装置 102 は、通信処理部 51 と、監視部 62 と、取得部 63 と、検知部 64 と、通知部 55 と、記憶部 56 とを備える。

[0152] ゲートウェイ装置 102 における通信処理部 51 および通知部 55 の動作は、図 3 に示すゲートウェイ装置 101 における通信処理部 51 および通知部 55 とそれぞれ同様である。

[0153] [監視部]

監視部 62 は、第 1 のタイミングにおける通信負荷 L として、通信負荷 L の時系列データの移動平均を算出する。

[0154] たとえば、記憶部 56 は、通信負荷 L の取得周期 C1、および通信負荷 L の時系列データの移動平均を算出する際のウィンドウサイズなどを示す設定情報を記憶している。監視部 62 は、記憶部 56 から設定情報を取得し、取得した設定情報に従って、取得周期 C1 に従う取得タイミングにおいて、検知対象バスの通信負荷 L を取得するとともに当該通信負荷 L の時系列データの移動平均 A を算出する。

[0155] たとえば、監視部 62 は、取得周期 C1 に従う取得タイミング t において検知対象バスの通信負荷 L t を取得すると、取得した通信負荷 L t を、時系

列データの一つとして記憶部56に保存する。さらに、監視部62は、記憶部56に保存した通信負荷Lの時系列データの中から、設定情報のウィンドウサイズが示す数の通信負荷Lであって、直近の各取得タイミングにおける各通信負荷Lを取得し、取得した各通信負荷Lの平均値を、通信負荷Lの時系列データの移動平均Aとして算出する。

[0156] 以下では、監視部62によって取得タイミングtにおける通信負荷L_tの取得に伴って新たに算出された移動平均Aを、移動平均A_tと称する。監視部62は、取得タイミングtにおける通信負荷L_tの取得に伴って算出した移動平均A_tを、検知部54へ出力する。

[0157] [取得部]

取得部63は、自己または他の車載ネットワークにおける通信負荷Lの履歴を取得する。より詳細には、取得部63は、監視部62によって取得された移動平均Aの履歴を取得する。

[0158] 取得部63は、たとえば、移動平均Aの履歴として、サーバ等の他の装置によって予め作成された移動平均Aの度数分布を示す分布情報F2を取得する。

[0159] サーバは、監視部62によって一定期間にわたって取得されたバス13ごとの移動平均Aに基づいて、移動平均Aの度数分布D2をバス13ごとに作成する。この移動平均Aは、たとえば、対象車両と同じ種類のテスト車両すなわち他の車載ネットワークにおいて取得される。なお、サーバは、対象車両すなわち自己の車載ネットワークにおいて取得された移動平均Aに基づいて度数分布D2を作成してもよい。

[0160] サーバは、作成した度数分布D2に基づいて、移動平均Aの標本平均および標本標準偏差などを算出する。サーバは、取得部63から分布情報F2の送信要求を受けると、移動平均Aの標本平均および標本標準偏差などを含む分布情報F2を要求元の対象車両へ送信する。

[0161] 再び図8を参照して、取得部63は、検知対象バスの分布情報F2の送信要求をサーバへ送信することにより、分布情報F2を取得する。取得部63

は、車載通信機 1 1 1 および通信処理部 5 1 経由でサーバから分布情報 F 2 を受信すると、受信した分布情報 F 2 を検知部 5 4 へ出力する。

[0162] [検知部]

検知部 6 4 は、取得部 6 3 によって取得された移動平均 A の履歴、および、監視部 6 2 によって当該履歴に含まれる各移動平均 A の取得タイミングよりも後の取得タイミング t において算出された移動平均 A t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0163] たとえば、検知部 6 4 は、取得部 6 3 から受けた分布情報 F 2、および監視部 6 2 から受けた移動平均 A t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0164] より詳細には、検知部 6 4 は、取得部 6 3 から分布情報 F 2 を受けると、分布情報 F 2 に基づいて、通信トラフィックが正常である場合における移動平均 A の平均値の信頼区間の下限値 A 2 および上限値 B 2 を算出し、算出した上限値 B 2 をしきい値 T h A 2 として設定する。

[0165] 検知部 6 4 は、監視部 6 2 から移動平均 A t を受けると、受けた移動平均 A t としきい値 T h A 2 とを比較する。

[0166] 検知部 5 4 は、移動平均 A t およびしきい値 T h A 2 に基づいて、検知対象バスにおけるトラフィック異常が発生しているか否かを判断し、判断結果を示す判断情報を通信処理部 5 1 および通知部 5 5 へ出力する。

[0167] [動作]

図 9 は、本発明の第 2 の実施の形態に係るゲートウェイ装置が検知対象バスにおけるトラフィック異常の検知を行う際の動作手順を定めたフローチャートである。

[0168] 図 9 を参照して、まず、ゲートウェイ装置 1 0 2 は、検知対象バスの移動平均 A の度数分布 D 2 を示す分布情報 F 2 を取得する（ステップ S 2 0 2）。

[0169] 次に、ゲートウェイ装置 1 0 2 は、分布情報 F 2 に基づいて、しきい値 T h A 2 を設定する（ステップ S 2 0 4）。

- [0170] 次に、ゲートウェイ装置102は、取得タイミング t における検知対象バスの通信負荷 L_t を取得するとともに、移動平均 A_t を算出する（ステップS206）。
- [0171] 次に、ゲートウェイ装置102は、設定したしきい値 $ThA2$ と算出した移動平均 A_t とを比較する（ステップS208）。
- [0172] 次に、ゲートウェイ装置102は、移動平均 A_t がしきい値 $ThA2$ 以下である場合（ステップS210でNO）、検知対象バスにおけるトラフィック異常が発生しておらず、通信トラフィックは正常であると判断する（ステップS212）。
- [0173] 次に、ゲートウェイ装置102は、次の取得タイミング $t+1$ における検知対象バスの移動平均 A_{t+1} を算出する処理（ステップS206）、および移動平均 A_{t+1} としきい値 $ThA2$ とを比較する処理（ステップS208）等を行う。
- [0174] 一方、ゲートウェイ装置102は、移動平均 A_t がしきい値 $ThA2$ より大きい場合（ステップS210でYES）、検知対象バスにおけるトラフィック異常が発生していると判断する（ステップS214）。
- [0175] 次に、ゲートウェイ装置102は、検知対象バスにおけるトラフィック異常が発生していることを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する（ステップS216）。
- [0176] 次に、ゲートウェイ装置102は、次の取得タイミング $t+1$ における検知対象バスの移動平均 A_{t+1} を算出する処理（ステップS206）、および移動平均 A_{t+1} としきい値 $ThA2$ とを比較する処理（ステップS208）等を行う。
- [0177] なお、本発明の第2の実施の形態に係る車載通信システム301では、取得部63が移動平均 A の度数分布 $D2$ を示す分布情報 $F2$ を取得する構成であるとしたが、これに限定するものではない。取得部63は、本発明の第1の実施の形態に係る取得部53と同様に、通信負荷 L の度数分布 $D1$ を示す分布情報 $F1$ を取得する構成であってもよい。

[0178] 図10は、本発明の第2の実施の形態に係る車載通信システムにおける通信負荷の時間変化の一例を示す図である。なお、図10において、縦軸は通信負荷 L を示し、横軸は時刻を示す。図10において、実線は、監視部62が各取得タイミング t において取得した検知対象バスの通信負荷 L_t を示し、破線は、監視部62が各取得タイミング t において算出した移動平均 A_t を示す。

[0179] 図10を参照して、検知対象バスの通信負荷 L_t は一定でなく、ばらついている。このため、たとえば、監視部62が取得タイミング t における通信負荷 L_t をそのまま検知部64へ出力する構成では、検知対象バスにおけるトラフィック異常が発生していない場合であっても、検知部64が、通信負荷 L_t としきい値 $ThA2$ とを比較した結果、通信負荷 L_t がしきい値 $ThA2$ を超え、検知対象バスにおけるトラフィック異常が発生していると誤って判断する場合がある。

[0180] これに対して、第2の実施の形態に係る検知装置では、監視部62は、取得タイミング t における検知対象バスの通信負荷 L_t として、検知対象バスの通信負荷 L の移動平均 A_t を算出する。監視部62は、算出した移動平均 A_t を検知部64へ出力する。検知部64は、受けた移動平均 A_t としきい値 $ThA2$ とを比較し、比較結果に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0181] このような構成により、通信負荷 L_t よりもばらつきが小さい移動平均 A_t としきい値 $ThA2$ とを比較した結果を、検知対象バスにおけるトラフィック異常の検知に用いることができる。これにより、検知対象バスにおけるトラフィック異常をより正しく検知することができる。

[0182] その他の構成および動作は第1の実施の形態に係る車載通信システム301と同様であるため、ここでは詳細な説明を繰り返さない。

[0183] 次に、本発明の他の実施の形態について図面を用いて説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰り返さない。

[0184] <第3の実施の形態>

本実施の形態は、第2の実施の形態に係るゲートウェイ装置と比べて、取得タイミング t における通信負荷 L_t の推定値を用いて、車載ネットワーク12における不正メッセージの発生を推定するゲートウェイ装置に関する。以下で説明する内容以外は第1の実施の形態に係るゲートウェイ装置と同様である。

[0185] 図11は、本発明の第3の実施の形態に係るゲートウェイ装置の構成を示す図である。

[0186] 図11を参照して、ゲートウェイ装置103は、通信処理部51と、監視部72と、取得部73と、検知部74と、通知部75、記憶部56と、推定部77とを備える。

[0187] ゲートウェイ装置103における通信処理部51の動作は、図3に示すゲートウェイ装置101における通信処理部51と同様である。

[0188] 監視部72は、たとえば、第2の実施の形態の監視部62と同様に、取得タイミング t において通信負荷 L_t を取得するとともに移動平均 A_t を算出する。

[0189] 監視部72は、取得した通信負荷 L_t および算出した移動平均 A_t を、検知部74および推定部77へ出力するとともに、記憶部56に保存する。

[0190] [推定部]

推定部77は、監視部72によって取得された、第1のタイミングより前のタイミングにおける通信負荷 L に基づいて、第1のタイミングにおける通信負荷 L の推定値 P を算出する。

[0191] より詳細には、推定部77は、たとえば自己回帰和分移動平均モデル（ARIMAモデル）を用いて、取得タイミング t より前の過去のタイミングにおける通信負荷 L に基づいて、取得タイミング t における通信負荷 L_t の推定値 P_t を算出する。

[0192] たとえば、記憶部56は、自己回帰和分移動平均モデル、および、推定値 P の算出に用いる過去の通信負荷 L のデータ数などを示す設定情報を記憶している。推定部77は、記憶部56から設定情報を取得し、設定情報に従っ

て、取得タイミング t における通信負荷 L_t の推定値 P_t を算出する。

[0193] 図 12 は、本発明の第 3 の実施の形態に係る車載通信システムにおける通信負荷の時間変化の一例を示す図である。図 12 において、縦軸は通信負荷 L を示し、横軸は時刻を示す。また、図 12 において、黒いドットは通信負荷 L の測定値を示し、白いドットは通信負荷 L の推定値 P を示す。

[0194] なお、ここでは、記憶部 56 に保存された上記設定情報において、推定値 P の算出に用いる過去の通信負荷 L のデータ数として、3 が設定されているものとする。

[0195] 図 12 を参照して、推定部 77 は、監視部 72 から取得タイミング $t-1$ における通信負荷 L_{t-1} を受けると、一つ前の取得タイミング $t-2$ における通信負荷 L_{t-2} と、二つ前の取得タイミング $t-3$ における通信負荷 L_{t-3} とを記憶部 56 から取得する。

[0196] 推定部 77 は、通信負荷 L_{t-1} 、 L_{t-2} 、 L_{t-3} に基づいて、次の取得タイミング t における通信負荷 L_t の推定値 P_t を算出する。

[0197] より詳細には、推定部 77 は、以下の式 (1) に従って、取得タイミング t における通信負荷 L_t の推定値 P_t を算出し、算出した推定値 P_t を検知部 74 へ出力する。

[数1]

$$P_t = y_{t-1} + \sum_{k=1}^A \phi_k \{y_{t-k} - B(y_{t-(k+1)})\} + \sum_{k=1}^C \theta_k \varepsilon_{t-k} + \text{Constant} \cdots (1)$$

[0198] ここで、 P_t は、取得タイミング t における検知対象バスの通信負荷の推定値である。 y_t は、取得タイミング t における検知対象バスの通信負荷の測定値である。 ϕ 、 θ および B は、予め設定された任意の適切なパラメータである。 ε は誤差項である。 A は自己回帰の次数であり、 C は移動平均の次数である。

[0199] [取得部]

取得部 73 は、第 2 の実施の形態の取得部 63 と同様に、監視部 72 によ

って取得された移動平均Aの履歴を取得する。

[0200] 再び図12を参照して、取得部73は、監視部72によって取得された通信負荷Lから、推定部77によって算出された当該通信負荷Lに対応する推定値Pを差し引いた値（以下、誤差Eとも称する。）の履歴を取得する。

[0201] 取得部73は、たとえば、誤差Eの履歴として、サーバ等の他の装置によって予め作成された誤差Eの度数分布を示す分布情報F3を取得する。

[0202] 図13は、本発明の第3の実施の形態に係る車載通信システムにおける通信負荷の誤差の度数分布の一例を示す図である。なお、図13において、縦軸は度数を示し、横軸は誤差Eを示す。

[0203] 図13を参照して、サーバは、監視部72によって一定期間にわたって取得されたバス13ごとの通信負荷Lと、推定部77によって算出された対応の推定値Pとに基づいて、誤差Eの度数分布D3をバス13ごとに作成する。この誤差Eは、たとえば、対象車両と同じ種類のテスト車両すなわち他の車載ネットワークにおいて取得される。なお、サーバは、対象車両すなわち自己の車載ネットワークにおいて取得された誤差Eに基づいて度数分布D3を作成してもよい。

[0204] サーバは、作成した度数分布D3に基づいて、誤差Eの標本平均および標本標準偏差などを算出する。サーバは、取得部73から分布情報F3の送信要求を受けると、誤差Eの標本平均および標本標準偏差などを含む分布情報F3を要求元の対象車両へ送信する。

[0205] 再び図11を参照して、取得部73は、検知対象バスの分布情報F3の送信要求をサーバへ送信することにより、分布情報F3を取得する。取得部73は、車載通信機111および通信処理部51経由でサーバから分布情報F3を受信すると、受信した分布情報F3を検知部54へ出力する。

[0206] なお、ゲートウェイ装置103では、取得部73が、車載通信機111および通信処理部51経由でサーバから分布情報F3を受信する構成であるとしたが、これに限定するものではない。たとえば、サーバまたは整備用端末装置によって記憶部56に各バス13の分布情報F3が保存されており、取

得部 5 3 が記憶部 5 6 から検知対象バスの分布情報 F 3 を取得する構成であってもよい。

[0207] [検知部]

検知部 7 4 は、第 2 の実施の形態の検知部 6 4 と同様に、取得部 7 3 によって取得された移動平均 A の履歴、および、監視部 7 2 によって取得された、当該履歴に含まれる各移動平均 A の取得タイミングよりも後の取得タイミング t において算出された移動平均 A t に基づいて、検知対象バスにおけるトラフィック異常を検知する。

[0208] さらに、検知部 7 4 は、監視部 7 2 によって取得された第 1 のタイミングにおける通信負荷 L と、推定部 7 7 によって算出された第 1 のタイミングにおける通信負荷 L の推定値 P とを比較し、比較結果に基づいて、車載ネットワーク 1 2 における不正メッセージの発生を推定する。

[0209] より詳細には、検知部 7 4 は、監視部 7 2 によって取得された取得タイミング t における通信負荷 L t と、推定部 7 7 によって算出された対応の推定値 P t との差分である誤差 E t を算出し、算出した誤差 E t に基づいて、検知対象バスにおける不正メッセージの発生を推定する。

[0210] たとえば、検知部 7 4 は、取得部 7 3 から受けた分布情報 F 3、監視部 7 2 から受けた通信負荷 L t、および、推定部 7 7 から受けた推定値 P t に基づいて、検知対象バスにおける不正メッセージの発生を推定する。

[0211] より詳細には、サーバが作成した度数分布 D 3 は、検知対象バスにおいて不正メッセージが発生していないときの誤差 E の度数分布であると仮定することができる。検知部 7 4 は、度数分布 D 3 に対応する分布情報 F 3、および、監視部 7 2 から受けた通信負荷 L t と推定部 7 7 から受けた推定値 P t とから算出される誤差 E t に基づいて、検知対象バスにおける不正メッセージの発生を推定する。

[0212] たとえば、検知部 7 4 は、取得部 7 3 から受けた分布情報 F 3 に基づいて、誤差 E の度数分布を正規分布で近似した確率密度関数をモデルとして作成し、作成したモデルと、算出した誤差 E t とに基づいて、検知対象バスにお

ける不正メッセージの発生を推定する。

[0213] 図14は、本発明の第3の実施の形態に係るゲートウェイ装置における検知部による不正メッセージの発生の推定例を示す図である。なお、図14において、横軸は差分を示す。図14の破線は、誤差Eの度数分布D3を正規分布で近似した確率密度関数を示す。

[0214] 図11および図14を参照して、検知部74は、取得部73から分布情報F3を受けると、分布情報F3に基づいて、不正メッセージが発生していない場合における誤差Eの平均値の信頼区間の下限値A3および上限値B3を算出し、算出した上限値B3をしきい値 T_{hA3} として設定する。

[0215] 検知部74は、監視部72から通信負荷 L_t を受け、かつ、推定部77から当該通信負荷 L_t に対応する推定値 P_t を受けると、通信負荷 L_t と推定値 P_t との差分を誤差 E_t として算出し、算出した誤差 E_t としきい値 T_{hA3} とを比較する。

[0216] たとえば、検知部74は、取得タイミング t_1 に対応する誤差 E_{t1} がしきい値 T_{hA3} 以下である場合、検知対象バスにおいて不正メッセージは発生していないと推定する。

[0217] これは、たとえば、取得タイミング t_1 において、検知対象バスにおいて不正メッセージが発生していない場合、誤差 E_{t1} は図14に示す確率密度関数の中心の近傍に位置する可能性が高く、しきい値 T_{hA3} を超える可能性は低いからである。

[0218] 一方、検知部74は、取得タイミング t_2 に対応する誤差 E_{t2} がしきい値 T_{hA3} より大きい場合、検知対象バスにおいて不正メッセージが発生したと推定する。

[0219] これは、たとえば、取得タイミング t_2 において、検知対象バスにおいて不正メッセージが発生した場合、誤差 E_{t2} は大きい値となり、しきい値 T_{hA3} を超える可能性が高いからである。

[0220] 検知部74は、誤差 E_t およびしきい値 T_{hA3} に基づく推定結果を示す推定情報を、通信処理部51、監視部72、および通知部75へ出力する。

- [0221] 通信処理部 5 1 は、検知部 7 4 から受けた推定情報が、検知対象バスにおいて不正メッセージが発生していないことを示す場合、当該検知対象バスを介してメッセージを送信先の制御装置 1 2 2 へ送信する。
- [0222] 一方、通信処理部 5 1 は、検知部 7 4 から受けた推定情報が、検知対象バスにおいて不正メッセージが発生したことを示す場合、たとえば、当該検知対象バスを介した中継処理を停止する。そして、通信処理部 5 1 は、当該推定情報が示すメッセージおよび検知対象バスをログとして記憶部 5 6 に記録する。
- [0223] 通知部 7 5 は、検知部 7 4 から受けた推定情報が、検知対象バスにおいて不正メッセージが発生したことを示す場合、検知対象バスにおいて不正メッセージが発生したことを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する。
- [0224] 通知部 7 5 は、検知部 7 4 によって車載ネットワーク 1 2 における異常が検知された場合、第 1 の警報情報 $A_r 1$ を出力し、検知部 7 4 によって車載ネットワーク 1 2 における不正メッセージの発生が推定された場合、第 1 の警報情報 $A_r 1$ とは異なる第 2 の警報情報 $A_r 2$ を出力する。
- [0225] たとえば、警報情報は緊急度合いを示す。対象車両内における車載装置は、警報情報を受けると、警報情報が示す緊急度合いを、表示装置等を介してユーザに通知する。通知部 7 5 は、検知対象バスにおけるトラフィック異常が発生していることを示す判断情報を受けた場合と、検知対象バスにおいて不正メッセージが発生したことを示す推定情報を受けた場合とで、緊急度合いが互いに異なる警報情報を送信する。
- [0226] 推定部 7 7 は、検知部 7 4 によって不正メッセージの発生が推定された場合、第 1 のタイミングより後のタイミングである第 2 のタイミングにおける推定値 P を、第 1 のタイミング以降のタイミングにおける通信負荷 L に基づいて算出する。
- [0227] より詳細には、推定部 7 7 は、検知対象バスにおいて不正メッセージが発生したことを示す推定情報を検知部 7 4 から受けると、しきい値 $Th A 3$ を

超える誤差 E が算出されたタイミングより前のタイミングにおいて取得された通信負荷 L を破棄し、新たな推定値 P を、しきい値 $ThA3$ を超える誤差 E が算出されたタイミング以降のタイミングにおいて取得された通信負荷 L に基づいて算出する。

[0228] また、監視部72は、検知部74から検知対象バスにおいて不正メッセージが発生したことを示す推定情報を受けると、新たな移動平均 A を、しきい値 $ThA3$ を超える誤差 E が算出されたタイミング以降のタイミングにおいて取得された通信負荷 L に基づいて算出する。

[0229] [動作]

図15は、本発明の第3の実施の形態に係るゲートウェイ装置が検知対象バスにおけるトラフィック異常の検知および不正メッセージの発生の推定を行う際の動作手順を定めたフローチャートである。

[0230] 図15を参照して、まず、ゲートウェイ装置103は、検知対象バスの移動平均 A の度数分布 $D2$ を示す分布情報 $F2$ 、および誤差 E の度数分布 $D3$ を示す分布情報 $F3$ を取得する（ステップS302）。

[0231] 次に、ゲートウェイ装置103は、分布情報 $F2$ に基づいてしきい値 $ThA2$ を設定し、また、分布情報 $F3$ に基づいてしきい値 $ThA3$ を設定する（ステップS304）。

[0232] 次に、ゲートウェイ装置103は、取得タイミング t における検知対象バスの通信負荷 L_t を取得するとともに、移動平均 A_t および推定値 P_t を算出する（ステップS306）。

[0233] 次に、ゲートウェイ装置103は、通信負荷 L_t と推定値 P_t とに基づいて誤差 E_t を算出する（ステップS308）。

[0234] 次に、ゲートウェイ装置103は、移動平均 A_t としきい値 $ThA2$ とを比較する（ステップS310）。

[0235] 次に、ゲートウェイ装置103は、移動平均 A_t がしきい値 $ThA2$ より大きい場合（ステップS312でYES）、検知対象バスにおけるトラフィック異常が発生していると判断する（ステップS314）。

- [0236] 次に、ゲートウェイ装置103は、検知対象バスにおけるトラフィック異常が発生していることを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する（ステップS316）。
- [0237] 次に、ゲートウェイ装置103は、次の取得タイミング $t+1$ における通信負荷 L_{t+1} を取得するとともに移動平均 A_{t+1} および推定値 P_{t+1} を算出する処理（ステップS306）、ならびに誤差 E_{t+1} を算出する処理（ステップS308）等を行う。
- [0238] 一方、ゲートウェイ装置103は、移動平均 A_t がしきい値 $ThA2$ 以下である場合（ステップS312でNO）、誤差 E_t としきい値 $ThA3$ とを比較する（ステップS318）。
- [0239] 次に、ゲートウェイ装置103は、誤差 E_t がしきい値 $ThA3$ 以下である場合（ステップS320でNO）、検知対象バスにおけるトラフィック異常は発生していないと判断し、また、不正メッセージは発生していないと推定する（ステップS322）。
- [0240] 次に、ゲートウェイ装置103は、次の取得タイミング $t+1$ における通信負荷 L_{t+1} を取得するとともに移動平均 A_{t+1} および推定値 P_{t+1} を算出する処理（ステップS306）、ならびに誤差 E_{t+1} を算出する処理（ステップS308）等を行う。
- [0241] 一方、ゲートウェイ装置103は、誤差 E_t がしきい値 $ThA3$ より大きい場合（ステップS320でYES）、検知対象バスにおいて不正メッセージが発生していると推定する（ステップS324）。
- [0242] 次に、ゲートウェイ装置103は、検知対象バスにおいて不正メッセージが発生していることを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する（ステップS326）。
- [0243] 次に、ゲートウェイ装置103は、次の取得タイミング $t+1$ における移動平均 A_{t+1} および推定値 P_{t+1} を、今回の取得タイミング t 以降の取得タイミングにおいて取得された通信負荷 L に基づいて算出する（ステップS328）。

[0244] 次に、ゲートウェイ装置 103 は、通信負荷 L_{t+1} と推定値 P_{t+1} とに基づいて誤差 E_{t+1} を算出する処理（ステップ S308）、および移動平均 A_{t+1} としきい値 $ThA2$ とを比較する処理（ステップ S310）等を行う。

[0245] なお、本発明の第 3 の実施の形態に係る車載通信システム 301 では、推定部 77 が過去のタイミングにおける通信負荷 L に基づいて推定値 P を算出する構成であるとしたが、これに限定するものではない。推定部 77 は過去のタイミングにおける移動平均 A に基づいて推定値 P を算出する構成であってもよい。

[0246] また、本発明の第 3 の実施の形態に係る車載通信システム 301 では、検知部 74 が、第 2 の実施の形態に係る車載通信システム 301 における検知部 64 と同様に、移動平均 A の履歴および移動平均 A_t に基づいて検知対象バスにおけるトラフィック異常を検知する構成であるとしたが、これに限定するものではない。検知部 74 は、第 1 の実施の形態に係る車載通信システム 301 における検知部 54 と同様に、通信負荷 L の履歴および通信負荷 L_t に基づいて検知対象バスにおけるトラフィック異常を検知する構成であってもよい。

[0247] <変形例>

本発明の第 3 の実施の形態に係る車載通信システム 301 では、ゲートウェイ装置 103 は、車載ネットワーク 12 における異常を検知する処理として、検知対象バスにおける不正メッセージによるトラフィック異常を検知する構成であるとしたが、これに限定するものではない。

[0248] ゲートウェイ装置 103 は、車載ネットワーク 12 における異常を検知する処理として、検知対象バスにおける不正メッセージの発生を推定する構成であってもよい。

[0249] より詳細には、ゲートウェイ装置 103 は、検知対象バスにおける不正メッセージの発生を推定した場合に、車載ネットワーク 12 における異常が発生していると判断する構成であってもよい。

- [0250] また、本発明の第3の実施の形態に係る車載通信システム301では、検知部74は、移動平均Aの履歴および移動平均 A_t に基づいて、検知対象バスにおけるトラフィック異常を検知し、かつ、通信負荷 L_t と推定値 P_t との差分である誤差 E_t に基づいて、検知対象バスにおける不正メッセージの発生を推定する構成であるとしたが、これに限定するものではない。
- [0251] 検知部74は、誤差 E_t に基づいて、検知対象バスにおける不正メッセージの発生を推定する一方で、移動平均Aの履歴および移動平均 A_t に基づいて、検知対象バスにおけるトラフィック異常を検知しない構成であってもよい。
- [0252] この場合、取得部73は、上述のように誤差Eの履歴を取得する一方で、移動平均Aの履歴を取得しない構成であってもよい。
- [0253] 図16は、本発明の第3の実施の形態の変形例に係るゲートウェイ装置が検知対象バスにおける不正メッセージの発生の推定を行う際の動作手順を定めたフローチャートである。
- [0254] 図16を参照して、まず、ゲートウェイ装置103は、検知対象バスについての誤差Eの度数分布D3を示す分布情報F3を取得する（ステップS402）。
- [0255] 次に、ゲートウェイ装置103は、分布情報F3に基づいてしきい値 $ThA3$ を設定する（ステップS404）。
- [0256] 次に、ゲートウェイ装置103は、取得タイミングtにおける検知対象バスの通信負荷 L_t を取得するとともに、推定値 P_t を算出する（ステップS406）。
- [0257] 次に、ゲートウェイ装置103は、通信負荷 L_t と推定値 P_t とに基づいて誤差 E_t を算出する（ステップS408）。
- [0258] 次に、ゲートウェイ装置103は、誤差 E_t としきい値 $ThA3$ とを比較する（ステップS410）。
- [0259] 次に、ゲートウェイ装置103は、誤差 E_t がしきい値 $ThA3$ より大きい場合（ステップS412でYES）、検知対象バスにおいて不正メッセー

ジが発生していると推定する（ステップS414）。

[0260] 次に、ゲートウェイ装置103は、検知対象バスにおいて不正メッセージが発生していることを示す警報情報を、対象車両内における車載装置または対象車両外における上位装置へ送信する（ステップS416）。

[0261] 次に、ゲートウェイ装置103は、次の取得タイミング $t+1$ における推定値 P_{t+1} を、今回の取得タイミング t 以降の取得タイミングにおいて取得された通信負荷 L に基づいて算出する（ステップS418）。

[0262] 次に、ゲートウェイ装置103は、通信負荷 L_{t+1} と推定値 P_{t+1} とに基づいて誤差 E_{t+1} を算出する処理（ステップS408）、および誤差 E_{t+1} としきい値 $ThA3$ とを比較する処理（ステップS410）等を行う。

[0263] 一方、ゲートウェイ装置103は、誤差 E_t がしきい値 $ThA3$ 以下である場合（ステップS412でNO）、検知対象バスにおいて不正メッセージは発生していないと推定する（ステップS420）。

[0264] 次に、ゲートウェイ装置103は、次の取得タイミング $t+1$ における通信負荷 L_{t+1} を取得するとともに推定値 P_{t+1} を算出する処理（ステップS406）、および誤差 E_{t+1} を算出する処理（ステップS408）等を行う。

[0265] [課題]

図17は、本発明の第3の実施の形態に係る車載通信システムにおける通信負荷の時間変化の一例を示す図である。なお、図17において、縦軸は通信負荷 L を示し、横軸は時刻を示す。図17において、実線は、監視部72が各取得タイミング t において取得した検知対象バスの通信負荷 L_t を示し、破線は、監視部72が各取得タイミング t において算出した移動平均 A_t を示す。

[0266] 本発明の第2の実施の形態に係るゲートウェイ装置102のように、検知部64が移動平均 A_t としきい値 $ThA2$ とを比較した結果に基づいて、検知対象バスにおけるトラフィック異常が発生しているか否かを判断する構成

では、判断結果に基づいて警報情報を送信するタイミングが、実際に不正メッセージの送信が開始されたタイミングから遅延してしまう場合がある。

[0267] より詳細には、図 17 を参照して、時刻 t_a において検知対象バスへの擬似的な不正メッセージの送信を開始した場合を想定する。移動平均 A_t は、時刻 t_a において増大し始める一方で、時刻 t_b においてはじめてしきい値 $ThA2$ を超える。したがって、警報情報を送信するタイミングは時刻 t_b となり、実際に不正メッセージの送信が開始されたタイミングである時刻 t_a から遅延が生じてしまう。

[0268] これに対して、本発明の第 3 の実施の形態に係るゲートウェイ装置 103 では、取得タイミング t より前の取得タイミングにおける通信負荷 L に基づいて、取得タイミング t における通信負荷 L_t の推定値 P_t を算出し、通信負荷 L_t と推定値 P_t との差分である誤差 E_t としきい値 $ThA3$ とを比較した結果に基づいて、検知対象バスにおいて不正メッセージが発生しているか否かを推定する。

[0269] このような構成により、取得タイミング t における移動平均 A_t がしきい値 $ThA2$ を超えない場合であっても、過去のタイミングにおける通信負荷 L から推定される推定値 P_t と通信負荷 L_t との差分がしきい値 $ThA3$ を超えた場合、不正メッセージが発生していると推定することができる。これにより、移動平均 A_t に基づいて検知対象バスにおけるトラフィック異常を検知できるタイミングよりも早く、検知対象バスにおける不正メッセージの発生を推定することができる。

[0270] また、本発明の第 3 の実施の形態に係るゲートウェイ装置 103 では、推定部 77 は、検知部 74 によって不正メッセージの発生が推定された場合、新たな推定値 P を、しきい値 $ThA3$ を超える誤差 E が算出されたタイミング以降のタイミングにおいて取得された通信負荷 L に基づいて算出する。

[0271] このような構成により、通信負荷 L が大幅に増大したタイミング以降の通信負荷 L に基づいて、新たな推定値 P をより正確に算出することができる。これにより、たとえば、通信負荷 L のさらなる変化が生じた場合であっても

、新たに算出した推定値 P に基づいて検知対象バスにおける不正メッセージの発生を正確に推定することができる。

[0272] また、本発明の第3の実施の形態に係るゲートウェイ装置103では、通知部75は、検知部74によって車載ネットワーク12における異常が検知された場合、第1の警報情報 A_r1 を出力し、検知部74によって車載ネットワーク12における不正メッセージの発生が推定された場合、第1の警報情報 A_r1 とは異なる第2の警報情報 A_r2 を出力する。

[0273] このような構成により、検知対象バスにおけるトラフィック異常が発生した場合と、検知対象バスにおいて不正メッセージが発生したと推定された場合とで、通知部75が互いに異なる警報情報を送信することにより、たとえば、状況に応じて緊急度合いが異なる警告をユーザに通知することができる。

[0274] また、本発明の第3の実施の形態に係る検知装置は、複数の車載装置を含む車載ネットワーク12における異常を検知する。監視部72は、車載ネットワーク12における送信メッセージを監視し、車載ネットワーク12における通信負荷 L を取得する。推定部77は、監視部72によって過去に取得された通信負荷 L に基づいて、監視部72によって取得される通信負荷 L の推定値 P を算出する。取得部73は、自己または他の車載ネットワークにおける通信負荷 L と通信負荷 L の推定値 P との差分である誤差 E の履歴を取得する。検知部74は、取得部73によって取得された通信負荷 L と通信負荷 L の推定値 P との差分の履歴、監視部72によって取得された、通信負荷 L と通信負荷 L の推定値 P との差分の履歴よりも後の取得タイミング t における通信負荷 L_t 、および推定部77によって算出された取得タイミング t における通信負荷 L_t の推定値 P_t に基づいて、車載ネットワークにおける異常を検知する。

[0275] たとえば、検知対象バスにおいて不正メッセージが発生すると、取得タイミング t における通信負荷 L_t と推定値 P_t との差分は大きな値となる。本発明の第3の実施の形態に係る検知装置は、通信負荷 L_t と推定値 P_t との

差分に着目し、通信負荷 L_t と推定値 P_t との差分の履歴、取得タイミング t における通信負荷 L_t 、および通信負荷 L_t の推定値 P_t に基づいて検知対象バスにおける不正メッセージの発生を推定する構成により、たとえば特許文献1に記載の異常検知装置および特許文献2に記載のセキュリティ装置と比べて、簡易な処理によって検知対象バスにおける不正メッセージの発生を推定することができる。

[0276] したがって、本発明の第3の実施の形態に係る検知装置では、簡易な処理によって車載ネットワーク12における異常を正しく検知することができる。

[0277] また、本発明の第3の実施の形態に係るゲートウェイ装置103は、車載ネットワーク12における車載装置間のメッセージを中継する。監視部72は、車載ネットワーク12における送信メッセージを監視し、車載ネットワーク12における通信負荷 L を取得する。推定部77は、監視部72によって過去に取得された通信負荷 L に基づいて、監視部72によって取得される通信負荷 L の推定値 P を算出する。取得部73は、自己または他の車載ネットワークにおける通信負荷 L と通信負荷 L の推定値 P との差分である誤差 E の履歴を取得する。検知部74は、取得部73によって取得された通信負荷 L と通信負荷 L の推定値 P との差分の履歴、監視部72によって取得された、通信負荷 L と通信負荷 L の推定値 P との差分の履歴よりも後の取得タイミング t における通信負荷 L_t 、および推定部77によって算出された取得タイミング t における通信負荷 L_t の推定値 P_t に基づいて、車載ネットワークにおける異常を検知する。

[0278] たとえば、検知対象バスにおいて不正メッセージが発生すると、取得タイミング t における通信負荷 L_t と推定値 P_t との差分は大きな値となる。本発明の第3の実施の形態に係るゲートウェイ装置103は、通信負荷 L_t と推定値 P_t との差分に着目し、通信負荷 L_t と推定値 P_t との差分の履歴、取得タイミング t における通信負荷 L_t 、および通信負荷 L_t の推定値 P_t に基づいて検知対象バスにおける不正メッセージの発生を推定する構成によ

り、たとえば特許文献１に記載の異常検知装置および特許文献２に記載のセキュリティ装置と比べて、簡易な処理によって検知対象バスにおける不正メッセージの発生を推定することができる。

[0279] したがって、本発明の第３の実施の形態に係るゲートウェイ装置１０３では、簡易な処理によって車載ネットワーク１２における異常を正しく検知することができる。

[0280] その他の構成および動作は第１の実施の形態に係る車載通信システム３０１と同様であるため、ここでは詳細な説明を繰り返さない。

[0281] 上記実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記説明ではなく請求の範囲によって示され、請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

[0282] 以上の説明は、以下に付記する特徴を含む。

[付記１]

複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、

前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷の時系列データの移動平均を算出する監視部と、

前記監視部によって算出された前記移動平均の度数分布を示す第１の分布情報を取得する取得部と、

前記取得部によって取得された前記第１の分布情報に基づいて第１のしきい値を設定し、設定した前記第１のしきい値、および前記監視部によって取得された、前記度数分布に含まれる前記移動平均の取得タイミングよりも後の第１のタイミングにおける前記移動平均に基づいて、前記車載ネットワークにおける異常を検知する検知部と、

前記監視部によって取得された、前記第１のタイミングより前のタイミングにおける前記移動平均に基づいて、前記第１のタイミングにおける前記移動平均の推定値を算出する推定部とを備え、

前記監視部は、さらに、前記第1のタイミングにおける前記移動平均と前記推定値との差分を誤差として算出し、

前記取得部は、さらに、前記監視部によって算出された前記誤差の度数分布を示す第2の分布情報を取得し、

前記検知部は、さらに、前記取得部によって取得された前記第2の分布情報に基づいて第2のしきい値を設定し、設定した前記第2のしきい値、および前記監視部によって取得された前記第1のタイミングにおける前記誤差に基づいて、前記車載ネットワークにおける不正メッセージの発生を推定する、検知装置。

[0283] [付記2]

車載ネットワークにおける車載装置間のメッセージを中継するゲートウェイ装置であって、

前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷の時系列データの移動平均を算出する監視部と、

前記監視部によって算出された前記移動平均の度数分布を示す第1の分布情報を取得する取得部と、

前記取得部によって取得された前記第1の分布情報に基づいて第1のしきい値を設定し、設定した前記第1のしきい値、および前記監視部によって取得された、前記度数分布に含まれる前記移動平均の取得タイミングよりも後の第1のタイミングにおける前記移動平均に基づいて、前記車載ネットワークにおける異常を検知する検知部と、

前記監視部によって取得された、前記第1のタイミングより前のタイミングにおける前記移動平均に基づいて、前記第1のタイミングにおける前記移動平均の推定値を算出する推定部とを備え、

前記監視部は、さらに、前記第1のタイミングにおける前記移動平均と前記推定値との差分を誤差として算出し、

前記取得部は、さらに、前記監視部によって算出された前記誤差の度数分布を示す第2の分布情報を取得し、

前記検知部は、さらに、前記取得部によって取得された前記第2の分布情報に基づいて第2のしきい値を設定し、設定した前記第2のしきい値、および前記監視部によって取得された前記第1のタイミングにおける前記誤差に基づいて、前記車載ネットワークにおける不正メッセージの発生を推定する、ゲートウェイ装置。

符号の説明

- [0284] 1 2 車載ネットワーク
- 1 3, 1 4 バス
- 5 1 通信処理部
- 5 2 監視部
- 5 3 取得部
- 5 4 検知部
- 5 5 通知部
- 5 6 記憶部
- 6 2 監視部
- 6 3 取得部
- 6 4 検知部
- 7 2 監視部
- 7 3 取得部
- 7 4 検知部
- 7 5 通知部
- 1 0 1 ゲートウェイ装置
- 1 0 2 ゲートウェイ装置
- 1 0 3 ゲートウェイ装置
- 1 1 1 車載通信機
- 1 1 2 ポート
- 1 2 1 バス接続装置群
- 1 2 2 制御装置

1 3 1 検知装置

3 0 1 車載通信システム

請求の範囲

- [請求項1] 複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、
- 前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、
- 自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、
- 前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える、検知装置。
- [請求項2] 前記検知装置は、さらに、
- 前記監視部によって取得された、前記第1のタイミングより前のタイミングにおける前記通信負荷に基づいて、前記第1のタイミングにおける前記通信負荷の推定値を算出する推定部を備え、
- 前記検知部は、前記監視部によって取得された前記第1のタイミングにおける前記通信負荷と、前記推定部によって算出された前記第1のタイミングにおける前記推定値とを比較し、比較結果に基づいて、前記車載ネットワークにおける不正メッセージの発生を推定する、請求項1に記載の検知装置。
- [請求項3] 前記推定部は、前記検知部によって前記不正メッセージの発生が推定された場合、前記第1のタイミングより後のタイミングである第2のタイミングにおける前記推定値を、前記第1のタイミング以降のタイミングにおける前記通信負荷に基づいて算出する、請求項2に記載の検知装置。
- [請求項4] 前記検知装置は、さらに、
- 前記検知部によって前記車載ネットワークにおける異常が検知された場合、第1の警報情報を出力し、前記検知部によって前記車載ネッ

トワークにおける不正メッセージの発生が推定された場合、前記第1の警報情報とは異なる第2の警報情報を出力する通知部を備える、請求項2または請求項3に記載の検知装置。

[請求項5] 前記監視部は、前記第1のタイミングにおける前記通信負荷として、前記通信負荷の時系列データの移動平均を算出する、請求項1から請求項4のいずれか1項に記載の検知装置。

[請求項6] 複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、

前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、

前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、

自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、

前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部とを備える、検知装置。

[請求項7] 複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置における検知方法であって、

前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、

自己または他の車載ネットワークにおける通信負荷の履歴を取得するステップと、

取得した前記履歴、および前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常

を検知するステップとを含む、検知方法。

[請求項8] 複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置における検知方法であって、

前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得するステップと、

過去に取得した前記通信負荷に基づいて、前記通信負荷の推定値を算出するステップと、

自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得するステップと、

取得した前記履歴、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知するステップとを含む、検知方法。

[請求項9] 複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置において用いられる検知プログラムであって、

コンピュータを、

前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、

自己または他の車載ネットワークにおける通信負荷の履歴を取得する取得部と、

前記取得部によって取得された前記履歴、および前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷に基づいて、前記車載ネットワークにおける異常を検知する検知部、

として機能させるための、検知プログラム。

[請求項10] 複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置において用いられる検知プログラムであって、

コンピュータを、

複数の車載装置を含む車載ネットワークにおける異常を検知する検知装置であって、

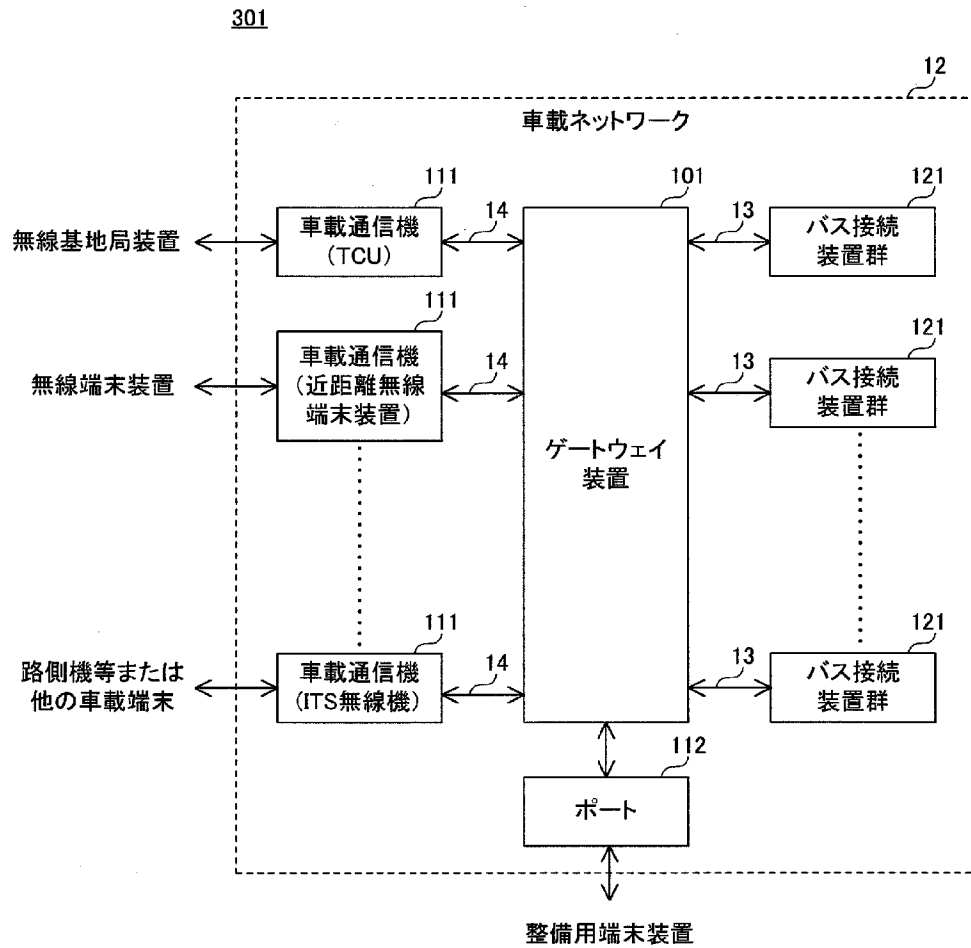
前記車載ネットワークにおける送信メッセージを監視し、前記車載ネットワークにおける通信負荷を取得する監視部と、

前記監視部によって過去に取得された前記通信負荷に基づいて、前記監視部によって取得される前記通信負荷の推定値を算出する推定部と、

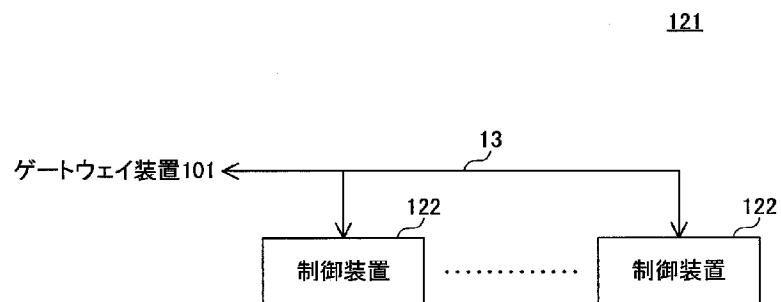
自己または他の車載ネットワークにおける通信負荷と推定値との差分の履歴を取得する取得部と、

前記取得部によって取得された前記履歴、前記監視部によって取得された、前記履歴よりも後の第1のタイミングにおける前記通信負荷、および前記推定部によって算出された、前記第1のタイミングにおける前記通信負荷の前記推定値に基づいて、前記車載ネットワークにおける異常を検知する検知部、
として機能させるための、検知プログラム。

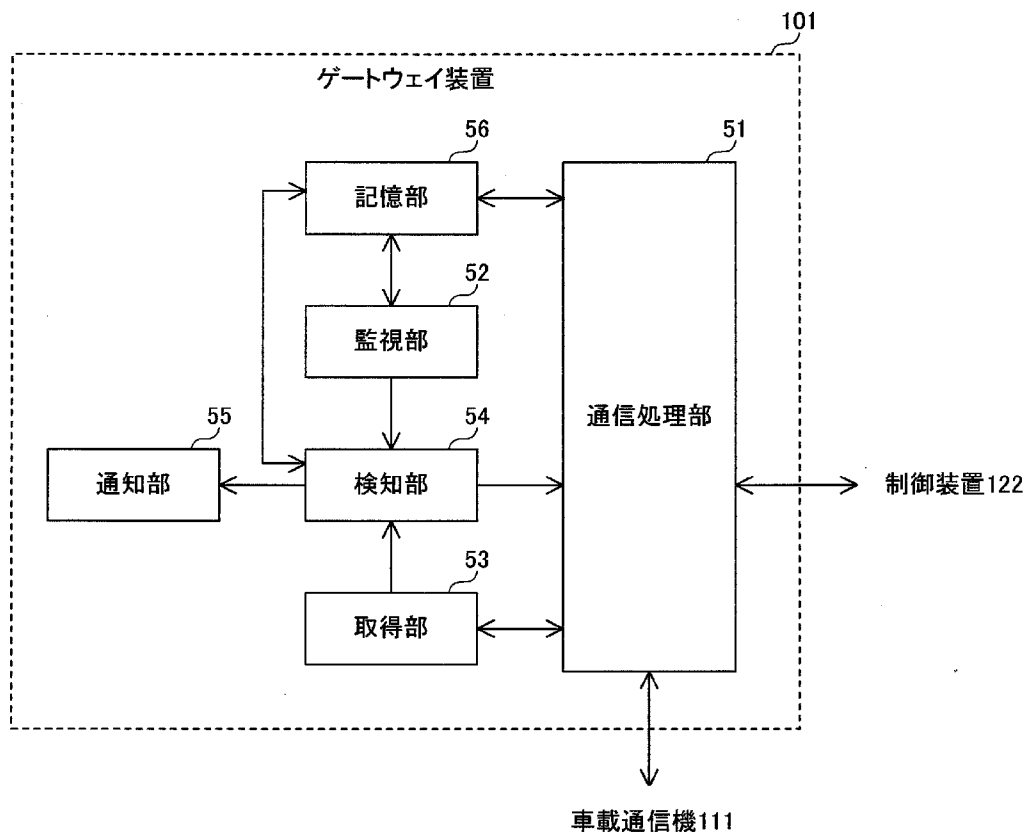
[図1]



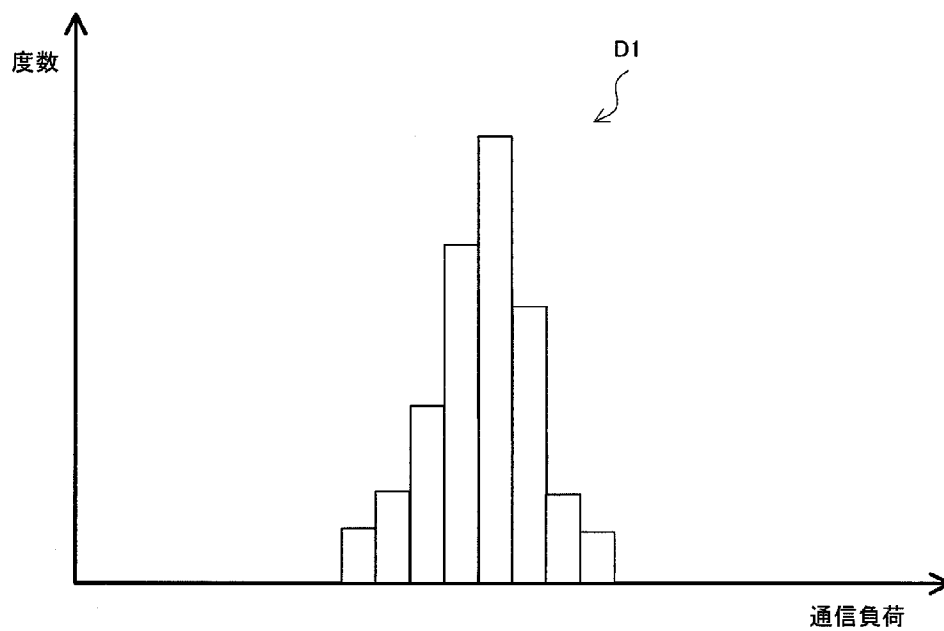
[図2]



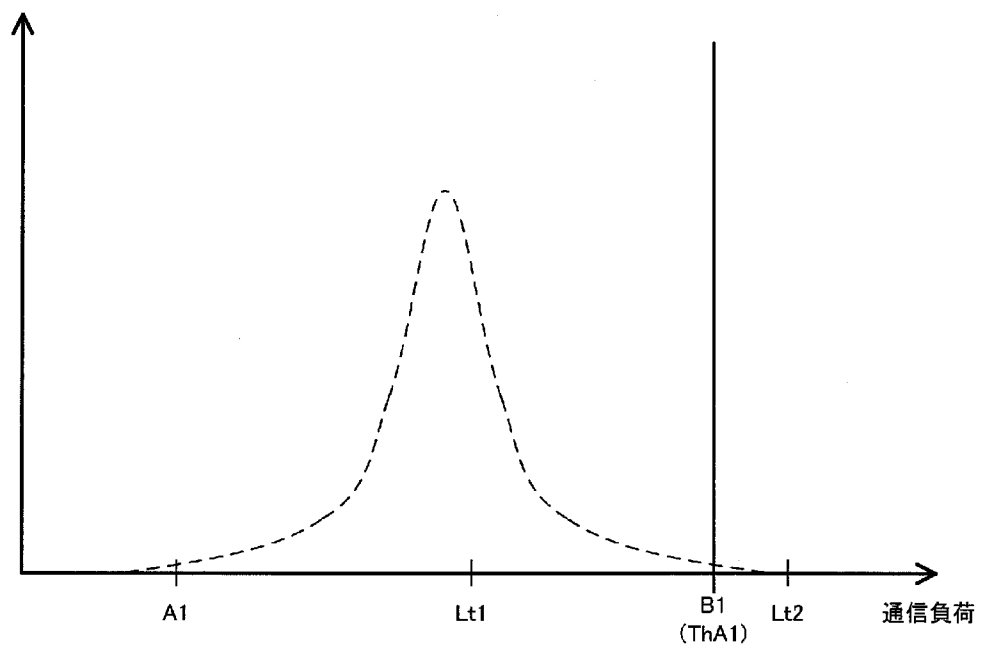
[図3]



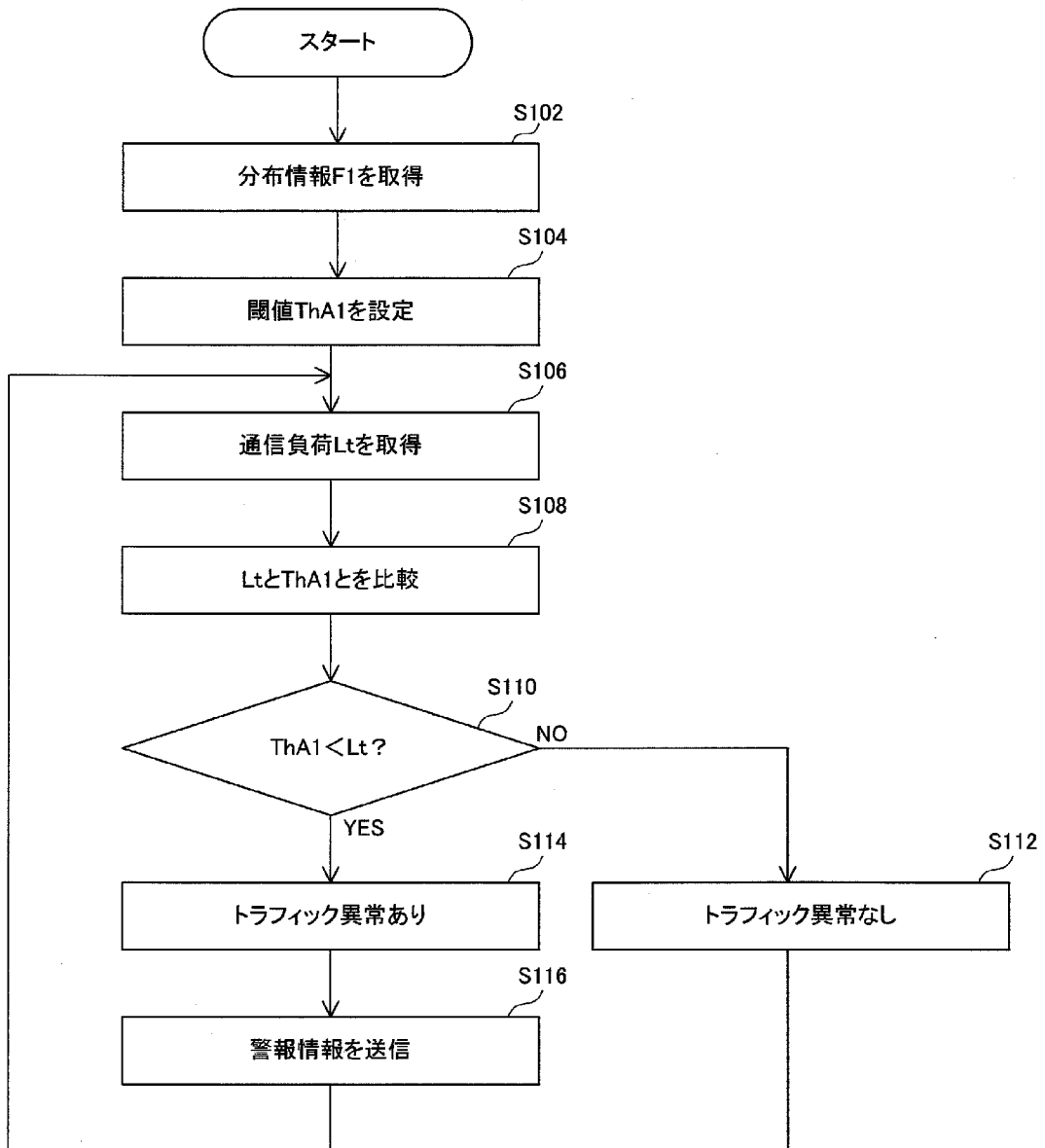
[図4]



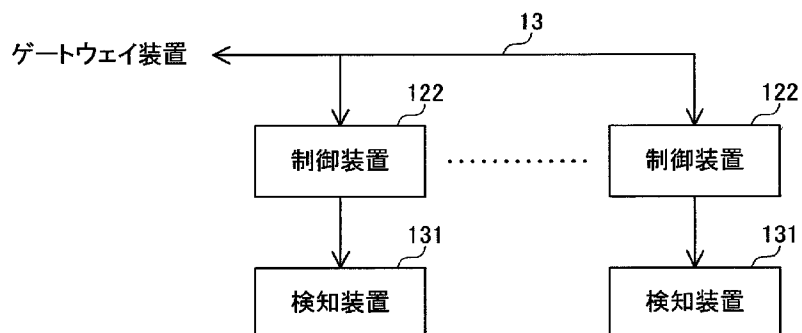
[図5]



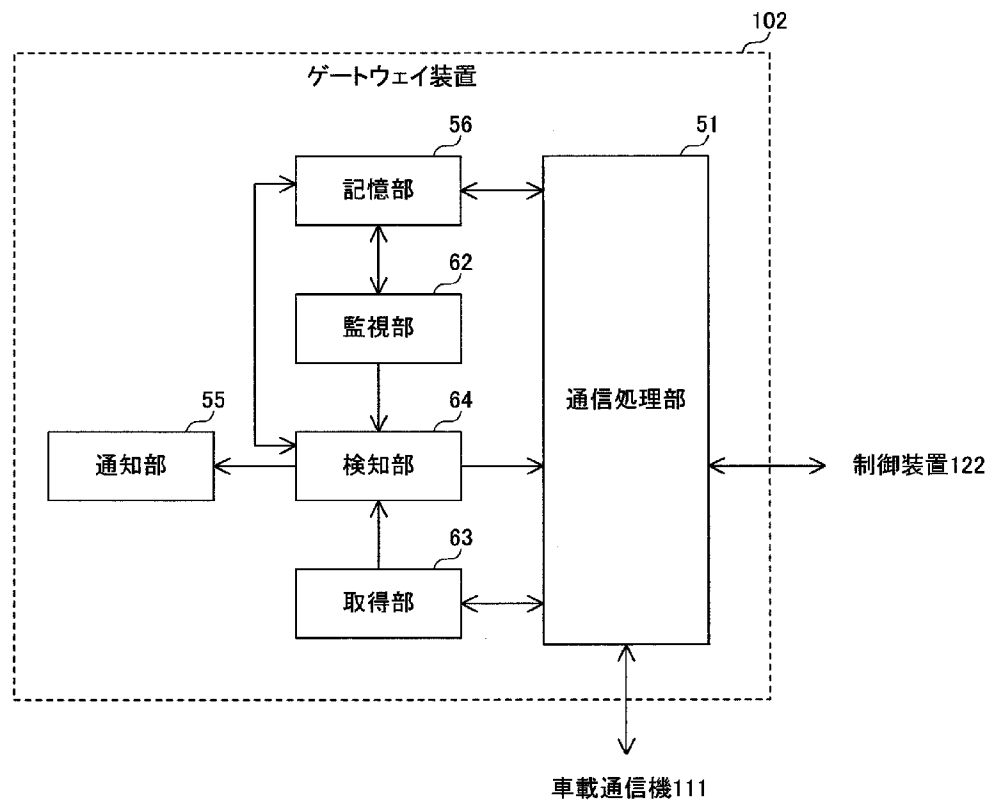
[図6]



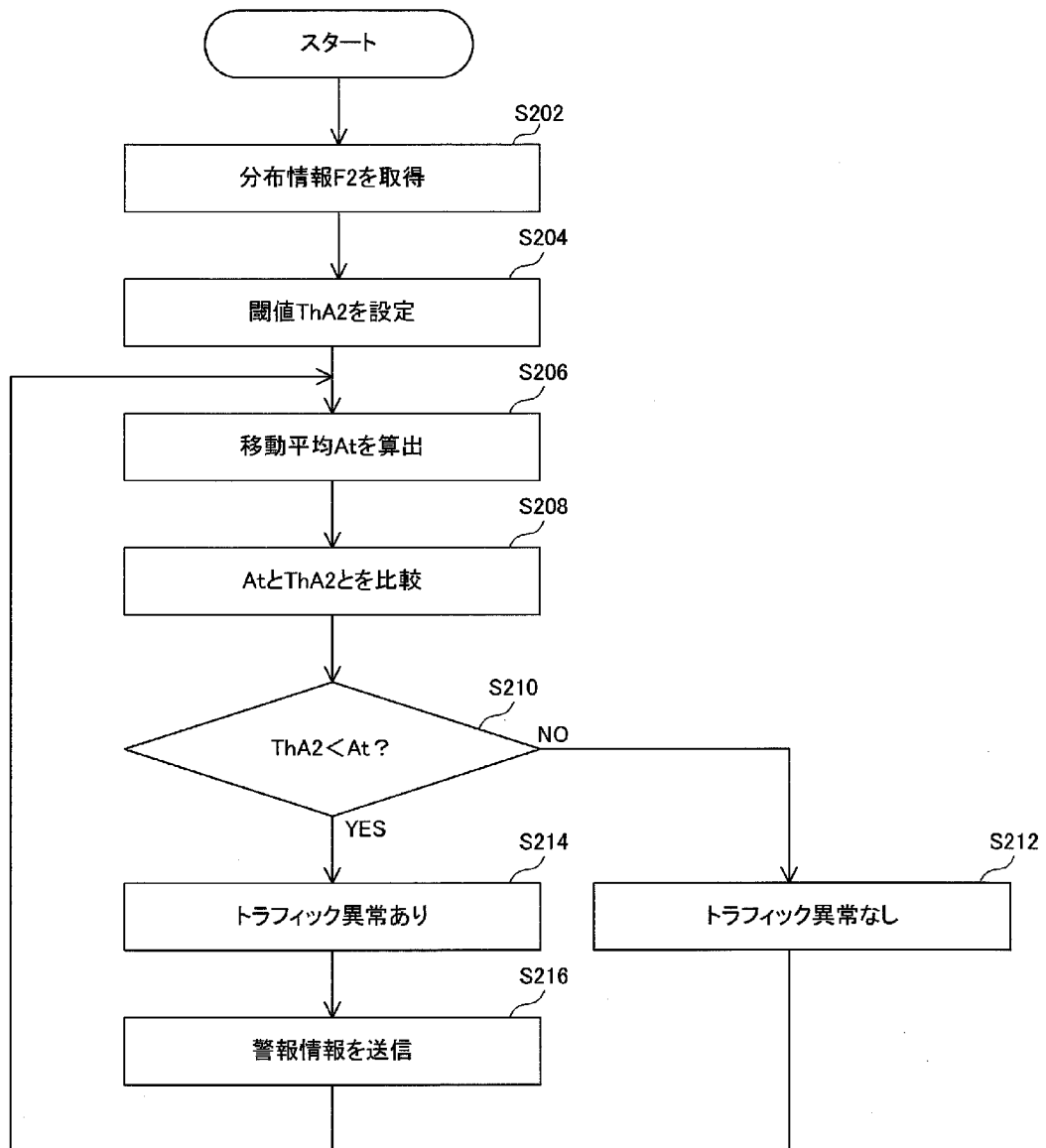
[図7]



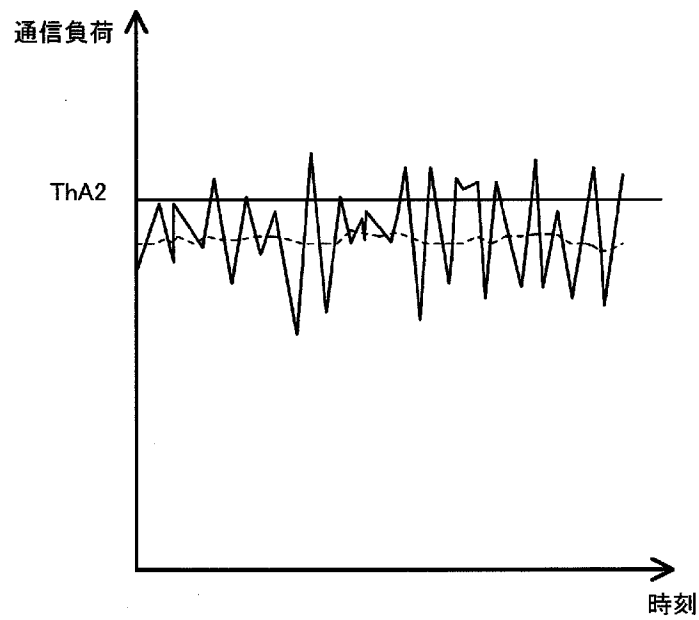
[図8]



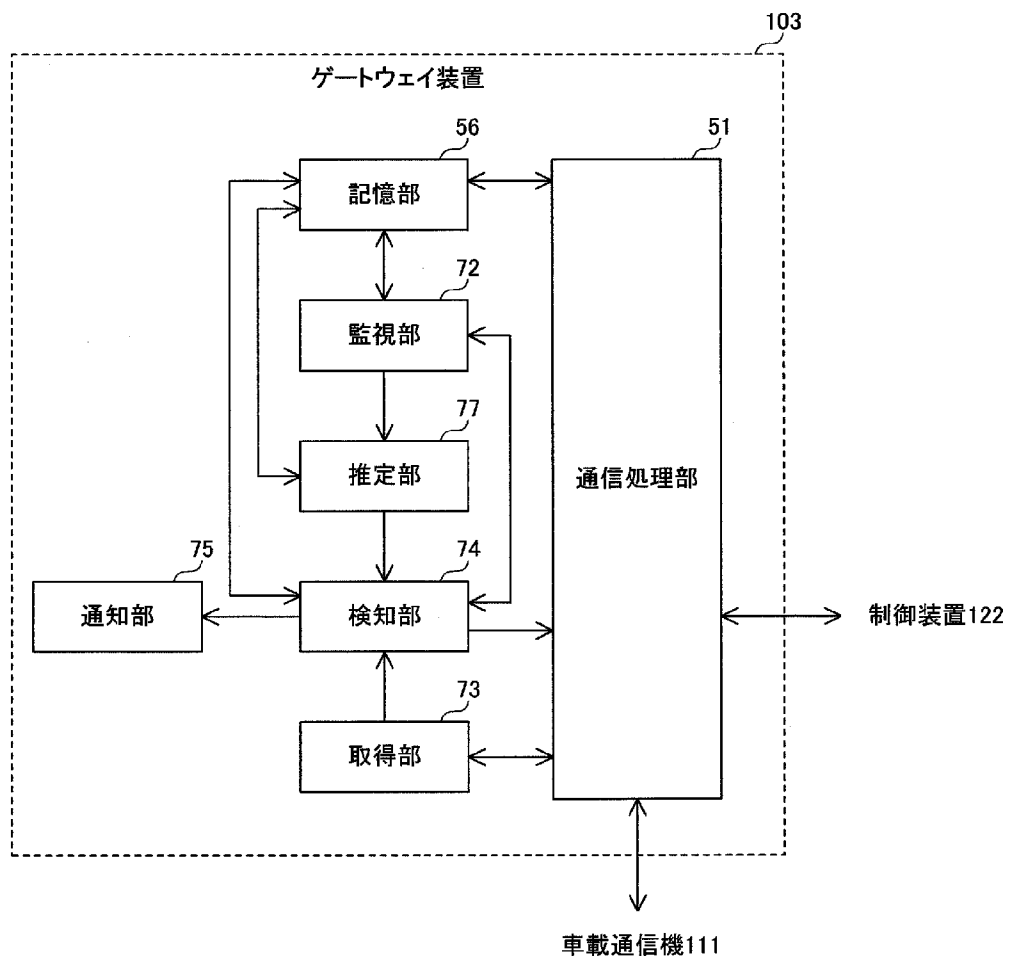
[図9]



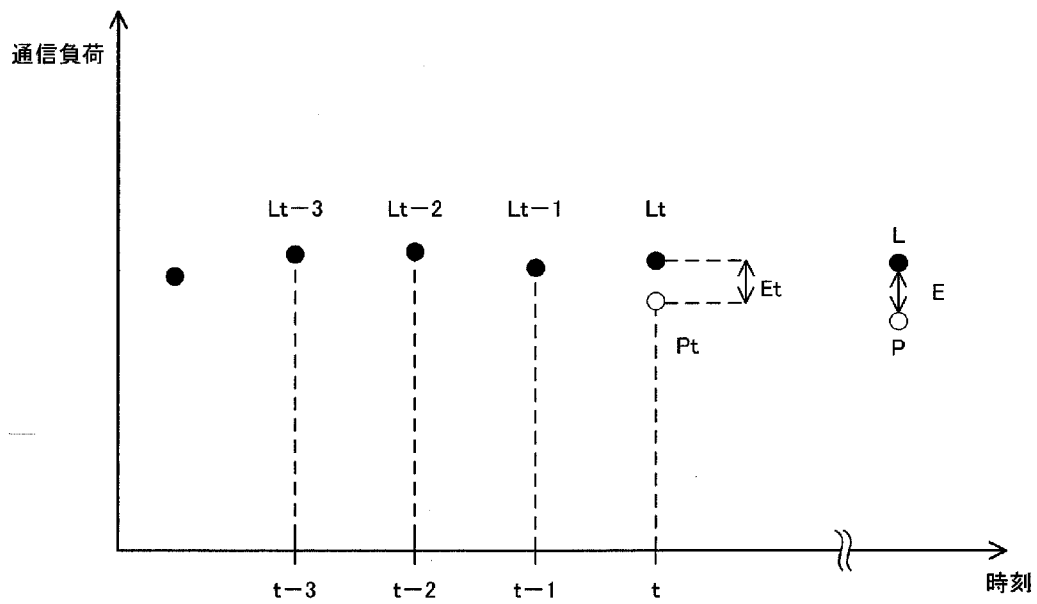
[図10]



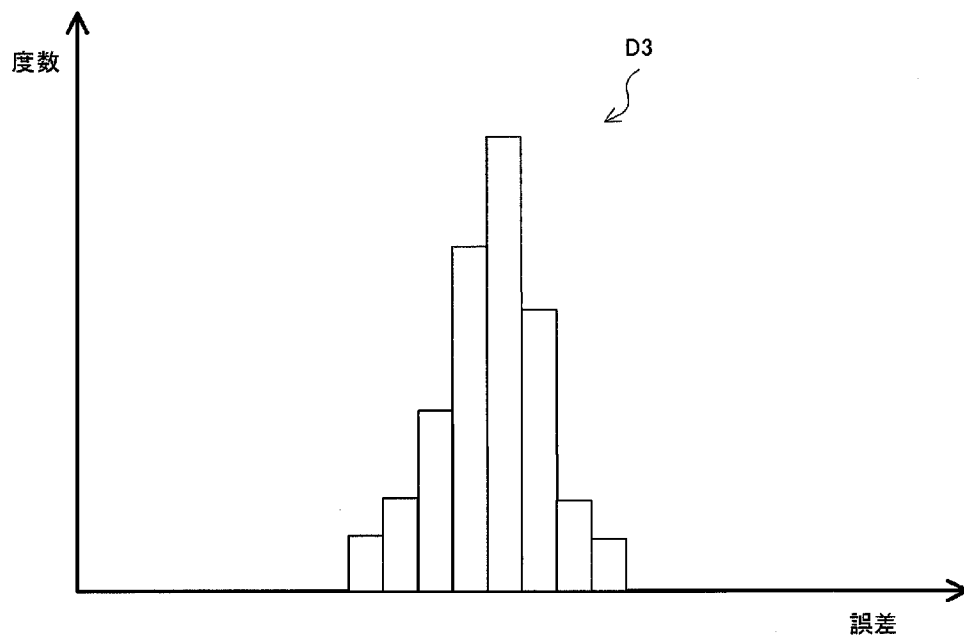
[図11]



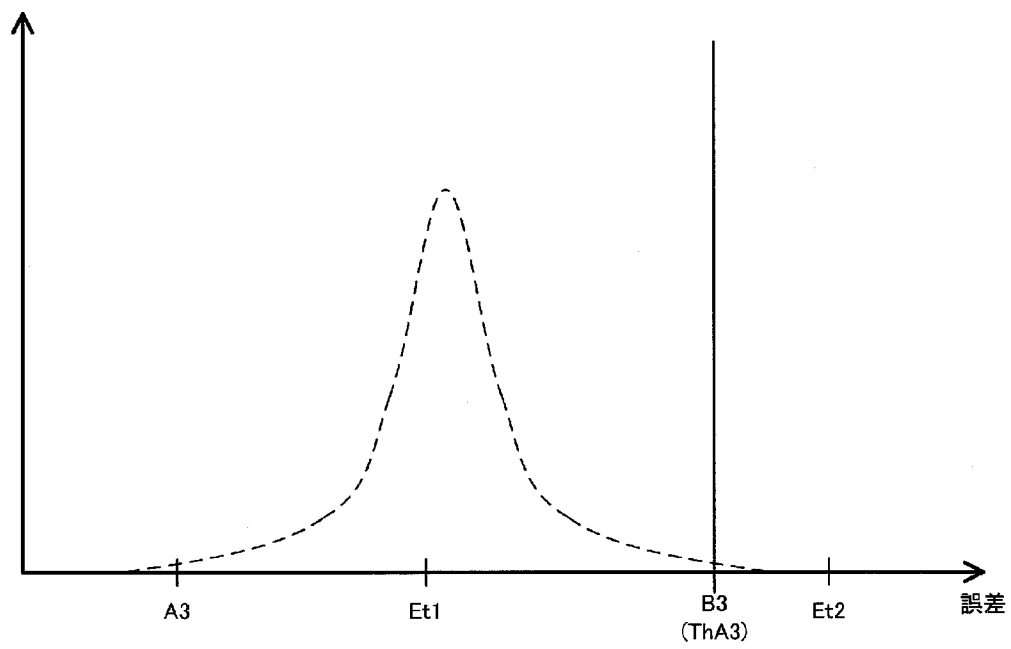
[図12]



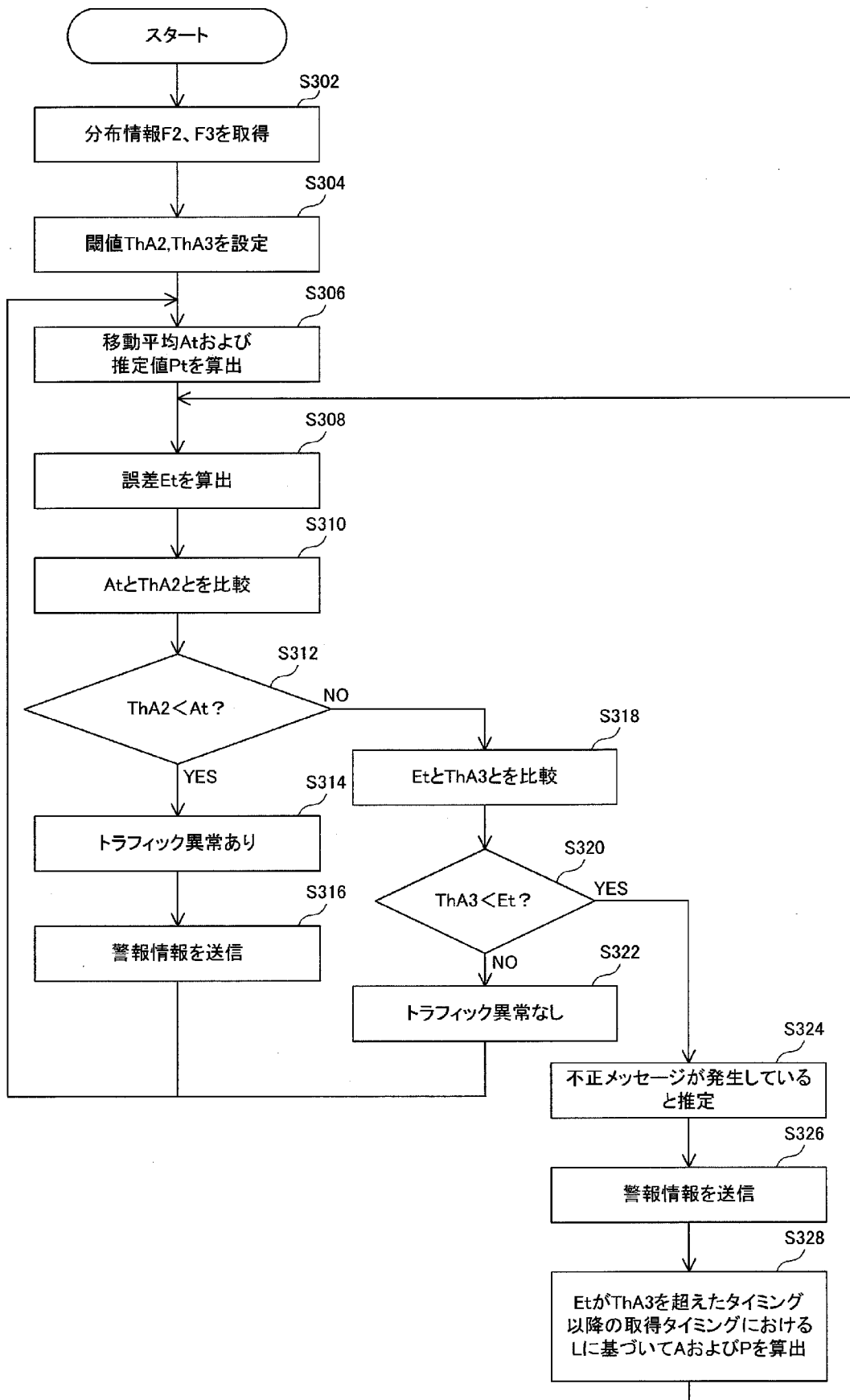
[図13]



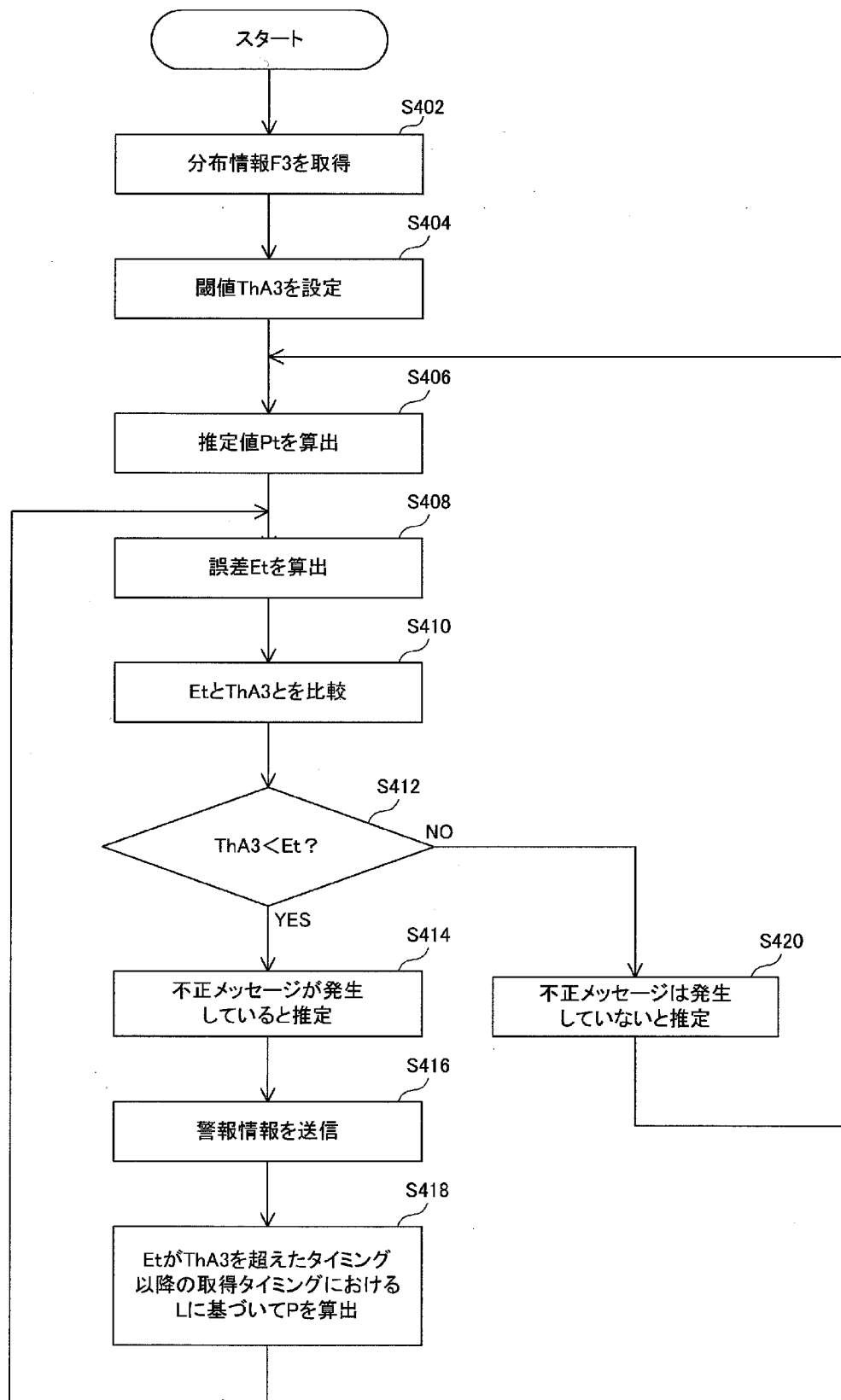
[図14]



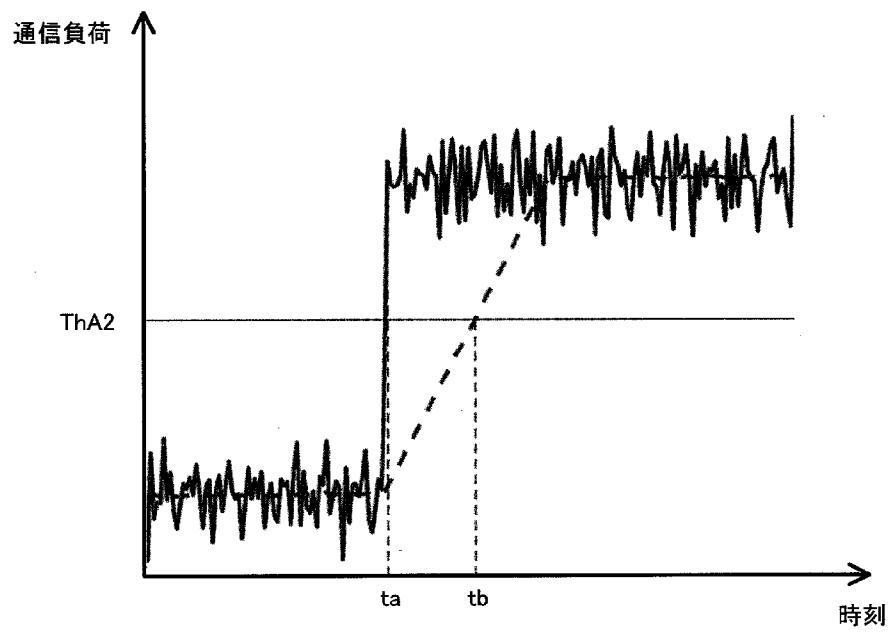
[図15]



[図16]



[図17]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/034553

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L12/28 (2006.01) i, B60R16/023 (2006.01) i, H04L12/46 (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)

Int.Cl. H04L12/28, B60R16/023, H04L12/46

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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 A	芳賀 智之 他, クラウドを利用した車載ネットワーク向け統計的異常検知システムの提案, SCIS2016, January 2016, pp. 1-8, 「7.1 提案システム」, 「8.1 実車データを用いた統計的異常検知の実験」, (HAGA, Tomoyuki et al.), non-official translation (Proposal of statistical anomaly detection system for in-vehicle network using cloud, "7.1 Proposed system", "8.1 Statistical anomaly detection experiments using actual vehicle data")	1-5, 7, 9 6, 8, 10
Y A	JP 2016-143963 A (DENSO CORPORATION) 08 August 2016, claims 1, 4, paragraphs [0017]-[0022] (Family: none)	1-5, 7, 9 6, 8, 10
Y	JP 2008-141641 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 19 June 2008, abstract, claims 2, 4 (Family: none)	2-4

☐

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
01.11.2019

Date of mailing of the international search report
12.11.2019

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

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. H04L12/28(2006.01)i, B60R16/023(2006.01)i, H04L12/46(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. H04L12/28, B60R16/023, H04L12/46

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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 請求項の番号
Y A	芳賀 智之 他, クラウドを利用した車載ネットワーク向け統計的異常検知システムの提案, SCIS2016, 2016.01, pp.1-8, 「7.1 提案システム」, 「8.1 実車データを用いた統計的異常検知の実験」	1-5, 7, 9 6, 8, 10
Y A	JP 2016-143963 A (株式会社デンソー) 2016.08.08, 請求項 1, 4, [0017]-[0022] (ファミリーなし)	1-5, 7, 9 6, 8, 10
Y	JP 2008-141641 A (日本電信電話株式会社) 2008.06.19, 要約, 請求項 2, 4 (ファミリーなし)	2-4

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

01.11.2019

国際調査報告の発送日

12.11.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

玉木 宏治

5 X

3047

電話番号 03-3581-1101 内線 3596