(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7007632号
(P7007632)

(45)発行日　令和4年1月24日(2022.1.24)

(24)登録日　令和4年1月12日(2022.1.12)

(51)国際特許分類		FI		
G06F 21/55 (2013.01)		G06F	21/55	
B60R 16/023 (2006.01)		B60R	16/023	P
H04L 12/28 (2006.01)		H04L	12/28	
H04W 12/121 (2021.01)		H04W	12/121	

請求項の数　13　（全49頁）

(21)出願番号　特願2017-150807(P2017-150807)
(22)出願日　平成29年8月3日(2017.8.3)
(65)公開番号　特開2019-29961(P2019-29961A)
(43)公開日　平成31年2月21日(2019.2.21)
審査請求日　令和2年2月21日(2020.2.21)

(73)特許権者　000002130
住友電気工業株式会社
大阪府大阪市中央区北浜四丁目５番３３号
(73)特許権者　000183406
住友電装株式会社
三重県四日市市西末広町１番１４号
(73)特許権者　395011665
株式会社オートネットワーク技術研究所
三重県四日市市西末広町１番１４号
(74)代理人　110000682
特許業務法人ワンディーＩＰパートナーズ
(72)発明者　濱田 芳博
大阪府大阪市中央区北浜四丁目５番３３
最終頁に続く

(54)【発明の名称】　検知装置、検知方法および検知プログラム

(57)【特許請求の範囲】
【請求項１】
車両に搭載される車載ネットワークにおける不正メッセージ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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部と、
予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶する記憶部と、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部とを備え、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて１つの前記検出条件が作成され、
前記検知部は、前記データ取得部によって取得された前記ある種類の前記データおよび前記複数種類の前記相関データ、ならびに前記検出条件に基づいて、前記ある種類の前記データの推定誤差を算出し、算出した前記推定誤差、および前記検出条件を用いて作成された前記推定誤差の分布に基づいて、前記ある種類の前記データの正当性を評価し、評価結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する

、検知装置。
【請求項２】
車両に搭載される車載ネットワークにおける不正メッセージ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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部と、
予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶する記憶部と、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部とを備え、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて１つの前記検出条件が作成され、
前記ある種類の前記データは、状態を表すデータであり、
前記検知部は、前記データ取得部によって取得された前記複数種類の前記相関データ、および前記検出条件に基づいて、前記ある種類の前記データの値を推定し、推定した前記値と前記ある種類の前記データとの比較結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する、検知装置。
【請求項３】
車両に搭載される車載ネットワークにおける不正メッセージ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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部と、
予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶する記憶部と、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部とを備え、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて複数の前記検出条件がそれぞれ作成されている、検知装置。
【請求項４】
前記データ取得部は、異なる前記送信メッセージにそれぞれ含まれる前記複数種類のデータの組を取得する、請求項１から請求項３のいずれか１項に記載の検知装置。
【請求項５】
前記メッセージ取得部は、取得した複数の前記送信メッセージを記憶部に保存し、
前記データ取得部は、前記記憶部に保存された各前記送信メッセージから前記組を取得する、請求項４に記載の検知装置。
【請求項６】
前記検知装置は、さらに、
前記データ取得部によって取得された前記組に基づいて前記検出条件を更新する更新部を備える、請求項１から請求項５のいずれか１項に記載の検知装置。
【請求項７】
前記検知装置は、さらに、
前記車載ネットワークにおける前記送信メッセージを監視する監視部と、
前記送信メッセージの送信間隔の分布を取得する分布取得部とを備え、
前記検知部は、前記監視部による監視結果および前記分布取得部によって取得された前記

分布に基づいて前記不正メッセージを検知し、
前記検知部は、前記不正メッセージとすべきでないと判断した前記送信メッセージについては、前記データ取得部によって取得された前記組、および前記検出条件に基づいて、前記不正メッセージであるか否かについて判断する、請求項１から請求項６のいずれか１項に記載の検知装置。
【請求項８】
車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するステップと、
取得した前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するステップとを含み、
前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、
前記検知方法は、さらに、
取得した前記組、および前記検出条件に基づいて前記不正メッセージを検知するステップを含み、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて１つの前記検出条件が作成され、
前記不正メッセージを検知するステップにおいて、取得した前記ある種類の前記データおよび前記複数種類の前記相関データ、ならびに前記検出条件に基づいて、前記ある種類の前記データの推定誤差を算出し、算出した前記推定誤差、および前記検出条件を用いて作成された前記推定誤差の分布に基づいて、前記ある種類の前記データの正当性を評価し、評価結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する、検知方法。
【請求項９】
車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するステップと、
取得した前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するステップとを含み、
前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、
前記検知方法は、さらに、
取得した前記組、および前記検出条件に基づいて前記不正メッセージを検知するステップを含み、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて１つの前記検出条件が作成され、
前記ある種類の前記データは、状態を表すデータであり、
前記不正メッセージを検知するステップにおいて、取得した前記複数種類の前記相関データ、および前記検出条件に基づいて、前記ある種類の前記データの値を推定し、推定した前記値と前記ある種類の前記データとの比較結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する、検知方法。
【請求項１０】
車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するステップと、

取得した前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するステップとを含み、
前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、
前記検知方法は、さらに、
取得した前記組、および前記検出条件に基づいて前記不正メッセージを検知するステップを含み、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて複数の前記検出条件がそれぞれ作成されている、検知方法。
【請求項１１】
車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部、
として機能させるためのプログラムであり、
前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、
さらに、コンピュータを、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部、
として機能させるためのプログラムであり、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて１つの前記検出条件が作成され、
前記検知部は、前記データ取得部によって取得された前記ある種類の前記データおよび前記複数種類の前記相関データ、ならびに前記検出条件に基づいて、前記ある種類の前記データの推定誤差を算出し、算出した前記推定誤差、および前記検出条件を用いて作成された前記推定誤差の分布に基づいて、前記ある種類の前記データの正当性を評価し、評価結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する、検知プログラム。
【請求項１２】
車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部、
として機能させるためのプログラムであり、
前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、
さらに、コンピュータを、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部、

として機能させるためのプログラムであり、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて１つの前記検出条件が作成され、
前記ある種類の前記データは、状態を表すデータであり、
前記検知部は、前記データ取得部によって取得された前記複数種類の前記相関データ、および前記検出条件に基づいて、前記ある種類の前記データの値を推定し、推定した前記値と前記ある種類の前記データとの比較結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する、検知プログラム。
【請求項１３】
車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部、
として機能させるためのプログラムであり、
前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、
さらに、コンピュータを、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部、
として機能させるためのプログラムであり、
前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成され、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて複数の前記検出条件がそれぞれ作成されている、検知プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、検知装置、検知方法および検知プログラムに関する。
【背景技術】
【０００２】
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。
【０００３】
たとえば、特許文献１（特開２０１６－１１６０７５号公報）には、以下のような車載通信システムが開示されている。すなわち、車載通信システムは、通信データの送信側が生成するメッセージ認証コードである送信側コードと、前記通信データの受信側が生成するメッセージ認証コードである受信側コードとを使用してメッセージ認証を行う車載通信システムであって、車載ネットワークに接続され、第１の暗号鍵と前記第１の暗号鍵とは異なる第２の暗号鍵のうち前記第１の暗号鍵だけを保持する第１のＥＣＵと、前記車載ネットワークに接続され、前記第１の暗号鍵を少なくとも保持する第２のＥＣＵと、前記車載ネットワーク及び車外ネットワークに接続され、前記第１の暗号鍵と前記第２の暗号鍵のうち前記第２の暗号鍵だけを保持して、前記第２の暗号鍵を使用して前記車載ネットワークにおける通信時に前記送信側コード又は前記受信側コードを生成する第３のＥＣＵとを備え、前記第２のＥＣＵは、前記第１の暗号鍵を使用して生成した送信側コードを付与した通信データを送信し、前記第１のＥＣＵは、前記通信データを受信した場合に、前記第

１の暗号鍵を使用して生成した受信側コードによって、前記受信した通信データに付与された送信側コードの検証を行う。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２０１６－１１６０７５号公報
特開２０１６－５７４３８号公報
特開２０１６－９７８７９号公報
特開２０１５－１３６１０７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
特許文献１には、車載ネットワークに限定して接続される第１のＥＣＵおよび第２のＥＣＵがメッセージ認証に用いる第１の暗号鍵と、車載ネットワークおよび車外ネットワークの両方に接続される第３のＥＣＵが用いる第２の暗号鍵とが異なることにより、車外ネットワークに接続されない第１のＥＣＵおよび第２のＥＣＵに対する車外ネットワークからのサイバー攻撃を防ぐ構成が開示されている。
【０００６】
しかしながら、メッセージ認証を用いるセキュリティ対策では、プロトコルの脆弱性を突いた攻撃、第１の暗号鍵の不正入手による攻撃、および暗号アルゴリズムの陳腐化を突いた攻撃等により、当該セキュリティ対策が無効化されることがある。
【０００７】
このような攻撃を受けた場合において、攻撃者が車載ネットワークに侵入したことを正しく検知するための技術が求められる。
【０００８】
この発明は、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、車載ネットワークにおける不正メッセージを正しく検知することが可能な検知装置、検知方法および検知プログラムを提供することである。
【課題を解決するための手段】
【０００９】
（１）上記課題を解決するために、この発明のある局面に係わる検知装置は、車両に搭載される車載ネットワークにおける不正メッセージ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１または複数の送信メッセージを取得するメッセージ取得部と、前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部と、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶する記憶部と、前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部とを備える。
【００１０】
（１１）上記課題を解決するために、この発明のある局面に係わる検知方法は、車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するステップと、取得した前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するステップとを含み、前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、前記検知方法は、さらに、取得した前記組、および前記検出条件に基づいて前記不正メッセージを検知するステップを含む。
【００１１】
（１２）上記課題を解決するために、この発明のある局面に係わる検知プログラムは、車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備える検知

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１または複数の送信メッセージを取得するメッセージ取得部と、前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部、として機能させるためのプログラムであり、前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、さらに、コンピュータを、 前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部、として機能させるためのプログラムである。

【００１２】

本発明は、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することができるだけでなく、検知装置を備える車載通信システムとして実現することができる。また、本発明は、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することができる。

【発明の効果】

【００１３】

本発明によれば、車載ネットワークにおける不正メッセージを正しく検知することができる。

【図面の簡単な説明】

【００１４】

【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ゲートウェイ装置が用いる通常モデルの作成過程を説明するための図である。

【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いて行われる同期処理のタイミングを説明するための図である。

【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において行われる同期処理のタイミングを説明するための図である。

【図７】図７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が行う不正メッセージの検知を説明するための図である。

【図８】図８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効果を説明するための図である。

【図９】図９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効果を説明するための図である。

【図１０】図１０は、本発明の第１の実施の形態に係る通常モデルの変形例についての学習フェーズにおける作成処理を説明するための図である。

【図１１】図１１は、本発明の第１の実施の形態に係る通常モデルの変形例についてのテストフェーズにおける検証処理を説明するための図である。

【図１２】図１２は、本発明の第１の実施の形態に係る通常モデルの変形例を用いた不正メッセージの検知処理を説明するための図である。

【図１３】図１３は、本発明の第１の実施の形態に係る通常モデルの変形例についての学習フェーズにおける作成処理を説明するための図である。

【図１４】図１４は、本発明の第１の実施の形態に係る通常モデルの変形例を用いた不正メッセージの検知処理を説明するための図である。

【図１５】図１５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メッセージを受信する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１の実施の形態に係るゲートウェイ装置が、受信したメッセージを記憶部に保存した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２の実施の形態に係るゲートウェイ装置における誤検知

の一例を説明するための図である。
【図１８】図１８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ゲートウェイ装置の構成を示す図である。
【図１９】図１９は、本発明の第２の実施の形態に係るゲートウェイ装置における更新部が行う通常モデルの更新を説明するための図である。
【図２０】図２０は、本発明の第２の実施の形態に係るゲートウェイ装置における更新部が更新した通常モデルを説明するための図である。
【図２１】図２１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ゲートウェイ装置の構成を示す図である。
【図２２】図２２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監視対象の周期メッセージの送信間隔の時間変化の一例を示す図である。
【図２３】図２３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対象メッセージの送信間隔の度数分布の一例を示す図である。
【図２４】図２４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検出例を示す図である。
【図２５】図２５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対象メッセージを受信する際の動作手順を定めたフローチャートである。
【図２６】図２６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判断処理を行う際の動作手順を定めたフローチャートである。
【発明を実施するための形態】
【００１５】
最初に、本発明の実施形態の内容を列記して説明する。
【００１６】
（１）本発明の実施の形態に係る検知装置は、車両に搭載される車載ネットワークにおける不正メッセージ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１または複数の送信メッセージを取得するメッセージ取得部と、前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部と、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶する記憶部と、前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部とを備える。
【００１７】
たとえば、複数種類のデータ間に何らかの関係がある場合、当該関係を用いて、あるデータから他のデータがとり得る値の範囲を算出することができる。上記のような構成により、たとえば、上記組におけるあるデータから当該組における他のデータがとり得る値の範囲を検出条件に基づいて算出することができるので、当該他のデータの正当性を正しく判断することができる。これにより、不正と判断したデータを含むメッセージを不正メッセージとして検知することができる。したがって、車載ネットワークにおける不正メッセージを正しく検知することができる。
【００１８】
（２）好ましくは、前記検出条件は、所定の相関関係を有する複数種類のデータの前記組に基づいて作成されている。
【００１９】
このように、データ間においてある程度の関係が存在する複数種類のデータの組に基づいて検出条件が作成される構成により、組におけるあるデータから当該組における他のデータがとり得る値の範囲をより狭めることが可能な検出条件を作成することができる。これにより、当該他のデータの正当性をより正しく判断することができる。すなわち、適切な検出条件を作成することができる。
【００２０】
（３）より好ましくは、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関デ

ータとに基づいて１つの前記検出条件が作成されている。
【００２１】
このような構成により、たとえば、攻撃者が、ある種類のデータおよび複数種類の相関データのうちの一部のデータを改変した場合においても、改変したデータと残りのデータとの関係に基づいて、上記組のデータの異常を判断することができる。すなわち、攻撃者は、不正侵入するためには、ある種類のデータおよび複数種類の相関データの全部を改変しなければならないので、車載ネットワークに対する不正侵入を困難にすることができる。これにより、車載ネットワークにおけるセキュリティを向上させることができる。
【００２２】
（４）より好ましくは、前記検知部は、前記データ取得部によって取得された前記ある種類の前記データおよび前記複数種類の前記相関データ、ならびに前記検出条件に基づいて、前記ある種類の前記データの推定誤差を算出し、算出した前記推定誤差、および前記検出条件を用いて作成された前記推定誤差の分布に基づいて、前記ある種類の前記データの正当性を評価し、評価結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する。
【００２３】
このような構成により、たとえば、ある種類のデータが、センサによって計測された値のように連続して変化する値である場合において、ある種類のデータが正しい値を有する可能性をより正しく評価することができるので、ある種類のデータの正当性をより正しく判断することができる。
【００２４】
（５）より好ましくは、前記ある種類の前記データは、状態を表すデータであり、前記検知部は、前記データ取得部によって取得された前記複数種類の前記相関データ、および前記検出条件に基づいて、前記ある種類の前記データの値を推定し、推定した前記値と前記ある種類の前記データとの比較結果に基づいて、前記ある種類の前記データが前記不正メッセージであるか否かを判断する。
【００２５】
このような構成により、たとえば、ある種類のデータが、ギアのシフトポジションまたはシートベルトの状態のように不連続に変化する値である場合において、ある種類のデータが示すべき値をより正しく推定することができるので、ある種類のデータの正当性をより正しく判断することができる。
【００２６】
（６）より好ましくは、ある種類の前記データと前記相関関係を有する前記データである相関データが複数種類ある場合、前記ある種類の前記データと前記複数種類の前記相関データとに基づいて複数の前記検出条件がそれぞれ作成されている。
【００２７】
このような構成により、車載ネットワークに対する不正侵入を困難にするとともに、検出条件の算出における計算負荷を軽減することができる。
【００２８】
（７）好ましくは、前記データ取得部は、異なる前記送信メッセージにそれぞれ含まれる前記複数種類のデータの組を取得する。
【００２９】
受信時刻、送信時刻または作成時刻等が異なる複数種類のデータは、異なる送信メッセージにそれぞれ含まれることが多い。上記のような構成により、時刻によって検知対象のデータの種類が制限されることを防ぐことができる。
【００３０】
（８）より好ましくは、前記メッセージ取得部は、取得した複数の前記送信メッセージを記憶部に保存し、前記データ取得部は、前記記憶部に保存された各前記送信メッセージから前記組を取得する。
【００３１】

このような構成により、たとえば、記憶部に保存された複数の送信メッセージにおけるデータをリサンプリングすることができるので、複数種類のデータの時刻を合わせることができる。これにより、同じ時刻に対応する複数種類のデータの組を容易に取得することができる。

【００３２】

（９）好ましくは、前記検知装置は、さらに、前記データ取得部によって取得された前記組に基づいて前記検出条件を更新する更新部を備える。

【００３３】

このような構成により、たとえば、検出条件の算出に用いた組が母集団として不完全であっても、新たに取得した組を母集団に含めることができるので、母集団の完成度をより高めることができる。これにより、より適切な検出条件に更新することができる。

【００３４】

（１０）好ましくは、前記検知装置は、さらに、前記車載ネットワークにおける前記送信メッセージを監視する監視部と、前記送信メッセージの送信間隔の分布を取得する分布取得部とを備え、前記検知部は、前記監視部による監視結果および前記分布取得部によって取得された前記分布に基づいて前記不正メッセージを検知し、前記検知部は、前記不正メッセージとすべきでないと判断した前記送信メッセージについては、前記データ取得部によって取得された前記組、および前記検出条件に基づいて、前記不正メッセージであるか否かについて判断する。

【００３５】

送信間隔を精度よく偽装した送信メッセージは、上記監視結果および上記分布に基づいて不正メッセージとして検知することが困難である。上記のような構成により、当該送信メッセージを、上記組および検出条件に基づいて不正メッセージとして検知することができるので、車載ネットワークにおけるセキュリティを向上させることができる。

【００３６】

（１１）本発明の実施の形態に係る検知方法は、車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するステップと、取得した前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するステップとを含み、前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、前記検知方法は、さらに、取得した前記組、および前記検出条件に基づいて前記不正メッセージを検知するステップを含む。

【００３７】

たとえば、複数種類のデータ間に何らかの関係がある場合、当該関係を用いて、あるデータから他のデータがとり得る値の範囲を算出することができる。上記のような構成により、たとえば、上記組におけるあるデータから当該組における他のデータがとり得る値の範囲を検出条件に基づいて算出することができるので、当該他のデータの正当性を正しく判断することができる。これにより、不正と判断したデータを含むメッセージを不正メッセージとして検知することができる。したがって、車載ネットワークにおける不正メッセージを正しく検知することができる。

【００３８】

（１２）本発明の実施の形態に係る検知プログラムは、車両に搭載される車載ネットワークにおける不正メッセージを検知し、記憶部を備え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１または複数の送信メッセージを取得するメッセージ取得部と、前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部、として機能させるためのプログラムであり、前記記憶部は、予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶し、さらに、コンピュータを、前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部、として機能させるためのプログラムである。

【００３９】
たとえば、複数種類のデータ間に何らかの関係がある場合、当該関係を用いて、あるデータから他のデータがとり得る値の範囲を算出することができる。上記のような構成により、たとえば、上記組におけるあるデータから当該組における他のデータがとり得る値の範囲を検出条件に基づいて算出することができるので、当該他のデータの正当性を正しく判断することができる。これにより、不正と判断したデータを含むメッセージを不正メッセージとして検知することができる。したがって、車載ネットワークにおける不正メッセージを正しく検知することができる。
【００４０】
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。
【００４１】
＜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。
【００４２】
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。
【００４３】
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。
【００４４】
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。
【００４５】
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。）１に搭載される。車載ネットワーク１２は、対象車両１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。
【００４６】
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。
【００４７】
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１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。
【００４８】
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。
【００４９】
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１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、エンターテイメント等のサービスに用いる情報を中継する。

【００５０】

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、スマートエントリおよびＴＰＭＳ（Ｔｉｒｅ Ｐｒｅｓｓｕｒｅ Ｍｏｎｉｔｏｒｉｎｇ Ｓｙｓｔｅｍ）等のサービスに用いる情報を中継する。

【００５１】

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。

【００５２】

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１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。

【００５３】

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。

【００５４】

この例では、車載通信機１１１は、イーサネットの規格に従う対応のバス１４を介してゲートウェイ装置１０１と接続されている。また、バス接続装置群１２１における各制御装置１２２は、ＣＡＮの規格に従う対応のバス１３を介してゲートウェイ装置１０１と接続されている。制御装置１２２は、たとえば、対象車両１における機能部を制御可能である。

【００５５】

バス１３は、たとえば系統別に設けられる。具体的には、バス１３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。

【００５６】

駆動系バスには、制御装置１２２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。

【００５７】

シャーシ／安全系バスには、制御装置１２２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。

【００５８】

ボディ／電装系バスには、制御装置１２２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。

【００５９】

ＡＶ／情報系バスには、制御装置１２２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、ＥＴＣ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。

【００６０】

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、たとえばセンサが接続されてもよい。

【００６１】

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。

【００６２】

ゲートウェイ装置１０１は、たとえば、対象車両１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。

【００６３】

より詳細には、対象車両１では、たとえば、所定の取り決めに従って、ある車載装置から他の車載装置へ周期的にメッセージが送信される。この例では、ある制御装置１２２から他の制御装置１２２へ周期的に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。

【００６４】

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。以下、周期的に送信されるメッセージを周期メッセージとも称する。

【００６５】

また、対象車両１では、周期メッセージの他に、ある制御装置１２２から他の制御装置１２２へ不定期に送信されるメッセージが存在する。メッセージには、メッセージの内容および送信元等を識別するためのＩＤが含まれる。メッセージが周期メッセージであるか否かをＩＤによって識別することが可能である。

【００６６】

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。

【００６７】

図３を参照して、ゲートウェイ装置１０１は、通信処理部５１と、記憶部５２と、データ取得部５３と、検知部５４と、メッセージ取得部５５とを備える。

【００６８】

ゲートウェイ装置１０１は、検知装置として機能し、対象車両１に搭載される車載ネットワーク１２における不正メッセージを検知する。

【００６９】

詳細には、ゲートウェイ装置１０１における通信処理部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他の制御装置１２２へ対応のバス１３経由で送信する。

【００７０】

メッセージ取得部５５は、車載ネットワーク１２における複数の送信メッセージを取得する。メッセージ取得部５５は、たとえば、取得した複数の送信メッセージを記憶部５２に保存する。

【００７１】
より詳細には、記憶部５２には、たとえば、メッセージ取得部５５が監視対象とすべきデータの種類を含む検出条件情報が登録されている。検出条件情報の詳細については、後述する。
【００７２】
メッセージ取得部５５は、記憶部５２に登録されている検出条件情報に基づいて、自己が監視対象とすべきデータの種類を認識する。
【００７３】
メッセージ取得部５５は、通信処理部５１が中継するメッセージに含まれるデータを監視し、監視対象の種類のデータを含むメッセージを検出するごとに、以下の処理を行う。
【００７４】
すなわち、メッセージ取得部５５は、検出したメッセージを通信処理部５１から取得し、取得したメッセージに、当該メッセージの受信時刻を示すタイムスタンプを付す。
【００７５】
そして、メッセージ取得部５５は、タイムスタンプを付したメッセージを記憶部５２に保存する。
【００７６】
図４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用いる通常モデルの作成過程を説明するための図である。なお、図４において、横軸はデータＸを示し、縦軸はデータＹを示す。
【００７７】
図４を参照して、記憶部５２は、予め作成された、複数の時刻たとえばデータの作成時刻にそれぞれ対応する複数の組に基づく検出条件を記憶する。ここで、組は、たとえば、メッセージ取得部５５によって取得された送信メッセージに含まれる、同じ作成時刻に対応する２種類のデータの組である。
【００７８】
具体的には、記憶部５２は、たとえば、サーバによって予め作成された通常モデルＭ２を記憶する。通常モデルＭ２は、たとえば、所定の相関関係を有する２種類のデータの組に基づいて作成されている。
【００７９】
より具体的には、サーバには、たとえば、互いに異なる種類の時系列の生データＲ１～生データＲＮがユーザによって登録される。ここで、Ｎは、２以上の整数である。この例では、生データＲ１～生データＲＮは、たとえば、対象車両１と同じ種類のテスト車両において開発時に取得されたデータである。
【００８０】
サーバは、たとえば、時系列の生データＲ１～生データＲＮを、共通の複数の作成時刻におけるデータ１～データＮに変換する。
【００８１】
より詳細には、サーバは、たとえば、生データＲ１および生データＲ２の作成時刻が同期していない場合、生データＲ２をリサンプリングすることにより、生データＲ２の作成時刻を生データＲ１の作成時刻に同期させる。
【００８２】
同様に、サーバは、たとえば、生データＲ１および生データＲ３の作成時刻が同期していない場合、生データＲ３をリサンプリングすることにより、生データＲ３の作成時刻を生データＲ１の作成時刻に同期させる。
【００８３】
サーバは、生データＲ４～生データＲＮに対しても同様の処理を施すことにより、生データＲ４～生データＲＮの作成時刻を生データＲ１の作成時刻に同期させる。これにより、時系列の生データＲ１～生データＲＮが、共通の複数の作成時刻におけるデータ１～データＮに変換される。

【００８４】
サーバは、たとえば、共通の複数の作成時刻におけるデータ１～データＮの中から、共通の複数の作成時刻におけるデータＸ，Ｙを選択する。ここで、Ｘ，Ｙは、互いに異なり、かつ１～Ｎのうちのいずれかの整数である。データＸ，Ｙの選択は、たとえば総当たりで行われる。
【００８５】
図４には、共通の複数の作成時刻にそれぞれ対応する、データＸおよびデータＹの組が黒丸によって示される。
【００８６】
サーバは、たとえば、選択したデータＸおよびデータＹの複数の組に基づいて相関係数を算出する。
【００８７】
サーバは、たとえば、算出した相関係数が０．４以上かつ０．７以下である場合、データＸおよびデータＹに相関有りと判断する。また、サーバは、たとえば、算出した相関係数が０．７より大きい場合、データＸおよびデータＹに強い相関有りと判断する。
【００８８】
サーバは、データＸおよびデータＹについて相関有り、または強い相関有りと判断した場合、データＸおよびデータＹに基づいて通常モデルＭ２を作成する。
【００８９】
具体的には、サーバは、たとえば、マハラノビス、Ｏｎｅｃｌａｓｓ－ＳＶＭ（Ｓｕｐｐｏｒｔ Ｖｅｃｔｏｒ Ｍａｃｈｉｎｅ）、ＬＯＦ（Ｌｏｃａｌ Ｏｕｔｌｉｅｒ Ｆａｃｔｏｒ）、Ｉｓｏｌａｔｉｏｎ ｆｏｒｅｓｔ、およびＮＮ（Ｎｅａｒｅｓｔ－Ｎｅｉｇｈｂｏｒ）等のアルゴリズムに従って、機械学習により通常モデルＭ２を作成する。
【００９０】
一方、サーバは、データＸおよびデータＹについて相関有りと判断せず、かつ強い相関有りと判断しなかった場合、通常モデルＭ２を作成しない。
【００９１】
サーバは、たとえば、複数の通常モデルＭ２を作成し、作成した通常モデルＭ２ごとにモデル情報を作成する。ここで、モデル情報は、通常モデルＭ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示す。
【００９２】
データＸおよびデータＹの種類の組み合わせは、たとえば、エンジン回転数および速度、ヨーレートおよび舵角、ヨーレートおよび車高、ならびにアクセル開度および車体加速度等である。
【００９３】
サーバによって作成された複数のモデル情報は、たとえば、検出条件情報としてまとめられた後、対象車両１の製造時において記憶部５２に登録される。
【００９４】
なお、検出条件情報は、更新されてもよい。具体的には、たとえば、通信処理部５１は、サーバによってアップデートされた検出条件情報を車載通信機１１１経由でサーバから受信し、記憶部５２に登録された検出条件情報を、受信した検出条件情報に更新する。
【００９５】
また、サーバは、複数の通常モデルＭ２を作成する構成に限らず、１つの通常モデルＭ２を作成する構成であってもよい。
【００９６】
再び図３を参照して、データ取得部５３は、メッセージ取得部５５によって取得された送信メッセージに含まれる、同じ時刻たとえば受信時刻に対応する２種類のデータの組を取得する。
【００９７】
より詳細には、データ取得部５３は、記憶部５２が保存する検出条件情報に含まれる複数

のモデル情報を記憶部５２から取得する。
【００９８】
［２種類のデータが同じ送信メッセージに含まれる場合］
データ取得部５３は、たとえば、記憶部５２に保存された各送信メッセージから２種類のデータの組を取得する。
【００９９】
より詳細には、データ取得部５３は、たとえば、取得した複数のモデル情報に基づいて、同じ送信メッセージに含まれる２種類のデータの組を記憶部５２から取得する。
【０１００】
具体的には、たとえば、モデル情報の示す種類の組み合わせに合ったデータが同じメッセージに格納されて車載ネットワーク１２において伝送される場合、データ取得部５３は、記憶部５２に保存された当該同じメッセージから当該２種類のデータを取得する。
【０１０１】
データ取得部５３は、たとえば、当該２種類のデータを含むメッセージがメッセージ取得部５５によって記憶部５２に新たに保存されると、新たに保存されたメッセージから当該２種類のデータを取得し、取得した２種類のデータの組、およびモデル情報の示す種類の組み合わせを検知部５４へ出力する。
【０１０２】
［２種類のデータが異なる送信メッセージにそれぞれ含まれる場合］
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いて行われる同期処理のタイミングを説明するための図である。なお、図５において、横軸は時間を示す。
【０１０３】
図５を参照して、データ取得部５３は、たとえば、取得した複数のモデル情報に基づいて、異なる送信メッセージにそれぞれ含まれる２種類のデータの組を記憶部５２から取得する。
【０１０４】
具体的には、たとえば、モデル情報の示す種類の組み合わせに合ったデータが別個のメッセージに格納されて車載ネットワーク１２において伝送される場合、データ取得部５３は、以下の処理を行う。
【０１０５】
すなわち、データ取得部５３は、たとえば、一方の種類のデータＤＪを含む複数のメッセージＭＪ、および他方の種類のデータＤＫを含む複数のメッセージＭＫを記憶部５２から取得する。ここで、メッセージＭＪおよびメッセージＭＫは、たとえば車載ネットワーク１２において同じ周期で伝送されるメッセージである。
【０１０６】
データ取得部５３は、たとえば、一方の種類のデータＤＪを含む複数のメッセージＭＪに付されたタイムスタンプに基づいて、一方の種類のデータＤＪに受信時刻を対応付ける。
【０１０７】
具体的には、データ取得部５３は、データＤＪの一例であるデータＤＪ１，ＤＪ２に、それぞれ受信時刻ｔｊ１，ｔｊ２を対応付ける。
【０１０８】
同様に、データ取得部５３は、たとえば、他方の種類のデータＤＫを含む複数のメッセージＭＫに付されたタイムスタンプに基づいて、他方の種類のデータＤＫに受信時刻を対応付ける。
【０１０９】
具体的には、データ取得部５３は、データＤＫの一例であるデータＤＫ１，ＤＫ２に、それぞれ受信時刻ｔｋ１，ｔｋ２を対応付ける。
【０１１０】
データ取得部５３は、たとえば、一方の種類のデータＤＪに対応付けた受信時刻、および他方の種類のデータＤＫに対応付けた受信時刻に基づいて他方の種類のデータＤＫをリサ

ンプリングすることにより、一方の種類のデータＤＪの受信時刻と他方の種類のデータＤＫの受信時刻とを同期させる同期処理を行う。

【０１１１】

データ取得部５３は、たとえば、一方の種類のデータＤＪを含むメッセージＭＪがメッセージ取得部５５によって記憶部５２に新たに保存されると、同期処理を行う。

【０１１２】

具体的には、データ取得部５３は、たとえば、受信時刻ｔｊ２に対応するメッセージＭＪがメッセージ取得部５５によって記憶部５２に新たに保存されると、データＤＫ１，ＤＫ２等を含むデータＤＫをリサンプリングすることにより、受信時刻ｔｊ１，ｔｊ２にそれぞれ対応するリサンプルデータＲＤＫ１，ＲＤＫ２を生成する。

【０１１３】

データ取得部５３は、たとえば、同期処理が完了すると、同期させた２種類のデータから最新の２種類のデータの組を取得し、取得した２種類のデータの組、およびモデル情報の示す種類の組み合わせを検知部５４へ出力する。

【０１１４】

具体的には、データ取得部５３は、たとえば、データＤＪ２およびリサンプルデータＲＤＫ２の組、ならびにモデル情報の示す種類の組み合わせを検知部５４へ出力する。

【０１１５】

なお、データ取得部５３が同期処理を行うタイミングは、たとえば、他方の種類のデータＤＫを含むメッセージＭＫがメッセージ取得部５５によって記憶部５２に新たに保存されるタイミングであってもよい。

【０１１６】

具体的には、データ取得部５３は、たとえば、受信時刻ｔｋ２に対応するメッセージＭＫがメッセージ取得部５５によって記憶部５２に新たに保存されると、データＤＫ１，ＤＫ２等を含むデータＤＫをリサンプリングすることにより、受信時刻ｔｊ１に対応するリサンプルデータＲＤＫ１を生成する。

【０１１７】

そして、データ取得部５３は、たとえば、データＤＪ１およびリサンプルデータＲＤＫ１の組、ならびにモデル情報の示す種類の組み合わせを検知部５４へ出力する。

【０１１８】

また、データ取得部５３が同期処理を行うタイミングは、たとえば、一方の種類のデータを含むメッセージおよび他方の種類のデータを含むメッセージの両方がメッセージ取得部５５によって記憶部５２に新たに保存されるタイミングであってもよい。

【０１１９】

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において行われる同期処理のタイミングを説明するための図である。なお、図６において、横軸は時間を示す。

【０１２０】

図６を参照して、一方の種類のデータＤＰを含むメッセージＭＰ、および他方の種類のデータＤＱを含むメッセージＭＱは、たとえば車載ネットワーク１２において異なる周期で伝送されるメッセージである。

【０１２１】

データ取得部５３は、データＤＰの一例であるデータＤＰ１，ＤＰ２に、それぞれ受信時刻ｔｐ１，ｔｐ２を対応付ける。

【０１２２】

また、データ取得部５３は、データＤＱの一例であるデータＤＱ１，ＤＱ２，ＤＱ３，ＤＱ４に、それぞれ受信時刻ｔｑ１，ｔｑ２，ｔｑ３，ｔｑ４を対応付ける。

【０１２３】

データ取得部５３は、たとえば、メッセージＭＰ，ＭＱの両方がメッセージ取得部５５によって記憶部５２に新たに保存されると、同期処理を行う。

【０１２４】

具体的には、データ取得部５３は、たとえば、受信時刻ｔｐ１において、メッセージＭＰ，ＭＱの両方がメッセージ取得部５５によって記憶部５２に新たに保存されたと判断し、同期処理を行う。

【０１２５】

同様に、データ取得部５３は、たとえば、受信時刻ｔｐ２において、メッセージＭＰ，ＭＱの両方がメッセージ取得部５５によって記憶部５２に新たに保存されたと判断し、同期処理を行う。

【０１２６】

データ取得部５３は、たとえば、受信時刻ｔｐ２における同期処理では、データＤＱ１～ＤＱ４等を含むデータＤＱをリサンプリングすることにより、受信時刻ｔｐ１，ｔｐ２にそれぞれ対応するリサンプルデータＲＤＱ１，ＲＤＱ２を生成する。

【０１２７】

データ取得部５３は、たとえば、データＤＰ２およびリサンプルデータＲＤＱ２の組、ならびにモデル情報の示す種類の組み合わせを検知部５４へ出力する。

【０１２８】

なお、データ取得部５３は、受信時刻ｔｐ２における同期処理では、データＤＰ１，ＤＰ２等を含むデータＤＰをリサンプリングすることにより、受信時刻ｔｑ１～ｔｑ４にそれぞれ対応する、図示しないリサンプルデータＲＤＰ１～ＲＤＰ４を生成してもよい。

【０１２９】

この場合、データ取得部５３は、リサンプルデータＲＤＰ４およびデータＤＱ４の組、ならびにモデル情報の示す種類の組み合わせを検知部５４へ出力する。

【０１３０】

この際、データ取得部５３は、リサンプルデータＲＤＰ２およびデータＤＱ２の組、ならびにリサンプルデータＲＤＰ３およびデータＤＱ３の組も合わせて検知部５４へ出力してもよい。これにより、不正メッセージの検知に用いるデータ数を増やすことができる。

【０１３１】

図７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が行う不正メッセージの検知を説明するための図である。なお、図７の見方は、図４と同様である。

【０１３２】

図７を参照して、検知部５４は、データ取得部５３によって取得された組、および検出条件に基づいて、データ取得部５３によって取得された組に対応する不正メッセージを検知する。

【０１３３】

より詳細には、検知部５４は、データ取得部５３から２種類のデータの組、およびモデル情報の示す種類の組み合わせを受けると、記憶部５２における検出条件情報に含まれる複数のモデル情報を参照し、受けた組み合わせに対応する通常モデルＭ２を記憶部５２における対応のモデル情報から取得する。

【０１３４】

検知部５４は、データ取得部５３から受けた２種類のデータの組、および対応のモデル情報から取得した通常モデルＭ２に基づいて、当該組に対応する不正メッセージを検知する。

【０１３５】

具体的には、検知部５４は、たとえば、２種類のデータの組に基づく位置が位置Ｐｎである場合、位置Ｐｎが通常モデルＭ２の境界Ｂ２の内側に位置するので、当該２種類のデータを含む１つまたは２つのメッセージは正当メッセージであると判断する。

【０１３６】

一方、検知部５４は、たとえば、データ取得部５３から受けた２種類のデータの組に基づく位置が位置Ｐａである場合、位置Ｐａが通常モデルＭ２の境界Ｂ２の外側に位置するので、当該２種類のデータを含む１つまたは２つのメッセージは不正メッセージであると判断する。

【０１３７】

ここで、通常モデルＭ２は、作成時刻の同じ２種類のデータの複数の組に基づいて作成されている一方、位置Ｐｎ，Ｐａは、受信時刻の同じ２種類のデータの組に基づいている。

【０１３８】

車載ネットワーク１２ではメッセージの伝送が高速に行われるので、データの作成時刻およびデータの受信時刻が略同じであるとみなすことができる。これにより、通常モデルＭ２、および２種類のデータの組に基づく位置に基づいて不正メッセージの検知を行うことができる。なお、データの送信時刻も、データの作成時刻およびデータの受信時刻と略同じであるとみなすことができる。

【０１３９】

検知部５４は、不正メッセージを確認した場合、たとえば、以下の処理を行う。すなわち、検知部５４は、不正であると判断した１つまたは２つのメッセージのＩＤ、および対応の種類の組み合わせ等を記憶部５２に記録する。

【０１４０】

また、検知部５４は、バス１３において不正メッセージが伝送されていることを対象車両１内または対象車両１外における上位装置へ通信処理部５１経由で通知する。

【０１４１】

［効果］

図８および図９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効果を説明するための図である。なお、図８および図９の見方は、図４と同様である。

【０１４２】

図８に示す通常モデルＭ２は、図７に示す通常モデルＭ２と同様である。図９に示す通常モデルＭＲ２は、たとえば、相関関係のないデータＸおよびデータＹを用いて、通常モデルＭ２の作成手順と同様の作成手順に従って作成されたモデルである。

【０１４３】

位置Ｐａは、通常モデルＭ２を用いる場合、異常と判断されるのに対して、通常モデルＭＲ２を用いる場合、位置Ｐａが通常モデルＭＲ２の境界ＢＲ２の内側に位置するので、正常と判断される。

【０１４４】

これは、位置ＰａのデータＸの成分に対するデータＹの許容範囲が、図８における許容範囲Ｒ１より図９における許容範囲Ｒ２の方が大きいためである。

【０１４５】

したがって、通常モデルＭ２を用いてデータフィールドの監視を行う場合、攻撃者が対象車両１を不正制御するためのデータＹをメッセージに挿入したとしても、データＸとの相関関係によってデータＹの許容範囲がより狭くなるため、攻撃を正しく検知することが可能となる。

【０１４６】

また、攻撃者が対象車両１を不正制御するためのデータＸをメッセージに挿入した場合も、データＹとの相関関係によってデータＸの許容範囲がより狭くなるため、攻撃を同様に正しく検知することが可能となる。

【０１４７】

［通常モデルの変形例１］

再び図３を参照して、通常モデルは、所定の相関関係を有する２種類のデータの組に基づいて作成される構成であるとしたが、これに限定するものではなく、所定の相関関係を有するたとえば３種類のデータの組に基づいて作成される構成であってもよい。

【０１４８】

具体的には、通常モデルＭ３は、たとえば、所定の相関関係を有する３種類のデータの組に基づいて作成されている。

【０１４９】

より詳細には、たとえば、ある種類のデータと相関関係を有するデータである相関データが２種類ある場合、当該ある種類のデータと当該２種類の相関データとに基づいて１つの

通常モデルＭ３が作成されている。
【０１５０】
より具体的には、サーバは、たとえば、共通の複数の作成時刻におけるデータ１～データＮにおいて、データＳおよびデータＴに相関有りまたは強い相関有りと判断し、かつデータＳおよびデータＵに相関有りまたは強い相関有りと判断した場合、以下の処理を行う。
【０１５１】
すなわち、サーバは、データＴおよびデータＵ間の相関係数の大小に関わらず、データＳ，Ｔ，Ｕに基づいて通常モデルＭ３を作成する。ここで、Ｓ，Ｔ，Ｕは、互いに異なり、かつ１～Ｎのうちのいずれかの整数である。
【０１５２】
サーバは、たとえば、複数の通常モデルＭ３を作成し、作成した通常モデルＭ３ごとにモデル情報を作成する。モデル情報は、通常モデルＭ３、ならびに対応のデータＳ、データＴおよびデータＵの種類の組み合わせを示す。
【０１５３】
データＳおよびデータＴの種類の組み合わせ、ならびにデータＳおよびデータＵの種類の組み合わせは、たとえば、ヨーレートおよび舵角、ならびにヨーレートおよび車高である。
【０１５４】
サーバによって作成された複数のモデル情報は、たとえば、検出条件情報としてまとめられた後、対象車両１の製造時において記憶部５２に登録される。
【０１５５】
なお、検出条件情報には、通常モデルＭ３に基づくモデル情報だけが含まれる構成であってもよいし、通常モデルＭ３に基づくモデル情報、および通常モデルＭ２に基づくモデル情報が含まれる構成であってもよい。
【０１５６】
データ取得部５３は、記憶部５２から検出条件情報を取得し、取得した検出条件情報に含まれる複数のモデル情報を取得する。
【０１５７】
データ取得部５３は、モデル情報の示す組み合わせに合ったデータを含むメッセージがメッセージ取得部５５によって記憶部５２に新たに保存されると、以下の処理を行う。
【０１５８】
すなわち、データ取得部５３は、モデル情報に基づいて、同じ送信メッセージに含まれる３種類のデータの組を記憶部５２から取得し、取得した３種類のデータの組、およびモデル情報の示す種類の組み合わせを検知部５４へ出力する。
【０１５９】
また、データ取得部５３は、たとえば、モデル情報の示す組み合わせに合ったデータをそれぞれ含む複数のメッセージのいずれか１つがメッセージ取得部５５によって記憶部５２に新たに保存されると、以下の処理を行う。
【０１６０】
すなわち、データ取得部５３は、モデル情報に基づいて、異なる送信メッセージにそれぞれ含まれる３種類のデータの組を記憶部５２から取得し、取得した３種類のデータに対して同期処理を行う。
【０１６１】
データ取得部５３は、同期処理が完了すると、同期させた３種類のデータから最新の３種類のデータの組を取得し、取得した３種類のデータの組、およびモデル情報の示す種類の組み合わせを検知部５４へ出力する。
【０１６２】
検知部５４は、データ取得部５３から３種類のデータの組、およびモデル情報の示す種類の組み合わせを受けると、記憶部５２における検出条件情報に含まれる複数のモデル情報を参照し、受けた組み合わせに対応する通常モデルＭ３を記憶部５２における対応のモデル情報から取得する。

【０１６３】
検知部５４は、データ取得部５３から受けた３種類のデータの組、および対応のモデル情報から取得した通常モデルＭ３に基づいて、当該組に対応する不正メッセージを検知する。
【０１６４】
具体的には、通常モデルＭ３は３次元であるので、検知部５４は、データ取得部５３から受けた３種類のデータの組に基づく３次元空間での位置が、通常モデルＭ３の境界面の内部に存在する場合、当該３種類のデータを含む１つ、２つまたは３つのメッセージは正当メッセージであると判断する。
【０１６５】
一方、検知部５４は、データ取得部５３から受けた３種類のデータの組に基づく３次元空間での位置が、通常モデルＭ３の境界面の外部に存在する場合、当該３種類のデータを含む１つ、２つまたは３つのメッセージは不正メッセージであると判断する。
【０１６６】
通常モデルＭ３を用いる構成により、不正メッセージをより精度よく検知することができる。
【０１６７】
［通常モデルの変形例２］
図１０は、本発明の第１の実施の形態に係る通常モデルの変形例についての学習フェーズにおける作成処理を説明するための図である。
【０１６８】
図１０を参照して、通常モデルの変形例２では、検知部５４は、監視対象のセンサデータ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を検知する。
【０１６９】
この例では、監視対象センサデータとたとえばｑ種類のデータを含む相関データ群とに基づいて１つの通常モデルＭ４が作成されている。
【０１７０】
監視対象センサデータは、センサによって計測されたデータ（以下、センサデータとも称する。）であり、具体的には、車速、エンジン回転数およびヨーレート等の連続して変化するデータである。
【０１７１】
相関データ群に含まれるｑ種類のデータは、センサデータであってもよいし、予め定義された状態を表すデータであるステータスデータであってもよい。ここで、ステータスデータは、具体的には、たとえば対象車両１におけるギアおよびシートベルト等の操作部の状態を表す。
【０１７２】
監視対象センサデータと相関データ群に含まれるｑ種類のデータの各々とは、相関関係を有する。また、相関データ群に含まれるｑ種類のデータ間には、相関関係があってもよいし、なくてもよい。
【０１７３】
サーバは、たとえば、学習データセットに基づいて、ＬＡＳＳＯ（Ｌｅａｓｔ　Ａｂｓｏｌｕｔｅ　Ｓｈｒｉｎｋａｇｅ　ａｎｄ　Ｓｅｌｅｃｔｉｏｎ　Ｏｐｅｒａｔｏｒ）および回帰木等を用いて、通常モデルＭ４を学習させる。
【０１７４】
ここで、学習データセットは、複数の同じ時刻、具体的にはｔｍ１，ｔｍ２，ｔｍ３，ｔｍ４，ｔｍ５等にそれぞれ対応する監視対象センサデータおよび相関データ群を含む。
【０１７５】
より詳細には、サーバは、たとえば、同じ時刻に対応する相関データ群を通常モデルＭ４に入力したときに、対応の監視対象センサデータの値に近い推定値が出力されるように通常モデルＭ４を作成する。
【０１７６】

図１１は、本発明の第１の実施の形態に係る通常モデルの変形例についてのテストフェーズにおける検証処理を説明するための図である。

【０１７７】

図１１を参照して、通常モデルＭ４は、学習データセットと同様の、テストデータセットを用いて検証される。

【０１７８】

詳細には、サーバは、通常モデルＭ４を用いて推定誤差の分布を作成する。より詳細には、サーバは、テストデータセットの一部である時刻ｔｔ１における相関データ群を通常モデルＭ４に入力することにより、通常モデルＭ４から出力される推定値を取得する。

【０１７９】

そして、サーバは、たとえば、以下の式（１）を用いて推定誤差ｙｅｒｒを算出する。

【数１】

$$y_{err} = y_{obs} - y_{calc} \quad \cdots (1)$$

【０１８０】

ここで、ｙｏｂｓは、対応の監視対象センサデータの値、すなわち時刻ｔｔ１における監視対象センサデータの値である。また、ｙｃａｌｃは、通常モデルＭ４から出力された推定値である。

【０１８１】

サーバは、テストデータセットにおける、時刻ｔｔ１と異なる時刻における相関データ群および監視対象センサデータも同様に処理することにより、各時刻における推定誤差ｙｅｒｒを含む検証データを作成する。

【０１８２】

サーバは、検証データに基づいて、推定誤差ｙｅｒｒの分布を作成する。この分布は、推定誤差ｙｅｒｒの頻度を表す。この例では、当該分布は、単峰である。

【０１８３】

サーバは、作成した分布が単峰である場合、検証データに含まる各推定誤差ｙｅｒｒの平均値μおよび分散σ＾２を算出する。ここで、「ａ＾ｂ」は、ａのｂ乗を意味する。

【０１８４】

サーバは、たとえば、通常モデルＭ４、平均値μおよび分散σ＾２、ならびに監視対象センサデータおよび相関データ群におけるｑ種類のデータの種類の組み合わせを示すモデル情報Ｍｄ１を作成する。

【０１８５】

サーバによって作成されたモデル情報Ｍｄ１は、たとえば、対象車両１の製造時において検出条件情報として記憶部５２に登録される。

【０１８６】

再び図３を参照して、データ取得部５３は、記憶部５２から検出条件情報を取得し、取得した検出条件情報に含まれるモデル情報Ｍｄ１を取得する。

【０１８７】

データ取得部５３は、モデル情報Ｍｄ１の示す組み合わせに合ったデータを含むメッセージがメッセージ取得部５５によって記憶部５２に新たに保存されると、以下の処理を行う。

【０１８８】

すなわち、データ取得部５３は、モデル情報Ｍｄ１に基づいて、同じ送信メッセージに含まれる監視対象センサデータおよび相関データ群の組を記憶部５２から取得し、取得した組、およびモデル情報Ｍｄ１の示す種類の組み合わせを検知部５４へ出力する。

【０１８９】

また、データ取得部５３は、たとえば、モデル情報Ｍｄ１の示す組み合わせに合ったデータをそれぞれ含む複数のメッセージのいずれか１つがメッセージ取得部５５によって記憶

部５２に新たに保存されると、以下の処理を行う。

【０１９０】

すなわち、データ取得部５３は、モデル情報Ｍｄ１に基づいて、異なる送信メッセージにそれぞれ含まれる監視対象センサデータおよび相関データ群の組を記憶部５２から取得し、取得した監視対象センサデータおよび相関データ群に対して同期処理を行う。

【０１９１】

データ取得部５３は、同期処理が完了すると、同期させた監視対象センサデータおよび相関データ群から最新の監視対象センサデータおよび相関データ群の組を取得し、取得した組、およびモデル情報Ｍｄ１の示す種類の組み合わせを検知部５４へ出力する。

【０１９２】

図１２は、本発明の第１の実施の形態に係る通常モデルの変形例を用いた不正メッセージの検知処理を説明するための図である。

【０１９３】

図１２を参照して、検知部５４は、たとえば、データ取得部５３から時刻ｔｄ１における監視対象センサデータおよび相関データ群の組、およびモデル情報Ｍｄ１の示す種類の組み合わせを受けると、記憶部５２における検出条件情報に含まれる複数のモデル情報を参照し、受けた組み合わせに対応するモデル情報Ｍｄ１を記憶部５２から取得する。

【０１９４】

検知部５４は、たとえば、データ取得部５３によって取得された監視対象センサデータおよび相関データ群の組、ならびにモデル情報Ｍｄ１に含まれる通常モデルＭ４に基づいて、監視対象センサデータの推定誤差を算出する。

【０１９５】

より詳細には、検知部５４は、データ取得部５３から受けた相関データ群を、モデル情報Ｍｄ１に含まれる通常モデルＭ４に入力することにより、通常モデルＭ４から出力される推定値を取得する。

【０１９６】

そして、検知部５４は、取得した推定値および時刻ｔｄ１における監視対象センサデータの値を、それぞれｙｃａｌｃおよびｙｏｂｓとして上述の式（１）に代入することにより推定誤差ｙｅｒｒを算出する。

【０１９７】

検知部５４は、たとえば、算出した推定誤差ｙｅｒｒ、および通常モデルＭ４を用いて作成された推定誤差ｙｅｒｒの分布に基づいて、監視対象センサデータの正当性を評価し、評価結果に基づいて、監視対象センサデータが不正メッセージであるか否かを判断する。

【０１９８】

より詳細には、検知部５４は、たとえば、算出した推定誤差ｙｅｒｒ、ならびにモデル情報Ｍｄ１に含まれる平均値μおよび分散σ＾２を以下の式（２）に代入することによりスコアＳを算出する。このスコアＳは、マハラノビス距離に相当し、監視対象センサデータの正当性の評価値である。

【数２】

$$S = \log \frac{(y_{err} - \mu)^2}{\sigma^2} \quad \cdots (2)$$

【０１９９】

検知部５４は、たとえば、算出したスコアＳが所定のしきい値Ｔｈ１以上である場合、監視対象センサデータは不正メッセージであると判断する。

【０２００】

一方、検知部５４は、たとえば、算出したスコアＳが所定のしきい値Ｔｈ１より小さい場合、監視対象センサデータは正当メッセージであると判断する。

【０２０１】
なお、サーバが作成する推定誤差ｙｅｒｒの分布が単峰であるとしたが、これに限定するものではない。サーバが作成する推定誤差ｙｅｒｒの分布は、多峰であってもよい。
【０２０２】
この場合、サーバは、推定誤差ｙｅｒｒの分布を、たとえば、Ｋ個のガウス分布を重ね合わせた混合ガウス分布によって近似し、各ガウス分布の平均値μ１～μＫおよび分散σ１＾２～σＫ＾２、ならびに各ガウス分布の混合比Ｃ１～ＣＫを算出する。
【０２０３】
サーバは、たとえば、通常モデルＭ４、平均値μ１～μＫ、分散σ１＾２～σＫ＾２および混合比Ｃ１～ＣＫ、ならびに監視対象センサデータおよび相関データ群におけるｑ種類のデータの種類の組み合わせを示すモデル情報Ｍｄ１を作成する。
【０２０４】
この場合、検知部５４は、算出した推定誤差ｙｅｒｒ、ならびにモデル情報Ｍｄ１に含まれる平均値μ１～μＫ、分散σ１＾２～σＫ＾２および混合比Ｃ１～ＣＫを以下の式（３）に代入することによりスコアＳを算出する。
【数３】

$$S = -\log \sum_{k=1}^{K} C_k \cdot \frac{1}{\sqrt{2\pi\sigma_k^2}} \cdot \exp(B) \quad \cdots (3)$$

【０２０５】
ここで、式（３）におけるＢは、以下の式（４）により表される。
【数４】

$$B = -\frac{(y_{err} - \mu_k)^2}{2\sigma_k^2} \quad \cdots (4)$$

【０２０６】
［通常モデルの変形例３］
図１３は、本発明の第１の実施の形態に係る通常モデルの変形例についての学習フェーズにおける作成処理を説明するための図である。
【０２０７】
図１３を参照して、通常モデルの変形例３では、検知部５４は、監視対象のステータスデータ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を検知する。
【０２０８】
この例では、監視対象ステータスデータとたとえばｑ種類のデータを含む相関データ群とに基づいて１つの通常モデルＭ５が作成されている。
【０２０９】
監視対象ステータスデータは、ステータスデータであり、具体的には、ギアのシフトポジションおよびシートベルトの状態等の不連続に変化するデータである。
【０２１０】
相関データ群に含まれるｑ種類のデータは、センサデータであってもよいし、ステータスデータであってもよい。
【０２１１】
監視対象ステータスデータと相関データ群に含まれるｑ種類のデータの各々とは、相関関係を有する。また、相関データ群に含まれるｑ種類のデータ間には、相関関係があってもよいし、なくてもよい。

【０２１２】
サーバは、たとえば、学習データセットに基づいて、決定木およびＲａｎｄｏｍ　Ｆｏｒｅｓｔ等を用いて、通常モデルＭ５を学習させる。
【０２１３】
ここで、学習データセットは、複数の同じ時刻、具体的にはｔｍ１，ｔｍ２，ｔｍ３，ｔｍ４，ｔｍ５等にそれぞれ対応する監視対象ステータスデータおよび相関データ群を含む。
【０２１４】
より詳細には、サーバは、たとえば、同じ時刻に対応する相関データ群を通常モデルＭ５に入力したときに、対応の監視対象ステータスデータの値と一致する推定値が出力されるように通常モデルＭ５を作成する。
【０２１５】
サーバは、たとえば、通常モデルＭ５、ならびに監視対象ステータスデータおよび相関データ群におけるｑ種類のデータの種類の組み合わせを示すモデル情報Ｍｄ２を作成する。
【０２１６】
サーバによって作成されたモデル情報Ｍｄ２は、たとえば、対象車両１の製造時において検出条件情報として記憶部５２に登録される。
【０２１７】
再び図３を参照して、データ取得部５３は、記憶部５２から検出条件情報を取得し、取得した検出条件情報に含まれるモデル情報Ｍｄ２を取得する。
【０２１８】
データ取得部５３は、モデル情報Ｍｄ２の示す組み合わせに合ったデータを含むメッセージがメッセージ取得部５５によって記憶部５２に新たに保存されると、以下の処理を行う。
【０２１９】
すなわち、データ取得部５３は、モデル情報Ｍｄ２に基づいて、同じ送信メッセージに含まれる監視対象ステータスデータおよび相関データ群の組を記憶部５２から取得し、取得した組、およびモデル情報Ｍｄ２の示す種類の組み合わせを検知部５４へ出力する。
【０２２０】
また、データ取得部５３は、たとえば、モデル情報Ｍｄ２の示す組み合わせに合ったデータをそれぞれ含む複数のメッセージのいずれか１つがメッセージ取得部５５によって記憶部５２に新たに保存されると、以下の処理を行う。
【０２２１】
すなわち、データ取得部５３は、モデル情報Ｍｄ２に基づいて、異なる送信メッセージにそれぞれ含まれる監視対象ステータスデータおよび相関データ群の組を記憶部５２から取得し、取得した監視対象ステータスデータおよび相関データ群に対して同期処理を行う。
【０２２２】
データ取得部５３は、同期処理が完了すると、同期させた監視対象ステータスデータおよび相関データ群から最新の監視対象ステータスデータおよび相関データ群の組を取得し、取得した組、およびモデル情報Ｍｄ２の示す種類の組み合わせを検知部５４へ出力する。
【０２２３】
図１４は、本発明の第１の実施の形態に係る通常モデルの変形例を用いた不正メッセージの検知処理を説明するための図である。
【０２２４】
図１４を参照して、検知部５４は、たとえば、データ取得部５３から時刻ｔｄ１における監視対象ステータスデータおよび相関データ群の組、およびモデル情報Ｍｄ２の示す種類の組み合わせを受けると、記憶部５２における検出条件情報に含まれる複数のモデル情報を参照し、受けた組み合わせに対応するモデル情報Ｍｄ２を記憶部５２から取得する。
【０２２５】
検知部５４は、たとえば、データ取得部５３によって取得された相関データ群、およびモデル情報Ｍｄ２に含まれる通常モデルＭ５に基づいて、監視対象ステータスデータの値を推定する。

【０２２６】
より詳細には、検知部５４は、データ取得部５３から受けた相関データ群を、モデル情報Ｍｄ２に含まれる通常モデルＭ５に入力することにより、通常モデルＭ５から出力される監視対象ステータスデータの推定値を取得する。
【０２２７】
そして、検知部５４は、取得した推定値と監視対象ステータスデータとの比較結果に基づいて、監視対象ステータスデータが不正メッセージであるか否かを判断する。
【０２２８】
より詳細には、検知部５４は、たとえば、取得した推定値と時刻ｔｄ１における監視対象ステータスデータの値とを比較し、これらの値が一致しない場合、監視対象ステータスデータは不正メッセージであると判断する。
【０２２９】
一方、検知部５４は、たとえば、取得した推定値と時刻ｔｄ１における監視対象ステータスデータの値とが一致する場合、監視対象ステータスデータは正当メッセージであると判断する。
【０２３０】
［通常モデルの変形例４］
ゲートウェイ装置１０１は、データＳ，Ｔ，Ｕに基づく通常モデルＭ３を用いる構成であるとしたが、これに限定するものではない。
【０２３１】
たとえば、ある種類のデータと相関関係を有するデータである相関データが２種類ある場合、ある種類のデータと当該２種類の相関データとに基づいて２つの検出条件がそれぞれ作成されている。
【０２３２】
具体的には、サーバは、共通の複数の作成時刻におけるデータ１～データＮにおいて、データＳおよびデータＴに相関有りまたは強い相関有りと判断し、かつデータＳおよびデータＵに相関有りまたは強い相関有りと判断した場合、以下の処理を行う。
【０２３３】
すなわち、サーバは、データＴおよびデータＵ間の相関係数の大小に関わらず、データＳ，Ｔに基づいて通常モデルＭ２を作成するとともに、データＳ，Ｕに基づいて通常モデルＭ２を作成する。
【０２３４】
このような構成により、データＳ，Ｔ，Ｕに基づいて通常モデルＭ３を作成する構成とくらべて、通常モデルの作成における計算負荷を軽減することができる。
【０２３５】
［通常モデルの変形例５］
ゲートウェイ装置１０１は、データＳ，Ｔ，Ｕに基づく、１つの通常モデルＭ３または２つの通常モデルＭ２を用いる構成であるとしたが、これに限定するものではない。
【０２３６】
より詳細には、たとえば、多次元のデータの組は、特許文献２（特開２０１６－５７４３８号公報）に記載の主成分分析を用いて、より低次元のデータの組に変換することが可能である。
【０２３７】
具体的には、サーバは、たとえば、３種類のデータの組を、主成分分析を用いて２種類のデータの組に変換し、変換後の組に基づいて通常モデルＭ２を作成する。
【０２３８】
ゲートウェイ装置１０１における記憶部５２には、３種類のデータの組を２種類のデータの組に変換するための固有ベクトル、サーバによって作成された通常モデルＭ２、ならびに対応のデータＳ、データＴおよびデータＵの種類の組み合わせを示すモデル情報が登録される。

【０２３９】
検知部５４は、データ取得部５３から３種類のデータの組、およびモデル情報の示す種類の組み合わせを受けると、記憶部５２におけるモデル情報を参照し、受けた組み合わせに対応する通常モデルＭ２および固有ベクトルを記憶部５２における対応のモデル情報から取得する。
【０２４０】
検知部５４は、取得した固有ベクトルを用いて、データ取得部５３から受けた３種類のデータの組を２種類のデータの組に変換し、変換後の組および通常モデルＭ２に基づいて、当該３種類のデータを含む１つ、２つまたは３つのメッセージが不正メッセージであるか否かを判断する。
【０２４１】
［動作の流れ］
車載通信システム３０１における各装置は、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、以下のシーケンス図または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図示しない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。
【０２４２】
図１５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メッセージを受信する際の動作手順を定めたフローチャートである。
【０２４３】
図１５を参照して、モデル情報が、通常モデルＭ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示す状況を想定する。
【０２４４】
まず、ゲートウェイ装置１０１は、たとえば制御装置１２２からメッセージを受信するまで待機する（ステップＳ１０２でＮＯ）。
【０２４５】
そして、ゲートウェイ装置１０１は、制御装置１２２からメッセージを受信すると（ステップＳ１０２でＹＥＳ）、受信したメッセージに監視対象の種類のデータが含まれるか否かを確認する（ステップＳ１０４）。
【０２４６】
次に、ゲートウェイ装置１０１は、受信したメッセージに監視対象の種類のデータが含まれる場合（ステップＳ１０４でＹＥＳ）、受信したメッセージを記憶部５２に保存する（ステップＳ１０６）。この際、ゲートウェイ装置１０１は、メッセージにタイムスタンプを付す。
【０２４７】
次に、ゲートウェイ装置１０１は、受信したメッセージを記憶部５２に保存するか（ステップＳ１０６）、または受信したメッセージに監視対象の種類のデータが含まれない場合（ステップＳ１０４でＮＯ）、受信したメッセージの中継処理を行った後、制御装置１２２から新たなメッセージを受信するまで待機する（ステップＳ１０２でＮＯ）。
【０２４８】
図１６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、受信したメッセージを記憶部に保存した際の動作手順を定めたフローチャートである。
【０２４９】
図１６を参照して、モデル情報が、通常モデルＭ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示す状況を想定する。
【０２５０】
まず、ゲートウェイ装置１０１は、メッセージが記憶部５２に保存されるまで待機する（ステップＳ２０２でＮＯ）。
【０２５１】

そして、ゲートウェイ装置１０１は、メッセージが記憶部５２に保存されると（ステップＳ２０２でＹＥＳ）、モデル情報の示す２種類の組み合わせに合ったデータが当該メッセージすなわち同じメッセージに格納されているか否かを確認する（ステップＳ２０４）。

【０２５２】

次に、ゲートウェイ装置１０１は、モデル情報の示す２種類の組み合わせに合ったデータが同じメッセージに含まれない場合、すなわち別個のメッセージに分かれて含まれる場合（ステップＳ２０４でＮＯ）、モデル情報の示す２種類のデータに対して同期処理を行う（ステップＳ２０６）。

【０２５３】

次に、ゲートウェイ装置１０１は、当該メッセージからモデル情報の示す２種類のデータの組を取得するか、または同期処理を行った２種類のデータからモデル情報の示す２種類のデータの最新の組を取得する（ステップＳ２０８）。

【０２５４】

次に、ゲートウェイ装置１０１は、取得した２種類のデータの組に対応する通常モデルＭ２を記憶部５２から取得する（ステップＳ２１０）。

【０２５５】

次に、ゲートウェイ装置１０１は、取得した２種類のデータの組に基づく位置が、通常モデルＭ２の境界Ｂ２の内側に位置するか否かを確認する（ステップＳ２１２）。

【０２５６】

ゲートウェイ装置１０１は、取得した２種類のデータの組に基づく位置が境界Ｂ２の内側に位置する場合（ステップＳ２１２でＹＥＳ）、当該２種類のデータを含む１つまたは２つのメッセージは正当メッセージであると判断する（ステップＳ２１４）。

【０２５７】

一方、ゲートウェイ装置１０１は、取得した２種類のデータの組に基づく位置が境界Ｂ２の外側に位置する場合（ステップＳ２１２でＮＯ）、当該２種類のデータを含む１つまたは２つのメッセージは不正メッセージであると判断する（ステップＳ２１６）。

【０２５８】

次に、ゲートウェイ装置１０１は、新たなメッセージが記憶部５２に保存されるまで待機する（ステップＳ２０２でＮＯ）。

【０２５９】

なお、上記動作の流れでは、モデル情報が、通常モデルＭ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示す状況を想定したが、これに限定するものではない。モデル情報が、たとえば、通常モデルＭ３、ならびに対応のデータＳ、データＴおよびデータＵの種類の組み合わせを示してもよい。この場合、ゲートウェイ装置１０１は、上記ステップＳ２０８において、３種類のデータの組を取得し、上記ステップＳ２１０において、対応の通常モデルＭ３を記憶部５２から取得する。

【０２６０】

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では、メッセージ取得部５５は、車載ネットワーク１２における複数の送信メッセージ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。メッセージ取得部５５は、車載ネットワーク１２における１つの送信メッセージを取得する構成であってもよい。たとえば、モデル情報の示す２種類の組み合わせに合ったデータが当該１つの送信メッセージに含まれる場合、送信メッセージが不正メッセージであるか否かを判断することが可能である。

【０２６１】

また、本発明の第１の実施の形態に係る車載通信システムでは、ゲートウェイ装置１０１が、車載ネットワーク１２における不正メッセージ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において、ゲートウェイ装置１０１とは別の検知装置が、車載ネットワーク１２における不正メッセージを検知する構成であってもよい。

【０２６２】

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では、データ取得部５３は、同じ受信時刻に対応する２種類のデータの組および３種類のデータの組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。データ取得部５３は、同じ受信時刻に対応するＭ種類のデータの組を取得する構成であってもよい。ここで、Ｍは４以上の整数である。この場合、通常モデルは、Ｍ種類のデータに基づいて作成される。

【０２６３】

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では、データ取得部５３は、同じ受信時刻に対応する複数種類のデータの組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。データ取得部５３は、受信時刻に限らず、同じ送信時刻または同じ作成時刻等に対応する複数種類のデータの組を取得する構成であってもよい。具体的には、たとえば、制御装置１２２がデータの作成時刻またはメッセージの送信時刻をメッセージに格納して送信する場合、データ取得部５３は、同じ送信時刻または同じ作成時刻に対応する複数種類のデータの組を取得することが可能である。

【０２６４】

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では、検知部５４は、制御装置１２２間でやり取りされるメッセージを不正メッセージの検知対象と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、制御装置１２２および車載通信機１１１間でやり取りされるメッセージ、ならびに車載通信機１１１間でやり取りされるメッセージを不正メッセージの検知対象とする構成であってもよい。

【０２６５】

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では、通常モデルは、所定の相関関係を有する複数種類のデータの組に基づいて作成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。通常モデルは、所定の相関関係を有さない複数種類のデータの組に基づいて作成される構成であってもよい。

【０２６６】

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では、データ取得部５３は、メッセージ取得部５５によって記憶部５２に保存された各送信メッセージから複数種類のデータを取得し、取得したデータをリサンプリング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、各送信メッセージの受信時刻が近い場合、データ取得部５３は、メッセージ取得部５５から各送信メッセージを直接受けて、受けた各送信メッセージから複数種類のデータを取得し、取得したデータをリサンプリングせずに検知に用いる構成であってもよい。

【０２６７】

ところで、特許文献１には、車載ネットワークに限定して接続される第１のＥＣＵおよび第２のＥＣＵがメッセージ認証に用いる第１の暗号鍵と、車載ネットワークおよび車外ネットワークの両方に接続される第３のＥＣＵが用いる第２の暗号鍵とが異なることにより、車外ネットワークに接続されない第１のＥＣＵおよび第２のＥＣＵに対する車外ネットワークからのサイバー攻撃を防ぐ構成が開示されている。

【０２６８】

しかしながら、メッセージ認証を用いるセキュリティ対策では、プロトコルの脆弱性を突いた攻撃、第１の暗号鍵の不正入手による攻撃、および暗号アルゴリズムの陳腐化を突いた攻撃等により、当該セキュリティ対策が無効化されることがある。

【０２６９】

このような攻撃を受けた場合において、攻撃者が車載ネットワークに侵入したことを正しく検知するための技術が求められる。

【０２７０】

これに対して、本発明の第１の実施の形態に係るゲートウェイ装置は、対象車両１に搭載される車載ネットワーク１２における不正メッセージを検知する。メッセージ取得部５５は、車載ネットワーク１２における１または複数の送信メッセージを取得する。データ取得部５３は、メッセージ取得部５５によって取得された送信メッセージに含まれる、同じ

時刻に対応する複数種類のデータの組を取得する。記憶部５２は、予め作成された、複数の時刻にそれぞれ対応する複数の組に基づく検出条件を記憶する。そして、検知部５４は、データ取得部５３によって取得された組、および検出条件に基づいて不正メッセージを検知する。

【０２７１】

たとえば、複数種類のデータ間に何らかの関係がある場合、当該関係を用いて、あるデータから他のデータがとり得る値の範囲を算出することができる。上記のような構成により、たとえば、上記組におけるあるデータから当該組における他のデータがとり得る値の範囲を検出条件に基づいて算出することができるので、当該他のデータの正当性を正しく判断することができる。これにより、不正と判断したデータを含むメッセージを不正メッセージとして検知することができる。したがって、車載ネットワークにおける不正メッセージを正しく検知することができる。

【０２７２】

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では、検出条件は、所定の相関関係を有する複数種類のデータの組に基づいて作成されている。

【０２７３】

このように、データ間においてある程度の関係が存在する複数種類のデータの組に基づいて検出条件が作成される構成により、組におけるあるデータから当該組における他のデータがとり得る値の範囲をより狭めることが可能な検出条件を作成することができる。これにより、当該他のデータの正当性をより正しく判断することができる。すなわち、適切な検出条件を作成することができる。

【０２７４】

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では、ある種類のデータと相関関係を有するデータである相関データが複数種類ある場合、当該ある種類のデータと当該複数種類の相関データとに基づいて１つの検出条件が作成されている。

【０２７５】

このような構成により、たとえば、攻撃者が、ある種類のデータおよび複数種類の相関データのうちの一部のデータを改変した場合においても、改変したデータと残りのデータとの関係に基づいて、上記組のデータの異常を判断することができる。すなわち、攻撃者は、不正侵入するためには、ある種類のデータおよび複数種類の相関データの全部を改変しなければならないので、車載ネットワーク１２に対する不正侵入を困難にすることができる。これにより、車載ネットワーク１２におけるセキュリティを向上させることができる。

【０２７６】

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では、検知部５４は、データ取得部５３によって取得されたある種類のデータおよび複数種類の相関データ、ならびに検出条件に基づいて、ある種類のデータの推定誤差を算出する。そして、検知部５４は、算出した推定誤差、および検出条件を用いて作成された推定誤差の分布に基づいて、ある種類のデータの正当性を評価し、評価結果に基づいて、ある種類のデータが不正メッセージであるか否かを判断する。

【０２７７】

このような構成により、たとえば、ある種類のデータが、センサによって計測された値のように連続して変化する値である場合において、ある種類のデータが正しい値を有する可能性をより正しく評価することができるので、ある種類のデータの正当性をより正しく判断することができる。

【０２７８】

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では、ある種類のデータは、状態を表すデータである。検知部５４は、データ取得部５３によって取得された複数種類の相関データ、および検出条件に基づいて、ある種類のデータの値を推定し、推定した値とある種類のデータとの比較結果に基づいて、ある種類のデータが不正メッセージであるか否かを判断する。

【０２７９】
このような構成により、たとえば、ある種類のデータが、ギアのシフトポジションまたはシートベルトの状態のように不連続に変化する値である場合において、ある種類のデータが示すべき値をより正しく推定することができるので、ある種類のデータの正当性をより正しく判断することができる。
【０２８０】
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では、ある種類のデータと相関関係を有するデータである相関データが複数種類ある場合、当該ある種類のデータと当該複数種類の相関データとに基づいて複数の検出条件がそれぞれ作成されている。
【０２８１】
このような構成により、車載ネットワーク１２に対する不正侵入を困難にするとともに、検出条件の算出における計算負荷を軽減することができる。
【０２８２】
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では、データ取得部５３は、異なる送信メッセージにそれぞれ含まれる複数種類のデータの組を取得する。
【０２８３】
受信時刻、送信時刻または作成時刻等が異なる複数種類のデータは、異なる送信メッセージにそれぞれ含まれることが多い。上記のような構成により、時刻によって検知対象のデータの種類が制限されることを防ぐことができる。
【０２８４】
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では、メッセージ取得部５５は、取得した複数の送信メッセージを記憶部５２に保存する。そして、データ取得部５３は、記憶部５２に保存された各送信メッセージから上記組を取得する。
【０２８５】
このような構成により、たとえば、記憶部５２に保存された複数の送信メッセージにおけるデータをリサンプリングすることができるので、複数種類のデータの時刻を合わせることができる。これにより、同じ時刻に対応する複数種類のデータの組を容易に取得することができる。
【０２８６】
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。
【０２８７】
＜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、通常モデルを更新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。
【０２８８】
［課題］
図１７は、本発明の第２の実施の形態に係るゲートウェイ装置における誤検知の一例を説明するための図である。なお、図１７の見方は、図４と同様である。
【０２８９】
図１７を参照して、通常モデルＭ２は、図４に示す、共通の複数の作成時刻におけるデータＸおよびデータＹの組（以下、母集団とも称する。）に基づくモデルである。この母集団は、対象車両１の開発時において、偏りがより小さくなるように取得されたデータとする。したがって、この母集団は、真の母集団に近い。
【０２９０】
たとえば、対象車両１の開発時に取得されたデータが偏っている場合、偏った母集団に基づく通常モデルＭＥ２が作成される。
【０２９１】
この通常モデルＭＥ２を用いて不正メッセージの検知を行う場合、位置Ｐｓ１，Ｐｓ２は

通常モデルＭＥ２の境界ＢＥ２の外側に位置するので、位置Ｐｓ１のデータＸまたはデータＹを含むメッセージ、および位置Ｐｓ２のデータＸまたはデータＹを含むメッセージは不正メッセージであると判断される。

【０２９２】

しかしながら、位置Ｐｓ１は、より正しい通常モデルＭ２の境界Ｂ２の内側に位置しているので、通常モデルＭＥ２を用いた場合において、位置Ｐｓ１のデータＸまたはデータＹを含むメッセージを不正メッセージであると判断することは誤検知である。

【０２９３】

予め作成された通常モデルＭＥ２の母集団が偏っている場合においても、より正しい通常モデルを利用可能にするための技術が求められる。

【０２９４】

［構成および基本動作］

図１８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ゲートウェイ装置の構成を示す図である。

【０２９５】

図１８を参照して、ゲートウェイ装置（検知装置）１０２は、通信処理部５１と、記憶部５２と、データ取得部５３と、検知部５４と、メッセージ取得部５５と、更新部５６とを備える。

【０２９６】

ゲートウェイ装置１０２における通信処理部５１、記憶部５２、データ取得部５３、検知部５４およびメッセージ取得部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、記憶部５２、データ取得部５３、検知部５４およびメッセージ取得部５５とそれぞれ同様である。

【０２９７】

図１９は、本発明の第２の実施の形態に係るゲートウェイ装置における更新部が行う通常モデルの更新を説明するための図である。なお、図１９の見方は、図４と同様である。

【０２９８】

図１８および図１９を参照して、通常モデルＭＥ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示すモデル情報を含む検出条件情報が記憶部５２に登録されている状況を想定する。

【０２９９】

データ取得部５３は、記憶部５２から検出条件情報を取得し、取得した検出条件情報に含まれる複数のモデル情報を取得する。

【０３００】

データ取得部５３は、たとえば、取得したモデル情報に基づいて２種類のデータの組を記憶部５２から取得する。

【０３０１】

ここでは、データＸおよびデータＹの組が同じ送信メッセージに含まれる状況を想定する。データ取得部５３は、たとえば、上記送信メッセージがメッセージ取得部５５によって記憶部５２に新たに保存されると、モデル情報の示す組み合わせに基づいて、データＸおよびデータＹの組を上記送信メッセージから取得する。

【０３０２】

データ取得部５３は、取得したデータＸおよびデータＹの組、およびモデル情報の示す種類の組み合わせを検知部５４および更新部５６へ出力する。

【０３０３】

更新部５６は、たとえば、データ取得部５３によって取得された組に基づいて検出条件を更新する。

【０３０４】

より詳細には、たとえば、ゲートウェイ装置１０２では、通常モデルを更新すべき更新期間がユーザによって定められており、更新部５６は、更新期間において通常モデルを更新

する。
【０３０５】
具体的には、更新部５６は、データ取得部５３からデータＸおよびデータＹの組、およびモデル情報の示す種類の組み合わせを受けると、記憶部５２における検出条件情報に含まれる複数のモデル情報を参照し、受けた組み合わせに対応する通常モデルＭＥ２を記憶部５２における対応のモデル情報から取得する。
【０３０６】
そして、更新部５６は、更新期間である場合、所定のアルゴリズムに従って、取得した通常モデルＭＥ２に基づいて、許容範囲を示す境界ＡＥ２を設定する。境界ＡＥ２は、通常モデルＭＥ２の境界ＢＥ２の外側に位置する。
【０３０７】
更新部５６は、データＸおよびデータＹの組に基づく位置が、位置Ｐｓ２のように境界ＡＥ２の外側に存在する場合、通常モデルＭＥ２を更新しない。
【０３０８】
一方、更新部５６は、データＸおよびデータＹの組に基づく位置が、位置Ｐｓ１のように境界ＡＥ２の内側に存在する場合、通常モデルＭＥ２を更新する。
【０３０９】
図２０は、本発明の第２の実施の形態に係るゲートウェイ装置における更新部が更新した通常モデルを説明するための図である。なお、図２０の見方は、図４と同様である。
【０３１０】
図１８および図２０を参照して、更新部５６は、たとえば、位置Ｐｓ１のデータＸおよびデータＹの組に基づいて、通常モデルＭＥ２を更新することにより通常モデルＭＦ２を作成する。境界ＡＦ２は、通常モデルＭＦ２に応じた境界であり、通常モデルＭＦ２の境界ＢＦ２の外側に位置する。
【０３１１】
データ取得部５３は、記憶部５２に保存された、通常モデルＭＥ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示すモデル情報を、通常モデルＭＦ２、ならびに対応のデータＸおよびデータＹの種類の組み合わせを示すモデル情報に更新する。
【０３１２】
位置Ｐｓ１は、更新後の通常モデルＭＦ２の境界ＢＦ２の内側に位置しているので、更新後の通常モデルＭＦ２を用いる場合、位置Ｐｓ１のデータＸまたはデータＹを含むメッセージを正当メッセージであると正しく判断することができる。
【０３１３】
また、更新部５６が、更新期間において通常モデルＭＦ２をさらに更新することにより、真の母集団に基づく通常モデルにより近づけることができる。
【０３１４】
なお、本発明の第２の実施の形態に係るゲートウェイ装置では、更新部５６は、２種類のデータの組に基づいて検出条件を更新する構成であるとしたが、これに限定するものではない。更新部５６は、３種類以上のデータの組に基づいて検出条件を更新する構成であってもよい。
【０３１５】
その他の構成および動作は第１の実施の形態に係るゲートウェイ装置と同様であるため、ここでは詳細な説明を繰り返さない。
【０３１６】
以上のように、本発明の第２の実施の形態に係るゲートウェイ装置では、更新部５６はデータ取得部５３によって取得された組に基づいて検出条件を更新する。
【０３１７】
このような構成により、たとえば、検出条件の算出に用いた組が母集団として不完全であっても、新たに取得した組を母集団に含めることができるので、母集団の完成度をより高めることができる。これにより、より適切な検出条件に更新することができる。

【０３１８】
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。
【０３１９】
＜第３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、メッセージの送信間隔に基づく不正メッセージの検知を組み込んだ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。
【０３２０】
［構成および基本動作］
図２１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ゲートウェイ装置の構成を示す図である。
【０３２１】
図２１を参照して、ゲートウェイ装置（検知装置）１０３は、通信処理部５１と、記憶部５２と、データ取得部５３と、メッセージ取得部５５と、監視部５７と、分布取得部５８と、検知部６４とを備える。
【０３２２】
ゲートウェイ装置１０３における通信処理部５１、記憶部５２、データ取得部５３およびメッセージ取得部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、記憶部５２、データ取得部５３およびメッセージ取得部５５とそれぞれ同様である。
【０３２３】
図２２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監視対象の周期メッセージの送信間隔の時間変化の一例を示す図である。なお、図２２において、縦軸は送信間隔を示し、横軸は時間を示す。
【０３２４】
図２２を参照して、送信間隔は、たとえば、ある監視対象の周期メッセージ（以下、対象メッセージとも称する。）がバス１３において伝送されるタイミングの間隔である。
【０３２５】
図２２に示すように、対象メッセージの送信間隔は一定でなく、ばらついている。これは、対象メッセージが伝送される際に調停が行われたり、クロックのずれによる内部処理の遅延ばらつきが発生したりするからである。
【０３２６】
ここで、調停について説明する。メッセージには、たとえば、ＩＤに応じて優先度が割り当てられている。たとえば、複数のメッセージの送信タイミングが重なる場合、車載ネットワーク１２では、優先度の高いメッセージを、優先度の低いメッセージより優先的にバス１３を伝送させる調停が行われる。このような調停により、送信間隔のばらつきが発生する。
【０３２７】
図２３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対象メッセージの送信間隔の度数分布の一例を示す図である。なお、図２３において、縦軸は度数を示し、横軸は送信間隔を示す。
【０３２８】
図２３を参照して、送信間隔の度数分布は、Ｃｔミリ秒を中心としてほぼ対称である。送信間隔の度数分布は、たとえば所定のモデル関数Ｆｕｎｃ１により近似することが可能である。
【０３２９】
再び図２１を参照して、監視部５７は、たとえば、車載ネットワーク１２における送信メッセージを監視する。より詳細には、監視部５７は、たとえば、通信処理部５１におけるメッセージの中継処理を監視し、監視結果に基づいて対象メッセージの送信間隔を測定する。

【０３３０】
具体的には、たとえば、監視部５７には、対象メッセージを示すＩＤ（以下、登録ＩＤとも称する。）が１つ登録されている。なお、監視部５７には、複数の登録ＩＤが登録されてもよい。
【０３３１】
監視部５７は、たとえば、通信処理部５１がメッセージを受信すると、通信処理部５１によって受信されたメッセージに含まれるＩＤを確認する。監視部５７は、確認したＩＤが登録ＩＤと一致する場合、通信処理部５１によって受信されたメッセージすなわち対象メッセージの受信時刻ｔ１をたとえば測定基準として保持する。
【０３３２】
そして、監視部５７は、通信処理部５１において登録ＩＤを含む新たな対象メッセージが受信されると、新たに受信された対象メッセージの受信時刻ｔ２を保持するとともに、以下の処理を行う。
【０３３３】
すなわち、監視部５７は、受信時刻ｔ２から受信時刻ｔ１を差し引くことにより、対象メッセージの送信間隔を算出し、算出した送信間隔および登録ＩＤを検知部６４へ出力する。
【０３３４】
分布取得部５８は、たとえば、送信メッセージの送信間隔の分布を取得する。詳細には、分布取得部５８は、たとえば、他の装置、具体的にはサーバによって予め作成された送信間隔の分布を示す分布情報を取得する。
【０３３５】
より詳細には、サーバは、たとえば、対象メッセージの送信間隔を複数取得する。この送信間隔は、たとえば、対象車両１と同じ種類のテスト車両において測定される。なお、サーバは、対象車両１において測定された送信間隔を取得してもよい。
【０３３６】
サーバは、たとえば、モデル関数Ｆｕｎｃ１として、以下の式（５）に示す、変数をｘとする正規分布の確率密度関数（以下、正規分布関数とも称する。）ｐを用いる。
【数５】

$$p(x|\bar{x},\sigma^2)=\frac{1}{\sqrt{2\pi\sigma^2}}exp\left\{-\frac{(x-\overline{x})^2}{2\sigma^2}\right\} \quad \cdots (5)$$

【０３３７】
ここで、ｘバーおよびσ＾２は、パラメータであり、それぞれ複数の送信間隔の平均値および分散である。ｘバーおよびσ＾２は、それぞれ、以下の式（６）および（７）により算出される。
【数６】

$$\bar{x}=\frac{1}{t}\sum_{i=1}^{t}x_i \quad \cdots (6)$$

【数７】

$$\sigma^2 = \frac{1}{t}\sum_{i=1}^{t}(x_i - \bar{x})^2 \quad \cdots (7)$$

【０３３８】
ここで、ｔは、送信間隔のサンプル数である。ｘｉは、ｉ番目の送信間隔である。サーバは、たとえば、所定の頒布タイミングにおいて、ｘバーおよびσ＾２を含む分布情報を対象車両１へ送信する。
【０３３９】
分布取得部５８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を受信すると、受信した分布情報に基づいて、式（５）により示されるモデル関数Ｆｕｎｃ１を作成し、作成したモデル関数Ｆｕｎｃ１を検知部６４へ出力する。
【０３４０】
なお、ゲートウェイ装置１０１では、分布取得部５８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を受信して検知部６４へ出力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、ゲートウェイ装置１０１が不揮発性メモリを保持しており、分布取得部５８が、整備用端末装置によってポート１１２経由で分布情報が書き込まれた不揮発性メモリから分布情報を取得して検知部６４へ出力する構成であってもよい。
【０３４１】
図２４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検出例を示す図である。なお、図２４において、縦軸はスコアを示し、横軸は変数ｘを示す。
【０３４２】
図２４を参照して、検知部６４は、たとえば、監視部５７による監視結果および分布取得部５８によって取得された送信間隔の分布に基づいて不正メッセージを検知する。
【０３４３】
詳細には、検知部６４は、たとえば、監視部５７によって測定された送信間隔と、当該送信間隔の分布を示す分布情報と、所定のしきい値とに基づいて、送信メッセージを不正メッセージとすべきか否かについて判断する。ここでは、検知部６４には、しきい値ＴｈＢが登録されている。
【０３４４】
言い換えると、検知部６４は、たとえば、監視部５７によって測定された送信間隔の、当該送信間隔の分布における位置に基づいて不正メッセージを検知する。
【０３４５】
検知部６４は、分布取得部５８からモデル関数Ｆｕｎｃ１を受けると、受けたモデル関数Ｆｕｎｃ１を変形することによりスコア関数Ｓｃ１を作成する。より詳細には、検知部６４は、たとえば、－ｌｏｇ（Ｆｕｎｃ１）をスコア関数Ｓｃ１として作成する。ここで、「ｌｏｇ（ｃ）」は、ｃの常用対数を意味する。
【０３４６】
図２４では、スコア関数Ｓｃ１は、測定基準の時刻がｘ＝０になるように表されている。したがって、図２４に示す横軸は、送信間隔を示す。また、スコア関数Ｓｃ１は、変数ｘが平均値すなわちｘバーである場合に最小値を示す。
【０３４７】
検知部６４は、監視部５７から受けた送信間隔をスコア関数Ｓｃ１における変数ｘに代入することによりスコアを算出する。
【０３４８】

検知部６４は、算出したスコアがたとえばしきい値ＴｈＢ以下である場合、今回伝送された対象メッセージを不正メッセージとすべきでないと判断する、すなわち対象メッセージが正当メッセージ、または送信間隔が偽装されたメッセージ（以下、偽装メッセージとも称する。）であると判断する。具体的には、検知部６４は、図２４に示す送信間隔Ｔｃを監視部５７から受けた場合、今回伝送された対象メッセージＣが正当メッセージまたは偽装メッセージであると判断する。

【０３４９】

これは、たとえば、対象メッセージが正当メッセージまたは偽装メッセージである場合、調停および内部処理の遅延等によるばらつきを含めても、図２３に示す度数分布の中心の近傍に送信間隔が位置する可能性が高いからである。

【０３５０】

一方、検知部６４は、算出したスコアがしきい値ＴｈＢより大きい場合、今回伝送された対象メッセージが不正メッセージであると判断する。具体的には、検知部６４は、図２４に示す送信間隔Ｔａを監視部５７から受けた場合、今回伝送された対象メッセージＡが不正メッセージであると判断する。同様に、検知部６４は、送信間隔Ｔｂを監視部５７から受けた場合、今回伝送された対象メッセージＢが不正メッセージであると判断する。

【０３５１】

これは、たとえば、対象メッセージが不正メッセージである場合、当該対象メッセージが所定の取り決めに従って送信されていない可能性が高いからである。

【０３５２】

また、セキュリティのレベルを下げる場合、検知部６４に登録されたしきい値をＴｈＢより大きいＴｈＡに変更する。これにより、たとえば、送信間隔Ｔｂに対応する対象メッセージＢのように、検知部６４により不正メッセージと判断されたメッセージが、しきい値の変更後において正当メッセージまたは偽装メッセージと判断される。

【０３５３】

検知部６４は、監視部５７から受けた送信間隔に基づく判断結果を監視部５７へ通知する。

【０３５４】

監視部５７は、たとえば、正当メッセージまたは偽装メッセージと判断された送信メッセージの受信タイミングを送信間隔の測定基準として用いる。

【０３５５】

より詳細には、監視部５７は、検知部６４から通知された判断結果が、今回伝送された対象メッセージが正当メッセージまたは偽装メッセージであることを示す場合、受信時刻ｔ２を送信間隔の新たな測定基準として用いる。

【０３５６】

そして、監視部５７は、通信処理部５１において登録ＩＤを含む新たな対象メッセージが受信されると、新たに受信された対象メッセージの受信時刻ｔ３を保持するとともに、以下の処理を行う。

【０３５７】

すなわち、監視部５７は、受信時刻ｔ３から受信時刻ｔ２を差し引くことにより、対象メッセージの新たな送信間隔を算出し、算出した送信間隔を検知部６４へ出力する。

【０３５８】

一方、監視部５７は、検知部６４から通知された判断結果が、今回伝送された対象メッセージが不正メッセージであることを示す場合、受信時刻ｔ１を測定基準のまま維持する。

【０３５９】

そして、監視部５７は、通信処理部５１において登録ＩＤを含む新たな対象メッセージが受信されると、新たに受信された対象メッセージの受信時刻ｔ３を保持するとともに、以下の処理を行う。

【０３６０】

すなわち、監視部５７は、受信時刻ｔ３から受信時刻ｔ１を差し引くことにより、対象メッセージの新たな送信間隔を算出し、算出した送信間隔を検知部６４へ出力する。

【０３６１】
検知部６４は、たとえば、不正メッセージとすべきでないと判断した送信メッセージについては、データ取得部５３によって取得された組、および検出条件に基づいて、不正メッセージであるか否かについて判断する。
【０３６２】
より詳細には、検知部６４は、今回伝送された対象メッセージＣが正当メッセージまたは偽装メッセージであると判断した場合、監視部５７から受けた登録ＩＤをデータ取得部５３へ出力する。
【０３６３】
データ取得部５３は、検知部６４から登録ＩＤを受けると、記憶部５２に保存された複数のメッセージの中から、受けた登録ＩＤを有する最新のメッセージすなわち最新の対象メッセージを取得する。
【０３６４】
この例では、対象メッセージにおいて１つのデータが含まれる。データ取得部５３は、取得した最新の対象メッセージに含まれる１つのデータの種類（以下、対象種類とも称する。）を認識する。なお、対象メッセージにおいて、２つ以上のデータが含まれてもよい。
【０３６５】
データ取得部５３は、記憶部５２が保存する検出条件情報に含まれる複数のモデル情報を参照し、参照した複数のモデル情報の中から、認識した対象種類を示すモデル情報を記憶部５２から取得する。
【０３６６】
データ取得部５３は、取得したモデル情報に基づいて、対象種類と組み合わされるデータの種類（以下、相手方種類とも称する。）を特定する。
【０３６７】
データ取得部５３は、たとえば、対象種類のデータを含む複数の対象メッセージ、および相手方種類のデータを含む複数のメッセージを記憶部５２から取得し、取得した各メッセージに基づいて、対象種類のデータの受信時刻と相手方種類のデータの受信時刻とを同期させる同期処理を行う。
【０３６８】
データ取得部５３は、同期処理が完了すると、同期させた２種類のデータから最新の２種類のデータの組を取得し、取得した２種類のデータの組、およびモデル情報の示す種類の組み合わせを検知部６４へ出力する。
【０３６９】
検知部６４は、データ取得部５３から２種類のデータの組、およびモデル情報の示す種類の組み合わせを受けると、記憶部５２における検出条件情報に含まれる複数のモデル情報を参照し、受けた組み合わせに対応する通常モデルＭ２を記憶部５２における対応のモデル情報から取得する。
【０３７０】
検知部６４は、データ取得部５３から受けた２種類のデータの組に基づく位置、および取得した通常モデルＭ２に基づいて、対象メッセージが不正メッセージであるか否かについて判断する。
【０３７１】
具体的には、検知部６４は、図７に示すように、データ取得部５３から受けた２種類のデータの組に基づく位置が位置Ｐｎである場合、位置Ｐｎが通常モデルＭ２の境界Ｂ２の内側に位置するので、対象メッセージが正当メッセージであると判断する。
【０３７２】
一方、検知部６４は、データ取得部５３から受けた２種類のデータの組に基づく位置が位置Ｐａである場合、位置Ｐａが通常モデルＭ２の境界Ｂ２の外側に位置するので、対象メッセージが偽装メッセージすなわち不正メッセージであると判断する。
【０３７３】

検知部６４は、対象メッセージが不正メッセージであると判断した場合、たとえば、以下の処理を行う。すなわち、検知部６４は、登録ＩＤ、相手方種類のデータを含むメッセージのＩＤ、および対応の種類の組み合わせ等を記憶部５２に記録する。

【０３７４】

また、検知部６４は、バス１３において不正メッセージが伝送されていることを対象車両１内または対象車両１外における上位装置へ通信処理部５１経由で通知する。

【０３７５】

［動作の流れ］

図２５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対象メッセージを受信する際の動作手順を定めたフローチャートである。

【０３７６】

図２５を参照して、まず、ゲートウェイ装置１０３は、最初の対象メッセージを受信し、当該対象メッセージの受信時刻を測定基準として設定する（ステップＳ３０２）。

【０３７７】

次に、ゲートウェイ装置１０３は、対象メッセージを受信するまで待機する（ステップＳ３０４でＮＯ）。

【０３７８】

そして、ゲートウェイ装置１０３は、対象メッセージを受信すると（ステップＳ３０４でＹＥＳ）、受信した対象メッセージを不正メッセージとすべきか否かについて判断する判断処理を行う（ステップＳ３０６）。

【０３７９】

次に、ゲートウェイ装置１０３は、新たな対象メッセージを受信するまで待機する（ステップＳ３０６でＮＯ）。

【０３８０】

図２６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判断処理を行う際の動作手順を定めたフローチャートである。図２６は、図２５のステップＳ３０６における動作の詳細を示している。

【０３８１】

図２６を参照して、ゲートウェイ装置１０３は、対象メッセージの受信時刻から測定基準を差し引くことにより送信間隔を算出する（ステップＳ４０２）。

【０３８２】

次に、ゲートウェイ装置１０３は、算出した送信間隔をスコア関数Ｓｃ１に代入することによりスコアを算出する（ステップＳ４０４）。

【０３８３】

次に、ゲートウェイ装置１０３は、算出したスコアがしきい値ＴｈＢより大きい場合（ステップＳ４０６でＮＯ）、今回伝送された対象メッセージが不正メッセージであると判断する（ステップＳ４２４）。

【０３８４】

一方、ゲートウェイ装置１０３は、算出したスコアがしきい値ＴｈＢ以下である場合（ステップＳ４０６でＹＥＳ）、今回伝送された対象メッセージが正当メッセージまたは偽装メッセージであると判断する（ステップＳ４０８）。

【０３８５】

次に、ゲートウェイ装置１０３は、測定基準を、今回伝送された対象メッセージの受信時刻に更新する（ステップＳ４１０）。

【０３８６】

次に、ゲートウェイ装置１０３は、対象種類のデータおよび相手方種類のデータの両方が対象メッセージに格納されているか否かを確認する（ステップＳ４１２）。

【０３８７】

次に、ゲートウェイ装置１０３は、対象種類のデータおよび相手方種類のデータの両方が対象メッセージに含まれない場合、すなわち別個のメッセージに分かれて含まれる場合（

ステップＳ４１２でＮＯ）、対象種類のデータおよび相手方種類のデータに対して同期処理を行う（ステップＳ４１４）。

【０３８８】

次に、ゲートウェイ装置１０３は、２種類のデータの組、より詳細には対象種類のデータおよび相手方種類のデータの組を対象メッセージから取得するか、または同期処理を行った対象種類のデータおよび相手方種類のデータから、対象種類のデータおよび相手方種類のデータの最新の組を取得する（ステップＳ４１６）。

【０３８９】

次に、ゲートウェイ装置１０３は、対象種類のデータおよび相手方種類のデータの組に対応する通常モデルＭ２を記憶部５２から取得する（ステップＳ４１８）。

【０３９０】

次に、ゲートウェイ装置１０３は、取得した対象種類のデータおよび相手方種類のデータの組に基づく位置が、通常モデルＭ２の境界Ｂ２の内側に位置するか否かを確認する（ステップＳ４２０）。

【０３９１】

ゲートウェイ装置１０３は、取得した対象種類のデータおよび相手方種類のデータの組に基づく位置が境界Ｂ２の内側に位置する場合（ステップＳ４２０でＹＥＳ）、今回伝送された対象メッセージが正当メッセージであると判断する（ステップＳ４２２）。

【０３９２】

一方、ゲートウェイ装置１０３は、取得した対象種類のデータおよび相手方種類のデータの組に基づく位置が境界Ｂ２の外側に位置する場合（ステップＳ４２０でＮＯ）、今回伝送された対象メッセージが偽装メッセージすなわち不正メッセージであると判断する（ステップＳ４２４）。

【０３９３】

なお、本発明の第３の実施の形態に係るゲートウェイ装置では、監視部５７は、対象メッセージの受信時刻に基づいて送信間隔を測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。監視部５７は、たとえば、対象メッセージの送信時刻を取得し、取得した送信時刻に基づいて送信間隔を測定する構成であってもよい。

【０３９４】

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は、テスト車両において測定された対象メッセージの送信間隔の分布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。ゲートウェイ装置１０３は、対象車両１において測定された送信間隔を蓄積し、蓄積した送信間隔に基づいて当該分布を作成する構成であってもよい。

【０３９５】

以上のように、本発明の第３の実施の形態に係るゲートウェイ装置では、監視部５７は、車載ネットワーク１２における送信メッセージを監視する。分布取得部５８は、送信メッセージの送信間隔の分布を取得する。検知部６４は、監視部５７による監視結果および分布取得部５８によって取得された分布に基づいて不正メッセージを検知する。そして、検知部６４部は、不正メッセージとすべきでないと判断した送信メッセージについては、データ取得部５３によって取得された組、および検出条件に基づいて、不正メッセージであるか否かについて判断する。

【０３９６】

送信間隔を精度よく偽装した送信メッセージは、上記監視結果および上記分布に基づいて不正メッセージとして検知することが困難である。上記のような構成により、当該送信メッセージを、上記組および検出条件に基づいて不正メッセージとして検知することができるので、車載ネットワーク１２におけるセキュリティを向上させることができる。

【０３９７】

その他の構成および動作は第１の実施の形態に係るゲートウェイ装置と同様であるため、ここでは詳細な説明を繰り返さない。

【０３９８】

なお、本発明の第１の実施の形態～第３の実施の形態に係る各装置の構成要素および動作のうち、一部または全部を適宜組み合わせることも可能である。

【０３９９】

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、上記説明ではなく特許請求の範囲によって示され、特許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。

【０４００】

以上の説明は、以下に付記する特徴を含む。

【０４０１】

［付記１］

車両に搭載される車載ネットワークにおける不正メッセージ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１または複数の送信メッセージを取得するメッセージ取得部と、
前記メッセージ取得部によって取得された前記送信メッセージに含まれる、同じ時刻に対応する複数種類のデータの組を取得するデータ取得部と、
予め作成された、複数の時刻にそれぞれ対応する複数の前記組に基づく検出条件を記憶する記憶部と、
前記データ取得部によって取得された前記組、および前記検出条件に基づいて前記不正メッセージを検知する検知部とを備え、
前記検知装置は、前記送信メッセージを中継するゲートウェイ装置であり、
前記車載ネットワークは、前記車両の内部における装置である車載装置を含み、
前記車載装置は、前記車載ネットワークの設けられた車両の外部における装置と通信する車載通信機、または前記車両における機能部を制御可能な制御装置であり、
前記送信メッセージは、ＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＦｌｅｘＲａｙ、ＭＯＳＴ（Ｍｅｄｉａ Ｏｒｉｅｎｔｅｄ Ｓｙｓｔｅｍｓ Ｔｒａｎｓｐｏｒｔ）、イーサネットまたはＬＩＮ（Ｌｏｃａｌ Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｎｅｔｗｏｒｋ）の通信規格に従って前記車載ネットワークにおいて伝送され、
前記検出条件は、通常モデルであり、サーバにおいて予め作成され、
前記時刻は、受信時刻、送信時刻または作成時刻である、検知装置。

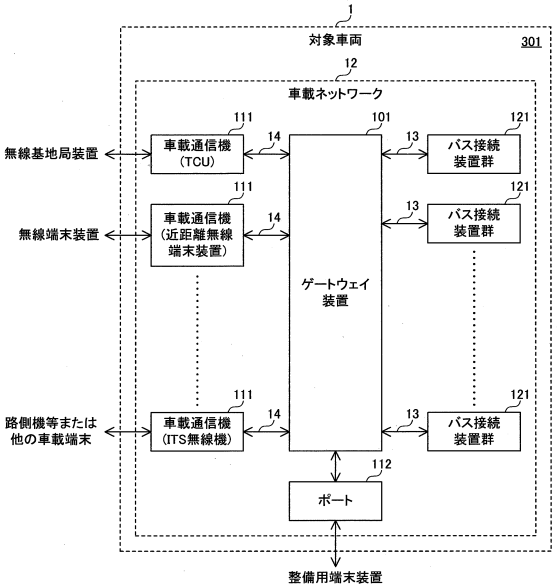
【符号の説明】

【０４０２】

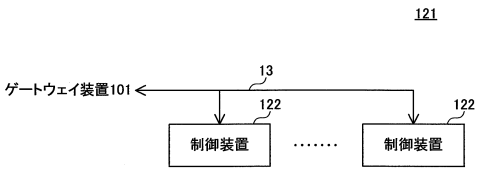
１　対象車両
１２　車載ネットワーク
１３，１４　バス
５１　通信処理部
５２　記憶部
５３　データ取得部
５４　検知部
５５　メッセージ取得部
５６　更新部
５７　監視部
５８　分布取得部
６４　検知部
１０１，１０２，１０３　ゲートウェイ装置（検知装置）
１１１　車載通信機
１１２　ポート
１２１　バス接続装置群
１２２　制御装置
３０１　車載通信システム

【図面】

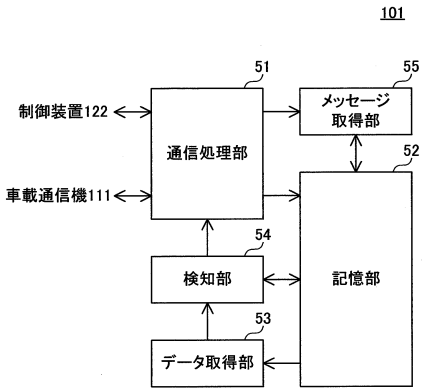
【図１】


1
対象車両
301
12
車載ネットワーク
111
101
121
無線基地局装置
車載通信機
(TCU)
14
13
バス接続
装置群
111
121
無線端末装置
車載通信機
(近距離無線
端末装置)
14
13
バス接続
装置群
ゲートウェイ
装置
111
121
路側機等または
他の車載端末
車載通信機
(ITS無線機)
14
13
バス接続
装置群
112
ポート
整備用端末装置

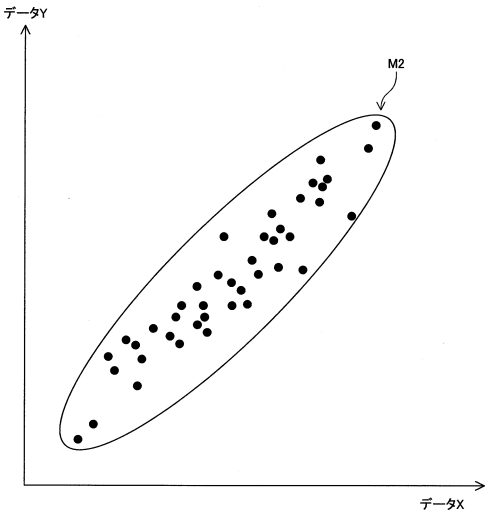
【図２】


121
13
ゲートウェイ装置101
122
122
制御装置
制御装置

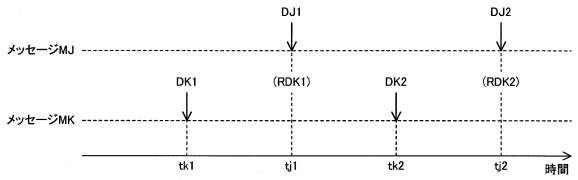
【図３】


101
51
55
制御装置122
メッセージ
取得部
通信処理部
52
車載通信機111
54
検知部
記憶部
53
データ取得部

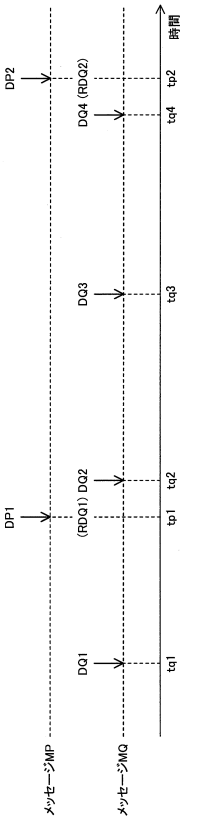
【図４】


データY
M2
データX

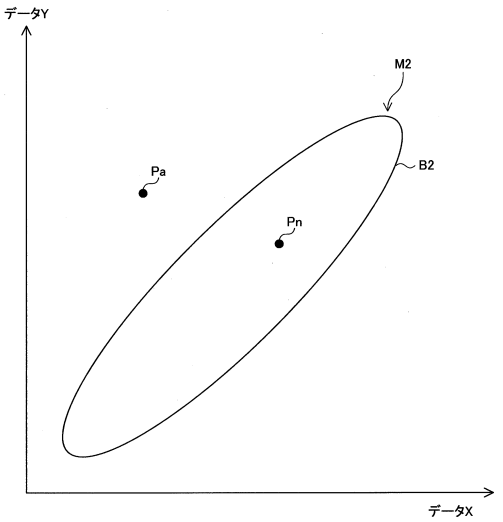
【図５】


DJ1
DJ2
メッセージMJ
DK1
(RDK1)
DK2
(RDK2)
メッセージMK
tk1
tj1
tk2
tj2
時間

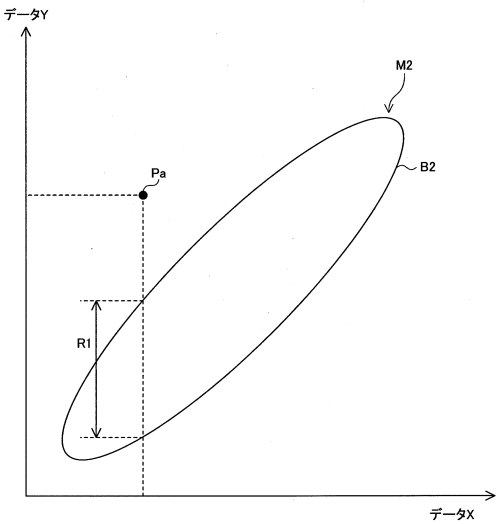
【図６】


時間
DP2
DQ4 (RDQ2)
tq4
tp2
DQ3
tq3
DQ2
tq2
DP1
(RDQ1)
tp1
DQ1
tq1
メッセージMP
メッセージMQ

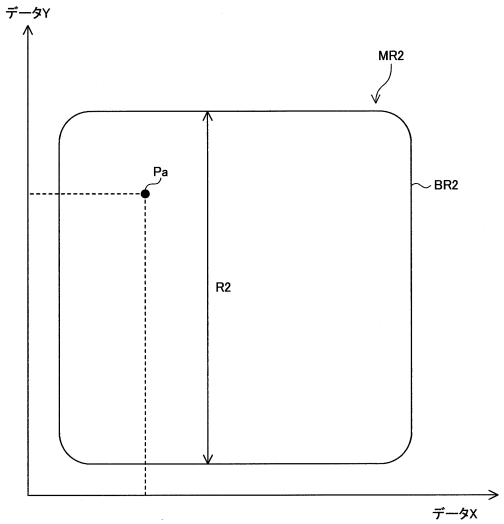
【図７】


データY
M2
B2
Pa
Pn
データX

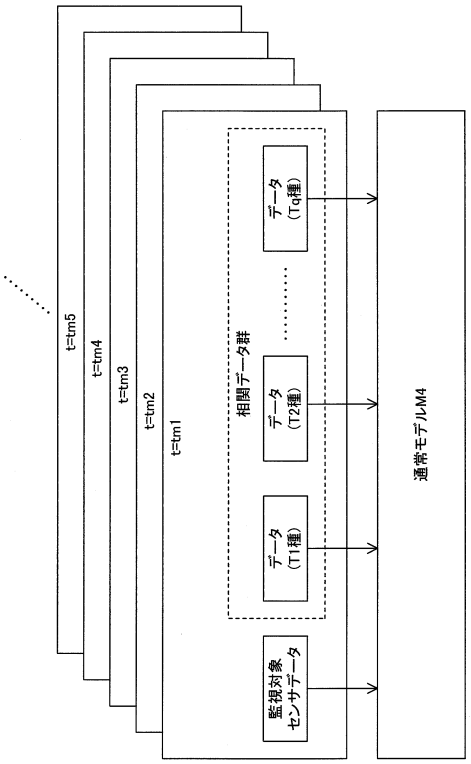
【図８】


データY
M2
B2
Pa
R1
データX

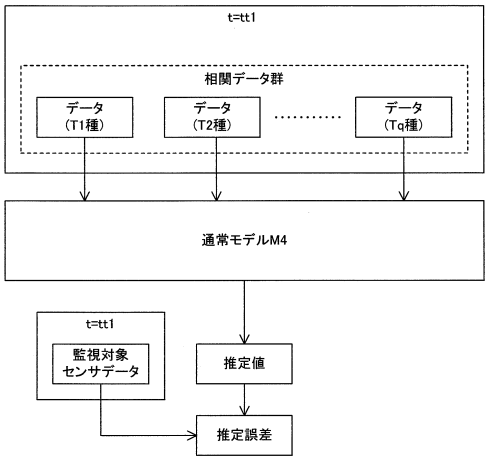
【図９】



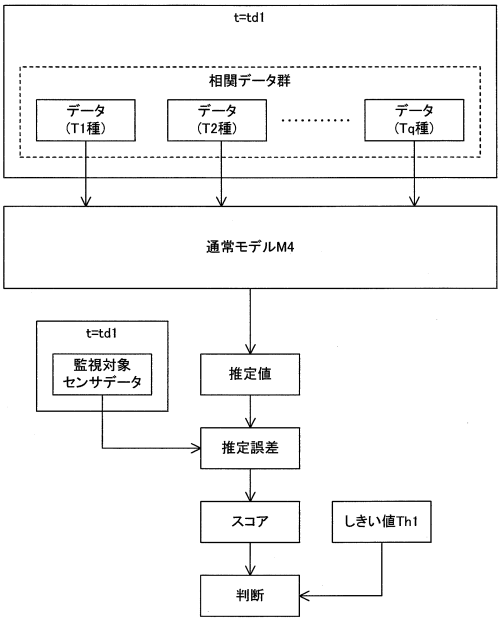
【図１０】



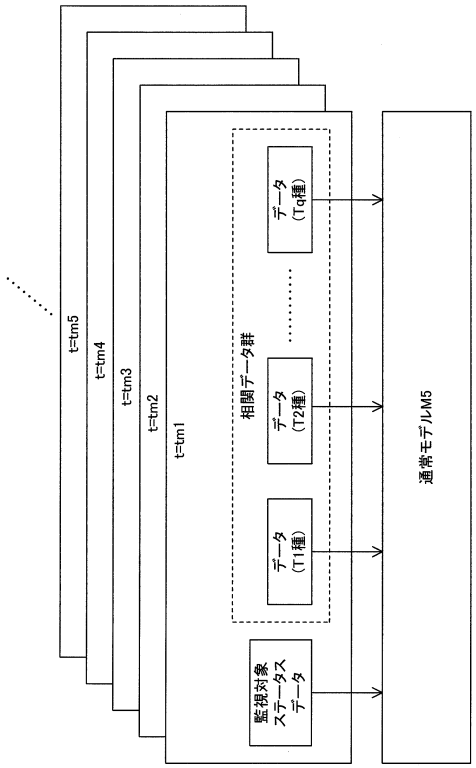
【図１１】



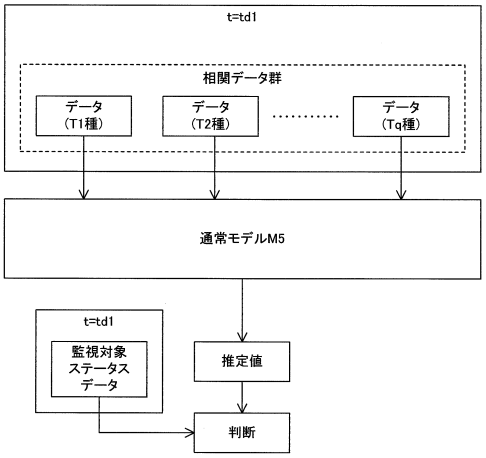
【図１２】



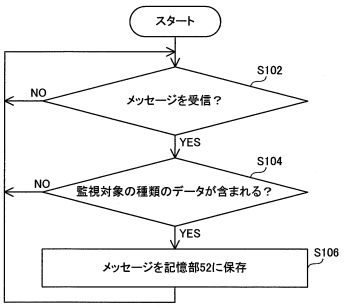
【図１３】



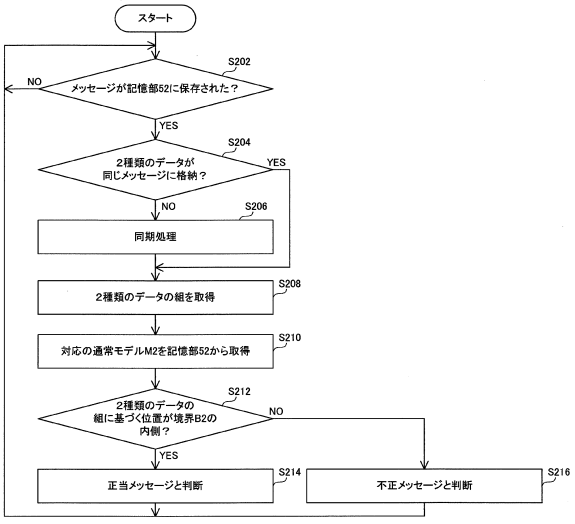
【図１４】



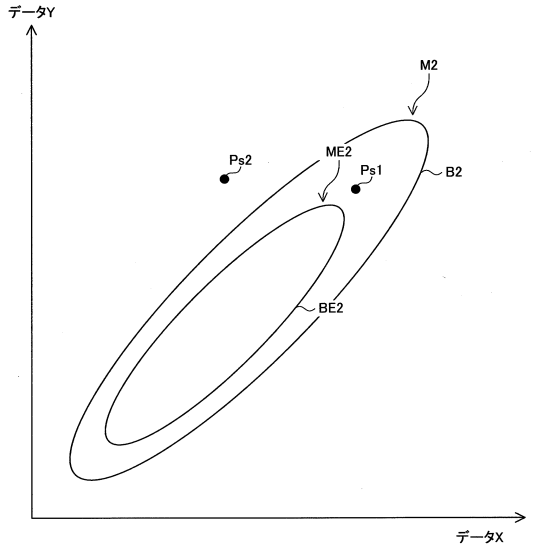
【図１５】



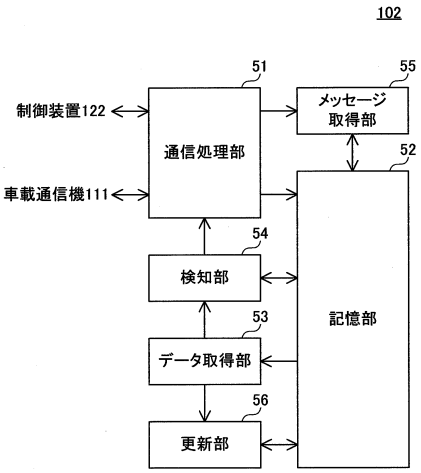
【図１６】



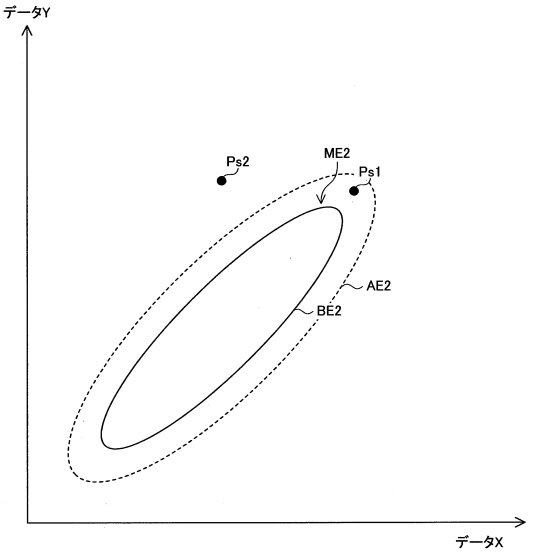
【図１７】



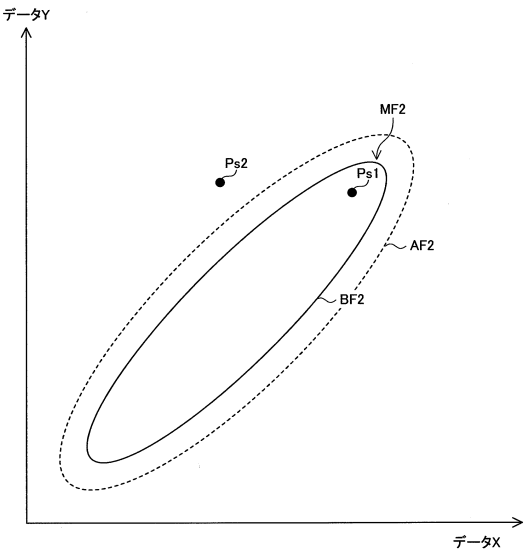
【図１８】



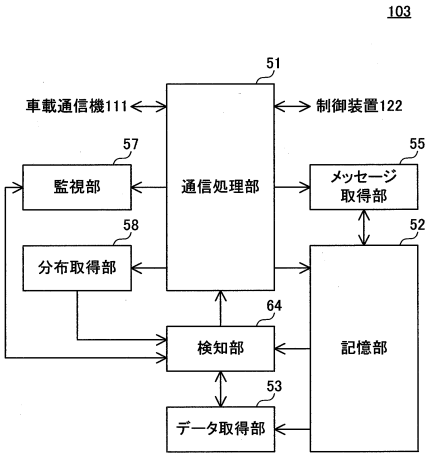
【図１９】



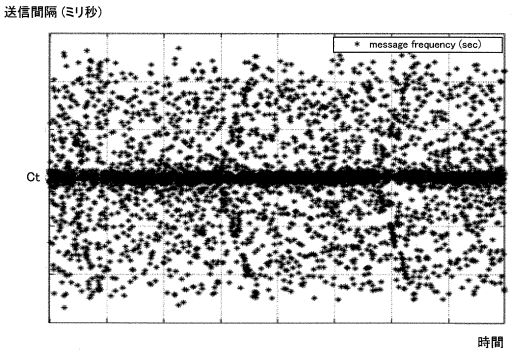
【図２０】



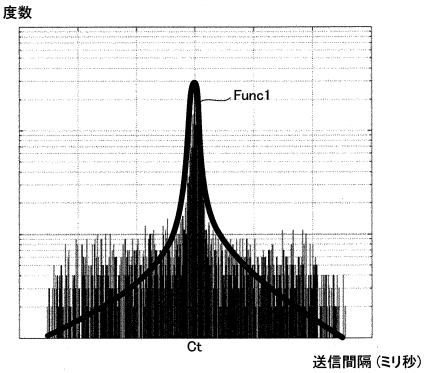
【図２１】



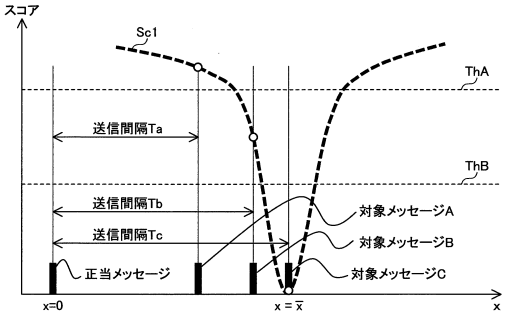
【図２２】



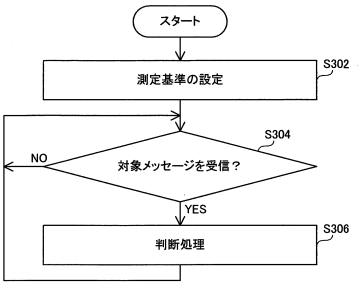
【図２３】



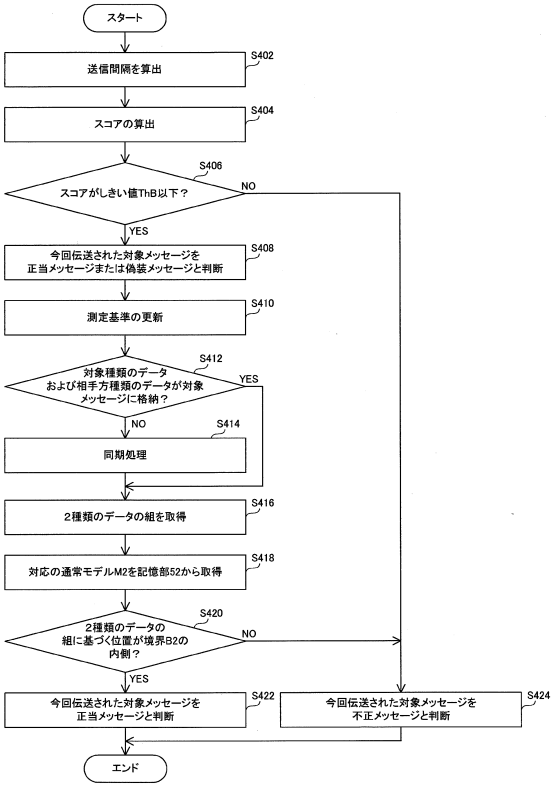
【図２４】



【図２５】


スタート
測定基準の設定
S302
S304
対象メッセージを受信？
NO
YES
判断処理
S306

【図２６】


スタート
送信間隔を算出
S402
スコアの算出
S404
S406
スコアがしきい値ThB以下？
NO
YES
今回伝送された対象メッセージを
正当メッセージまたは偽装メッセージと判断
S408
測定基準の更新
S410
S412
対象種類のデータ
および相手方種類のデータが対象
メッセージに格納？
YES
NO
S414
同期処理
2種類のデータの組を取得
S416
対応の通常モデルM2を記憶部52から取得
S418
S420
2種類のデータの
組に基づく位置が境界B2の
内側？
NO
YES
今回伝送された対象メッセージを
正当メッセージと判断
S422
今回伝送された対象メッセージを
不正メッセージと判断
S424
エンド

フロントページの続き

号 住友電気工業株式会社内
審査官 青木 健

(56)参考文献 特開２００５－２６５４５４（ＪＰ，Ａ）
欧州特許出願公開第０３１０９７７１（ＥＰ，Ａ１）
米国特許出願公開第２００７／０２９４１８７（ＵＳ，Ａ１）
特開２０１６－１３４９１３（ＪＰ，Ａ）
芳賀 智之 ほか，機械学習による車載ネットワーク攻撃検知システム，パナソニック技報，日本，2017年05月15日，Ｖｏｌ．６３ Ｎｏ．１，ｐｐ．１６－２１
伊達 友裕 ほか，車載ＬＡＮのセキュリティゲートウェイにおける機械学習を用いた動的ルール生成，ＳＣＩＳ２０１６，日本，ＳＣＩＳ２０１６実行委員会，2016年01月22日，３Ｆ２－１，ｐｐ．１－６

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５５
Ｂ６０Ｒ １６／０２３
Ｈ０４Ｌ １２／２８
Ｈ０４Ｗ １２／１２