

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6839963号
(P6839963)

(45) 発行日 令和3年3月10日 (2021.3.10)

(24) 登録日 令和3年2月18日 (2021.2.18)

(51) Int.Cl. F I
H O 4 L 12/40 (2006.01) H O 4 L 12/40 M

請求項の数 18 (全 36 頁)

(21) 出願番号	特願2016-212574 (P2016-212574)	(73) 特許権者	514136668
(22) 出願日	平成28年10月31日 (2016.10.31)		パナソニック インテレクチュアル プロ
(65) 公開番号	特開2017-126978 (P2017-126978A)		パティ コーポレーション オブ アメリ
(43) 公開日	平成29年7月20日 (2017.7.20)		カ
審査請求日	令和1年8月28日 (2019.8.28)		Panasonic Intellectual
(31) 優先権主張番号	特願2016-3035 (P2016-3035)		Property Corporation of America
(32) 優先日	平成28年1月8日 (2016.1.8)		アメリカ合衆国 90503 カリフォル
(33) 優先権主張国・地域又は機関	日本国 (JP)		ニア州, トーランス, スイート 200,
			マリナー アベニュー 20000
		(74) 代理人	100109210
			弁理士 新居 広守
		(74) 代理人	100137235
			弁理士 寺谷 英作

最終頁に続く

(54) 【発明の名称】 異常検知方法、異常検知装置及び異常検知システム

(57) 【特許請求の範囲】

【請求項 1】

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ける異常の検知のための異常検知方法であって、

前記車両のエンジン始動又はアクセサリオンの際または所定時間毎に、前記車両の識別のための車両識別情報に基づいて単位時間の決定を行い、

前記決定された単位時間内に前記バスから受信されたメッセージの数に基づく特徴情報と、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を行い、当該演算処理の結果に応じて異常か否かを判定する

異常検知方法。

【請求項 2】

前記単位時間の決定は、

前記車両のエンジン始動又はアクセサリオンの際または所定時間毎に、前記車両の識別のための車両識別情報を、サーバに送信し、前記サーバが前記車両識別情報に応じて特定した単位時間情報を前記サーバから受信し、前記単位時間の決定を行う

請求項 1 記載の異常検知方法。

【請求項 3】

前記メッセージは、メッセージの種類を示すメッセージ ID を含み、

前記異常検知方法は、

10

20

前記車両のエンジン始動又はアクセサリーオンの際または所定時間毎に、前記車両の識別のための車両識別情報に基づいて単位時間の前記決定を行う決定ステップと、

前記決定ステップで決定された単位時間内に前記バスから受信されたメッセージID毎のメッセージの数を成分とする特徴ベクトルを前記特徴情報として特定する特定ステップと、

前記特定ステップで特定された前記特徴情報と前記所定モデルとを用いて前記演算処理を行い、当該演算処理の結果に応じて前記判定を行う判定ステップとを含む

請求項1記載の異常検知方法。

【請求項4】

前記車両識別情報は、前記車両の製造事業者を示す

10

請求項3記載の異常検知方法。

【請求項5】

前記車両識別情報は、前記車両の車種を示す

請求項3記載の異常検知方法。

【請求項6】

前記車両識別情報は、前記車両を他の車両と区別する情報である

請求項3記載の異常検知方法。

【請求項7】

前記決定ステップでは、前記車両識別情報により識別される車両の集合における各車両の車載ネットワークシステムで当該車両内のバスに正常状態で送信されるべき、互いに異なる複数種類のメッセージのうち、送信周期が最短の一種類のメッセージの当該送信周期を、単位時間とするように前記決定を行う

20

請求項3～6のいずれか一項に記載の異常検知方法。

【請求項8】

前記判定ステップでは、前記車両識別情報に対応した前記所定モデルを用いて前記演算処理を行う

請求項3～7のいずれか一項に記載の異常検知方法。

【請求項9】

前記特定ステップでは、前記決定ステップで決定された単位時間毎に、当該単位時間内で前記バスから受信されたメッセージの数に基づく前記特徴情報を、逐次特定し、

30

前記判定ステップでは、前記特定ステップで逐次特定された各前記特徴情報について、当該特徴情報と前記所定モデルとを用いて前記演算処理を行い、

前記異常検知方法は更に、前記特定ステップで逐次特定された複数の前記特徴情報に基づいて前記所定モデルを逐次更新する更新ステップを含む

請求項3～8のいずれか一項に記載の異常検知方法。

【請求項10】

前記決定ステップでは、前記車両の製造の際に規定された情報に基づいて、前記車両において単位時間の前記決定を行い、

前記特定ステップでは、前記車両において前記特徴情報を特定する

請求項3～9のいずれか一項に記載の異常検知方法。

40

【請求項11】

前記決定ステップでは、前記車両のエンジン始動又はアクセサリーオンの際に、前記車両において単位時間の前記決定を行い、

前記特定ステップでは、前記車両において前記特徴情報を特定する

請求項3～9のいずれか一項に記載の異常検知方法。

【請求項12】

前記決定ステップでは、所定時間毎に単位時間の前記決定を行い、

前記特定ステップでは、前記決定ステップで決定された最新の単位時間毎に、当該単位時間内で前記バスから受信されたメッセージの数に基づく前記特徴情報を、逐次特定し、

前記判定ステップでは、前記特定ステップで逐次特定された各前記特徴情報について、

50

当該特徴情報と前記所定モデルとを用いて前記演算処理を行う

請求項 3～9 のいずれか一項に記載の異常検知方法。

【請求項 1 3】

前記メッセージは、メッセージの種類を示すメッセージ I D を含み、

前記特徴情報は、前記決定された単位時間内に前記バスから受信された、全てのメッセージ I D のメッセージの総数を示す

請求項 1 記載の異常検知方法。

【請求項 1 4】

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ける異常の検知のための異常検知方法であって、

単位時間の決定を行い、

前記決定された単位時間内に前記バスから受信されたメッセージの数に基づく特徴情報と、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を行い、当該演算処理の結果に応じて異常か否かを判定し、

前記メッセージは、メッセージの種類を示すメッセージ I D を含み、

前記異常検知方法は、

単位時間の前記決定を行う決定ステップと、

前記決定ステップで決定された単位時間内に前記バスから受信されたメッセージ I D 毎のメッセージの数を成分とする特徴ベクトルを前記特徴情報として特定する特定ステップと、

前記特定ステップで特定された前記特徴情報と前記所定モデルとを用いて前記演算処理を行い、当該演算処理の結果に応じて前記判定を行う判定ステップとを含み、

前記決定ステップでは、前記車両のエンジン始動又はアクセサリーオンの際または所定時間毎に、前記車両の識別のための車両識別情報に基づいて単位時間の前記決定を行い、

前記決定ステップでは、前記車両識別情報により識別される車両の集合における各車両の車載ネットワークシステムで当該車両内のバスに正常状態で送信されるべき、互いに異なる複数種類のメッセージのうち、送信周期が最短の一種類のメッセージの当該送信周期を、単位時間とするように前記決定を行う

異常検知方法。

【請求項 1 5】

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ける異常の検知のための異常検知方法であって、

前記車両のエンジン始動又はアクセサリーオンの際または所定時間毎に、前記車両の識別のための車両識別情報に基づいて単位時間の決定を行い、

前記決定された単位時間内に前記バスから受信されたメッセージの数に基づく特徴情報と、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を行い、当該演算処理の結果に応じて異常か否かを判定し、

前記メッセージは、メッセージの種類を示すメッセージ I D を含み、

前記異常検知方法は、

単位時間の前記決定を行う決定ステップと、

前記決定ステップで決定された単位時間内に前記バスから受信されたメッセージ I D 毎のメッセージの数を成分とする特徴ベクトルを前記特徴情報として特定する特定ステップと、

前記特定ステップで特定された前記特徴情報と前記所定モデルとを用いて前記演算処理を行い、当該演算処理の結果に応じて前記判定を行う判定ステップとを含み、

前記特定ステップでは、前記決定ステップで決定された単位時間毎に、当該単位時間内で前記バスから受信されたメッセージの数に基づく前記特徴情報を、逐次特定し、

前記判定ステップでは、前記特定ステップで逐次特定された各前記特徴情報について、

当該特徴情報と前記所定モデルとを用いて前記演算処理を行い、

前記異常検知方法は更に、前記特定ステップで逐次特定された複数の前記特徴情報に基づいて前記所定モデルを逐次更新する更新ステップを含む

異常検知方法。

【請求項 16】

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、

前記車両のエンジン始動又はアクセサリーオンの際または所定時間毎に前記車両の識別のための車両識別情報に基づいて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

異常検知装置。

【請求項 17】

一の車両とサーバとを備える異常検知システムであって、

前記一の車両は、CAN (Controller Area Network) プロトコルに従って前記一の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と当該バスに接続された異常検知装置とを備える車載ネットワークシステムを有し、

前記異常検知装置は、

前記バスからメッセージを受信する受信部と、

前記車両のエンジン始動又はアクセサリーオンの際または所定時間毎に前記一の車両の識別のための車両識別情報を前記サーバに送信し、前記サーバからの応答に基づいて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、

前記サーバは、前記一の車両から前記車両識別情報を受信し、当該車両識別情報に基づいて特定した単位時間を示す情報を、前記一の車両に送信する通信部を備える

異常検知システム。

【請求項 18】

一の車両とサーバとを備える異常検知システムであって、

前記一の車両は、CAN (Controller Area Network) プロトコルに従って前記一の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と当該バスに接続された異常検知装置とを備える車載ネットワークシステムを有し、

前記異常検知装置は、

前記バスからメッセージを受信する受信部と、

前記一の車両の識別のための車両識別情報を前記サーバに送信し、前記サーバからの応答に基づいて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、

前記サーバは、前記一の車両から前記車両識別情報を受信し、当該車両識別情報に基づいて特定した単位時間を示す情報を、前記一の車両に送信する通信部を備え、

前記サーバは、更に、前記一の車両から受信した前記車両識別情報に基づいて特定した単位時間内に、当該車両識別情報により識別される車両の集合における 1 つ以上の車両の

10

20

30

40

50

車載ネットワークシステムで当該車両内のバスから受信されたメッセージの数に基づく所定情報を取得し、当該所定情報に基づいて、メッセージの出現頻度に係る基準を表す基準モデルを更新する学習部を備え、

前記通信部は、前記学習部により更新した前記基準モデルを示す情報を前記一の車両に送信し、

前記異常検知装置は、前記サーバから受信した前記基準モデルを示す情報に基づいて、前記所定モデルを更新し、

前記判定部は、前記特徴情報と、前記更新された前記所定モデルとを用いた演算処理を行い、当該演算処理の結果に応じて、異常か否かの前記判定を行う

異常検知システム。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、車載ネットワークにおいて送信されるメッセージについての異常を検知する技術に関する。

【背景技術】

【0002】

近年、自動車の中のシステムには、電子制御ユニット（ECU：Electronic Control Unit）と呼ばれる装置が多数配置されている。これらのECUをつなぐネットワークは車載ネットワークと呼ばれる。車載ネットワークには、多数の規格が存在する。その中でも最も主流な車載ネットワークの一つに、ISO11898-1で規定されているCAN（Controller Area Network）という規格が存在する。

20

【0003】

CANでは、通信路は2本のワイヤで構成されたバス（CANバス）であり、バスに接続されているECUはノードと呼ばれる。CANバスに接続されている各ノードは、フレーム（メッセージ）を送受信する。またCANでは、送信先や送信元を指す識別子は存在せず、送信ノードはフレーム毎に、メッセージIDと呼ばれるIDを付けて送信し（つまりバスに信号を送出することでブロードキャストし）、各受信ノードは予め定められたメッセージIDのみを受信する（つまりバスから信号を読み取る）。自動車の中のシステムにおいては、多数のECUそれぞれは、様々なフレームの授受を行う。

30

【0004】

CANバスに不正なノードを接続すること、或いは、携帯情報端末、車外の通信装置等と通信する機能を有するECU等を攻撃して不正なノードに変化させること等により、攻撃者が、攻撃フレームをCANバスに送信して、自動車を不正にコントロールする可能性がある。攻撃フレームは、不正な攻撃者によってCANバスに送信されたフレームであり、車載ネットワークの正常状態において本来は送信されないフレーム（異常なメッセージ）である。

【0005】

このような攻撃フレームを検知するための技術として、CANのバス上に送信されたフレームが異常なフレームか否かを統計的な手法を用いて判定する技術が知られている（特許文献1、特許文献2参照）。

40

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2015-026252号公報

【特許文献2】特開2015-170121号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

車載ネットワークでの攻撃フレームの検知（つまり異常の検知）のためには、特許文献

50

1、2の技術で十分とは限らず、異常検知のための更なる技術の研究開発が望まれている。

【0008】

そこで、本発明は、自動車等の車両の車載ネットワークで送信され得る異常なメッセージ（攻撃フレーム）の検知のために有用な異常検知方法を提供する。

【課題を解決するための手段】

【0009】

上記課題を解決するために本発明の一態様に係る異常検知方法は、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ける異常の検知のための異常検知方法であって、単位時間の決定を行い、前記決定された単位時間内に前記バスから受信されたメッセージの数に基づく特徴情報と、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を行い、当該演算処理の結果に応じて異常か否かを判定する異常検知方法である。

10

【0010】

また、上記課題を解決するために本発明の一態様に係る異常検知装置は、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異常検知装置である。

20

【0011】

また、上記課題を解決するために本発明の一態様に係る異常検知システムは、一の車両とサーバとを備える異常検知システムであって、前記一の車両は、CAN（Controller Area Network）プロトコルに従って前記一の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と当該バスに接続された異常検知装置とを備える車載ネットワークシステムを有し、前記異常検知装置は、前記バスからメッセージを受信する受信部と、前記一の車両の識別のための車両識別情報を前記サーバに送信し、前記サーバからの応答に基づいて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、前記サーバは、前記一の車両から前記車両識別情報を受信し、当該車両識別情報に基づいて特定した単位時間を示す情報を、前記一の車両に送信する通信部を備える異常検知システムである。

30

【発明の効果】

【0012】

本発明によれば、攻撃者により攻撃フレーム（メッセージ）がバスに流された場合に、車載ネットワークシステムで決定された単位時間におけるメッセージの数が基準と相違することとなり得るので、異常を検知し得る。

40

【図面の簡単な説明】

【0013】

【図1】実施の形態1に係る異常検知システムの全体構成を示す図である。

【図2】CANプロトコルで規定されるデータフレームのフォーマットを示す図である。

【図3】電子制御ユニット（ECU）の構成図である。

【図4】受信IDリストの一例を示す図である。

【図5】エンジンECUが送信するフレームにおけるID及びデータフィールドの一例を示す図である。

【図6】ブレーキECUが送信するフレームにおけるID及びデータフィールドの一例を

50

示す図である。

【図 7】ドア開閉センサ ECU が送信するフレームにおける ID 及びデータフィールドの一例を示す図である。

【図 8】ウィンドウ開閉センサ ECU が送信するフレームにおける ID 及びデータフィールドの一例を示す図である。

【図 9】実施の形態 1 に係るゲートウェイの構成図である。

【図 10】実施の形態 1 に係るゲートウェイが保持する車両識別情報の一例を示す図である。

【図 11】実施の形態 1 に係るゲートウェイが用いる転送ルールの一列を示す図である。

【図 12】実施の形態 1 に係るサーバの構成図である。

【図 13】実施の形態 1 に係るサーバが保持する検出窓サイズ特定用テーブルの一例を示す図である。

【図 14】ECU におけるフレーム送信処理シーケンスの一例を示す図である。

【図 15】実施の形態 1 に係るゲートウェイにおけるフレーム転送処理シーケンスの一例を示す図である。

【図 16】実施の形態 1 に係るゲートウェイ及びサーバにおける検出窓サイズ決定処理シーケンスの一例を示す図である。

【図 17】実施の形態 1 に係るゲートウェイ及びサーバにおける学習処理シーケンスの一例を示す図である。

【図 18】実施の形態 1 に係るゲートウェイが用いる検出窓の説明のための図である。

【図 19】実施の形態 1 に係るゲートウェイ及びサーバにおけるモデル更新処理シーケンスの一例を示す図である。

【図 20】実施の形態 1 に係るゲートウェイ及びサーバにおける異常検知処理シーケンスの一例を示す図である。

【図 21】実施の形態 2 に係る車両の車載ネットワークシステムの構成図である。

【図 22】実施の形態 2 に係るゲートウェイの構成図である。

【図 23】実施の形態 2 に係るゲートウェイにおける検出窓サイズ決定処理シーケンスの一例を示す図である。

【図 24】実施の形態 2 に係るゲートウェイにおける学習処理シーケンスの一例を示す図である。

【図 25】実施の形態 2 に係るゲートウェイにおける異常検知処理シーケンスの一例を示す図である。

【図 26】実施の形態の変形例に係る検出窓の一例を示す図である。

【発明を実施するための形態】

【0014】

(本発明の基礎となった知見等)

攻撃者により攻撃フレーム（メッセージ）が車載ネットワークのバスに流された場合に、単位時間においてバスから受信されたフレームの数が、正常状態においてその単位時間におけるフレームの出現頻度を示す基準（モデル）と相違することとなれば、異常を検知し得る。車載ネットワークシステムの構成、仕様等（バスで接続された ECU の編成、仕様等）によって正常状態における単位時間におけるバスへのフレームの出現頻度は限定的となり得るためである。このとき単位時間が適切であるか否かは、異常の検知精度に影響を及ぼす。そこで、車両の車載ネットワークシステムで、多様な時間幅の中から例えば 10 ms 等と単位時間を決定（選定）し、決定した単位時間を用いて異常を検知し得る異常検知方法に想到した。車載ネットワークシステムの構成、仕様等は、例えば車両毎或いは車種毎等に異なり得るので、一例としては、車両の車載ネットワークシステムにおいて、その車両、車種等の識別のための車両識別情報に基づいて単位時間を決定し得る。また、攻撃手法の変化、多様化等により、攻撃された状態と正常状態とを区別するために適した単位時間が過去から不変とは限らないので、車両の車載ネットワークシステムにおいて異常の検知のために、単位時間を決定してから異常を検知する方法は有用となり得る。例え

10

20

30

40

50

ば、同一車種の複数車両から集積した、フレームに係る情報の最新の解析結果等に基づいて、異常の検知のために用いる単位時間を決定すること等が有用となる。

【0015】

本発明の一態様に係る異常検知方法は、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ける異常の検知のための異常検知方法であって、単位時間の決定を行い、前記決定された単位時間内に前記バスから受信されたメッセージの数に基づく特徴情報と、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を行い、当該演算処理の結果に応じて異常か否かを判定する異常検知方法である。これにより、攻撃者により攻撃フレーム (メッセージ) がバスに流された場合に、車載ネットワークシステムで決定された単位時間 (例えば 10 ms 等) におけるメッセージの数が基準と相違することとなり得るので、適切に異常が検知され得る。

10

【0016】

また、例えば、前記メッセージは、メッセージの種類を示すメッセージIDを含み、前記異常検知方法は、単位時間の前記決定を行う決定ステップと、前記決定ステップで決定された単位時間内に前記バスから受信されたメッセージID毎のメッセージの数を成分とする特徴ベクトルを前記特徴情報として特定する特定ステップと、前記特定ステップで特定された前記特徴情報と前記所定モデルとを用いて前記演算処理を行い、当該演算処理の結果に応じて前記判定を行う判定ステップとを含むこととしても良い。これにより、車載ネットワークシステムにおいてメッセージの種類別の受信数に基づきメッセージの出現状況を適切に表す特徴ベクトルが定められることとなり、適切な異常の検知が可能となり得る。

20

【0017】

また、例えば、前記決定ステップでは、前記車両の識別のための車両識別情報に基づいて単位時間の前記決定を行うこととしても良い。これにより、車両識別情報で識別される車載ネットワークシステムに対応して精度良い異常の検知が可能となり得る。

【0018】

また、例えば、前記車両識別情報は、前記車両の製造事業者を示すこととしても良い。これにより、車両製造事業者毎の車載ネットワークの特徴に対応して、異常の検知に用いる単位時間を定め得るので、精度良い異常の検知が可能となり得る。

30

【0019】

また、例えば、前記車両識別情報は、前記車両の車種を示すこととしても良い。これにより、車種毎の車載ネットワークの特徴に対応して、異常の検知に用いる単位時間を定め得るので、精度良い異常の検知が可能となり得る。

【0020】

また、例えば、前記車両識別情報は、前記車両を他の車両と区別する情報であることとしても良い。これにより、個々の車両毎の車載ネットワークシステムの特徴に適応した異常の検知が可能となり得る。

【0021】

また、例えば、前記決定ステップでは、前記車両識別情報により識別される車両の集合における各車両の車載ネットワークシステムで当該車両内のバスに正常状態で送信されるべき、互いに異なる複数種類のメッセージのうち、送信周期が最短の一種のメッセージの当該送信周期を、単位時間とするように前記決定を行うこととしても良い。これにより、精度良い異常の検知が可能となり得る。

40

【0022】

また、例えば、前記判定ステップでは、前記車両識別情報に対応した前記所定モデルを用いて前記演算処理を行うこととしても良い。これにより、車載ネットワークシステムにおいて決定した単位時間に対応した所定モデルと、車載ネットワークで単位時間において受信したメッセージの数とによって異常を検知することになるので、適切な異常の検知が可能となる。

50

【0023】

また、例えば、前記特定ステップでは、前記決定ステップで決定された単位時間毎に、当該単位時間内で前記バスから受信されたメッセージの数に基づく前記特徴情報を、逐次特定し、前記判定ステップでは、前記特定ステップで逐次特定された各前記特徴情報について、当該特徴情報と前記所定モデルとを用いて前記演算処理を行い、前記異常検知方法は更に、前記特定ステップで逐次特定された複数の前記特徴情報に基づいて前記所定モデルを逐次更新する更新ステップを含むこととしても良い。これにより、異常の検知に用いる所定モデルを逐次更新するので、例えば、車載ネットワークの最近の状況（例えば車両の最近の使用状況等）に対応して、適切に異常の検知を行うことが可能となり得る。

【0024】

10

また、例えば、前記決定ステップでは、前記車両の製造の際に規定された情報に基づいて、前記車両において単位時間の前記決定を行い、前記特定ステップでは、前記車両において前記特徴情報を特定することとしても良い。これにより、車両において異常の検知に用いる特徴情報の生成の基礎となる単位時間を、車両の製造の際に規定された情報（例えば車台番号等）に基づいて決定し得るので、車両に適応した適切な異常の検知が可能となり得る。

【0025】

また、例えば、前記決定ステップでは、前記車両のエンジン始動又はアクセサリーオンの際に、前記車両において単位時間の前記決定を行い、前記特定ステップでは、前記車両において前記特徴情報を特定することとしても良い。これにより、車両において異常の検知に用いる特徴情報の生成の基礎となる単位時間を、車両の使用開始の際（走行開始の際等）に決定し得るので、例えば最近の状況に適応して、適切な異常の検知が可能となり得る。

20

【0026】

また、例えば、前記決定ステップでは、所定時間毎に単位時間の前記決定を行い、前記特定ステップでは、前記決定ステップで決定された最新の単位時間毎に、当該単位時間内で前記バスから受信されたメッセージの数に基づく前記特徴情報を、逐次特定し、前記判定ステップでは、前記特定ステップで逐次特定された各前記特徴情報について、当該特徴情報と前記所定モデルとを用いて前記演算処理を行うこととしても良い。これにより、車両において異常の検知に用いる特徴情報の生成の基礎となる単位時間を、所定時間毎に決定するので、例えば最近の状況に適応して、適切な異常の検知が可能となり得る。

30

【0027】

また、例えば、前記メッセージは、メッセージの種類を示すメッセージIDを含み、前記特徴情報は、前記決定された単位時間内に前記バスから受信された、全てのメッセージIDのメッセージの総数を示すこととしても良い。これにより、IDを区別しないことで効率的に異常の検知を行うことが可能となり得る。

【0028】

また、本発明の一態様に係る異常検知装置は、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異常検知装置である。演算処理は、例えば、異常検知装置で行っても、外部の装置（サーバ）で行っても良く、その結果に応じて、異常検知装置の判定部で判定を行えば良い。演算処理をサーバで行う場合においては、異常検知装置は、例えば、特定部で特定された特徴情報をサーバに送信し、演算処理の結果をサーバから受信することとしても良い。これにより、攻撃者により攻撃フレーム（メッセージ）がバスに流された場合に、異常検知装置で決定された単位時間（例えば10ms等）にお

40

50

けるメッセージの数が基準と相違することとなり得るので、適切に異常が検知され得る。

【0029】

また、本発明の一態様に係る異常検知システムは、一の車両とサーバとを備える異常検知システムであって、前記一の車両は、CAN (Controller Area Network) プロトコルに従って前記一の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と当該バスに接続された異常検知装置とを備える車載ネットワークシステムを有し、前記異常検知装置は、前記バスからメッセージを受信する受信部と、前記一の車両の識別のための車両識別情報を前記サーバに送信し、前記サーバからの応答に基づいて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、前記サーバは、前記一の車両から前記車両識別情報を受信し、当該車両識別情報に基づいて特定した単位時間を示す情報を、前記一の車両に送信する通信部を備える異常検知システムである。例えば、判定部は、特定部で特定された特徴情報をサーバに送信し、サーバからの応答（例えば、異常か否かを示す情報等）に応じて異常か否かを判定するものであっても良い。この場合にはサーバは、例えば、受信した特徴情報を用いて、所定モデルに係る演算処理を行ってその結果に基づく情報を、受信した特徴情報に対する応答として車両に送信し得る。これにより、車両の車両識別情報に対応して単位時間が決定されるので、車両の車載ネットワークに係る異常か否かの判定が適切に行われ得る。

10

20

【0030】

また、例えば、前記サーバは、更に、前記一の車両から受信した前記車両識別情報に基づいて特定した単位時間内に、当該車両識別情報により識別される車両の集合における1つ以上の車両の車載ネットワークシステムで当該車両内のバスから受信されたメッセージの数に基づく所定情報を取得し、当該所定情報に基づいて、メッセージの出現頻度に係る基準を表す基準モデルを更新する学習部を備え、前記通信部は、前記学習部により更新した前記基準モデルを示す情報を前記一の車両に送信し、前記異常検知装置は、前記サーバから受信した前記基準モデルを示す情報に基づいて、前記所定モデルを更新し、前記判定部は、前記特徴情報と、前記更新された前記所定モデルとを用いた演算処理を行い、当該演算処理の結果に応じて、異常か否かの前記判定を行うこととしても良い。これにより、サーバでは、車両識別情報により識別される車両の集合（例えば同一車種の車両等）における車載ネットワークで受信されたメッセージの数に基づく所定情報（例えば特徴情報と同様の情報）を用いた学習により基準モデルを更新する。そして、車両の異常検知装置では、基準モデルに基づいて、例えば一致させるように、所定モデルを更新して異常か否かの判定に利用できる。従って、異常検知装置では、自装置を搭載する車両（車両識別情報で識別される車両）に適応した、適切な異常の検知（判定）の実行が可能となり得る。

30

【0031】

なお、これらの全般的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータで読み取り可能なCD-ROM等の記録媒体で実現されても良く、システム、方法、集積回路、コンピュータプログラム又は記録媒体の任意な組み合わせで実現されても良い。

40

【0032】

以下、実施の形態に係る異常検知方法を用いる異常検知システム、異常検知装置等について、図面を参照しながら説明する。ここで示す実施の形態は、いずれも本発明の一具体例を示すものである。従って、以下の実施の形態で示される数値、構成要素、構成要素の配置及び接続形態、並びに、ステップ（工程）及びステップの順序等は、一例であって本発明を限定するものではない。以下の実施の形態における構成要素のうち、独立請求項に記載されていない構成要素については、任意に付加可能な構成要素である。また、各図は、模式図であり、必ずしも厳密に図示されたものではない。

【0033】

50

(実施の形態 1)

以下、本発明の実施の一態様として、車両において車載ネットワークの異常を検知する異常検知装置が、異常の検知に用いる検出窓サイズ（単位時間）を、車両外部のサーバとの連携により決定する異常検知システムについて、図面を用いて説明する。この異常検知システムにおいては、異常検知装置は、自装置を搭載している車両の車両識別情報をサーバに通知して応答を得ることで、異常の検知に用いる検出窓サイズを決定する。

【0034】

〔1. 1 異常検知システム 10 の全体構成〕

図 1 は、実施の形態 1 に係る異常検知システム 10 の全体構成を示す図である。

【0035】

異常検知システム 10 は、車載ネットワークシステムを有する車両と、相互に通信可能なサーバ 400 とを備える。異常検知システム 10 は、サーバ 400 と通信可能な複数台の車両を備えても良いが、図 1 では、便宜上、一台の車両について示している。

【0036】

図 1 に示す車両における車載ネットワークシステムは、CAN プロトコルに従って通信するネットワーク通信システムの一例であり、制御装置、センサ、アクチュエータ、ユーザインタフェース装置等の各種機器が搭載された車両におけるネットワーク通信システムである。この車載ネットワークシステムは、車両に搭載され各種機器に接続された ECU 100a（エンジン ECU）、ECU 100b（ブレーキ ECU）、ECU 100c（ドア開閉センサ ECU）、及び、ECU 100d（ウィンドウ開閉センサ ECU）と、バス 200a、200b と、ゲートウェイ 300（異常検知装置の一例）とを含んで構成される。なお、車載ネットワークシステムには、ゲートウェイ 300、ECU 100a～100d 以外にもいくつかの ECU が含まれ得るが、ここでは、便宜上ゲートウェイ 300 及び ECU 100a～100d に注目して説明を行う。ECU は、例えば、プロセッサ（マイクロプロセッサ）、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置である。メモリは、ROM、RAM 等であり、プロセッサにより実行される制御プログラム（ソフトウェアとしてのコンピュータプログラム）を記憶することができる。例えばプロセッサが、制御プログラム（コンピュータプログラム）に従って動作することにより、ECU は各種機能を実現することになる。なお、コンピュータプログラムは、所定の機能を達成するために、プロセッサに対する指令を示す命令コードが複数個組み合わされて構成されたものである。ECU は、CAN プロトコルに従って車両内のバス 200a、200b を介してフレームの授受を行い得る。

【0037】

ECU 100a～100d は、それぞれ、エンジン 101、ブレーキ 102、ドア開閉センサ 103、ウィンドウ開閉センサ 104 といった機器に接続されており、その機器の状態を取得し、周期的に状態を表すフレーム（データフレーム）を、バス 200a、バス 200b 等で構成される車載ネットワークに送信している。

【0038】

ゲートウェイ 300 は、ECU 100a と ECU 100b とが接続されたバス 200a、及び、ECU 100c と ECU 100d とが接続されたバス 200b と接続され、一方のバスから受信したフレームを他方のバスに転送する機能を有する一種の ECU である。また、ゲートウェイ 300 は、バスから受信したフレームに基づいて異常か否かを判定すること（例えば攻撃フレームがバスに流れている異常状態であるか否かを判定すること）で異常を検知し、その検知結果（異常検知結果）をサーバ 400 に通知する機能を有する異常検知装置である。異常検知装置としてのゲートウェイ 300 における異常の検知は、概ね、検出窓サイズの時間長を有する期間である検出窓毎に、その検出窓内に車載ネットワークに係るバス 200a、200b から受信されたデータフレーム（メッセージ）の数に基づく特徴情報と、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比較等の演算処理の結果に応じて異常か否かを判定することで、行われる。また、ゲートウェイ 300 は、ネットワーク 40 を介してサーバ 400 と通信することで、異常検知（異常

10

20

30

40

50

か否かの判定)に用いるための情報(例えば検出窓サイズ、所定モデルを表す情報等のパラメータ等)を決定する機能を有する。

【0039】

サーバ400は、車両外部のコンピュータであり、ネットワーク40を介して、各車両におけるゲートウェイ300と通信し、受信した車両識別情報に基づいて、異常検知用の情報(検出窓サイズを示す情報等)をゲートウェイ300に応答(返信)する機能を有する。また、サーバ400は、ゲートウェイ300より通知された異常検知結果を保存する機能を有する。また、サーバ400は、各車両におけるゲートウェイ300と通信し、各車両における車載ネットワークで受信されたフレームに係る情報を集積、解析等を行う機能を有しても良い。なお、ネットワーク40における通信には、無線通信、或いは、有線通信のいかなる通信プロトコルを適用しても良い。

10

【0040】

[1.2 データフレームフォーマット]

以下、CANプロトコルに従ったネットワークで用いられるフレームの1つであるデータフレーム(メッセージ)について説明する。

【0041】

図2は、CANプロトコルで規定されるデータフレームのフォーマットを示す図である。同図には、CANプロトコルで規定される標準IDフォーマットにおけるデータフレームを示している。データフレームは、SOF(Start Of Frame)、IDフィールド、RTR(Remote Transmission Request)、IDE(Identifier Extension)、予約ビット「r」、DLC(Data Length Code)、データフィールド、CRC(Cyclic Redundancy Check)シーケンス、CRCデリミタ「DEL」、ACK(Acknowledgement)スロット、ACKデリミタ「DEL」、及び、EOF(End Of Frame)の各フィールドで構成される。

20

【0042】

SOFは、1bitのドミナントで構成される。バスがアイドルの状態はレセシブになっており、SOFによりドミナントへ変更することでフレームの送信開始を通知する。

【0043】

IDフィールドは、11bitで構成される、データの種別を示す値であるID(メッセージID)を格納するフィールドである。複数のノードが同時に送信を開始した場合、このIDフィールドで通信調停を行うために、IDが小さい値を持つフレームが高い優先度となるよう設計されている。

30

【0044】

RTRは、データフレームとリモートフレームとを識別するための値であり、データフレームにおいてはドミナント1bitで構成される。

【0045】

IDEと「r」とは、両方ドミナント1bitで構成される。

【0046】

DLCは、4bitで構成され、データフィールドの長さを示す値である。なお、IDE、「r」及びDLCを合わせてコントロールフィールドと称する。

【0047】

データフィールドは、最大64bitで構成される送信するデータの内容を示す値である。8bit毎に長さを調整できる。送られるデータの仕様については、CANプロトコルで規定されておらず、車載ネットワークシステムにおいて定められる。従って、車種、製造者(製造メーカ)等に依存した仕様となる。

40

【0048】

CRCシーケンスは、15bitで構成される。SOF、IDフィールド、コントロールフィールド及びデータフィールドの送信値より算出される。

【0049】

CRCデリミタは、1bitのレセシブで構成されるCRCシーケンスの終了を表す区切り記号である。なお、CRCシーケンス及びCRCデリミタを合わせてCRCフィール

50

ドと称する。

【0050】

A C Kスロットは、1 b i tで構成される。送信ノードはA C Kスロットをレセシブにして送信を行う。受信ノードはC R Cシーケンスまで正常に受信ができていればA C Kスロットをドミナントとして送信する。レセシブよりドミナントが優先されるため、送信後にA C Kスロットがドミナントであれば、送信ノードは、いずれかの受信ノードが受信に成功していることを確認できる。

【0051】

A C Kデリミタは、1 b i tのレセシブで構成されるA C Kの終了を表す区切り記号である。

10

【0052】

E O Fは、7 b i tのレセシブで構成されており、データフレームの終了を示す。

【0053】

[1. 3 E C U 1 0 0 aの構成]

図3は、E C U 1 0 0 aの構成図である。E C U 1 0 0 aは、フレーム送受信部110と、フレーム解釈部120と、受信I D判断部130と、受信I Dリスト保持部140と、フレーム処理部150と、データ取得部160と、フレーム生成部170とを含んで構成される。これらの各構成要素の各機能は、例えばE C U 1 0 0 aにおける通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、E C U 1 0 0 b～100dも、E C U 1 0 0 aと同様の構成を備える。

20

【0054】

フレーム送受信部110は、バス200aに対して、C A Nのプロトコルに従ったフレームを送受信する。バス200aからフレームを1 b i tずつ受信し、フレーム解釈部120に転送する。また、フレーム生成部より通知を受けたフレームの内容をバス200aに送信する。

【0055】

フレーム解釈部120は、フレーム送受信部110よりフレームの値を受け取り、C A Nプロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。I Dフィールドと判断した値は受信I D判断部130へ転送する。フレーム解釈部120は、受信I D判断部130から通知される判定結果に応じて、I Dフィールドの値と、I Dフィールド以降に現れるデータフィールドとを、フレーム処理部150へ転送するか、その判定結果を受けた以降においてフレームの受信を中止する（つまりそのフレームとしての解釈を中止する）かを決定する。また、フレーム解釈部120は、C A Nプロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部170へ通知する。また、フレーム解釈部120は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

30

【0056】

受信I D判断部130は、フレーム解釈部120から通知されるI Dフィールドの値を受け取り、受信I Dリスト保持部140が保持しているメッセージI Dのリストに従い、そのI Dフィールド以降のフレームの各フィールドを受信するかどうかの判定を行う。この判定結果を、受信I D判断部130は、フレーム解釈部120へ通知する。

40

【0057】

受信I Dリスト保持部140は、E C U 1 0 0 aが受信するI D（メッセージI D）のリストである受信I Dリストを保持する。図4に、受信I Dリストの一例を示す。

【0058】

フレーム処理部150は、受信したフレームのデータに応じてE C U毎に異なる機能に係る処理を行う。例えば、エンジン101に接続されたE C U 1 0 0 aは、時速が30 k mを超えた状態でドアが開いている状態だと、アラーム音を鳴らす機能を備える。E C U

50

100aは、例えばアラーム音を鳴らすためのスピーカ等を有している。そして、ECU100aのフレーム処理部150は、他のECUから受信したデータ（例えばドアの状態を示す情報）を管理し、エンジン101から取得された時速に基づいて一定条件下でアラーム音を鳴らす処理等を行う。なお、フレーム処理部150は、ここで例示した以外のフレームのデータに係る処理を行っても良い。

【0059】

データ取得部160は、ECUにつながっている機器、センサ等の状態を示すデータを取得し、フレーム生成部170に通知する。

【0060】

フレーム生成部170は、フレーム解釈部120から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部110へ通知して送信させる。また、フレーム生成部170は、データ取得部160より通知されたデータの値に対して、予め定められたメッセージIDをつけてフレーム（データフレーム）を構成し、フレーム送受信部110へ通知する。なお、ECU100a～100dのそれぞれが送信するフレームの内容については後に図5～図8を用いて説明する。

【0061】

[1.4 受信IDリスト例]

図4は、ECU100a～100dのそれぞれにおいて保持される受信IDリストの一例を示す図である。同図に例示する受信IDリストは、ID（メッセージID）の値が「1」、「2」、「3」及び「4」のいずれかであるメッセージIDを含むフレーム（メッセージ）を選択的に受信して処理するために用いられる。例えば、ECU100aの受信IDリスト保持部140に図4の受信IDリストが保持されていると、メッセージIDが「1」、「2」、「3」及び「4」のいずれでもないフレームについては、フレーム解釈部120でのIDフィールド以後のフレームの解釈が中止される。

【0062】

[1.5 エンジンECU100aの送信フレーム例]

図5は、エンジン101に接続されたECU100aから送信されるフレームにおけるID（メッセージID）及びデータフィールド（データ）の一例を示す図である。ECU100aが送信するフレームのメッセージIDは「1」である。データは、時速（km/時）を表し、最低0（km/時）～最高180（km/時）までの範囲の値を取り、データ長は1byteである。図5の上行から下行へと、ECU100aから逐次送信される各フレームに対応する各メッセージID及びデータを例示しており、0km/時から1km/時ずつ加速されている様子を表している。

【0063】

[1.6 ブレーキECU100bの送信フレーム例]

図6は、ブレーキ102に接続されたECU100bから送信されるフレームにおけるID（メッセージID）及びデータフィールド（データ）の一例を示す図である。ECU100bが送信するフレームのメッセージIDは「2」である。データは、ブレーキのかり具合を割合（％）で表し、データ長は1byteである。この割合は、ブレーキを全くかけていない状態を0（％）、ブレーキを最大限かけている状態を100（％）としたものである。図6の上行から下行へと、ECU100bから逐次送信される各フレームに対応する各メッセージID及びデータを例示しており、100％から徐々にブレーキを弱めている様子を表している。

【0064】

[1.7 ドア開閉センサECU100cの送信フレーム例]

図7は、ドア開閉センサ103に接続されたECU100cから送信されるフレームにおけるID（メッセージID）及びデータフィールド（データ）の一例を示す図である。ECU100cが送信するフレームのメッセージIDは「3」である。データは、ドアの開閉状態を表し、データ長は1byteである。データの値は、ドアが開いている状態が「1」、ドアが閉まっている状態が「0」である。図7の上行から下行へと、ECU100

0 c から逐次送信される各フレームに対応する各メッセージ ID 及びデータを例示しており、ドアが開いている状態から次第に閉められた状態へと移った様子を表している。

【0065】

[1. 8 ウィンドウ開閉センサ ECU100d の送信フレーム例]

図8は、ウィンドウ開閉センサ104に接続された ECU100d から送信されるフレームにおける ID (メッセージ ID) 及びデータフィールド (データ) の一例を示す図である。 ECU100d が送信するフレームのメッセージ ID は「4」である。データは、窓 (ウィンドウ) の開閉状態を割合 (%) で表し、データ長は 1 byte である。この割合は、窓が完全に閉まっている状態を 0 (%)、窓が全開の状態を 100 (%) としたものである。図8の上行から下行へと、 ECU100d から逐次送信される各フレームに対応する各メッセージ ID 及びデータを例示しており、窓が閉まっている状態から徐々に開いていく様子を表している。

10

【0066】

[1. 9 ゲートウェイ300の構成]

図9は、ゲートウェイ300の構成図である。ゲートウェイ300は、フレーム送受信部310と、フレーム解釈部320と、受信 ID 判断部330と、受信 ID リスト保持部340と、加工処理部350と、外部通信部360と、車両識別情報保持部361と、異常検知処理部370と、モデル保持部371と、転送処理部380と、転送ルール保持部381と、フレーム生成部390とを含んで構成される。これらの各構成要素の各機能は、例えばゲートウェイ300における通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。

20

【0067】

フレーム送受信部310は、バス200a、200bそれぞれに対して、CAN プロトコルに従ったフレームを送受信する。フレーム送受信部310は、バスからフレームを 1 bit ずつ受信する受信部として機能し、受信したフレームをフレーム解釈部320に転送する。また、フレーム生成部390より通知を受けた転送先のバスを示すバス情報及びフレームに基づいて、そのフレームの内容をバス200a、200bに 1 bit ずつ送信する。

【0068】

フレーム解釈部320は、フレーム送受信部310よりフレームの値を受け取り、CAN プロトコルで規定されているフレームフォーマットにおける各フィールドにマッピングするよう解釈を行う。 ID フィールドと判断した値は受信 ID 判断部330へ転送する。フレーム解釈部320は、受信 ID 判断部330から通知される判定結果に応じて、 ID フィールドの値と、 ID フィールド以降に現れるデータフィールド (データ) とを、転送処理部380へ転送するか、その判定結果を受けた以降においてフレームの受信を中止するかを決定する。また、フレーム解釈部320は、 ID フィールドの値を、加工処理部350に通知する。また、フレーム解釈部320は、CAN プロトコルに則っていないフレームと判断した場合は、エラーフレームを送信するようにフレーム生成部390へ通知する。また、フレーム解釈部320は、エラーフレームを受信した場合、つまり受け取ったフレームにおける値からエラーフレームになっていると解釈した場合には、それ以降はそのフレームを破棄する、つまりフレームの解釈を中止する。

30

40

【0069】

受信 ID 判断部330は、フレーム解釈部320から通知される ID フィールドの値を受け取り、受信 ID リスト保持部340が保持しているメッセージ ID のリストに従い、その ID フィールド以降のフレームの各フィールドを受信するかどうかの判定を行う。この判定結果を、受信 ID 判断部330は、フレーム解釈部320へ通知する。

【0070】

受信 ID リスト保持部340は、ゲートウェイ300が受信する ID (メッセージ ID) のリストである受信 ID リスト (図4参照) を保持する。

【0071】

50

加工処理部 350 は、サーバ 400 から通知された検出窓サイズを示す情報に基づいて検出窓サイズを決定してその検出窓サイズを保持する。つまり加工処理部 350 は、検出窓サイズを決定する決定部として機能する。加工処理部 350 は、フレーム解釈部 320 から通知される ID フィールドの値に基づいて、検出窓サイズの時間長の検出窓毎に、バス 200a、200b から逐次受信されたフレームの集合（逐次通知された ID フィールドの値の集合）を、検出窓における ID（メッセージ ID）別のフレームの受信数（検出窓サイズの検出窓内でフレームの受信を ID 別にカウントして得られたカウント数）を示す特徴情報に変換して特徴情報を外部通信部 360 へ通知する。つまり加工処理部 350 は、特徴情報を特定する特定部としても機能する。また、加工処理部 350 は、バス 200a、200b から検出窓サイズの検出窓内に逐次受信されたフレームの数に基づくその特徴情報を異常検知処理部 370 へ逐次通知する。

10

【0072】

外部通信部 360 は、車両識別情報保持部 361 が保持する車両識別情報を、ネットワーク 40 を介してサーバ 400 へ通知（送信）し、応答としてサーバ 400 から通知された検出窓サイズを示す情報を加工処理部 350 へ通知する。また、外部通信部 360 は、加工処理部 350 から通知された特徴情報をサーバ 400 に通知（送信）する。また、外部通信部 360 は、サーバ 400 から通知されたモデル情報（データフレームの出現頻度に係る基準を表す基準モデルを示す情報）を異常検知処理部 370 へと通知する。また、外部通信部 360 は、異常検知処理部 370 から通知された異常検知結果をサーバ 400 へ通知（送信）する。

20

【0073】

車両識別情報保持部 361 は、車両の識別のための車両識別情報を保持する。図 10 に、車両識別情報の一例を示す。

【0074】

異常検知処理部 370 は、サーバ 400 から通知されたモデル情報を、外部通信部 360 を介して取得し、モデル情報に従ってモデル保持部 371 が保持している所定モデル（データフレームの出現頻度に係る基準を表すモデル）を更新する。例えば、異常検知処理部 370 は、モデル情報が示す基準モデルと一致させるように所定モデルを更新し得る。また、異常検知処理部 370 は、フレーム解釈部 320 から通知される ID フィールドの値に基づいて加工処理部 350 で変換された特徴情報を受け取り、モデル保持部 371 が保持している所定モデルと、その特徴情報とを用いた演算処理を行い、その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して機能する。即ち、異常検知処理部 370 は、バスから受信されたフレームの集合に係る特徴情報が、所定モデルが表す基準に適合しているか否かを、特徴情報及び所定モデルを用いた演算処理により判定する。この判定では、特徴情報に反映された検出窓サイズでの ID 別のデータフレームの受信数が、所定モデルが表す基準（例えば正常状態におけるデータフレームの出現頻度を示す基準）に適合していると正常であり、基準に適合していない（つまり基準を逸脱している）と異常であると判定される。このように判定するために演算処理は定められており、演算処理は、例えば所定モデルと特徴情報との比較、算術演算、論理演算、条件判断等といった各種処理の 1 つ以上の組み合わせである。異常検知処理部 370 は、その演算処理による異常か否かの判定結果（つまり異常検知結果）を、外部通信部 360 へ通知する。

30

40

【0075】

モデル保持部 371 は、異常検知処理部 370 から通知された所定モデルを保持する。

【0076】

転送処理部 380 は、転送ルール保持部 381 が保持する転送ルールに従って、受信したフレームの ID（メッセージ ID）に応じて、転送するバス（転送先のバス）を決定し、転送するバスを示すバス情報とフレーム解釈部 320 より通知されたメッセージ ID とデータとをフレーム生成部 390 へ通知する。

【0077】

転送ルール保持部 381 は、バス毎のフレームの転送についてのルールを表す情報であ

50

る転送ルールを保持する。図 11 に、転送ルールの一例を示す。

【0078】

フレーム生成部 390 は、フレーム解釈部 320 から通知されたエラーフレームの送信を指示する通知に従い、エラーフレームを構成し、エラーフレームをフレーム送受信部 310 へ通知して送信させる。また、フレーム生成部 390 は、転送処理部 380 より通知されたメッセージ ID とデータとを使ってフレームを構成し、そのフレーム及びバス情報をフレーム送受信部 310 へ通知する。

【0079】

[1.10 車両識別情報]

図 10 は、ゲートウェイ 300 が保持する車両識別情報の一例を示す。車両識別情報は、車両の識別のための情報であり、図 10 では、車両識別情報が、カーメーカ（車両の製造事業者）、車種、及び、車台番号を示す例を示している。この例では、例えば、車台番号は、個々の車両を他の車両と区別する情報（各車両を識別する情報）であり、型式（車両形式）と製造番号とから構成される。ここで、車種が同一の車両同士は、車載ネットワークの構成が同一であり、車載ネットワークの CAN バスに流れるデータフレーム（メッセージ）の利用に関する仕様（メッセージ ID 毎のデータフィールドの内容の規定等）は同じである。即ち、ここでの車種が同一の車両は、例えば、車両型式が同一の車両である。なお、車両識別情報は、この例に限られず、例えば、車両識別番号（VIN: Vehicle Identification Number）等であっても良い。例えば、車両識別番号における先頭からシリアル番号の前までの桁の値が同一の車両は、同一車種の車両である。なお、車両識別情報は、必ずしも、それだけで個々の車両が識別可能となる情報である必要はない。例えば、車両識別情報は、車両の車種のみを示す情報であっても良く、車両の製造事業者のみを示す情報であっても良く、車台番号のみを示す情報であっても良く、或いはこれらのいずれかと他の情報とを組み合わせた情報等であっても良い。

【0080】

[1.11 転送ルール]

図 11 は、ゲートウェイ 300 の転送ルール保持部 381 が保持する転送ルールの一例を示す。

【0081】

この転送ルールは、転送元のバスと転送先のバスと転送対象の ID（メッセージ ID）とを対応付けている。図 11 中の「＊」はメッセージ ID にかかわらずフレームの転送がなされることを表している。図 11 の例は、バス 200a から受信されるフレームはメッセージ ID にかかわらず、バス 200b に転送するように設定されていることを示している。また、バス 200b から受信されるフレームのうちメッセージ ID が「3」であるフレームのみがバス 200a に転送されるように設定されていることを示している。

【0082】

[1.12 サーバ 400 の構成]

サーバ 400 は、車両外部に所在し、例えば複数の車両を管理し得るコンピュータであり、メモリ、ハードディスク等の記憶媒体、プロセッサ、通信回路等を含む。

【0083】

図 12 は、サーバ 400 の構成図である。サーバ 400 は、同図に示すように、通信部 410 と、データ蓄積部 420 と、学習部 430 と、検出窓サイズ特定部 440 と、検出窓サイズ特定用テーブル保持部 450 と、異常検知結果保持部 460 とを含んで構成される。これらの各構成要素は、サーバ 400 における通信回路、メモリに格納された制御プログラムを実行するプロセッサ等により実現される。

【0084】

通信部 410 は、ネットワーク 40 を介して各車両のゲートウェイ 300 と通信する。また、通信部 410 は、ゲートウェイ 300 から逐次通知される、検出窓サイズ当たりの ID 別のカウント数を反映した特徴情報を、車両毎に区別して、データ蓄積部 420 に蓄積する。また、通信部 410 は、学習部 430 から通知された基準モデルを示すモデル情

報を、ゲートウェイ 300 へ通知（送信）する。また、通信部 410 は、ゲートウェイ 300 から通知された車両識別情報を検出窓サイズ特定部 440 に通知して、検出窓サイズ特定部 440 から通知された検出窓サイズを示す情報をゲートウェイ 300 に通知（送信）する。また、通信部 410 は、ゲートウェイ 300 から通知された異常検知結果を異常検知結果保持部 460 に保持させる。

【0085】

データ蓄積部 420 は、通信部 410 から通知された特徴情報を車両毎に区別して蓄積（保持）する。

【0086】

学習部 430 は、データ蓄積部 420 に蓄積された車両毎の特徴情報に基づいて、車両毎に対応する基準モデル（車両の車載ネットワークのバスに現れるデータフレームの出現頻度に係る基準を表すモデル）を構築し保持し、特徴情報に基づいて必要に応じて基準モデルを更新する。学習部 430 は、例えば、通信部 410 及びデータ蓄積部 420 によって逐次収集される特徴情報に基づいて、例えば機械学習により、保持している基準モデルを逐次更新する。

【0087】

検出窓サイズ特定部 440 は、検出窓サイズ特定用テーブル保持部 450 が保持する検出窓サイズ特定用テーブルを参照して、通信部 410 から通知された車両識別情報に応じて検出窓サイズを特定し、特定した検出窓サイズを示す情報を通信部 410 へと通知する。

【0088】

検出窓サイズ特定用テーブル保持部 450 は、車両識別情報に応じて検出窓サイズを特定するために用いられる検出窓サイズ特定用テーブルを保持する。検出窓サイズ特定用テーブルの一例を図 13 に示す。

【0089】

異常検知結果保持部 460 は、通信部 410 から通知された異常検知結果を、車両毎にログとして保持する。なお、サーバ 400 が複数の車両を管理する場合においては、例えば、車両から受信した車両識別情報に基づいて各車両からの情報を類別して管理しても良く、例えば、車両のゲートウェイ 300 は、特徴情報或いは異常検知結果をサーバ 400 へ送信する際にも車両識別情報の全部或いは一部を付して送信することとしても良い。

【0090】

[1.13 検出窓サイズ特定用テーブル]

図 13 は、サーバ 400 で保持する検出窓サイズ特定用テーブルの一例を示す。図 13 に示す検出窓サイズ特定用テーブルは、車両識別情報と検出窓サイズとを対応付けたテーブルである。図 13 に例示する検出窓サイズ特定用テーブルの車両識別情報は、図 10 の例と同様に、カーメーカ、車種、及び、車台番号を含む。この検出窓サイズは、例えば、車両識別情報により識別される車両の集合における各車両の車載ネットワークシステムで CAN バスに正常状態で送信されるべき、複数種類のデータフレーム（つまりメッセージ ID が互いに異なる複数のデータフレーム）のうち、送信周期が最短の一種類のデータフレームのその送信周期と一致するように定められ得る。この検出窓サイズを定めるために、車載ネットワークシステムの仕様、或いは、車載ネットワークシステムの正常状態の実情の分析結果等が参照され得る。例えば、車両識別情報が、個々の車両ではなく車種のみを識別するものであれば、その車種の各車両における車載ネットワークシステムで、正常状態で送信される複数の ID のフレームの送信周期のうち最短の周期のものと一致するように、検出窓サイズが定められ得る。検出窓サイズ特定用テーブルにおける検出窓サイズの定め方は、この他の方法によっても良く、結果的に車両の異常検知装置（ゲートウェイ 300）において、正常状態と攻撃された状態とを適切に区別できるように、検出窓サイズを定めておくことが有用である。

【0091】

[1.14 ECU 100a のフレーム送信処理]

図14は、ECU100aにおけるフレーム送信処理シーケンスの一例を示す。以下、同図に即してECU100aによるフレーム送信処理について説明する。

【0092】

ECU100aは、データ取得部160により、センサからデータ（例えばエンジン101に関連してセンサで測定された車速）を取得する（ステップS1101）。

【0093】

次にECU100aは、取得したセンサのデータに基づいて、フレーム生成部170により、送信すべきフレーム（データフレーム）を生成する（ステップS1102）。

【0094】

次にECU100aは、生成したフレームをバス200aに対して送信（ブロードキャスト）する（ステップS1103）。このステップS1101からS1103までの処理は、概ね一定の周期で、周期的に繰り返され得る。

【0095】

ECU100b～100dにおいても、ECU100aと同様な手順でフレーム送信処理が行われ得る。但し、送信の周期は、ECU毎に異なり得る。

【0096】

[1.15 ゲートウェイ300のフレーム転送処理]

図15は、ゲートウェイ300におけるフレーム転送処理シーケンスの一例を示す。以下、同図に即してゲートウェイ300によるフレーム転送処理について説明する。ゲートウェイ300は、バス200a及びバス200bのいずれかからフレーム（データフレーム）を受信する度にこのフレーム転送処理を行う。ここでは、ゲートウェイ300が、バス200aから受信したフレームをバス200bに転送する例を用いて説明する。

【0097】

ゲートウェイ300は、バス200aに送信（ブロードキャスト）されたフレームを受信する（ステップS1201）。

【0098】

次に、ゲートウェイ300は、転送ルール（図11参照）を確認する（ステップS1202）。

【0099】

ゲートウェイ300は、転送ルールに基づいて、受信したフレームが転送されるべきフレームであると判定した場合には、そのフレームの内容に基づいて転送用フレームを生成する（ステップS1203）。

【0100】

次に、ゲートウェイ300は、転送用フレームをバス200bに送信（ブロードキャスト）して、フレーム転送処理を終える（ステップS1204）。なお、ステップS1202で確認した転送ルールに基づいて、受信したフレームが転送されるべきフレームでないと判定した場合には、ゲートウェイ300は、フレームの転送を行わずにフレーム転送処理を終える。

【0101】

[1.16 検出窓サイズ決定処理シーケンス]

図16は、ゲートウェイ300及びサーバ400の連携による検出窓サイズ決定処理シーケンスの一例を示す。以下、同図に即して検出窓サイズ決定処理シーケンスについて説明する。

【0102】

ゲートウェイ300は、車両識別情報を取得する（ステップS1301）。ゲートウェイ300は、車両識別情報を車両識別情報保持部361から取得する。車両識別情報保持部361には、例えば、ゲートウェイ300が車両に搭載された際（例えば車両の製造の際等）において車両識別情報が保持されていても良いし、予め記録された車両識別情報を保持する車両内のECUからゲートウェイ300がその車両識別情報を受信することで、車両識別情報保持部361に保持させることとしても良い。

10

20

30

40

50

【0103】

ゲートウェイ300は、ステップS1301で取得した車両識別情報を、サーバ400に送信する（ステップS1302a）。これにより、サーバ400は、車両識別情報を受信する（ステップS1302b）。なお、ゲートウェイ300が、サーバ400に車両識別情報を送信するタイミングは、例えば、ゲートウェイ300が車両に搭載された際（例えば車両の製造の際等）であるが、この他のタイミングであっても良いし、そのタイミングは複数であっても良い。この他のタイミング（ゲートウェイ300がサーバ400に車両識別情報を送信するタイミング）の例としては、車両の走行開始時等といった車両を使用する際毎（例えば車両のエンジン始動の際、アクセサリオン（ACC-ON）の際等）、所定時間（例えば1日）毎等が挙げられる。そして、ゲートウェイ300が、サーバ400に車両識別情報を送信するタイミングの到来に合わせて図16に示す検出窓サイズ決定処理シーケンスの全体が実行され得る。

10

【0104】

サーバ400では、ステップS1302bで受信した車両識別情報に応じて、検出窓サイズ特定部440により検出窓サイズを特定し（ステップS1303）、特定した検出窓サイズを示す情報（検出窓サイズ情報）を、車両識別情報に対する応答として、ゲートウェイ300に送信する（ステップS1304a）。これにより、ゲートウェイ300は、検出窓サイズ情報を受信する（ステップS1304b）。

【0105】

ゲートウェイ300は、受信した検出窓サイズ情報に従って、加工処理部350において検出窓サイズを決定して、検出窓サイズを保持する（ステップS1305）。

20

【0106】

[1.17 学習処理シーケンス]

図17は、ゲートウェイ300及びサーバ400の連携による学習処理シーケンスの一例を示す。学習処理シーケンスでは、車両の車載ネットワークにおいてゲートウェイ300が受信したフレームの集合に加工処理を加えてなる特徴情報をサーバ400に送信し、サーバ400では特徴情報を基準モデルへ反映する。以下、図17に即して学習処理シーケンスについて説明する。

【0107】

ゲートウェイ300は、加工処理部350において、保持している検出窓サイズの時間長の検出窓毎に、バス200a及びバス200bからフレーム（データフレーム）を受信すると（ステップS1401）、検出窓内におけるID（メッセージID）別のフレームの受信数をカウントする（ステップS1402）。

30

【0108】

加工処理部350は、検出窓サイズ分の時間の経過（つまり1つの検出窓の終期の到来）を判定し（ステップS1403）、検出窓の終期が到来したら、ID別のフレームの受信数（カウント数）に基づき加工処理により特徴情報を生成する（ステップS1404）。続いてゲートウェイ300は、加工処理部350で生成した特徴情報をサーバ400に送信し（ステップS1405a）、加工処理部350ではカウント数をクリアして（ステップS1406）、次の検出窓についての処理に戻る（つまりステップS1401での処理へ戻る）。なお、ゲートウェイ300は、ステップS1403で、検出窓の終期が到来していないと判定された場合には、ステップS1401での処理に戻る。

40

【0109】

ステップS1405aでのゲートウェイ300による特徴情報の送信に呼応して、サーバ400では、特徴情報を受信し（ステップS1405b）、学習部430で、受信した特徴情報を基準モデルに反映する（ステップS1407）。なお、サーバ400は、特徴情報を受信する毎に基準モデルへの反映を行うこととしても良いし、複数の特徴情報を受信してからデータ蓄積部420に蓄積し、複数の特徴情報をまとめて学習部430で特徴情報の基準モデルへの反映を行うこととしても良い。この学習処理シーケンスは、車両の車載ネットワークにおいて正常状態で受信されたフレームに係る特徴情報を基準モデルに

50

反映することで、基準モデルが、その車両の車載ネットワークのバスに現れるフレームの出現頻度に係る基準となることを想定している。基準モデルは、例えば、車両から取得した車両識別情報毎に定められる。基準モデルは、例えば車両毎に定められるが、例えば、同一車種の車両においては共通にすることとしても良い。即ち、サーバ400が車両からの車両識別情報に応じて検出窓サイズを示す情報を送信したその送信先の車両に対応して、基準モデルが存在し、その基準モデルを示すモデル情報が、後述のモデル更新処理シーケンスでその車両に送信される。なお、特徴情報の基準モデルへの反映は、例えば、特徴情報を用いた機械学習により基準モデルを更新することで行われるようにしても良い。

【0110】

以下、学習処理シーケンスで用いた検出窓サイズの時間長の検出窓と加工処理により生成された特徴情報との一例について、図18を用いて説明する。

【0111】

ゲートウェイ300の加工処理部350では、検出窓サイズの時間長の各期間（各検出窓T1、T2、T3）において、検出窓内にバスから受信されたフレームの数に基づく特徴情報を特定する。図18では、特徴情報として、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を特徴情報として特定する例を示している。図18では、IDが1であるフレームをID1、IDが2であるフレームをID2等と表現している。特徴ベクトルは、例えば、検出窓内におけるID1の受信数（カウント数）、ID2の受信数、ID3の受信数、ID4の受信数のそれぞれを成分とするベクトルである。ベクトルの成分数は、例えば、バスに出現する全てのメッセージIDの数である。図18の例では、ID1、ID2、ID3、ID4の各受信数をこの順に並べた成分を有する特徴ベクトルを示している。検出窓T1においてID1、ID2、ID3の受信数は1でありID4の受信数は0であるので、検出窓T1における特徴ベクトルは[1, 1, 1, 0, ...]となっている。また、検出窓T2においてID1、ID2、ID4の受信数は1でありID3の受信数は0であるので、検出窓T2における特徴ベクトルは[1, 1, 0, 1, ...]となっている。また、検出窓T3においてID1、ID3の受信数は1でありID2、ID4の受信数は0であるので、検出窓T3における特徴ベクトルは[1, 0, 1, 0, ...]となっている。なお、ゲートウェイ300で検出窓サイズの期間においてカウントしたID毎の受信したフレームの数を、サーバ400の基準モデルへ反映するまでにおける、ゲートウェイ300とサーバ400との処理（加工処理等）の分担は、いかなるものでも良い。また、加工処理において、主成分分析等を用いることで、特徴情報としての特徴ベクトルの次元数（成分の数）を削減しても良い。

【0112】

サーバ400では、特徴情報を基準モデルに反映する際に、例えば、その基準モデルと同様の所定モデルを用いたゲートウェイ300での異常の検知を効率的に行えるようにするための加工等を施しても良い。一例としては、サーバ400は、ゲートウェイ300から逐次取得した特徴情報としての、上述の次元数を削減等した特徴ベクトルの集合を、kd木(k-dimensional tree)等の最近傍距離の計算に適したデータ構造にすることをもって基準モデルへの反映を行う。

【0113】

[1.18 モデル更新処理シーケンス]

図19は、ゲートウェイ300及びサーバ400の連携によるモデル更新処理シーケンスの一例を示す。モデル更新処理シーケンスでは、サーバ400において更新された基準モデルを、車両のゲートウェイ300が保持する所定モデルに反映する。以下、図19に即してモデル更新処理シーケンスについて説明する。モデル更新処理シーケンスは、任意のタイミング（例えば1日毎）に実行される。

【0114】

サーバ400は、上述の学習処理シーケンスの結果として基準モデルの更新（基準モデルの内容の変化）があったか否かを判定する（ステップS1501）。基準モデルの更新があった場合には、サーバ400は、更新後の基準モデルを示すモデル情報を、ゲートウ

エイ 300 に送信する（ステップ S 1502 a）。これに呼応してゲートウェイ 300 は、基準モデルを示すモデル情報を受信する（ステップ S 1502 b）。

【0115】

ゲートウェイ 300 は、モデル情報を受信すると、異常検知処理部 370 で、モデル情報に従ってモデル保持部 371 が保持している所定モデルを更新する（ステップ S 1503）。これにより、所定モデルは、例えばサーバ 400 における基準モデルと同様となる。

【0116】

[1. 19 異常検知処理シーケンス]

図 20 は、ゲートウェイ 300 及びサーバ 400 の連携による異常検知処理シーケンスの一例を示す。異常検知処理シーケンスは、例えば車両が使用される段階において実行される。ゲートウェイ 300 が車両の車載ネットワークのバス 200 a、200 b を流れるフレームを監視して、所定モデルを用いて異常状態が生じているか否かを判定することで異常を検知する処理を含む。所定モデルは、上述のモデル更新処理シーケンスにより、上述の学習処理シーケンスで更新された基準モデルと同様となるように構成されている。なお、上述の学習処理シーケンスは、この異常検知処理シーケンスより前（例えば、車両の使用前、つまり製造或いは検査段階等）に行われ得るが、車両が使用される段階で異常検知処理シーケンスと並行して行われても良い。以下、図 20 に即して異常検知処理シーケンスについて説明する。

【0117】

ゲートウェイ 300 では、フレームが受信されると（ステップ S 1601）、加工処理部 350 で、検出窓サイズの検出窓内における ID 別のフレームの受信数をカウントし（ステップ S 1602）、加工処理によって例えば特徴ベクトルである特徴情報を生成する（ステップ S 1603）。1つの検出窓においてステップ S 1601～ステップ S 1602 での処理が繰り返し行われ、検出窓の終期においてステップ S 1603 での特徴情報の生成が行われて ID 別のフレームの受信数をカウントするカウンタがクリアされる。

【0118】

次にゲートウェイ 300 は、異常検知処理部 370 により、加工処理部 350 で生成された特徴情報を受け取り、その特徴情報が、モデル保持部 371 が保持している所定モデルが示す基準に適合しているか、その基準を逸脱しているかを判定する（ステップ S 1604）。即ち、異常検知処理部 370 は、特徴情報と所定モデルとを用いた演算処理を行い、その演算処理の結果に応じて、特徴情報が、所定モデルが表す基準を逸脱しているか否か（つまり異常か否か）を判定する。演算処理の一例としては、加工処理部 350 から受け取った特徴情報としての特徴ベクトル（図 18 参照）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（例えば正常状態での特徴ベクトルの分布）に対する最近傍距離を計算して、閾値と比較する処理が、挙げられる。例えば、最近傍距離が正規分布に従うとして、閾値で定めた、平均から標準偏差の一定倍（例えば 3 倍）の範囲内を逸脱した場合に、異常と判定される。

【0119】

ゲートウェイ 300 は、ステップ S 1604 で特徴情報が、所定モデルが示す基準を逸脱していない（基準に適合している）と判定した場合には、正常と判定して（ステップ S 1605）、特にサーバ 400 への送信を行わない。一方、特徴情報が、所定モデルが示す基準を逸脱していると判定した場合には、異常と判定して（ステップ S 1606）、異常検知結果をサーバ 400 に送信する（ステップ S 1607 a）。

【0120】

サーバ 400 は、異常検知結果を受信すると（ステップ S 1607 b）、異常検知結果をログとして保存する（ステップ S 1608）。

【0121】

[1. 20 実施の形態 1 の効果]

実施の形態 1 に係る異常検知システム 10 では、車両に搭載された異常検知装置として

10

20

30

40

50

のゲートウェイ 300 が、その車両の識別のための車両識別情報をサーバ 400 に送信し、サーバ 400 からの応答に基づいて検出窓サイズ（異常検知のためにフレームの受信数をカウントするための単位時間）を決定する。これにより、車両毎に適切な検出窓サイズを用いて車載ネットワークの異常の検知を精度良く行うことが可能となり得る。また、異常検知システム 10 では、異常の判定（検知）に用いるモデル（所定モデル或いは基準モデル）の学習のために、ゲートウェイ 300 側で受信したフレームに係る特徴ベクトルを生成する加工処理を行うことで、サーバ 400 との間の通信量の削減が可能となる。また、加工処理では、主成分分析等による特徴ベクトルの次元の削減等も行い得るので、これにより更に通信量を削減することが可能となり、また、結果的にモデルに基づく異常の判定のための演算量を削減することが可能となり得る。また、サーバ 400 が、データ（車両から受信した特徴情報）の蓄積、特徴情報を反映したモデルの構築（基準モデルの更新等）を行うことで、車載のゲートウェイ 300 の限られたリソースにより制限を受けることなく、最適なモデルを構築し得る。また、サーバ 400 で構築（更新）した基準モデルをゲートウェイ 300 が取得して、異常の判定（検知）のために用いることで、車両において迅速に異常か否かの判定（つまり異常の検知）を行うことが可能となり得る。そして、ゲートウェイ 300 は、異常検知結果をサーバ 400 に通知するので、サーバ 400 では異常検知結果をログとして保存し、車両を管理することができ、また、その異常検知結果に基づいて、より適切な基準モデルを構築する等が可能となり得る。また、例えば、車両識別情報で車種を示すようにした場合においては、サーバ 400 は、同一車種の複数の車両から特徴情報を収集することでその車種に対応する基準モデルを、その車種で攻撃された状況と正常状態を区別可能に適切に構築することが可能となる。そして、サーバ 400 が、その同一車種の車両のゲートウェイ 300 に対して、基準モデルを示すモデル情報を送信することで、同一車種の各車両は、基準モデルと同様の所定モデルに基づいて適切に異常を検知し得る。なお、異常の検知により、異常に対する各種対処（警告の報知、安全のための走行制御その他の処理）が可能となり得る。

【0122】

（実施の形態 2）

以下、実施の形態 1 で示した異常検知システムにおける車両の車載ネットワークシステムを変形した実施態様について説明する。

【0123】

実施の形態 1 では、車両のゲートウェイ 300 が、車両外部のサーバ 400 と通信することで検出窓サイズを決定し、車載ネットワークの異常の検知のために用いる所定モデルの基礎となる基準モデルを学習により更新するために、検出窓サイズ分の時間における ID 別のフレームの受信数に基づく特徴情報をサーバ 400 に送信した。これに対して、本実施の形態では、車両の車載ネットワークシステムにおける異常検知装置が独立して（つまり車両外部のサーバに依存せずに）、異常の検知に用いる検出窓サイズを決定する例について説明する。

【0124】

〔2.1 車載ネットワークシステムの構成〕

図 21 は、本実施の形態に係る車両の車載ネットワークシステムの構成を示す。なお、実施の形態 1（図 1 参照）と同様の構成については、図 21 において図 1 と同一の符号を付しており、説明を省略する。

【0125】

図 21 に示す車両における車載ネットワークシステムは、ECU100a、ECU100b、ECU100c 及び ECU100d と、バス 200a、200b と、ゲートウェイ 1300（異常検知装置の一例）とを含んで構成される。各 ECU は、CAN プロトコルに従って車両内のバス 200a、200b を介してフレームの授受を行い得る。

【0126】

ゲートウェイ 1300 は、実施の形態 1 で示したゲートウェイ 300 を部分的に変形した異常検知装置であり、ここで特に示さない点についてはゲートウェイ 300 と同様であ

る。

【0127】

ゲートウェイ1300は、バス200a及びバス200bと接続され、一方のバスから受信したフレームを他方のバスに転送する機能を有し、バスから受信したフレームに基づいて異常か否かを判定すること（例えば攻撃フレームがバスに流れている異常状態であるか否かを判定すること）で異常を検知する機能を有する。また、ゲートウェイ1300は、異常検知（異常か否かの判定）等に用いるための検出窓サイズを決定する機能、検出窓サイズの時間長の期間である検出窓内に、車載ネットワークで受信されたフレームの数に係る特徴情報に基づいて、異常検知に用いるための所定モデルを更新する機能を有する。

【0128】

[2.2 ゲートウェイ1300の構成]

図22は、ゲートウェイ1300の構成図である。ゲートウェイ1300は、フレーム送受信部310と、フレーム解釈部320と、受信ID判断部330と、受信IDリスト保持部340と、加工処理部1350と、車両識別情報保持部361と、異常検知処理部1370と、モデル保持部1371と、転送処理部380と、転送ルール保持部381と、フレーム生成部390と、検出窓サイズ決定部1440と、検出窓サイズ特定用テーブル保持部450と、学習部1430と、異常検知結果保持部1460とを含んで構成される。これらの各構成要素の各機能は、例えばゲートウェイ1300における通信回路、メモリに格納された制御プログラムを実行するプロセッサ或いはデジタル回路等により実現される。なお、図9に示したゲートウェイ300と同様の構成、或いは、図12に示したサーバ400と同様の構成については、図22において同一の符号を付しており、説明を省略する。

【0129】

検出窓サイズ決定部1440は、検出窓サイズを決定する決定部として機能する。検出窓サイズ決定部1440は、車両識別情報保持部361が保持する車両識別情報に応じて、検出窓サイズ特定用テーブル保持部450が保持する検出窓サイズ特定用テーブル（図13参照）を用いて検出窓サイズを決定し、加工処理部1350へと通知する。

【0130】

加工処理部1350は、実施の形態1で示した加工処理部350の一部を変形したものであり、検出窓サイズ決定部1440から通知された検出窓サイズを保持し、フレーム解釈部320から通知されるIDフィールドの値に基づいて、検出窓サイズの時間長の検出窓毎に、バス200a、200bから逐次受信されたフレームの集合（逐次通知されたIDフィールドの値の集合）を、検出窓におけるID（メッセージID）別のフレームの受信数（検出窓サイズの検出窓内でフレームの受信をID別にカウントして得られたカウント数）を示す特徴情報に変換して特徴情報を定期的に学習部1430へ通知する。つまり加工処理部1350は、特徴情報を特定する特定部として機能する。また、加工処理部1350は、バス200a、200bから検出窓サイズの検出窓内に逐次受信されたフレームの数に基づくその特徴情報を異常検知処理部1370へ逐次通知する。

【0131】

モデル保持部1371は、所定モデル（車両の車載ネットワークのバスに現れるデータフレームの出現頻度に係る基準を表すモデル）を保持する。

【0132】

学習部1430は、加工処理部1350から通知された特徴情報に基づいて、所定モデルを構築して、モデル保持部1371に保持させる。即ち、学習部1430は、モデル保持部1371が保持する所定モデルを、特徴情報に基づいて更新する。学習部1430による所定モデルの更新は、実施の形態1で示した学習部430による基準モデルの更新と同様の方法で行われ得る。学習部1430は、例えば、逐次通知される特徴情報に基づいて、例えば機械学習により、所定モデルを逐次更新し得る。

【0133】

異常検知処理部1370は、フレーム解釈部320から通知されるIDフィールドの値

10

20

30

40

50

に基づいて加工処理部 1 3 5 0 で生成された特徴情報を受け取り、モデル保持部 1 3 7 1 が保持している所定モデルと、その特徴情報とを用いた演算処理を行い、その演算処理の結果に応じて異常か否かを判定する。即ち、異常検知処理部 1 3 7 0 は、バスから受信されたフレームの集合に係る特徴情報が、所定モデルが表す基準に適合しているか否かを、特徴情報及び所定モデルを用いた演算処理により判定する判定部として機能する。この判定では、特徴情報に反映された検出窓サイズでの I D 別のデータフレームの受信数が、所定モデルが表す基準（例えば正常状態におけるデータフレームの出現頻度を示す基準）に適合していると正常であり、基準に適合していない（つまり基準を逸脱している）と異常であると判定される。また、異常検知処理部 3 7 0 は、その演算処理による異常か否かの判定結果（つまり異常検知結果）を、異常検知結果保持部 1 4 6 0 にログとして保存する。

10

【0 1 3 4】

〔2. 3 検出窓サイズ決定処理シーケンス〕

図 2 3 は、ゲートウェイ 1 3 0 0 における検出窓サイズ決定処理シーケンスの一例を示す。以下、同図に即して検出窓サイズ決定処理シーケンスについて説明する。この検出窓サイズ決定処理シーケンスが実行されるタイミングは、例えば、ゲートウェイ 1 3 0 0 が車両に搭載された際（例えば車両の製造の際等）であるが、この他のタイミングであっても良いし、そのタイミングは複数であっても良い。この他のタイミングの例としては、車両を使用する際毎（例えば車両のエンジン始動の際、アクセサリオン（A C C - O N）の際等）、所定時間（例えば 1 日）毎等が挙げられる。なお、図 1 6 と同様のステップについては、図 2 3 において同一の符号を付しており、説明を適宜省略する。

20

【0 1 3 5】

ゲートウェイ 1 3 0 0 は、車両識別情報を取得する（ステップ S 1 3 0 1）。

【0 1 3 6】

次にゲートウェイ 1 3 0 0 は、ステップ S 1 3 0 1 で取得した車両識別情報に応じて、検出窓サイズ特定用テーブル（図 1 3 参照）を用いて検出窓サイズを決定する（ステップ S 2 3 0 3）。ゲートウェイ 1 3 0 0 は、決定した検出窓サイズを保持し、加工処理部 1 3 5 0 で加工処理を実行する際に検出窓サイズを用いる。なお、ゲートウェイ 1 3 0 0 は、車両外部との通信機能を有していても良く、その場合に、検出窓サイズ特定用テーブルを通信により、車両外部から取得することとしても良いし、記録媒体等から検出窓サイズ特定用テーブルを読み出すことで取得することとしても良い。

30

【0 1 3 7】

〔2. 4 学習処理シーケンス〕

図 2 4 は、ゲートウェイ 1 3 0 0 における学習処理シーケンスの一例を示す。学習処理シーケンスでは、ゲートウェイ 1 3 0 0 が、バス 2 0 0 a、2 0 0 b から受信したフレームの集合に加工処理を加えてなる特徴情報に基づく学習により、モデル保持部 1 3 7 1 が保持する所定モデルを更新する。以下、図 2 4 に即して学習処理シーケンスについて説明する。なお、図 1 7 と同様のステップについては、図 2 4 において同一の符号を付しており、説明を適宜省略する。

40

【0 1 3 8】

ゲートウェイ 1 3 0 0 は、検出窓サイズの時間長の検出窓毎に、バス 2 0 0 a 及びバス 2 0 0 b からフレームを受信すると（ステップ S 1 4 0 1）、検出窓内における I D 別のフレームの受信数をカウントする（ステップ S 1 4 0 2）。

【0 1 3 9】

加工処理部 1 3 5 0 は、検出窓サイズ分の時間が経過（検出窓の終期が到来）したら、I D 別のフレームの受信数（カウント数）に基づき加工処理により特徴情報を生成する（ステップ S 1 4 0 4）。

【0 1 4 0】

ゲートウェイ 1 3 0 0 は、加工処理部 1 3 5 0 で生成した特徴情報を、学習部 1 4 3 0 で、モデル保持部 1 3 7 1 が保持する所定モデルに反映する（ステップ S 2 4 0 7）。こ

50

の学習処理シーケンスは、車載ネットワークにおいて正常状態で受信されたフレームに係る特徴情報を所定モデルに反映することで、所定モデルが、この車載ネットワークのバスに現れるフレームの出現頻度に係る基準となることを想定している。特徴情報の所定モデルへの反映は、例えば、特徴情報を用いた機械学習により所定モデルを更新することで行われるようにしても良い。なお、加工処理部1350は、実施の形態1で示した加工処理部350と同様に、検出窓において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を特徴情報としても良く、加工処理において、主成分分析等を用いることで、特徴ベクトルの次元数を削減しても良い。また、学習部1430は、特徴情報を所定モデルに反映する際に、例えば、その所定モデルを用いた異常の検知を効率的に行えるようにするための加工等を施しても良い。一例としては、学習部1430は、特徴ベクトルの集合を、kd木の最近傍距離の計算に適したデータ構造にすることをもちいて所定モデルへの反映を行う。

10

【0141】

ステップS2407での処理に続いて、ゲートウェイ1300は、カウント数をクリアして（ステップS1406）、ステップS1401での処理に戻る。

【0142】

[2.5 異常検知処理シーケンス]

図25は、ゲートウェイ1300における異常検知処理シーケンスの一例を示す。異常検知処理シーケンスは、例えば車両が使用される段階において実行される。異常検知処理シーケンスでは、ゲートウェイ1300が、車両の車載ネットワークのバス200a、200bを流れるフレームを監視して、所定モデルを用いて異常状態が生じているか否かを判定することで異常を検知する。なお、上述の学習処理シーケンスは、この異常検知処理シーケンスより前（例えば、車両の使用前、つまり製造或いは検査段階等）に行われ得るが、車両が使用される段階で異常検知処理シーケンスと並行して行われても良い。以下、図25に即して異常検知処理シーケンスについて説明する。なお、図20と同様のステップについては、図25において同一の符号を付しており、説明を適宜省略する。

20

【0143】

ゲートウェイ1300では、フレームが受信されると（ステップS1601）、加工処理部1350で、検出窓サイズの検出窓内におけるID別のフレームの受信数をカウントし（ステップS1602）、加工処理によって例えば特徴ベクトルである特徴情報を生成する（ステップS1603）。1つの検出窓においてステップS1601～ステップS1602での処理が繰り返し行われ、検出窓の終期においてステップS1603での特徴情報の生成が行われてID別のフレームの受信数をカウントするカウンタがクリアされる。

30

【0144】

次にゲートウェイ1300は、異常検知処理部1370により、加工処理部1350で生成された特徴情報を受け取り、その特徴情報が、モデル保持部1371が保持している所定モデルが示す基準に適合しているか、その基準を逸脱しているかを判定する（ステップS1604）。

【0145】

ゲートウェイ1300は、ステップS1604で、特徴情報が、所定モデルが示す基準を逸脱していない（基準に適合している）と判定した場合には、正常と判定し（ステップS1605）、一方、特徴情報が、所定モデルが示す基準を逸脱していると判定した場合には、異常と判定して（ステップS1606）、その判定結果をログとして保存する（ステップS2608）。なお、ゲートウェイ1300は、この判定結果を用いて機械学習（例えば教師有り学習）等により所定モデルを更新しても良い。

40

【0146】

[2.6 実施の形態2の効果]

実施の形態2に係る異常検知装置（ゲートウェイ1300）は、サーバ等と通信しなくても、自ら自装置が搭載されている車両の識別のための車両識別情報を取得してその車両識別情報に応じて検出窓サイズ（異常検知のためにフレームの受信数をカウントするため

50

の単位時間)を決定し得る。これにより、ゲートウェイ1300は、自装置を搭載した車両に適切な検出窓サイズを用いて車載ネットワークの異常の検知を精度良く行うことが可能となり得る。また、ゲートウェイ1300は、車載ネットワークの監視に基づいて生成した特徴情報を反映した所定モデルの構築(所定モデルの更新等)を行い、所定モデルを用いて異常の判定(検知)を行うので、車両において迅速に異常か否かの判定(つまり異常の検知)を行うことが可能となり得る。また、ゲートウェイ1300は、異常か否かの判定結果をログとして保存でき、その判定結果を活用し得る。

【0147】

(その他変形例)

以上のように、本発明に係る技術の例示として実施の形態1、2を説明した。しかしながら、本発明に係る技術は、これに限定されず、適宜、変更、置き換え、付加、省略等を行った実施の形態にも適用可能である。例えば、以下のような変形例も本発明の一実施態様に含まれる。

【0148】

(1) 上記実施の形態では、決定された検出窓サイズの時間長の検出窓が重複なく連続する例を示したが(図18参照)、検出窓サイズ分の期間である各検出窓は、重複なく連続するものに限られない。図26に示すように、ゲートウェイ(異常検知装置)が、検出窓T1と一部重複する検出窓TA内においてもバスから受信されるフレームの数をID別にカウントすることで、ID別の受信数(カウント数)を成分とする特徴ベクトルを生成して特徴情報としても良い。この場合において、例えば、ゲートウェイは、検出窓TAの開始時点と基準となる開始時点(例えば先行する検出窓T1の開始時点)との差であるオフセット時間を示す情報を特徴情報に含ませてサーバに送信することとしても良い。また、例えば、検出窓サイズ(例えば10ms)分の各検出窓の開始時点を一定時間(例えば1ms)毎等と定めることとしても良い。また、バスから特定のIDのフレームを受信したタイミング等を検出窓の開始時点とすることとしても良い。

【0149】

(2) 上記の実施の形態では、データフレーム(メッセージ)の転送機能を有するゲートウェイ300、1300を、異常を検知する異常検知装置の一例として示したが、異常検知装置は、1つ以上のバスに接続された装置であれば良く、必ずしも転送機能を有する必要はない。異常検知装置は、異常を検知する機能以外の機能を併せ持つECUであっても良い。また、例えば、異常検知装置は、ゲートウェイ300、1300における1つ以上の構成要素を省略し得るし、その1つ以上の構成要素を他のECUに移動させても良い。

【0150】

(3) 上記実施の形態では、CANプロトコルにおけるデータフレーム(メッセージ)を標準IDフォーマット(図2参照)で記述しているが、拡張IDフォーマットであっても良く、メッセージIDは、拡張IDフォーマットでの拡張ID等であっても良い。また、上記実施の形態で示したCANプロトコルは、TTCAN(Time-Triggered CAN)、CANFD(CAN with Flexible Data Rate)等の派生的なプロトコルも包含する広義の意味のものとしても良い。

【0151】

(4) 上記実施の形態1では、ゲートウェイ300が外部通信部360を有する例を示したが、車載ネットワークに接続されたヘッドユニット或いは他のECU(車外と通信する機能を有する装置)を経由して通信することとしても良い。ヘッドユニットは、例えば、マルチメディア再生、カーナビゲーション等の機能のために、車両外部との通信機能を有しているECUである。また、車載ネットワークにおいて、OBD2(On-Board Diagnostics 2)等の診断ポートに接続される診断ツール(故障診断ツール)等が、サーバ400との通信機能を有する場合において、ゲートウェイ300は、その診断ツールを経由してサーバ400と通信することとしても良い。

【0152】

(5) 上記実施の形態では、ゲートウェイ300、1300は、検出窓サイズの期間でのID別のフレームの受信数に基づく特徴情報が、所定モデルが示す基準から逸脱する場合に異常と判定しているが、例えば所定モデルの示す内容を逆にすることで、所定モデルに適合する場合(逸脱しない場合)を異常と判定し、逸脱する場合を正常と判定しても良い。また、実施の形態1では、異常検知結果が異常である場合のみ、ゲートウェイ300がサーバ400へ異常検知結果を送信してサーバ400で異常検知結果を保存することとしたが、正常な場合にも異常検知結果を保存するとしても良い。

【0153】

(6) 上記実施の形態では、ゲートウェイ300、1300が検出窓サイズ分の期間である検出窓内にバスから受信したデータフレームの数をID別にカウントすることでその受信数(カウント数)に基づいて特徴情報を生成する例を示した。しかし、特徴情報は、ID別にカウントしたカウント数の総数(受信した全てのIDのデータフレームの総数)に基づいて、特徴情報を生成するようにしても良い。なお、この場合においては、IDを問わずに受信したデータフレームの数をカウントすることとしても良く、また、基準モデル或いは所定モデルは、その特徴情報と対比し得るように同様の構成(つまりIDを区別せずにフレームの出現頻度の基準を示す構成)とする。

【0154】

(7) 上記実施の形態では、所定モデルが、ゲートウェイ300、1300で検出窓サイズの期間にバスから受信されたフレームの数に基づく特徴情報と対比可能な基準(特徴情報が適合すべき基準)を表す例を示した。この他に、所定モデルを、バスから受信されたフレームと対比可能な基準を表すように構成することとしても良い。この場合には、図20及び図25におけるステップS1602、S1603を省略し、ステップS1604において、バスから受信されたフレームが、所定モデルが示す基準に適合するか否(逸脱する)かを判定することとしても良い。また、上記実施の形態1では、ゲートウェイ300で加工処理を行うことで特徴情報を生成してサーバ400に送信することとしたが(例えばステップS1404、S1405a)、ゲートウェイ300では、バスから受信した各フレームについてのID及び受信時刻をサーバ400に送信するようにして、サーバ400で加工処理を行うこととしても良い。

【0155】

(8) 上記実施の形態で示した異常検知結果に係るログは、サーバ400及びゲートウェイ1300以外の装置(例えば車内のデータ保存専用の装置、ストレージの豊富なヘッドユニット等)に保存することとしても良い。ログの情報は、必要に応じて読み出して、車両の管理、或いは、異常の検知に用いるモデルの設計、構築等に活用し得る。

【0156】

(9) 上記実施の形態におけるゲートウェイその他のECUは、例えば、プロセッサ、メモリ等のデジタル回路、アナログ回路、通信回路等を含む装置であることとしたが、ハードディスク装置、ディスプレイ、キーボード、マウス等のハードウェア構成要素を含んでも良い。また、上記実施の形態で示した各装置は、メモリに記憶された制御プログラムがプロセッサにより実行されてソフトウェア的に機能を実現する代わりに、専用のハードウェア(デジタル回路等)によりその機能を実現することとしても良い。

【0157】

(10) 上記実施の形態における各装置を構成する構成要素の一部又は全部は、1個のシステムLSI(Large Scale Integration:大規模集積回路)から構成されているとしても良い。システムLSIは、複数の構成部を1個のチップ上に集積して製造された超多機能LSIであり、具体的には、マイクロプロセッサ、ROM、RAM等を含んで構成されるコンピュータシステムである。前記RAMには、コンピュータプログラムが記録されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、システムLSIは、その機能を達成する。また、上記各装置を構成する構成要素の各部は、個別に1チップ化されていても良いし、一部又は全部を含むように1チップ化されても良い。また、ここでは、システムLSIとしたが、集積度の違いにより、IC、

10

20

30

40

50

L S I、スーパー L S I、ウルトラ L S I と呼称されることもある。また、集積回路化の手法は L S I に限るものではなく、専用回路又は汎用プロセッサで実現しても良い。L S I 製造後に、プログラムすることが可能な F P G A (Field Programmable Gate Array) や、L S I 内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用して良い。更には、半導体技術の進歩又は派生する別技術により L S I に置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行っても良い。バイオ技術の適用等が可能性としてあり得る。

【0158】

(11) 上記各装置を構成する構成要素の一部又は全部は、各装置に脱着可能な I C カード又は単体のモジュールから構成されているとしても良い。前記 I C カード又は前記モジュールは、マイクロプロセッサ、ROM、RAM等から構成されるコンピュータシステムである。前記 I C カード又は前記モジュールは、上記の超多機能 L S I を含むとしても良い。マイクロプロセッサが、コンピュータプログラムに従って動作することにより、前記 I C カード又は前記モジュールは、その機能を達成する。この I C カード又はこのモジュールは、耐タンパ性を有するとしても良い。

【0159】

(12) 本発明の一態様としては、例えば図14～図17、図19、図20、図23～図25等に示す処理手順の全部又は一部を含む異常検知方法であるとしても良い。例えば、異常検知方法は、CAN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 ECU を備える車載ネットワークシステムにおける異常の検知のための異常検知方法であって、単位時間（例えば検出窓サイズ分の時間）の決定を行い、決定された単位時間内にバスから受信されたメッセージの数に基づく特徴情報と、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を行い、演算処理の結果に応じて異常か否かを判定する。単位時間の決定は、例えば車両識別情報、車両に関連する者等の識別情報、その他の情報等に基づいて行い得る。メッセージは、メッセージの種類を示すメッセージ ID を含み、異常検知方法は、例えば、車両の識別のための車両識別情報に基づいて単位時間の決定を行う決定ステップ（例えばステップ S 1 3 0 5、S 2 3 0 3 等）と、決定ステップで決定された単位時間（決定が複数回行われる場合においては例えば最新の単位時間）内にバスから受信されたメッセージ ID 毎のメッセージの数を成分とする特徴ベクトルを特徴情報として特定する特定ステップ（例えばステップ S 1 4 0 4 等）と、特定ステップで特定された特徴情報と所定モデルとを用いて演算処理を行い、演算処理の結果に応じて異常か否かの判定を行う判定ステップ（例えばステップ S 1 6 0 4 等）を含む。また、例えば、異常検知方法は更に、特定ステップで逐次特定された複数の特徴情報に基づいて所定モデルを逐次更新する更新ステップ（例えばステップ S 1 5 0 3、S 2 4 0 7 等）を含む。また、本発明の一態様としては、この異常検知方法に係る処理をコンピュータにより実現するコンピュータプログラムであるとしても良いし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号をコンピュータで読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray (登録商標) Disc)、半導体メモリ等に記録したものとしても良い。また、これらの記録媒体に記録されている前記デジタル信号であるとしても良い。また、本発明の一態様としては、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク、データ放送等を経由して伝送するものとしても良い。また、本発明の一態様としては、マイクロプロセッサとメモリを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記録しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしても良い。また、前記プログラム若しくは前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム若しくは前記デジタル信号を、前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしても良い。

【0160】

(13) 上記実施の形態及び上記変形例で示した各構成要素及び機能を任意に組み合わせることで実現される形態も本発明の範囲に含まれる。

【産業上の利用可能性】

【0161】

本発明は、車載ネットワークに対する攻撃を検知するために利用可能である。

【符号の説明】

【0162】

10	異常検知システム	
40	ネットワーク	10
100a	エンジンECU	
100b	ブレーキECU	
100c	ドア開閉センサECU	
100d	ウィンドウ開閉センサECU	
101	エンジン	
102	ブレーキ	
103	ドア開閉センサ	
104	ウィンドウ開閉センサ	
110、310	フレーム送受信部	
120、320	フレーム解釈部	20
130、330	受信ID判断部	
140、340	受信IDリスト保持部	
150	フレーム処理部	
160	データ取得部	
170、390	フレーム生成部	
200a、200b	バス	
300、1300	ゲートウェイ（異常検知装置）	
350、1350	加工処理部	
360	外部通信部	
361	車両識別情報保持部	30
370、1370	異常検知処理部	
371、1371	モデル保持部	
380	転送処理部	
381	転送ルール保持部	
400	サーバ	
410	通信部	
420	データ蓄積部	
430、1430	学習部	
440	検出窓サイズ特定部	
450	検出窓サイズ特定用テーブル保持部	40
460、1460	異常検知結果保持部	
1440	検出窓サイズ決定部	

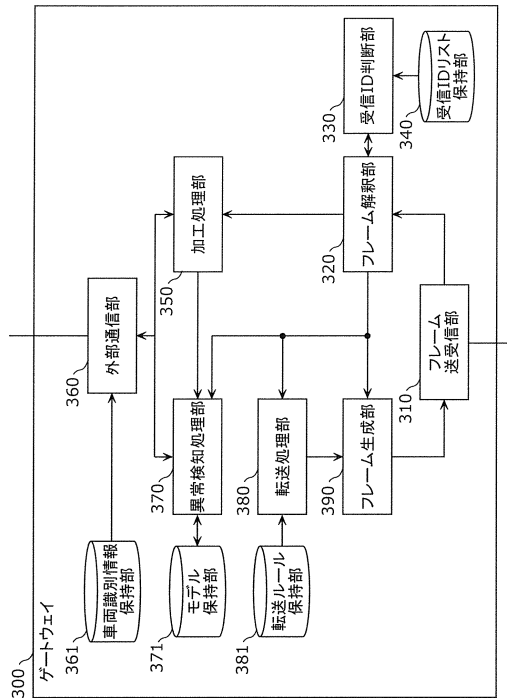
【図 7】

ID	データ
3	1
3	1
3	0
3	0
3	0
...	...

【図 8】

ID	データ
4	0
4	10
4	20
4	30
4	40
...	...

【図 9】



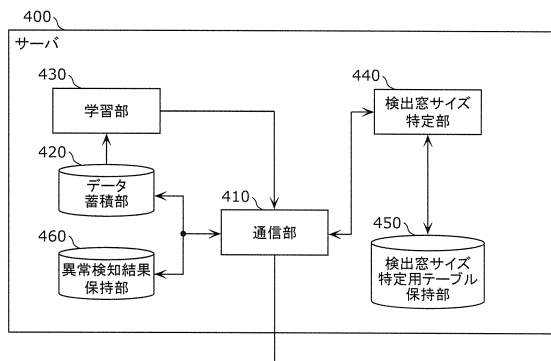
【図 10】

カーメーカ	車種	車台番号	
		型式	製造番号
A社	AX	AX-A001	10101010101010101

【図 1 1】

転送元	転送先	ID
200a	200b	*
200b	200a	3

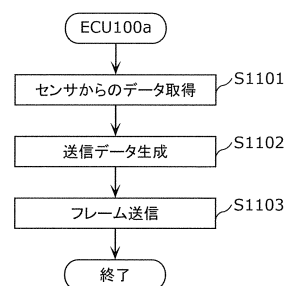
【図 1 2】



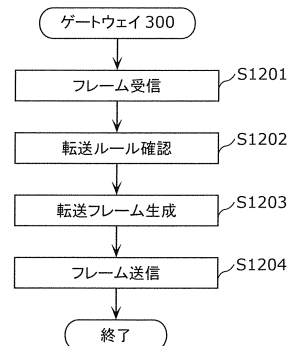
【図 13】

カーメーカ	車種	車台番号		検出窓サイズ [ms]
		型式	製造番号	
A社	AX	AX-A001	10101010101010101	10
A社	AC	AC-R002	10101010103010102	20
A社	AD	AD-K003	10101010102010102	40
B社	BA	BA-E001	10201010101010105	12
B社	BE	BE-B002	10201010102010101	24
C社	CK	CK-J001	10301010103010109	48

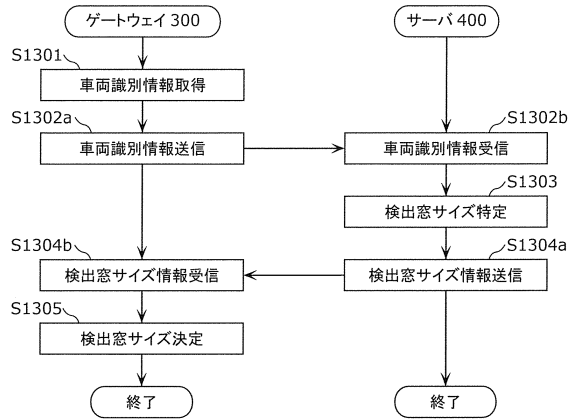
【図 14】



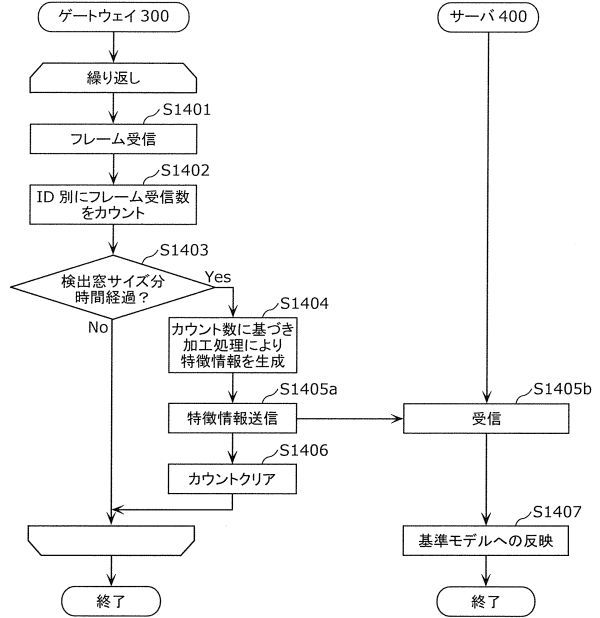
【図 15】



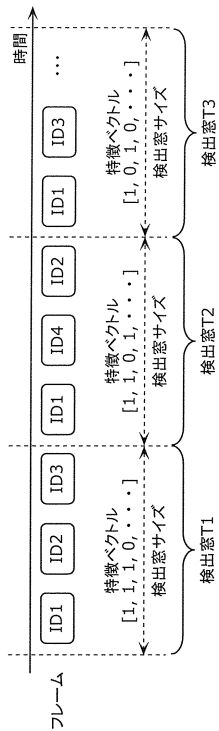
【図 16】



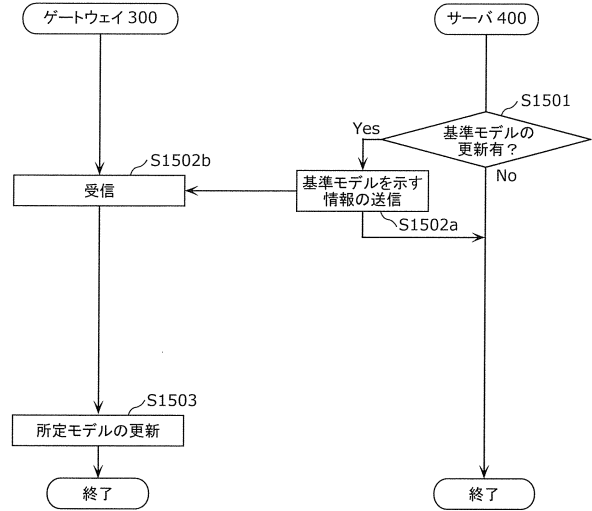
【図 17】



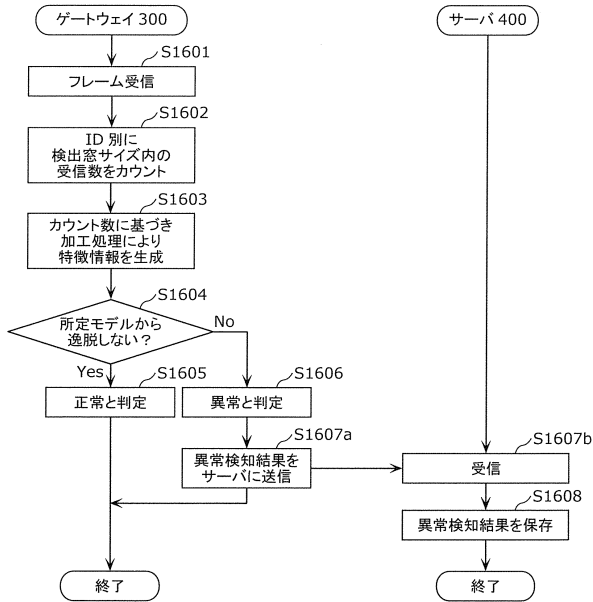
【図 18】



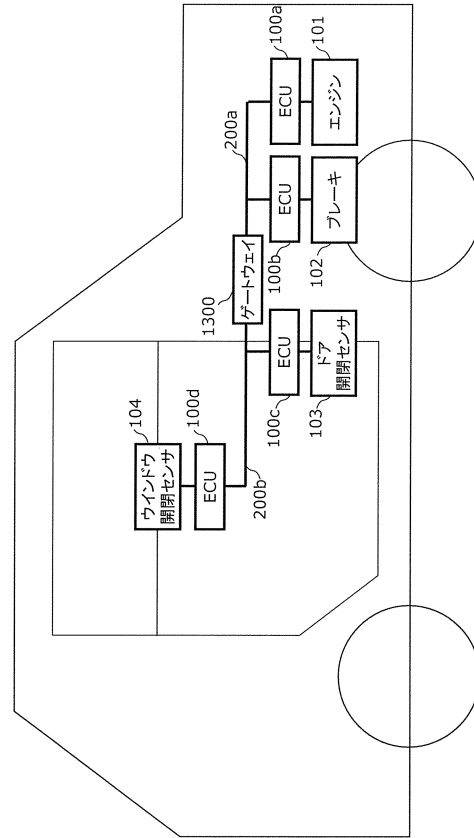
【図 19】



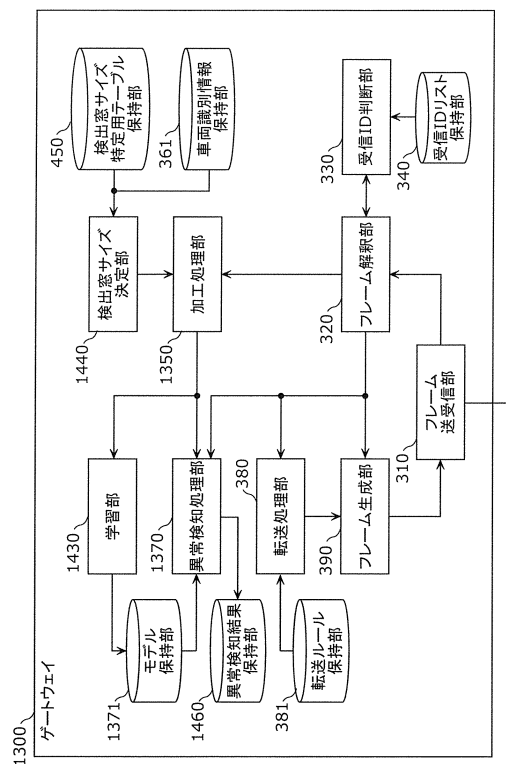
【図 20】



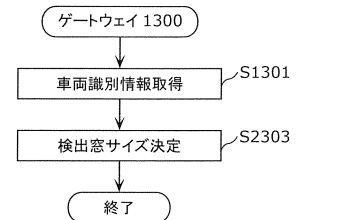
【図 2 1】



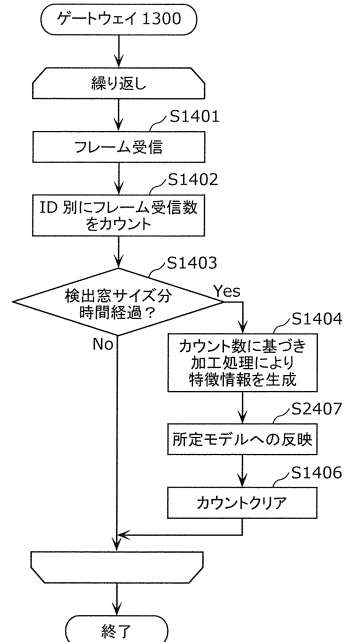
【図 2 2】



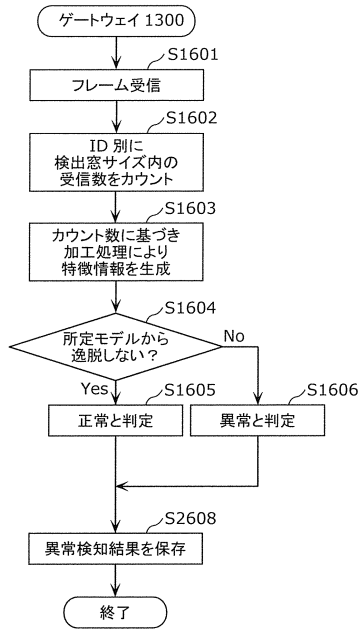
【图 2 3】



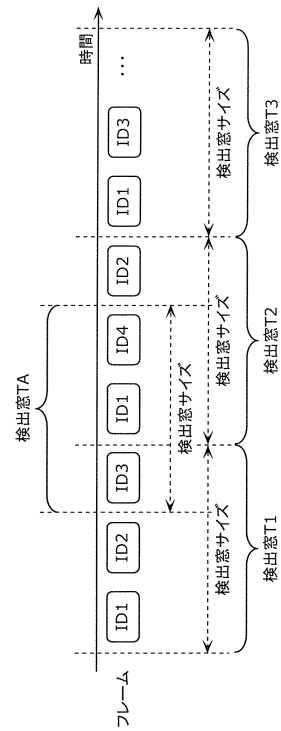
【図 24】



【図 25】



【図 26】



フロントページの続き

- (74)代理人 100131417
弁理士 道坂 伸一
- (72)発明者 氏家 良浩
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 芳賀 智之
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 前田 学
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 松島 秀樹
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 岸川 剛
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 鶴見 淳一
大阪府門真市大字門真1006番地 パナソニック株式会社内
- (72)発明者 鹿島 久嗣
京都府京都市左京区吉田本町36番地1 国立大学法人京都大学内
- (72)発明者 鳥海 雪乃
京都府京都市左京区吉田本町36番地1 国立大学法人京都大学内
- (72)発明者 桑原 拓也
京都府京都市左京区吉田本町36番地1 国立大学法人京都大学内

審査官 中川 幸洋

- (56)参考文献 特開2009-253557 (JP, A)
国際公開第2015/159520 (WO, A1)
特開2006-287739 (JP, A)
特開2009-035237 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
H04L 12/40