(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-205015
(P2019-205015A)
(43)公開日　令和1年11月28日(2019.11.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
G09C 1/00	(2006.01)	G09C	1/00	640D	
G06F 21/64	(2013.01)	G06F	21/64		
B60R 16/02	(2006.01)	B60R	16/02	660Q	
G06F 21/55	(2013.01)	G06F	21/55		

審査請求 未請求　請求項の数 9　ＯＬ　（全 14 頁）

(21)出願番号　特願2018-97533(P2018-97533)
(22)出願日　平成30年5月22日(2018.5.22)

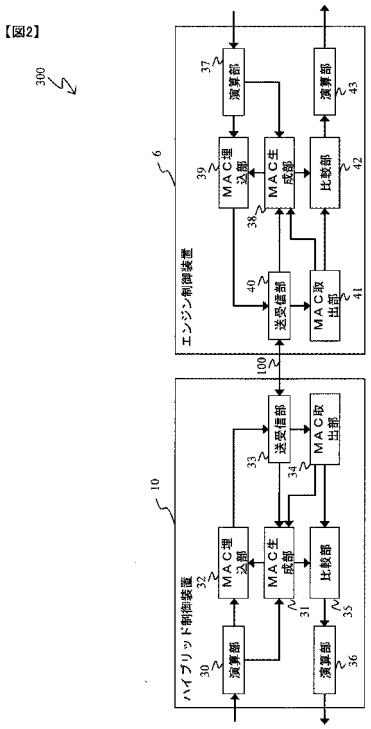
(71)出願人　509186579
日立オートモティブシステムズ株式会社
茨城県ひたちなか市高場２５２０番地
(74)代理人　100098660
弁理士　戸田　裕二
(72)発明者　石井　良和
茨城県ひたちなか市高場２５２０番地　日立オートモティブシステムズ株式会社内
(72)発明者　藤本　欽也
茨城県ひたちなか市高場２５２０番地　日立オートモティブシステムズ株式会社内

Ｆターム(参考)　5J104 AA08　LA02　LA05　PA07

(54)【発明の名称】車載ネットワークへの不正メッセージ注入防止技術

(57)【要約】
【課題】装置を追加せずに車載ネットワークへの不正なメッセージ注入を防止し、且つ制御の精度低下や遅延を抑えることが可能な車両制御システムを提供する。
【解決手段】車両制御システムにおいて、互いに接続される複数の制御装置（例えば、エンジン制御装置６、クラッチ制御装置７、モータ制御装置８、バッテリ制御装置９、ハイブリッド制御装置１０）と、複数の制御装置を互いに接続する複数の通信ネットワークと、を備え、算出可能な値を有する通信メッセージを送信する制御装置は、通信メッセージの値から第一アルゴリズムで算出した認証値と、認証値と通信メッセージの値を第二アルゴリズムで演算して、演算結果を通信メッセージの値を割り付けたデータフィールドに格納して、通信メッセージを受信する制御装置は、受信した通信メッセージから、認証値を第二アルゴリズムと関連を有する第三アルゴリズムによって抽出する。
【選択図】図２

【図2】



【特許請求の範囲】
【請求項１】
互いに接続される複数の制御装置と、
複数の前記制御装置を互いに接続する複数の通信ネットワークと、
を備え、
算出可能な値を有する通信メッセージを送信する前記制御装置は、
前記通信メッセージの前記値から第一アルゴリズムで算出した認証値と、
前記認証値と前記値を第二アルゴリズムで演算して、演算結果を前記通信メッセージ内の前記値を割り付けたデータフィールドに格納して、
前記通信メッセージを受信する前記制御装置は、
受信した前記通信メッセージから、前記認証値を前記第二アルゴリズムと関連を有する第三アルゴリズムによって抽出する、
ことを特徴とする車両制御システム。
【請求項２】
請求項１に記載の車両制御システムにおいて、
前記第二アルゴリズムに加算を含み、前記第三アルゴリズムに減算を含む、
ことを特徴とする車両制御システム。
【請求項３】
請求項１に記載の車両制御システムにおいて、
前記第二アルゴリズムは加算、前記第三アルゴリズムは減算、
又は、
前記第二アルゴリズムは減算、前記第三アルゴリズムは加算、
のいずれかを選択可能である
ことを特徴とする車両制御システム。
【請求項４】
請求項２～３のいずれかに記載の車両制御システムにおいて、
前記値はチェックサムである
ことを特徴とする車両制御システム。
【請求項５】
請求項２～３のいずれかに記載の車両制御システムにおいて、
前記値はＣＲＣである
ことを特徴とする車両制御システム。
【請求項６】
請求項２～３のいずれかに記載の車両制御システムにおいて、
前記値および前記認証値を１ｂｉｔ減らした構成とし、減らした前記１ｂｉｔ分を、前記第二アルゴリズム又は前記第三アルゴリズムでの加算による桁あふれｂｉｔとする
ことを特徴とする車両制御システム。
【請求項７】
請求項２～３のいずれかに記載の車両制御システムにおいて、
前記第二アルゴリズム又は前記第三アルゴリズムでの加算による桁あふれｂｉｔを、前記通信メッセージ内のデータフィールドの空きに有する
ことを特徴とする車両制御システム。
【請求項８】
請求項２に記載の車両制御システムにおいて、
前記第二アルゴリズムは、前記値を減算し、前記認証値を加算して、
前記第三アルゴリズムは停止させる
ことを特徴とする車両制御システム。
【請求項９】
請求項１～８のいずれかに記載の車両制御システムにおいて、
前記認証値のビット数は前記値のｂｉｔ数以下である

ことを特徴とする車両制御システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車載ネットワークへの不正メッセージ注入防止技術に関する。
【背景技術】
【０００２】
従来、車載通信ネットワークでは、自動車に搭載された制御用コンピュータ（車両用制御装置）であるＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）が相互に情報通信を行っている（例えば、特開２０１７－９２６３４号公報（以下、特許文献１）参照）。
【０００３】
特許文献１には、最新性情報と制御データとに基づいて生成された通信メッセージを他の情報処理装置から受信する情報処理装置が記載されている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２０１７－９２６３４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
車載ネットワークへの不正メッセージ注入対策として、特許文献１に開示される技術のように、通信メッセージに特定の情報を付加して、メッセージの正当性を判定する方法がある。特許文献１に開示される技術では、特定の情報を付加する場合、特定の情報のデータサイズ分だけ、通信メッセージで通信できるデータ量が減少する恐れがある。
【０００６】
一方、エンジン制御装置などの車両用制御装置は、様々な車両用装置を制御している。例えば、エンジン制御装置は、アクセルセンサから出力された信号に基づいて目標スロットル開度を演算し、実スロットル開度が目標スロットル開度になるようにスロットルモータを制御する。車両用制御装置による制御は、車両の走行に影響を与えるため、制御に関わる車載ネットワークへの不正なメッセージ注入を防止し、且つ制御の精度低下や遅延を抑えることが要請される。
【０００７】
本発明の目的は、装置を追加せずに車載ネットワークへの不正なメッセージ注入を防止し、且つ制御の精度低下や遅延を抑えることが可能な車両制御システムを提供することにある。
【課題を解決するための手段】
【０００８】
本発明は上記の目的を達成するために、互いに接続される複数の制御装置と、複数の前記制御装置を互いに接続する複数の通信ネットワークと、を備え、算出可能な値を有する通信メッセージを送信する前記制御装置は、前記通信メッセージの前記値から第一アルゴリズムで算出した認証値と、前記認証値と前記値を第二アルゴリズムで演算して、演算結果を前記通信メッセージ内の前記値を割り付けたデータフィールドに格納して、前記通信メッセージを受信する前記制御装置は、受信した前記通信メッセージから、前記認証値を前記第二アルゴリズムと関連を有する第三アルゴリズムによって抽出する。
【発明の効果】
【０００９】
本発明によれば、装置を追加せずに車載ネットワークへの不正なメッセージ注入を防止し、且つ制御の精度低下や遅延を抑えることが可能な車両制御システムを提供することができる。

【００１０】
上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。
【図面の簡単な説明】
【００１１】
【図１】本発明の第１の実施形態によるエンジン制御装置、ハイブリッド制御装置を含む車両制御システムの構成を示すブロック図。
【図２】本発明の第１の実施形態によるエンジン制御装置、ハイブリッド制御装置の構成を示すブロック図。
【図３】本発明の第１の実施形態によるハイブリッド制御装置の処理のフローチャートの例を示す図。
【図４】本発明の第１の実施形態によるエンジン制御装置の処理のフローチャートの例を示す図。
【図５】本発明の第１の実施形態によるエンジン制御装置の処理のフローチャートの例を示す図。
【図６】本発明の第１の実施形態によるハイブリッド制御装置の処理のフローチャートの例を示す図。
【発明を実施するための形態】
【００１２】
以下、図面を用いて本発明の第１の実施形態によるハイブリッド制御装置及びエンジン制御装置の構成及び動作を説明する。
【００１３】
（第１の実施形態）
最初に、図１を用いて、車両制御システムのハードウェア構成を説明する。図１は、本発明の第１の実施形態によるエンジン制御装置６、ハイブリッド制御装置１０を含む車両制御システムの構成を示すブロック図である。
【００１４】
本実施形態の車両制御システム３００は、燃料の燃焼によってトルクを発生するエンジン１と、クラッチ機構２と、車輪３ａの駆動軸３ｂに連結するモータ３と、モータ３を駆動するインバータ（電力変換装置）４と、バッテリ５と、アクセル開度を検出するアクセルセンサ１１と、スロットル開度を検出するスロットルセンサ１２と、スロットルモータ（スロットル装置）１３と、インジェクター（燃料噴射装置）１４と、点火装置１５と、ブレーキ１６と、エンジン制御装置６と、クラッチ制御装置７と、モータ制御装置８と、バッテリ制御装置９と、が搭載されて構成される。エンジン制御装置６は、スロットルセンサ１２による検出結果であるスロットル開度を入力し、スロットルモータ１３、インジェクター１４および点火装置１５を制御する。クラッチ制御装置７はクラッチ機構２を制御する。モータ制御装置８はインバータ４を制御することによってモータ３を制御する。バッテリ制御装置９はバッテリ５を制御する。なお、エンジン制御装置６、クラッチ制御装置７、モータ制御装置８、バッテリ制御装置９及びハイブリッド制御装置１０は、以下単に制御装置と称する場合がある。
【００１５】
さらに、車両制御システム３００には、上述の各制御装置６～９に対して、指令を出すハイブリッド制御装置１０が搭載される。各制御装置６～１０は、それぞれが不図示のＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）やＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）等を備えて構成され、予め定めた制御プログラムにしたがって信号処理を行う。
【００１６】
また、各制御装置６～１０は、互いに、通信線１００を介して種々の情報を送受信する。通信線１００は、多重通信線であり、ＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅ

ｔｗｏｒｋ）プロトコルに基づくネットワークを構成する。なお、通信線１００は、多重通信線に限られるものではない。

【００１７】

通信線１００は、主にハイブリッド制御に関わる制御装置を繋いでいるＣＡＮであり、例えば、ハイブリッド制御装置１０、エンジン制御装置６、クラッチ制御装置７、モータ制御装置８、バッテリ制御装置９などが繋がっている。ハイブリッド制御とは、例えば、所定の燃費や運転性を実現するために、トルク配分を決定、指令することである。

【００１８】

エンジン制御装置６は、スロットルセンサ１２からのスロットル開度などの入力に基づき、スロットルモータ１３、インジェクター１４、点火装置１５を制御する。具体的には、目標スロットル開度や燃料噴射量、点火時期などが制御されることにより、運転状態に応じてエンジン１の出力が制御される。

【００１９】

モータ３は、モータ（電動機）あるいはジェネレータ（発電機）として機能する。具体的には、モータ３は、加速時にはハイブリッド制御装置１０からの信号に基づいてモータ（電動機）として機能し、制動時にはジェネレータ（発電機）として機能してバッテリ５に回生電力を供給し蓄電する。

【００２０】

すなわち、インバータ４は、モータ制御装置８からの指令に基づきバッテリ５からの直流電力を交流電力に変換し、力行時に交流電力をモータ３に供給する。交流電力によりモータ３の固定子に回転磁界が形成され、モータ３の回転子が回転する。また、インバータ４は、回生時に、モータ制御装置８からの指令に基づきモータ３で発電された交流電力を直流電力に変換し、直流電力をバッテリ５に供給する。この直流電力によりバッテリ５が充電される。

【００２１】

なお、バッテリ５に蓄積された電気エネルギは、モータ３用の電力として用いられるほか、不図示のＤＣ－ＤＣコンバータなどを介してエアコンなどの補機類の電力としても用いられる。

【００２２】

次に、図２を用いて、本発明をハイブリッド制御装置１０、エンジン制御装置６に適用した場合の構成の一例を説明する。図２は、本発明の第１の実施形態によるハイブリッド制御装置１０、エンジン制御装置６の構成を示すブロック図である。

【００２３】

ハイブリッド制御装置１０、エンジン制御装置６はＣＡＮ通信で通信線１００を介して接続されている。

【００２４】

ハイブリッド制御装置１０は、演算部３０と、ＭＡＣ生成部３１と、ＭＡＣ埋込部３２と、送受信部３３と、ＭＡＣ取出部３４と、比較部３５と、演算部３６と、を備えて構成される。

【００２５】

なお、ＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）とは、通信メッセージを認証するための短い情報のことである。

【００２６】

演算部３０は、ハイブリッド制御装置１０の外部からの値を入力として演算を行い、通信メッセージに格納するデータを算出する。それらの通信メッセージに格納するデータ自身から算出可能な値（例えば、チェックサム）も算出し、両者をＭＡＣ生成部３１と、ＭＡＣ埋込部３２に出力する。外部からの入力値は、例えば、アクセルセンサ１１からのアクセル開度などである。すなわち、演算部３０は、外部からの入力値に基づいて、車両用装置の制御量（例えば、モータ３の制御量やバッテリ５の制御量など）を演算する。

【００２７】

ＭＡＣ生成部３１は、演算部３０からの値を入力として所定の演算を行い、ＭＡＣを生成して、ＭＡＣ埋込部３２にＭＡＣを出力する。さらに、送受信部３３からの値およびＭＡＣ取出部３４からの値（後述するＭＡＣ’）を入力として所定の演算を行い、ＭＡＣを生成して、比較部３５にＭＡＣを出力する。所定の演算は、例えば、ハッシュ関数である。

【００２８】

ＭＡＣ埋込部３２は、演算部３０からの値を入力として、通信メッセージを生成する。通信メッセージには、通信メッセージ自身から算出可能な値を含ませる。ＭＡＣ生成部３１からのＭＡＣを入力として、生成した通信メッセージ内の、前述した「通信メッセージ自身から算出可能な値」に加算する。具体的には例えば、８バイトのデータフィールドで構成されたＣＡＮフレームを生成した場合、８バイト目の値を、１～７バイト目の値から算出可能な値とする。ＭＡＣを８バイト目に加算することで、ＣＡＮフレームにＭＡＣを埋め込む。

【００２９】

送受信部３３は、通信線１００に対する送信部および受信部として機能する。

【００３０】

送受信部３３が送信部として機能する場合、ＭＡＣ埋込部３２から出力される通信メッセージを入力とし、ＩＤなどを含むＣＡＮフレームを、通信線１００を介してハイブリッド制御装置１０の外部へ送信する。すなわち、送受信部３３は、演算部３０の演算結果およびＭＡＣを含んだＣＡＮフレームをエンジン制御装置６の送受信部４０へ送信する。

【００３１】

送受信部３３が受信部として機能する場合、ハイブリッド制御装置１０の外部からの値を入力としており、通信線１００による値を受信し、ＭＡＣ生成部３１とＭＡＣ取出部３４に受信値を出力する。すなわち、送受信部３３は、エンジン制御装置６の送受信部４０から送信された値を、受信する。

【００３２】

ＭＡＣ取出部３４は、送受信部３３からの受信値を入力として所定の演算を行い、ＭＡＣ’を取り出して、ＭＡＣ生成部３１および比較部３５に、取り出したＭＡＣ’を出力する。所定の演算とは、具体的には、８バイトのデータフィールドで構成されたＣＡＮフレームで、８バイト目の値が１～７バイト目の値から算出可能な場合（つまり、通信メッセージ自身から算出可能な値の場合）、１～７バイト目の値から算出した値を８バイト目から減算することで、ＭＡＣ’を取り出す。

【００３３】

比較部３５は、ＭＡＣ生成部３１からのＭＡＣと、ＭＡＣ取出部３４からのＭＡＣ’を入力として、両者を比較する。比較した結果、ＭＡＣおよびＭＡＣ’が同一の場合、演算部３６へ受信値を出力する。同一ではない場合、受信値を破棄する。

【００３４】

なお、破棄とは、データを捨てることを意味する。例えば、メモリ等に記憶されたデータを削除したり、メモリ等に記憶されたデータを利用しないようにフラグを設定したりすることがデータの破棄に該当する。つまり、データが利用されないように処理がなされていればよい。

【００３５】

演算部３６は、比較部３５の受信値を入力とし、ハイブリッド制御装置１０の外部への出力値（制御用パラメータ）を演算する。外部への出力値は、例えば、不図示のＤＣ－ＤＣコンバータへの制御信号や、モータ制御装置８への目標トルクなどである。

【００３６】

なお、ＣＡＮ通信では、２本の通信線の電圧差により通信を行うため、外部ノイズの影響を受けにくい。

【００３７】

エンジン制御装置６は、演算部３７と、ＭＡＣ生成部３８と、ＭＡＣ埋込部３９と、送

受信部４０と、ＭＡＣ取出部４１と、比較部４２と、演算部４３と、を備えて構成される。

【００３８】

演算部３７は、エンジン制御装置６の外部からの値を入力として演算を行い、ＭＡＣ生成部３８と、ＭＡＣ埋込部３９に演算結果を出力する。外部からの入力値は、例えば、スロットルセンサ１２からのスロットル開度などである。

【００３９】

ＭＡＣ生成部３８は、演算部３７からの値を入力として所定の演算を行い、ＭＡＣを算出して、ＭＡＣ埋込部３９にＭＡＣを出力する。さらに、送受信部４０からの値およびＭＡＣ取出部４１からの値（後述するＭＡＣ’）を入力として所定の演算を行い、ＭＡＣを算出して、比較部４２にＭＡＣを出力する。所定の演算は、例えば、ハッシュ関数である。

【００４０】

ＭＡＣ埋込部３９は、演算部３７からの値を入力として、通信メッセージを生成する。通信メッセージには、通信メッセージ自身から算出可能な値を含ませる。ＭＡＣ生成部３８からのＭＡＣを入力として、生成した通信メッセージ内の、前述した「通信メッセージ自身から算出可能な値」に加算する。具体的には例えば、８バイトのデータフィールドで構成されたＣＡＮフレームを生成した場合、８バイト目の値を、１～７バイト目の値から算出可能な値とする。ＭＡＣを８バイト目に加算することで、ＣＡＮフレームにＭＡＣを埋め込む。

【００４１】

送受信部４０は、通信線１００に対する送信部および受信部として機能する。

【００４２】

送受信部４０が送信部として機能する場合、ＭＡＣ埋込部３９から出力される通信メッセージを入力とし、ＩＤなどを含むＣＡＮフレームを、通信線１００を介してエンジン制御装置６の外部へ送信する。すなわち、送受信部４０は、演算部３７の演算結果およびＭＡＣを含んだＣＡＮフレームをハイブリッド制御装置１０の送受信部３３へ送信する。

【００４３】

送受信部４０が受信部として機能する場合、エンジン制御装置６の外部からの値を入力としており、通信線１００による値を受信し、ＭＡＣ生成部３８とＭＡＣ取出部４１に受信値を出力する。すなわち、送受信部４０は、ハイブリッド制御装置１０の送受信部３３から送信された値を、受信する。

【００４４】

ＭＡＣ取出部４１は、送受信部４０からの受信値を入力として所定の演算を行い、ＭＡＣ’を取り出して、ＭＡＣ生成部３８および比較部４２に、取り出したＭＡＣ’を出力する。所定の演算とは、具体的には、８バイトのデータフィールドで構成されたＣＡＮフレームで、８バイト目の値が１～７バイト目の値から算出可能な場合（つまり、通信メッセージ自身から算出可能な値の場合）、１～７バイト目の値から算出した値を８バイト目から減算することで、ＭＡＣ’を取り出す。

【００４５】

比較部４２は、ＭＡＣ生成部３８からのＭＡＣと、ＭＡＣ取出部４１からのＭＡＣ’を入力として、両者を比較する。比較した結果、ＭＡＣおよびＭＡＣ’が同一の場合、演算部４３へ受信値を出力する。同一ではない場合、受信値を破棄する。

【００４６】

演算部４３は、比較部４２の受信値を入力とし、エンジン制御装置６の外部への出力値（制御用パラメータ）を演算する。外部への出力値は、例えば、スロットルモータ１３へのスロットル開度などである。

【００４７】

次に、図３を用いて、ハイブリッド制御装置１０の動作を説明する。図３は、本発明の第１の実施形態によるハイブリッド制御装置１０の通信線１００を介した送信処理を示す

フローチャートの例である。

【００４８】

ステップＳ１０では、演算部３０は、ハイブリッド制御装置１０の外部からの値を入力とし、制御値（制御量）を演算し、通信メッセージに格納するデータを演算する。

【００４９】

ステップＳ１１では、演算部３０は、ステップＳ１０で演算した「通信メッセージに格納するデータ」自身から算出可能な値Ａを算出し、通信メッセージを生成する。

【００５０】

ステップＳ１２では、ＭＡＣ生成部３１は、ステップＳ１１で生成した通信メッセージを入力として、ＭＡＣを生成する。

【００５１】

ステップＳ１３では、ＭＡＣ埋込部３２は、ステップＳ１２で生成したＭＡＣを、ステップＳ１１で生成した通信メッセージの値Ａを割り付けたデータフィールドに加算して格納する。例えば、８バイトのデータフィールドを有する通信メッセージにおいて、データフィールドの８バイト目に値Ａを割り付けたとする。値Ａ＝２８とすると、ステップＳ１１で生成した通信メッセージのデータフィールドの８バイト目には、２８が格納されている。ＭＡＣ＝５５とすると、ステップＳ１３では、通信メッセージのデータフィールドの８バイト目にＭＡＣを加算することにより、通信メッセージのデータフィールドの８バイト目には、８３が格納されることとなる。

【００５２】

ステップＳ１４では、送受信部３３は、ステップＳ１３で生成した通信メッセージを、エンジン制御装置６の送受信部４０へ、ＣＡＮ通信で通信線１００を介して送信する。

【００５３】

次に、図４を用いて、エンジン制御装置６の動作を説明する。図４は、本発明の第１の実施形態によるエンジン制御装置６の通信線１００を介した受信処理を示すフローチャートの例である。

【００５４】

ステップＳ２０では、送受信部４０は、ハイブリッド制御装置１０の送受信部３３から通信メッセージを受信する。

【００５５】

ステップＳ２１では、ＭＡＣ取出部４１は、ステップＳ２０で受信した通信メッセージから、通信メッセージに格納するデータ自身から算出可能な値Ａを算出する。次に、ステップＳ２０で受信した通信メッセージの値Ａを割り付けたデータフィールドから、算出した値Ａを減算して、ＭＡＣ’を取り出す。例えば、８バイトのデータフィールドを有する通信メッセージにおいて、データフィールドの８バイト目に値Ａを割り付けたとする。値Ａ＝２８、ＭＡＣ＝５５とすると、ステップＳ２１で受信した通信メッセージのデータフィールドの８バイト目には、８３が格納されている。ステップＳ２１では、通信メッセージのデータフィールドから値Ａ（＝２８）を算出し、データフィールドの８バイト目（＝８３）から値Ａを減算することにより、ＭＡＣ’＝５５を取り出す。

【００５６】

ステップＳ２２では、ＭＡＣ生成部３８は、ステップＳ２０で受信した通信メッセージから、ステップＳ２１で取り出したＭＡＣ’を取り除いた後の通信メッセージを入力として、ＭＡＣを生成する。

【００５７】

ステップＳ２３では、比較部４２は、ステップＳ２１で取り出したＭＡＣ’と、ステップＳ２２で生成したＭＡＣが等しいか比較する。ＭＡＣ’とＭＡＣが等しいかが真の場合は、ステップＳ２４に処理を進める。偽の場合は、ステップＳ２５に処理を進める。

【００５８】

ステップＳ２４では、演算部４３は、受信した通信メッセージの制御値を入力とし、エンジン制御装置６の外部への出力値を演算する。

【００５９】
ステップＳ２５では、比較部４２は、ハイブリッド制御装置１０の送受信部３３から受信した通信メッセージを破棄する。
【００６０】
次に、図５を用いて、エンジン制御装置６の動作を説明する。図５は、本発明の第１の実施形態によるエンジン制御装置６の通信線１００を介した送信処理を示すフローチャートの例である。
【００６１】
ステップＳ３０では、演算部３７は、エンジン制御装置６の外部からの値を入力とし、制御値（制御量）を演算し、通信メッセージに格納するデータを演算する。
【００６２】
ステップＳ３１では、演算部３７は、ステップＳ３０で演算した「通信メッセージに格納するデータ」自身から算出可能な値Ａを算出し、通信メッセージを生成する。
【００６３】
ステップＳ３２では、ＭＡＣ生成部３８は、ステップＳ３１で生成した通信メッセージを入力として、ＭＡＣを生成する。
【００６４】
ステップＳ３３では、ＭＡＣ埋込部３９は、ステップＳ３２で生成したＭＡＣを、ステップＳ３１で生成した通信メッセージの値Ａを割り付けたデータフィールドに加算して格納する。例えば、８バイトのデータフィールドを有する通信メッセージにおいて、データフィールドの８バイト目に値Ａを割り付けたとする。値Ａ＝２８とすると、ステップＳ３１で生成した通信メッセージのデータフィールドの８バイト目には、２８が格納されている。ＭＡＣ＝５５とすると、ステップＳ３３では、通信メッセージのデータフィールドの８バイト目にＭＡＣを加算することにより、通信メッセージのデータフィールドの８バイト目には、８３が格納されることとなる。
【００６５】
ステップＳ３４では、送受信部４０は、ステップＳ３３で生成した通信メッセージを、ハイブリッド制御装置１０の送受信部３３へ、ＣＡＮ通信で通信線１００を介して送信する。
【００６６】
次に、図６を用いて、ハイブリッド制御装置１０の動作を説明する。図６は、本発明の第１の実施形態によるハイブリッド制御装置１０の通信線１００を介した受信処理を示すフローチャートの例である。
【００６７】
ステップＳ４０では、送受信部３３は、エンジン制御装置６の送受信部４０から通信メッセージを受信する。
【００６８】
ステップＳ４１では、ＭＡＣ取出部３４は、ステップＳ４０で受信した通信メッセージから、通信メッセージに格納するデータ自身から算出可能な値Ａを算出する。次に、ステップＳ４０で受信した通信メッセージの値Ａを割り付けたデータフィールドから、算出した値Ａを減算して、ＭＡＣ’を取り出す。例えば、８バイトのデータフィールドを有する通信メッセージにおいて、データフィールドの８バイト目に値Ａを割り付けたとする。値Ａ＝２８、ＭＡＣ＝５５とすると、ステップＳ４１で受信した通信メッセージのデータフィールドの８バイト目には、８３が格納されている。ステップＳ４１では、通信メッセージのデータフィールドから値Ａ（＝２８）を算出し、データフィールドの８バイト目（＝８３）から値Ａを減算することにより、ＭＡＣ’＝５５を取り出す。
【００６９】
ステップＳ４２では、ＭＡＣ生成部３１は、ステップＳ４０で受信した通信メッセージから、ステップＳ４１で取り出したＭＡＣ’を取り除いた後の通信メッセージを入力として、ＭＡＣを生成する。

【００７０】
ステップＳ４３では、比較部３５は、ステップＳ４１で取り出したＭＡＣ’と、ステップＳ４２で生成したＭＡＣが等しいか比較する。ＭＡＣ’とＭＡＣが等しいかが真の場合は、ステップＳ４４に処理を進める。偽の場合は、ステップＳ４５に処理を進める。
【００７１】
ステップＳ４４では、演算部３６は、受信した通信メッセージの制御値を入力とし、ハイブリッド制御装置１０の外部への出力値を演算する。
【００７２】
ステップＳ４５では、比較部３５は、エンジン制御装置６の送受信部４０から受信した通信メッセージを破棄する。
【００７３】
上記の方法により、ＭＡＣを、通信メッセージ自身から算出可能な値に加算することで、通信メッセージ内のデータフィールドに格納できる制御量等の実データ量を減少させずにＭＡＣを使用可能となる。
【００７４】
上記実施形態では、制御装置がＣＡＮ通信を行う例を説明したが、これに限定せず、制御装置が例えば、ＬＩＮ（Ｌｏｃａｌ Ｉｎｔｅｒｃｏｎｎｅｃｔ Ｎｅｔｗｏｒｋ）、ＦｌｅｘＲａｙ（Daimler Chrysler AGの登録商標）、ＭＯＳＴ（Ｍｅｄｉａ Ｏｒｉｅｎｔｅｄ Ｓｙｓｔｅｍｓ Ｔｒａｎｓｐｏｒｔ。Standard Microsystems Corporationの登録商標）、ＰＬＣ（Ｐｏｗｅｒ Ｌｉｎｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）などの如何なるプロトコルで通信を行うものであってもよいし、複数の制御装置のそれぞれが異なるプロトコルで通信を行う構成に適用してもよい。
【００７５】
上記実施形態では、制御装置が有線の例を説明したが、これに限定せず、制御装置が無線である構成やＯＴＡ（Ｏｖｅｒ Ｔｈｅ Ａｉｒ）に適用してもよい。
【００７６】
以上説明したように、本実施形態によれば、通信メッセージ内のデータフィールドに格納できる制御量等の実データ量を減少させずにＭＡＣを使用可能となることで、単位時間当たりに通信可能な情報量を減らさずに、不正メッセージ注入を防止し、安全性を向上できる。通信可能な情報量を減らさないことで、制御の精度低下や遅延を抑えられる。
【００７７】
（第１の変形例）
通信ネットワークは、ＣＡＮ－ＦＤでもよい。例えば、図２の例では、通信線１００をＣＡＮ－ＦＤとしてもよい。
【００７８】
本変形例によれば、通信速度を向上し、通信可能なデータ量を増加できる。これにより、通信効率が向上する。
【００７９】
（第２の変形例）
通信ネットワークは、Ｅｔｈｅｒｎｅｔ（富士ゼロックス株式会社の登録商標）でもよい。例えば、図２の例では、通信線１００をＥｔｈｅｒｎｅｔとしてもよい。
【００８０】
本変形例によれば、通信速度を向上し、通信可能なデータ量を増加できる。これにより、通信効率が向上する。
【００８１】
（第３の変形例）
第１の実施形態では、ＭＡＣ埋込部３２は、ＭＡＣを「通信メッセージ自身から算出可能な値」に加算するとしたが、減算でもよいし、加算と減算のいずれかに選択可能としてもよい。減算とした場合、ＭＡＣ取出部３４は、通信メッセージ自身から算出可能な値を、加算することでＭＡＣ’を取り出す。ＭＡＣ埋込部３９およびＭＡＣ取出部４１におい

ても、同様に、加算と減算のいずれかに選択可能としてもよい。

【００８２】

本変形例によれば、算出方法を可変にすることで、攻撃者に解読されにくくなる。これにより、機密性が向上する。

【００８３】

（第４の変形例）

「通信メッセージ自身から算出可能な値」は、チェックサムでもよい。例えば、図２の例では、ＭＡＣ埋込部３２および３９は、通信メッセージにチェックサムを含ませる。

【００８４】

本変形例によれば、通信メッセージの誤り検出可能となる。これにより、通信メッセージの伝送が正しく行えたか確認可能となり、通信の信頼性が向上する。

【００８５】

（第５の変形例）

「通信メッセージ自身から算出可能な値」は、ＣＲＣ（巡回冗長符号：Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｈｅｃｋ）でもよい。例えば、図２の例では、ＭＡＣ埋込部３２および３９は、通信メッセージにＣＲＣを含ませる。

【００８６】

本変形例によれば、通信メッセージの誤り検出可能となる。これにより、通信メッセージの伝送が正しく行えたか確認可能となり、通信の信頼性が向上する。

【００８７】

（第６の変形例）

ＭＡＣおよび「通信メッセージ自身から算出可能な値」の、データサイズのビット数を１ｂｉｔ減らし、桁あふれビット用の領域を有するようにしてもよい。例えば、ＭＡＣおよび「通信メッセージ自身から算出可能な値」のデータサイズを８ｂｉｔとしていた場合は、７ｂｉｔをＭＡＣおよび「通信メッセージ自身から算出可能な値」とし、残りの１ｂｉｔを、加算時の桁あふれビットとして使用する。

【００８８】

本変形例によれば、ＭＡＣ取出部３４および４１が、ＭＡＣ’を取り出す際の減算において、計算負荷が減少する。これにより、ソフトウェアの効率性が向上する。

【００８９】

（第７の変形例）

通信メッセージのデータフィールドの空き領域に、桁あふれビット用の領域を有するようにしてもよい。

【００９０】

本変形例によれば、ＭＡＣ取出部３４および４１が、ＭＡＣ’を取り出す際の減算において、計算負荷が減少し、桁あふれビットの割付け自由度が向上する。これにより、ソフトウェアの効率性が向上する。

【００９１】

（第８の変形例）

第１の実施形態では、ＭＡＣ埋込部３２は、ＭＡＣを「通信メッセージ自身から算出可能な値」に加算するとしたが、置換でもよい。置換とした場合、ＭＡＣ取出部３４は、通信メッセージ自身から算出可能な値について特に考慮せず、通信メッセージからそのままＭＡＣ’を取り出す。ＭＡＣ埋込部３９およびＭＡＣ取出部４１においても、同様に、置換としてもよい。

【００９２】

本変形例によれば、ＭＡＣ取出部３４および４１が、ＭＡＣ’を取り出す際の演算において、計算負荷が減少する。これにより、ソフトウェアの効率性が向上する。

【００９３】

（第９の変形例）

ＭＡＣのデータサイズのビット数は、「通信メッセージ自身から算出可能な値」のデー

タサイズ以下でもよい。例えば、「通信メッセージ自身から算出可能な値」が８ｂｉｔの場合、ＭＡＣは８ｂｉｔ以下のデータサイズとする。

【００９４】

本変形例によれば、ＭＡＣ取出部３４および４１が、ＭＡＣ’を取り出す際において、計算負荷が減少する。さらに、通信メッセージのデータフィールドの空きが不要となる。これにより、ソフトウェアの効率性が向上する。

【００９５】

以上の実施例及び変形例は、次のように表現することができる。

【００９６】

互いに接続される複数の制御装置と、複数の前記制御装置を互いに接続する複数の通信ネットワークと、を備え、算出可能な値を有する通信メッセージを送信する前記制御装置は、前記通信メッセージの前記値から第一アルゴリズムで算出した認証値と、前記認証値と前記値を第二アルゴリズムで演算して、演算結果を前記通信メッセージ内の前記値を割り付けたデータフィールドに格納して、前記通信メッセージを受信する前記制御装置は、受信した前記通信メッセージから、前記認証値を前記第二アルゴリズムと関連を有する第三アルゴリズムによって抽出する。

【００９７】

また、前記第二アルゴリズムに加算を含み、前記第三アルゴリズムに減算を含む。

【００９８】

また、前記第二アルゴリズムは加算、前記第三アルゴリズムは減算、又は、前記第二アルゴリズムは減算、前記第三アルゴリズムは加算、のいずれかを選択可能である。

【００９９】

また、前記値はチェックサムである。

【０１００】

また、前記値はＣＲＣである。

【０１０１】

また、前記値および前記認証値を１ｂｉｔ減らした構成とし、減らした前記１ｂｉｔ分を、前記第二アルゴリズム又は前記第三アルゴリズムでの加算による桁あふれｂｉｔとする。

【０１０２】

また、前記第二アルゴリズム又は前記第三アルゴリズムでの加算による桁あふれｂｉｔを、前記通信メッセージ内のデータフィールドの空きに有する。

【０１０３】

また、前記第二アルゴリズムは、前記値を減算し、前記認証値を加算して、前記第三アルゴリズムは停止させる。

【０１０４】

また、前記認証値のビット数は前記値のｂｉｔ数以下である。

【０１０５】

なお、上記第１の実施形態では、ハイブリッド制御装置１０、エンジン制御装置６との間の通信の例を説明したが、他の制御装置、例えば、クラッチ制御装置７、モータ制御装置８、バッテリ制御装置９などの通信に適用してもよい。

【０１０６】

なお、本発明は上記した実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施形態は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、本発明は、搭載車両の種類に限定されるものではなく、例えば、自動運転機能や自動駐車機能を有する車両に搭載されていてもよい。

【０１０７】

また、上記の各構成、機能、処理部等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロ

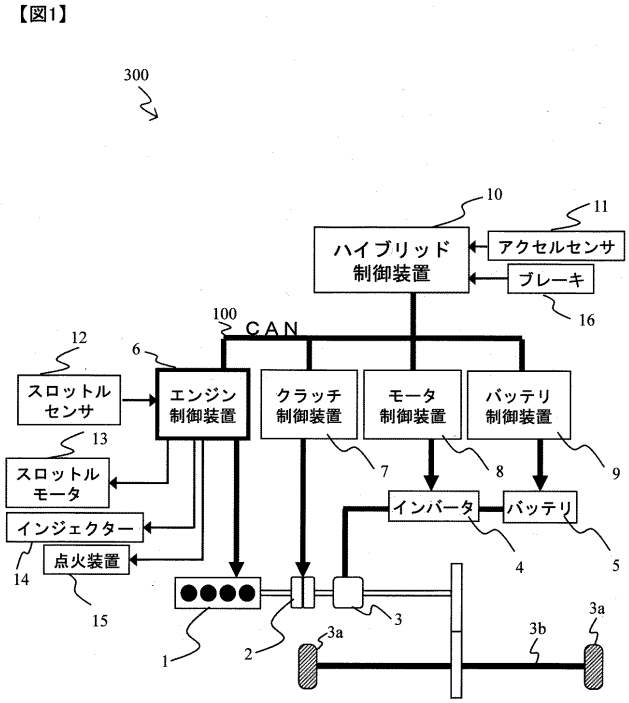
セッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）等の記録装置、または、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に置くことができる。

【符号の説明】

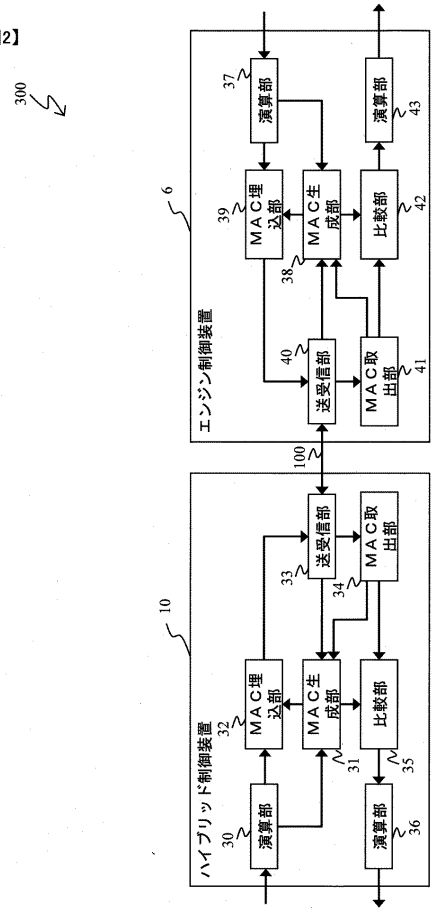
【０１０８】

１…エンジン、２…クラッチ機構、３…モータ、４…インバータ（電力変換装置）、５…バッテリ、６…エンジン制御装置（制御装置）、７…クラッチ制御装置（制御装置）、８…モータ制御装置（制御装置）、９…バッテリ制御装置（制御装置）、１０…ハイブリッド制御装置（制御装置）、１１…アクセルセンサ、１２…スロットルセンサ、１３…スロットルモータ（スロットル装置）、１４…インジェクター（燃料噴射装置）、１５…点火装置、１６…ブレーキ、３０…演算部、３１…ＭＡＣ生成部、３２…ＭＡＣ埋込部、３３…送受信部、３４…ＭＡＣ取出部、３５…比較部、３６…演算部、３７…演算部、３８…ＭＡＣ生成部、３９…ＭＡＣ埋込部、４０…送受信部、４１…ＭＡＣ取出部、４２…比較部、４３…演算部、１００…通信線、３００…車両制御システム。

【図１】

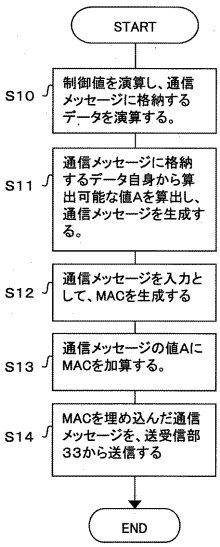


【図２】



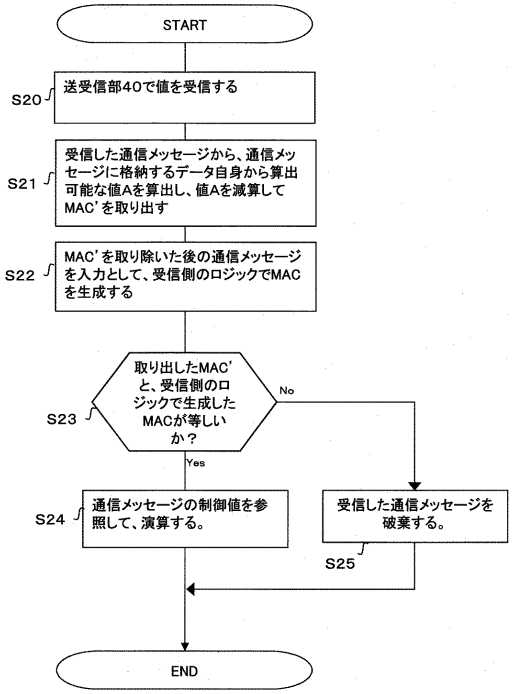
【図３】

【図3】



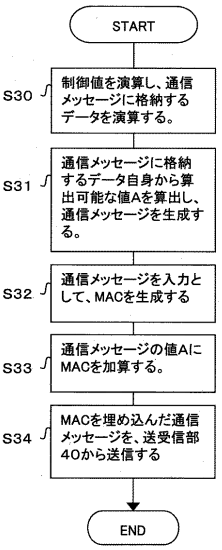
【図４】

【図4】



【図５】

【図5】



【図６】

【図6】