(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6541004号
(P6541004)

(45)発行日　令和1年7月10日(2019.7.10)　(24)登録日　令和1年6月21日(2019.6.21)

(51)Int.Cl.		F I		
H04L 12/28	(2006.01)	H04L	12/28	100A
H04L 12/40	(2006.01)	H04L	12/40	Z
H04L 1/00	(2006.01)	H04L	1/00	A

請求項の数 4　(全 16 頁)

(21)出願番号　特願2016-114829 (P2016-114829)
(22)出願日　平成28年6月8日 (2016.6.8)
(65)公開番号　特開2017-220836 (P2017-220836A)
(43)公開日　平成29年12月14日 (2017.12.14)
審査請求日　平成29年3月24日 (2017.3.24)

(73)特許権者　000005326
本田技研工業株式会社
東京都港区南青山二丁目１番１号
(74)代理人　100165179
弁理士　田▲崎▼　聡
(74)代理人　100126664
弁理士　鈴木　慎吾
(74)代理人　100154852
弁理士　酒井　太一
(74)代理人　100194087
弁理士　渡辺　伸一
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100146835
弁理士　佐伯　義文

最終頁に続く

(54)【発明の名称】通信システム

(57)【特許請求の範囲】
【請求項１】
誤り検出符号を付加したメッセージを送信する送信デバイスと、
受信した前記メッセージに含まれる情報であって前記誤り検出符号の生成演算の対象範囲の情報をもとに前記生成演算して得られる値と、前記付加された誤り検出符号が示す値との比較によって、異常を検出する受信デバイスと
を備える通信システムであって、
前記送信デバイスは、
前記生成演算して得られる値と前記付加された誤り検出符号が示す値とが不一致になるように、前記生成演算の対象範囲に含まれる情報であって制御量を含む指令値の情報を変更して、前記メッセージを生成し、
前記受信デバイスは、受信したメッセージについて、前記生成演算して得られる値と前記付加された誤り検出符号が示す値とが一致する場合に、異常を検出する、
通信システム。
【請求項２】
前記送信デバイスは、
前記生成演算の対象範囲に含まれる情報であって、前記生成演算に用いられる情報を示すビット列のうち少なくとも一部のビットについて、当該ビットを反転させることにより前記変更する、
請求項１記載の通信システム。

【請求項３】
前記送信デバイスは、
前記変更したメッセージを暗号化して、前記メッセージとする
請求項１又は請求項２記載の通信システム。
【請求項４】
前記送信デバイスと前記受信デバイスとは、
前記生成演算の対象範囲に含まれる情報のうち前記変更される部分である変更予定部分を示す情報を共有する
請求項１から請求項３のいずれか１項記載の通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信システムに関する。
【背景技術】
【０００２】
ネットワークを利用して各種制御対象を制御する通信システムでは、その信頼性を保つことが必要とされる。ネットワークを利用して車両を制御する技術が知られている（例えば、特許文献１参照。）。特許文献１には、自装置が、自装置から送信したことを示す識別情報を付与して通信メッセージを送信し、上記と同じ識別情報が附された通信メッセージを、自装置が受信した場合、その通信メッセージを不正なものと判断することが記載されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１４－１１６２１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１によれば、装置は、通信メッセージを選択して受信するように記憶しているが、自装置が受信すべき通信メッセージを特定する識別情報を、自装置が送信する際に用いる識別情報も含めることで上記の判断を実施する。これにより、自装置が本来受信すべき識別情報が附された通信メッセージの他に、少なくとも自装置が送信した通信メッセージ等も受信することになる。この技術では、通信メッセージを受信して処理する数が増大し、ネットワークにおける不正な状態を検出するための処理が煩雑になるという問題がある。
本発明は、このような事情を考慮してなされたものであり、より簡便な構成により、ネットワークにおける不正な状態を検出する通信システムを提供することを目的の一つとする。
【課題を解決するための手段】
【０００５】
請求項１記載の発明は、誤り検出符号を付加したメッセージを送信する送信デバイス（ＥＣＵ１０－１）と、受信した前記メッセージに含まれる情報であって前記誤り検出符号の生成演算の対象範囲の情報をもとに前記生成演算して得られる値と、前記付加された誤り検出符号が示す値との比較によって、異常を検出する受信デバイス（ＥＣＵ１０－２）とを備える通信システム（通信システム１）であって、前記送信デバイスは、前記生成演算して得られる値と前記付加された誤り検出符号が示す値とが不一致になるように、前記生成演算の対象範囲に含まれる情報であって制御量を含む指令値の情報を変更して、前記メッセージを生成し、前記受信デバイスは、受信したメッセージについて、前記生成演算して得られる値と前記付加された誤り検出符号が示す値とが一致する場合に、異常を検出する、通信システムである。

【０００６】
請求項２記載の発明における前記送信デバイスは、前記生成演算の対象範囲に含まれる情報であって、前記生成演算に用いられる情報を示すビット列のうち少なくとも一部のビットについて、当該ビットを反転させることにより前記変更する。
【０００７】
請求項３記載の発明における前記送信デバイスは、前記変更したメッセージを暗号化して、前記メッセージとする。
請求項４記載の発明における前記送信デバイスと前記受信デバイスとは、前記生成演算の対象範囲に含まれる情報のうち前記変更される部分である変更予定部分を示す情報を共有する。
【発明の効果】
【０００８】
請求項に記載の発明によれば、送信デバイスは、生成演算して得られる値とメッセージに付加された誤り検出符号が示す値とが不一致になるように、生成演算の対象範囲に含まれる情報の少なくとも一部を変更するかまたは前記生成演算して得られる値とは異なる値を前記誤り検出符号として付加して、そのメッセージを生成し、受信デバイスは、受信したメッセージについて、生成演算して得られる値と付加された誤り検出符号が示す値とが一致する場合に、異常を検出することにより、より簡便な構成により、ネットワークにおける不正な状態を検出する通信システムを提供することができる。
【図面の簡単な説明】
【０００９】
【図１】第１の実施形態の通信システム１の構成を示す図である。
【図２】本実施形態のＥＣＵ１０の構成例を示す図である。
【図３】本実施形態のＥＣＵ１０がバス２に送信するフレームＦの形式例である。
【図４】本実施形態の通信システムにおける送受信処理のデータフローを示す図である。
【図５】本実施形態の通信システムにおける送信処理の手順を示すフローチャートである。
【図６Ａ】本実施形態の通信システムにおける受信処理の手順を示すフローチャートである。
【図６Ｂ】本実施形態の第３変形例の受信処理の手順を示すフローチャートである。
【図７】第２の実施形態の通信システムにおける送受信処理のデータフローを示す図（その１）である。
【図８】本実施形態の通信システムにおける送受信処理のデータフローを示す図（その２）である。
【図９】本実施形態の通信システムにおける送信処理の手順を示すフローチャートである。
【図１０】本実施形態の通信システムにおける受信処理の手順を示すフローチャートである。
【発明を実施するための形態】
【００１０】
以下、図面を参照し、本発明の通信システムの実施形態について説明する。
【００１１】
（第１の実施形態）
図１は、本実施形態の通信システム１の構成を示す図である。通信システム１は、例えば車両に搭載される。通信システム１は、少なくとも車両内にネットワークＮＷを構成する。ネットワークＮＷでは、例えば、バス２を介してＣＡＮ（Controller Area Network）に基づく通信が行われる。
【００１２】
通信システム１は、バス２に接続されたＥＣＵ１０－１からＥＣＵ１０－３を備える。以下、ＥＣＵ１０－１からＥＣＵ１０－３を区別しない場合は、単にＥＣＵ１０と表記す

る。ＥＣＵ１０－１からＥＣＵ１０－３等の装置は、共通のバス２に接続されたものとして説明するが、不図示の中継装置等により互いに通信可能に接続された異なるバスに接続されていてもよい。

【００１３】

ＥＣＵ１０は、例えばエンジンを制御するエンジンＥＣＵや、シートベルトを制御するシートベルトＥＣＵ等である。ＥＣＵ１０は、自装置が所属するネットワークＮＷに送信されたフレームを受信する。以下、ネットワークＮＷに送信される各フレームのことをフレームＦという。フレームＦは、それぞれに附された識別子（以下、ＩＤという。）により識別される。ＥＣＵ１０は、自ＥＣＵ１０に係るフレームＦを識別するＩＤ（以下、登録ＩＤという）を記憶部２０（図２）に格納しておく。ＥＣＵ１０は、フレームＦを受信する際には、受信したフレームＦに附されたＩＤ（以下、受信ＩＤという）を参照して、登録ＩＤと同じ値の受信ＩＤが附されたフレームＦを抽出して取得する。

【００１４】

ネットワークＮＷには、検証装置等の外部装置５０が接続されるＤＬＣ３が設けられている。ＤＬＣ３は、外部装置５０と通信するための接続端子を有している。車両の点検時等にＤＬＣ３に接続される検証装置等は、バス２に接続されたＥＣＵ１０と通信して、通信システム１の状態を検査・検証する。車両の点検時等を除けば、ＤＬＣ３に検証装置等を接続することなく、通信システム１を機能させることができる。

【００１５】

図２は、ＥＣＵ１０の構成例を示す図である。ＥＣＵ１０は、例えば、記憶部２０と、制御部３０と、ＣＡＮコントローラ３６と、ＣＡＮトランシーバ３８とを備える。制御部３０は、例えば、ＣＰＵ（Central Processing Unit）等のプロセッサを有する。

【００１６】

記憶部２０は、例えば、ＲＯＭ（Read Only Memory）、ＥＥＰＲＯＭ（Electrically Erasable and Programmable Read Only Memory）、ＨＤＤ（Hard Disk Drive）等の不揮発性の記憶装置と、ＲＡＭ（Random Access Memory）、レジスタ等の揮発性の記憶装置によって実現される。記憶部２０は、アプリケーションプログラム２２や、通信制御プログラム２４等のプログラムと、上記のプログラムが参照する各種情報を格納する。また、記憶部２０は、送信バッファとして機能するＴＸＤ１記憶領域２６１とＴＸＤ２記憶領域２６２と、受信バッファとして機能するＲＸＤ記憶領域２６３とを含む一時記憶領域２６を有する。また、記憶部２０は、各種情報として、例えばネットワークＮＷを介して送受信するフレームＦのＩＤが格納されたＩＤテーブルを記憶する。例えば、フレームＦのＩＤは、送信元、宛先、フレームＦの種類等を示す情報を含む。より具体的には、ＩＤテーブルには、ＥＣＵ１０－１が受信すべきフレームＦのＩＤとＥＣＵ１０－１が送信すべきフレームＦのＩＤとが含まれる。

【００１７】

アプリケーションプログラム２２は、ＥＣＵ１０にそれぞれ割り当てられた情報処理を行うためのプログラムである。通信制御プログラム２４は、アプリケーションプログラム２２からの指示に応じてＣＡＮコントローラ３６を制御して通信処理を実施させるとともに、ＣＡＮコントローラ３６を介した通信に係る通信処理の結果を管理情報として取得するためのプログラムである。通信制御プログラム２４は、ＣＡＮコントローラ３６自身が実行する制御プログラムを含めて構成してもよく、或いは、ＣＡＮコントローラ３６自身が実行する制御プログラムをＣＡＮコントローラ３６が有する場合には、ＣＡＮコントローラ３６自身が実行する制御プログラムを含まずに構成してもよい。以下の説明では、通信制御プログラム２４は、ＣＡＮコントローラ３６の制御プログラムを含めて構成した場合を例示する。

【００１８】

制御部３０は、中央制御部３２と、通信制御部３４と、監視制御部３５とを備える。中央制御部３２は、アプリケーションプログラム２２を実行することにより機能し、ＥＣＵ１０に与えられた制御を実行する。

【００１９】
通信制御部３４は、通信制御プログラム２４を実行することにより機能し、中央制御部３２からの制御を受けＥＣＵ１０の通信処理を実行する。
【００２０】
例えば、通信制御部３４は、送信時には、記憶部２０の送信バッファに格納されたユーザデータを、ＣＡＮトランシーバ３８を介して送信する。その際、通信制御部３４は、自ＥＣＵ１０が送信するものであることを示すＩＤを、ＣＡＮトランシーバ３８によって生成されるフレームＦに付与して送信するようにＣＡＮトランシーバ３８を制御する。ユーザデータを送信する際に実施する処理の詳細については、後述する。
【００２１】
また、通信制御部３４は、受信時には、ＣＡＮトランシーバ３８を介して受信されたフレームＦの受信ＩＤとＩＤテーブルに格納された登録ＩＤとを参照し、受信されたフレームＦに関して自装置の中央制御部３２が使用する情報が含まれたフレームＦであるか否かを判定する。例えば、ＥＣＵ１０－１のＩＤテーブルに格納された登録ＩＤには、ＥＣＵ１０－１が受信すべきフレームＦのＩＤ（登録受信ＩＤ）とＥＣＵ１０－１が送信すべきフレームＦのＩＤ（登録送信ＩＤ）とが含まれる。通信制御部３４は、上記の判定を実施する際に、例えば、ＩＤテーブルにおける登録受信ＩＤを利用する。
【００２２】
通信制御部３４は、自ＥＣＵ１０が使用する情報がフレームＦに含まれる場合、フレームＦに含まれた情報を取得し、記憶部２０の一時記憶領域２６に格納する。一方、通信制御部３４は、自ＥＣＵ１０が使用する情報がフレームＦに含まれていない場合、例えば、フレームＦに含まれた情報を破棄するように制御する。
【００２３】
ＣＡＮトランシーバ３８を介して受信されたフレームＦには、送信側のＥＣＵ１０からの通信メッセージが含まれる場合がある。通信制御部３４は、フレームＦに対する誤り検出の結果を通して、通信システム１における不正な状態が生じていることを検出する。通信システム１における不正な状態の検出方法の詳細については後述する。
【００２４】
監視制御部３５は、通信制御部３４によって上記の不正な状態が生じていることが検出された場合、ＥＣＵ１０におけるフェイルセーフ処理を実施するように制御する。ＥＣＵ１０におけるフェイルセーフ処理とは、不正な状態を検知したＥＣＵ１０が車両の走行等に対する影響を低減させて、車両の制御状態を安全な状態を維持するために実施する処理のことである。
【００２５】
ＥＣＵ１０におけるフェイルセーフ処理として、例えば、監視制御部３５は、通信制御部３４が不正な状態を検出したとき以降の少なくとも一定時間の間においては、少なくとも新たにフレームＦを受信しないように制御する。通信制御部３４が受信しないようにするフレームＦは、上記の不正な状態が生じたことを検出したフレームＦに附されていた送信元を示すＩＤが附されたフレームＦに限定してもよい。上記のように、ＥＣＵ１０は、フェイルセーフ処理により、受信するフレームＦを制限することで、不正な状態を発生させた可能性が有る不正な装置や故障したＥＣＵ１０からの情報の受信を制限できる。なお、通信制御部３４が上記の不正な状態を検出する処理の詳細については、後述する。
【００２６】
通信制御部３４は、ＣＡＮコントローラ３６にＣＡＮトランシーバ３８からフレームＦを送信させる。
【００２７】
ＣＡＮコントローラ３６は、ＣＡＮトランシーバ３８を介して、バス２との間で種々のフレームＦを送受信する。また、ＣＡＮコントローラ３６は、ＣＡＮトランシーバ３８からフレームＦを受信する際には、ＣＡＮトランシーバ３８から供給される受信信号からフレームＦを抽出して、抽出したフレームＦを一時記憶領域２６の受信バッファに格納する

。ＣＡＮコントローラ３６は、フレームＦにおける誤り検出処理を実行する誤り検出処理部３６１を含む。誤り検出処理部は、フレームＦを送信する際には、フレームＦの一部に含めて送信する所定の誤り検出符号を生成する。誤り検出処理部は、フレームＦを受信する際には、フレームＦの一部に含まれた誤り検出情報の検出の結果を出力する。

【００２８】

ＣＡＮトランシーバ３８は、フレームＦを送信する送信部、またはフレームＦを受信する受信部として機能する。ＣＡＮトランシーバ３８は、バス２にフレームＦを送信する際には、ＣＡＮコントローラ３６から取得した送信信号の論理状態に応じた差動電圧を生成してバス２に出力する。また、ＣＡＮトランシーバ３８は、バス２からフレームＦを取得する際には、バス２の差動電圧から所定の電圧範囲に含まれるように整形した受信信号を生成して、ＣＡＮコントローラ３６に送信する。ＣＡＮコントローラ３６は、ＣＡＮトランシーバ３８から出力される信号からフレームＦを抽出して記憶部２０に格納する。

【００２９】

以上に示すように、各ＥＣＵ１０は、上記の通信処理に関する共通の構成を有する。

【００３０】

図３は、ＥＣＵ１０がバス２に送信するフレームＦの形式例である。図３（ａ）に、１回の送信において送信されるフレームＦを示す。フレームＦは、フレームＦの開始を表すスタートオブフレーム（ＳＯＦ）、フレームＦのＩＤ及びフレームＦとリモートフレームを識別するためのリモートトランスミッションリクエスト（ＲＴＲ）を含むアービトレーションフィールド、フレームＦのバイト数等を表すコントロールフィールド、転送するフレームＦの実体であるデータフィールド、フレームＦの誤りを検出するための誤り検出符号（ＣＲＣ）を付加するＣＲＣフィールド、正しいフレームＦを受信したユニットからの通知（ＡＣＫ）を受けるＡＣＫスロット及びＡＣＫデリミタ、フレームＦの終了を表すエンドオブフレーム（ＥＯＦ）等を含む。

【００３１】

ＥＣＵ１０は、フレームＦのデータフィールド内の所定の位置にユーザデータを割り付けて通信する。ＥＣＵ１０は、ユーザデータの他に、ユーザデータの誤りを検査するための誤り検査用情報等を含めて、データフィールドに割り付けてもよい。ユーザデータの誤りを検査するための誤り検査用情報等には、例えば、単一のフレームＦ内のユーザデータまたは複数のフレームＦを纏めたユーザデータの誤りを検査するための誤り検査用情報等を含めてもよい。ユーザデータに基づいて生成される誤り検査符号は、誤り検査用情報の一例である。

【００３２】

図３（ｂ）に、誤り検査用情報をデータフィールドに割り付けた一例を示す。誤り検査用情報は、例えば、ＳＵＭ値（check sum）、パリティ、ＣＲＣ（Cyclic Redundancy Check）等の誤り検出符号により構成される。

【００３３】

なお、ユーザデータと誤り検査用情報とを、データフィールド内に割り付ける位置は任意であり、例えば、予め決定されているものとする。以下の説明において、ユーザデータと、上記の誤り検査用情報とを割り付けたフレームＦを通信メッセージという。なお、フレームＦに割り付けられたユーザデータには、その一部又は全部のビットの論理が反転されたものも含まれる。

【００３４】

図４から図６を参照して、通信システムにおける不正な状態の検出処理について説明する。図４から図６に示す処理は、本実施形態におけるネットワークＮＷにおいて特段の不正な行為（不正行為ともいう。）が実施されない場合を示し、送信側の装置と受信側の装置が連携して機能することを示すものである。なお、ネットワークＮＷにおいて不正行為が実施されている場合には、受信側の装置が、その行為に対する検出処理を実施することになる。

【００３５】

図４は、通信システムにおける送受信処理のデータフローを示す図であり、図５は、通信システムにおける送信処理の手順を示すフローチャートである。図６Ａと図６Ｂは、通信システムにおける受信処理の手順を示すフローチャートである。以下の説明においてＥＣＵ１０－１を送信側の装置（送信デバイス）とし、ＥＣＵ１０－２を受信側の装置（受信デバイス）とする場合を例示して説明する。なお、図６Ｂについては後述する。

【００３６】

（データの送信）

通信システム１は、ＥＣＵ１０間で誤り検出符号を用いて通信を実施して、受信した通信メッセージについて誤り検出符号を用いて検証する。その対象とする通信は、通信システム１における一部又は全部のＥＣＵ１０間で実施されるものとする。通信システム１は、ユーザデータ（以下、送信データＴＸＤ１という。）に基づいて誤り検出符号（以下、ＥＣＣ１という。）を算出するための生成演算式（以下、生成演算式１という。）は、予め定められており、ＥＣＣ１を用いて通信するＥＣＵ１０間で予め共有される。例えば、ＥＣＵ１０－１とＥＣＵ１０－２とにおけるＣＡＮコントローラ３６は、生成演算式１による演算を可能とする。生成演算式１の対象とするデータは、送信データＴＸＤ１を含む。例えば、生成演算式１は、ＳＵＭ値、パリティ、ＣＲＣなどを算出するものであってもよい。

【００３７】

例えば、生成演算式１として、ＳＵＭ値、パリティ、ＣＲＣなどを生成する式を適用するならば、生成されるＥＣＣ１のデータ量は、演算の対象のデータ量（例えば、送信データＴＸＤ）に依存しない固定長にすることができ、更に演算の対象のデータ量よりも少ないデータ量にできる。例えば、送信データＴＸＤとして、逐次大きさが変化する制御量等を含む指令値、又は、送信時の時刻を示す時刻情報を含まれるように構成することにより、生成されるＥＣＣ１は逐次変化するものになる。上記の時刻情報は、送信データＴＸＤ１に含まれるデータの検出時刻、それを送信する送信時刻、送信に関連する処理の完了時刻など、送信データの送信に関する処理に伴う時刻とする。このようなＥＣＣ１は、送信データＴＸＤ１に基づいた擬似乱数とみなすことができる。

【００３８】

以下、図５を参照し、ＥＣＵ１０－１が通信メッセージをＥＣＵ１０－２宛に送信する際の手順を順に説明する。

【００３９】

まず、ＥＣＵ１０－１の制御部３０は、通信メッセージの基となる送信データＴＸＤ１を生成し（Ｓａ１２）、一時記憶領域２６内のＴＸＤ１記憶領域２６１に格納する。

【００４０】

次に、ＥＣＵ１０－１のＣＡＮコントローラ３６は、ＴＸＤ１記憶領域２６１に格納された送信データＴＸＤ１に基づいて、生成演算式１に基づいた生成演算の実施によりＥＣＣ１を算出する（Ｓａ１４）。この生成演算式１は、受信した通信メッセージの信ぴょう性を検証するための情報に利用する。

【００４１】

次に、ＥＣＵ１０－１の制御部３０（通信制御部３４）は、送信データＴＸＤ１に対し、所定のビットパターンで指定されるビットの論理を反転して、その結果の送信データＴＸＤ２を得て（Ｓａ１６）、一時記憶領域２６内のＴＸＤ２記憶領域２６２に格納する。例えば、所定のビットパターンによって、対象とするビットの位置が決定される。対象とするビットは、生成演算式１の対象範囲内の任意の位置の少なくとも１ビットが含まれていればよい。なお、送信データＴＸＤ２は、送信データＴＸＤ１と同様にＥＣＣ１に対応付けられるものになる。

【００４２】

次に、ＥＣＵ１０－１のＣＡＮコントローラ３６は、ＴＸＤ２記憶領域２６２に格納された送信データＴＸＤ２とＥＣＣ１を、フレームＦ内の所定の位置に格納して送信する（Ｓａ１８）。なお、フレームＦ内の所定の位置は、ＥＣＵ１０－１とＥＣＵ１０－２で予

め共有されるものである。通信システム１におけるフレームＦ内の所定の位置として、送信データＴＸＤ２とＥＣＣ１を、例えば、フレームＦのデータフィールド内に設けてもよい。ＥＣＵ１０－１は、送信データＴＸＤ２とＥＣＣ１の対応関係を保持して、共通するフレームＦに割り付けて送信する。

【００４３】

（データの受信）

【００４４】

以下、図６Ａを参照し、ＥＣＵ１０－２が通信メッセージを受信する際の手順を順に説明する。

【００４５】

ＥＣＵ１０－２は、フレームＦを受信して、受信したフレームＦ（受信フレーム）から、受信データＲＸＤとＥＣＣ１を抽出する（Ｓａ３２）。例えば、ＥＣＵ１０－２のＣＡＮトランシーバ３８は、受信データＲＸＤとＥＣＣ１を抽出し、記憶部２０のＲＸＤ記憶領域２６３に書き込む。

【００４６】

次に、ＥＣＵ１０－２は、受信データＲＸＤに対して、上記の生成演算式１を用いてＲＸＤ＿ＥＣＣ１を算出する（Ｓａ３４）。ＲＸＤ＿ＥＣＣ１は、送信側で算出されたＥＣＣ１と同じ長さの固定長のデータである。例えば、ＥＣＵ１０－２のＣＡＮトランシーバ３８は、受信データＲＸＤに基づいてＲＸＤ＿ＥＣＣ１を算出する。

【００４７】

次に、ＥＣＵ１０－２の制御部３０は、算出したＲＸＤ＿ＥＣＣ１と、受信フレームから抽出したＥＣＣ１とを比較する（Ｓａ３６）。

【００４８】

比較の結果、一致していなかった場合、ＥＣＵ１０－２の制御部３０は、受信フレームに異常がないと判定し（Ｓａ４２）、受信データＲＸＤに基づいた受信処理を実施する（Ｓａ４４）。

【００４９】

一方、比較の結果、一致した場合、ＥＣＵ１０－２の制御部３０は、受信フレームに異常があると判定し（Ｓａ４６）、判定の結果に基づいて異常状態を通知する（Ｓａ４８）。

【００５０】

上記の手順に従う処理を実施することにより、ＥＣＵ１０－２は、受信フレームから、ネットワークにおける不正な状態の有無を検出する。

【００５１】

上記の第１の実施形態によれば、ＥＣＵ１０－１は、ＥＣＣ１（誤り検出符号）を付加した通信メッセージを送信する。ＥＣＵ１０－２は、受信した通信メッセージに含まれる情報であって誤り検出符号（ＲＸＤ＿ＥＣＣ１）の生成演算の対象範囲の情報をもとに、生成演算して得られるＲＸＤ＿ＥＣＣ１の値と、付加されたＥＣＣ１が示す値との比較によって、異常を検出する。このようなＥＣＵ１０－１は、ＲＸＤ＿ＥＣＣ１とＥＣＣ１が示す値が不一致になるように、生成演算の対象範囲に含まれる情報の少なくとも一部を変更して、通信メッセージを生成する。ＥＣＵ１０－２は、受信した通信メッセージについて、ＲＸＤ＿ＥＣＣ１とＥＣＣ１が示す値が一致する場合に、異常を検出する。

【００５２】

通信システム１は、通信メッセージを選択して受信するが、上記の検出方法を採ることにより、自ＥＣＵ１０が送信する際に用いるＩＤを含む通信メッセージ、つまり自ＥＣＵ１０が送信した通信メッセージ等を受信する必要はなく、受信する通信メッセージの個数の増大を招くことはない。これにより、通信システム１は、ネットワークにおける不正な状態を検出するための処理を煩雑にすることなく、より簡便な構成により、ネットワークＮＷにおける不正な状態を検出することができる。

【００５３】

また、ＥＣＵ１０－１は、生成演算の対象範囲に含まれる情報であって、生成演算に用いられる情報を示すビット列のうち少なくとも一部のビットについて、当該ビットを反転させることにより、ＲＸＤ＿ＥＣＣ１とＥＣＣ１が示す値が不一致になるように変更してもよい。

【００５４】

（第１の実施形態の第１変形例）

第１の実施形態の第１変形例について説明する。第１の実施形態では、送信データＴＸＤ１において、所定のビットパターンで指定されたビットの論理を反転して送信データＴＸＤ２を得るものとして説明したが、これに代えて、本変形例では送信データＴＸＤ１において論理の反転を実施するビットは、検証用のビットとして利用可能な送信データＴＸＤ１内の未使用ビット又は未定義ビットを利用してもよい。ＥＣＣ１の生成演算において、バイト単位で処理をする場合、送信データＴＸＤ１がバイトの整数倍ではなかったり、送信データＴＸＤ１のビット列の途中に未使用ビット又は未定義ビットが発生したりすることがある。上記の本変形例によれば、このような未使用ビット又は未定義ビットを利用することにより、送信データＴＸＤ１のデータ量を増やすことなく、実施形態と同様の効果を奏することができ、更に、送信データＴＸＤ１として有意なデータの論理に影響することなく、上記のビットの反転を利用することができる。

【００５５】

（第１の実施形態の第２変形例）

第１の実施形態の第２変形例について説明する。第１の実施形態では、送信データＴＸＤ２とＥＣＣ１を、フレームＦのデータフィールド内の所定の位置に格納する場合について説明したが、これに代えて、本変形例ではフレームＦのデータフィールド以外にＥＣＣ１を割り付ける場合を例示する。

【００５６】

例えば、ＥＣＵ１０－１は、送信データＴＸＤ２をフレームＦのデータフィールド内に、ＥＣＣ１をフレームＦのＣＲＣフィールド内にそれぞれ割り付ける。この場合、ＥＣＣ１は、ＣＡＮ仕様のＣＲＣを算出する生成演算式１により算出される。上記の本変形例によれば、第１の実施形態と同様の効果を奏する他に、フレームＦのデータフィールド内で伝送可能なデータ量が、本変形例の方が多くなる。

【００５７】

（第１の実施形態の第３変形例）

第１の実施形態の第３の変形例について説明する。第１の実施形態では、ＥＣＵ１０－２は、受信した通信メッセージについて、生成演算して得られるＲＸＤ＿ＥＣＣ１の値と、ＥＣＵ１０－２によって付加された誤り検出符号（ＥＣＣ１）が示す値とが一致する場合に、異常を検出することとした。本変形例のＥＣＵ１０－２はこれに加えて、前記生成演算して得られるＲＸＤ　ＥＣＣ１の値と前記付加された誤り検出符号（ＥＣＣ１）が示す値とが、送信デバイス（ＥＣＵ１０－１）による変更操作の影響を超えて異なる場合にも、異常を検出する。ここで、「送信デバイスによる変更操作」とは、送信デバイス（ＥＣＵ１０－１）が、受信デバイスによりＲＸＤから生成演算して得られるＲＸＤ　ＥＣＣ１の値と付加された誤り検出符号（ＥＣＣ１）が示す値とが不一致になるように行う操作であって、生成演算の対象範囲に含まれる情報の少なくとも一部を変更する操作または生成演算して得られるＲＸＤ　ＥＣＣ１の値とは異なる値を誤り検出符号（ＥＣＣ１）として付加する操作のことをいう。

【００５８】

例えば、ＥＣＵ１０－１が、生成演算の対象範囲（ＴＸＤ１）に含まれる情報の少なくとも一部を変更しＴＸＤ２を生成する操作を、図４と図５に示すＳａ１６における処理において、上記の変更操作として行う場合について説明する。ＥＣＵ１０－１とＥＣＵ１０－２とは、予め、生成演算の対象範囲（ＴＸＤ１）に含まれる情報のうち、Ｓａ１６の処理により変更される部分（変更予定部分）を示す情報を共有している。例えば、変更予定部分を示す情報は、当該部分の位置を示す情報や当該部分を特定可能な識別情報であって

もよい。図６Ｂに示すように、前述の図６Ａと同様に処理を進め、ＥＣＵ１０－２は、受信したメッセージ（フレームＦ）から生成演算して得られるＲＸＤ　ＥＣＣ１の値と、受信フレームから抽出したＥＣＣ１とを比較する（Ｓａ３６）。

【００５９】

図６Ｂに示す本変形例においては、上記Ｓａ３６における比較の結果、一致していなかった場合に、ＥＣＵ１０－２の制御部３０は、その不一致が、生成演算の対象範囲に含まれる情報のどの部分が変更されたことに基づくものかを推定し（Ｓａ４１１）、変更された部分（変更部分）を特定する（Ｓａ４１２）。ＥＣＵ１０－２の制御部３０は、特定した変更部分と、予め共有されたルールで定められた変更予定部分とが異なるか否かを判定する（Ｓａ４１３）。

【００６０】

次に、Ｓａ４１３において一致すると判定した場合、ＥＣＵ１０－２の制御部３０は、受信フレームに異常がないと判定し（Ｓａ４２）、受信データＲＸＤに基づいた受信処理を実施する（Ｓａ４４）。

一方、Ｓａ３６における比較の結果、一致した場合、又は、Ｓａ４１３において異なると判定した場合に、ＥＣＵ１０－２の制御部３０は、受信フレームに異常があることを検出し（Ｓａ４６）、異常状態を通知する（Ｓａ４８）。

【００６１】

上記のように、ＥＣＵ１０－１が、受信データＲＸＤに基づいて生成演算して得られるＲＸＤ　ＥＣＣ１の値と、それに付加されていたＥＣＣ１Ａが示す値とが、送信デバイス（ＥＣＵ１０－１）による変更操作の影響を超えて異なる場合に、ＥＣＵ１０－２は、通信による異常を検出することができる。

【００６２】

（第１の実施形態の第４変形例）

第１の実施形態の第４変形例について説明する。第１の実施形態では、ＥＣＵ１０－１は、ＲＸＤ＿ＥＣＣ１とＥＣＣ１が示す値が不一致になるように、生成演算の対象範囲に含まれる情報の少なくとも一部を変更して、通信メッセージを生成するものとして説明した。本変形例のＥＣＵ１０－１は、これに代えて、ＲＸＤ＿ＥＣＣ１とＥＣＣ１が示す値が不一致になるように、ＲＸＤ＿ＥＣＣ１として得られる値とは異なる値をＥＣＣ１として付加して、通信メッセージを生成するものを例示する。

【００６３】

例えば、ＥＣＵ１０－１が、ＲＸＤ＿ＥＣＣ１として得られる値とは異なる値の誤り検出符号を付加した通信メッセージを送信した場合について説明する。その場合の一例として、ＥＣＵ１０－１が、送信データＴＸＤ１から生成されたＥＣＣ１を付加して通信メッセージを送信する前に、送信データＴＸＤ１から生成されたＥＣＣ１と異なる値のＥＣＣ１Ａ（誤り検出符号）に変更して、ＥＣＣ１としてＥＣＣ１Ａを付加した通信メッセージを送信する場合などが挙げられる。この場合、ＥＣＵ１０－２は、ＲＸＤ＿ＥＣＣ１とＥＣＣ１が示す値が不一致になることに変わりはない。

上記の変形例によれば、ＥＣＵ１０－１が、ＲＸＤ＿ＥＣＣ１として得られる値とは異なる値の誤り検出符号を付加した通信メッセージを送信する場合においても、第１の実施形態と同様の効果を奏するものになる。

【００６４】

さらに、本変形例のＥＣＵ１０－２は、これに加えて、受信データＲＸＤに基づいて生成演算して得られるＲＸＤ　ＥＣＣ１の値と、それに付加されていた誤り検出符号（ＥＣＣ１）が示す値とが、送信デバイス（ＥＣＵ１０－１）による変更操作の影響を超えて異なる場合にも、異常を検出するようにしてもよい。例えば、ＥＣＵ１０－１が、生成演算して得られるＲＸＤ　ＥＣＣ１の値とは異なる値のＥＣＣ１Ａを誤り検出符号として付加する操作を、変更操作として行う場合について説明する。ＥＣＵ１０－１とＥＣＵ１０－２とは、予め、どの値をどの値に置き換えて誤り検出符号に付加するのかを共有している。受信デバイス（ＥＣＵ１０－２）は、受信したメッセージから生成演算して得られるＲ

ＸＤ　ＥＣＣ１の値と付加された誤り検出符号（ＥＣＣ１Ａ）が示す値とが不一致の場合に、その不一致が、その誤り検出符号（ＥＣＣ１Ａ）がどの値から置き換えられたことに基づくものかを推定する。受信デバイス（ＥＣＵ１０－２）は、当該推定によって特定した変換前値と、予め共有されたルールから定められる変換前値とが異なっている場合に、通信の異常を検出する。

【００６５】

（第２の実施形態）

第２の実施形態について説明する。第１の実施形態では、送信データＴＸＤ２とＥＣＣ１を、フレームＦ内に格納して送信する場合について説明したが、これに代えて、本変形例では、ＥＣＵ１０－１が送信データＴＸＤ２とＥＣＣ１を秘匿して送信する場合を例示する。以下、相違点を中心に説明する。

【００６６】

第１の実施形態の構成では、ＥＣＵ１０－１は、送信データＴＸＤ２とＥＣＣ１とを暗号化することなく、そのままフレームＦに割り付けて送信しており、上記の位置の情報を有する受信モジュールは、送信された通信メッセージを傍受することが可能である。

【００６７】

第１の実施形態の構成において、送信データＴＸＤ２とＥＣＣ１をフレームＦに割り付ける位置の情報を秘匿することで、その位置の情報を有していない受信デバイス（受信装置）は、受信フレームから受信データＲＸＤ２とＥＣＣ２とを抽出することができないようにすることができる。このように、第１の実施形態の構成では、位置の情報が公開されないという条件付きで、送信データＴＸＤ２とＥＣＣ１を秘匿することが可能である。

【００６８】

そこで、本実施形態では、図７から図１０に示すように、送信データＴＸＤ２とＥＣＣ１とがフレームＦに割り付けられる位置の情報を有しているだけでは傍受することができないように構成する。つまり、送信モジュールが送信データＴＸＤ２とＥＣＣ１とを秘匿して送信するように構成し、とその処理について説明する。図７から図９に示す処理は、本実施形態におけるネットワークＮＷにおいて特段の不正な行為（不正行為ともいう。）が実施されない場合を示すものである。

【００６９】

図７と図８は、通信システムにおける送受信処理のデータフローを示す図であり、図９は、通信システムにおける送信処理の手順を示すフローチャートである。図１０は、通信システムにおける受信処理の手順を示すフローチャートである。以下の説明においてＥＣＵ１０－１が送信データＴＸＤ２とＥＣＣ１を秘匿して送信する暗号化手法を例示する。

【００７０】

（第１の手法）送信データＴＸＤ２とＥＣＣ１とを纏めて暗号化する。

送信データＴＸＤ２とＥＣＣ１とを纏めて暗号化することで、暗号化せずに送信される情報が無くなるため、秘匿性を確保できる。

【００７１】

（第２の手法）送信データＴＸＤ２を暗号化し、ＥＣＣ１は暗号化しない。

送信データＴＸＤ２のみを暗号化することで秘匿性を確保する。ＥＣＣ１は暗号化せずに送信されるが、ＥＣＣ１の情報から送信データＴＸＤ１も送信データＴＸＤ２も生成することができない。送信データＴＸＤ２の秘匿性が確保されれば、送信データＴＸＤ１とＥＣＣ１のデータの組としての秘匿性も確保できる。

【００７２】

上記のとおり、本実施形態の通信システム１では、少なくとも送信データＴＸＤ２を暗号化することで、送信データＴＸＤ２とＥＣＣ１のデータの組としての秘匿性を確保する。暗号化の具体的な方法としては、既知の暗号化手法の何れかを利用することができる。以下、第１の手法を例示して、その詳細を説明する。

【００７３】

（公開鍵の通知）

本実施形態におけるＥＣＵ１０－１の監視制御部３５は、暗号化時に用いる秘密鍵と対になる公開鍵を生成する。ＥＣＵ１０－１の監視制御部３５は、ＥＣＵ１０－２宛に、受信データＲＸＤに対する認証処理に用いる公開鍵を通知する。ＥＣＵ１０－２は、受信データＲＸＤに対する認証処理に用いる公開鍵を受信して保持する。

【００７４】

（データの送信）

まず、ＥＣＵ１０－１の制御部３０は、通信メッセージの基となる送信データＴＸＤ１を生成する（Ｓａ１２）。

【００７５】

次に、ＥＣＵ１０－１の制御部３０は、送信データＴＸＤ１に基づいて、生成演算式１に基づいた生成演算の実施によりＥＣＣ１を算出する（Ｓａ１４）。

【００７６】

次に、ＥＣＵ１０－１の制御部３０は、送信データＴＸＤ１に対し、所定のビットパターンで指定されたビットの論理を反転して送信データＴＸＤ２を得る（Ｓａ１６）。

【００７７】

次に、ＥＣＵ１０－１の監視制御部３５は、秘密鍵を用いて、送信データＴＸＤ２とＥＣＣ１の組に対する暗号化処理を実施する（Ｓａ２０）。

【００７８】

次に、ＥＣＵ１０－１の監視制御部３５は、暗号化処理された送信データＴＸＤ２とＥＣＣ１の組を、フレームＦのデータフィールド内の所定の位置に格納して、送信する（Ｓａ２２）。

【００７９】

（データの受信）

次に、ＥＣＵ１０－２のＣＡＮコントローラ３６は、フレームＦを受信して、受信したフレーム（受信フレーム）から、暗号化処理された送信データＴＸＤ２とＥＣＣ１の組を抽出する（Ｓａ３０）。

【００８０】

次に、ＥＣＵ１０－２の監視制御部３５は、公開鍵を用いて、抽出した送信データＴＸＤ２とＥＣＣ１の組に対する復号化処理を実施して、受信データＲＸＤとＥＣＣ１を取得する（Ｓａ３２Ａ）。

【００８１】

ＥＣＵ１０－２の監視制御部３５は、受信データＲＸＤに対して、上記の生成演算式１を用いてＲＸＤ＿ＥＣＣ１を算出する（Ｓａ３４）。Ｓａ３６以降の処理は、第１の実施形態と同様である。

【００８２】

上記の実施形態によれば、第１の実施形態と同様の効果を奏するものであるのに加えて、ＥＣＵ１０－１は、特定のビットの論理を変更した通信メッセージを暗号化して、ＥＣＵ１０－２宛に送信する通信メッセージとすることにより、ＥＣＵ１０間の通信を秘匿することができる。

【００８３】

上記の各変形例によれば、様々な構成や方式のネットワークＮＷを用いた場合においても、上記の実施形態と同様の効果を奏することができる。上記の実施形態では、通信プロトコルの一例としてＣＡＮを例示して説明したが、例えば、ＬＡＮ（Local Area Network）等で利用されるＥｔｈｅｒｎｅｔ（登録商標）を通信プロトコルと利用する場合にも適用することができる。この場合、例えば、ＥｔｈｅｒｎｅｔのＭＡＣ（media access control）フレームを上記のフレームＦとし、ＭＡＣフレームのペイロードに、上記の送信データＴＸＤ２を割り当てて、ＭＡＣフレームのＣＲＣに上記のＥＣＣ１を割り当ててもよい。

【００８４】

以上説明した少なくともひとつの実施形態によれば、通信システム１は、誤り検出符号

（ＥＣＣ１）を付加した通信メッセージを送信する送信デバイス（ＥＣＵ１０－１）と、受信した通信メッセージに含まれる情報であって誤り検出符号の生成演算の対象範囲の情報（送信データＴＸＤ１）をもとに生成演算して得られる値（ＲＸＤ＿ＥＣＣ１）と、前記付加された誤り検出符号が示す値（ＥＣＣ１）との比較によって、異常を検出する受信デバイス（ＥＣＵ１０－２）とを備える。送信デバイスは、前記生成演算して得られる値と前記付加された誤り検出符号が示す値とが不一致になるように、前記生成演算の対象範囲に含まれる情報の少なくとも一部を変更して、通信メッセージを生成する。前記受信デバイスは、受信した通信メッセージについて、前記生成演算して得られる値と前記付加された誤り検出符号が示す値とが一致する場合に、異常を検出することにより、より簡便な構成により、ネットワークにおける不正な状態を検出することができる。

【００８５】

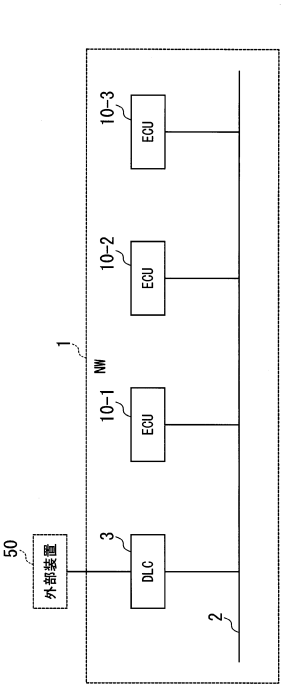
以上、本発明を実施するための形態について実施形態を用いて説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々の変形及び置換を加えることができる。

【符号の説明】

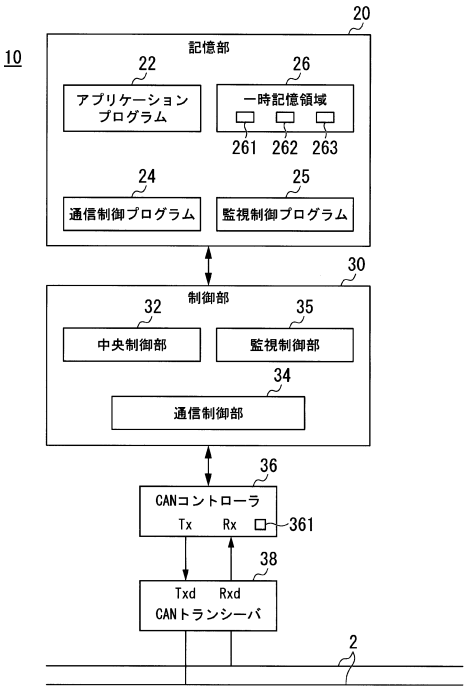
【００８６】

１‥通信システム、２…バス、３…ＤＬＣ、１０…ＥＣＵ、１０－１…ＥＣＵ（送信デバイス）、１０－２…ＥＣＵ（受信デバイス）、１０－３…ＥＣＵ、２０…記憶部、３０…制御部、５０…外部装置。

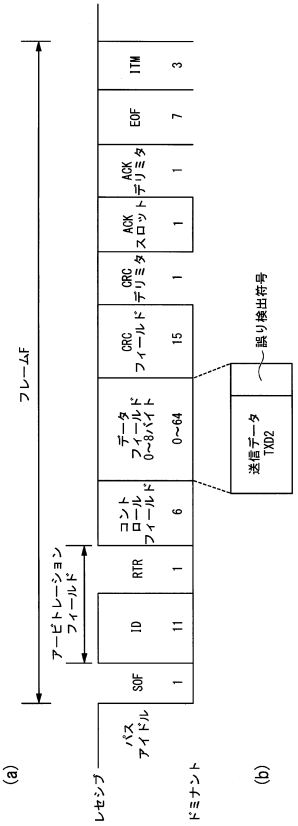
【図１】



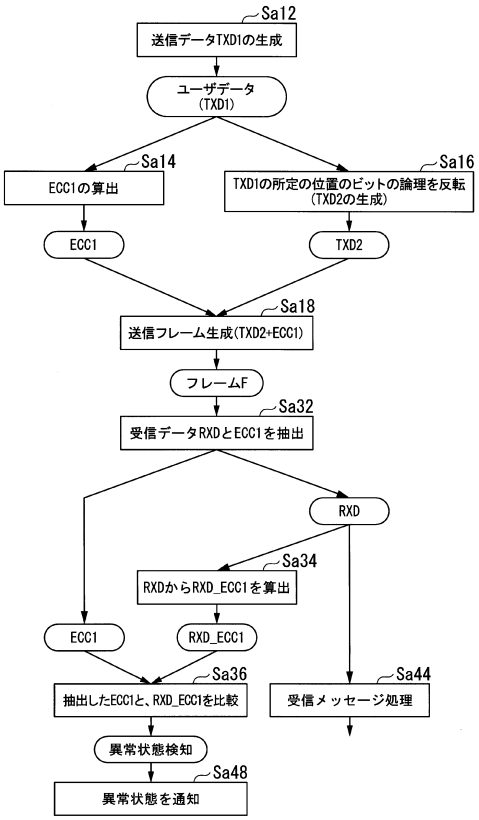
【図２】



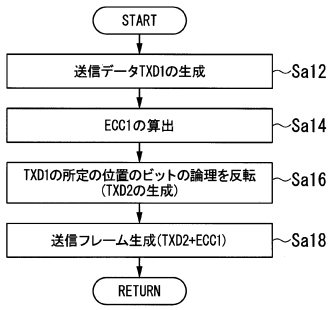
【図３】



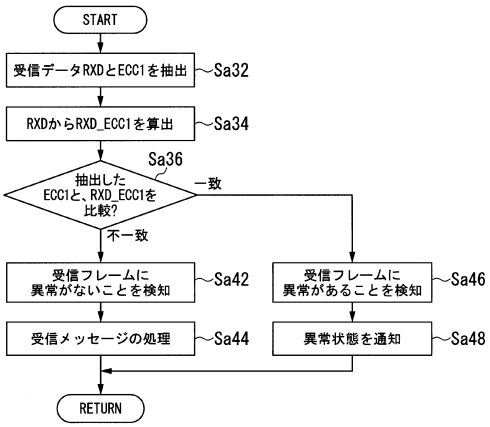
【図４】



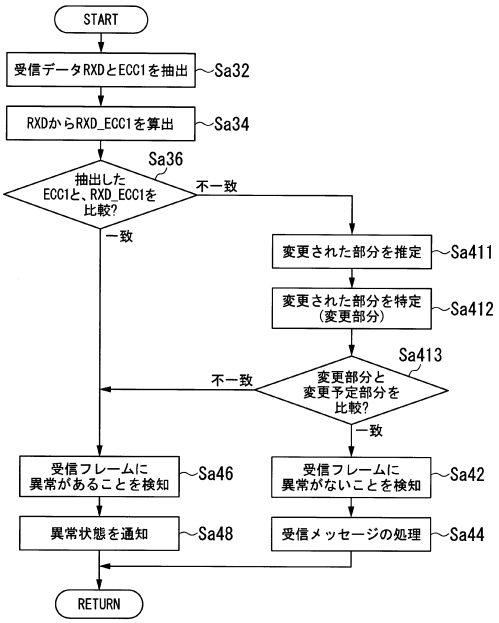
【図５】



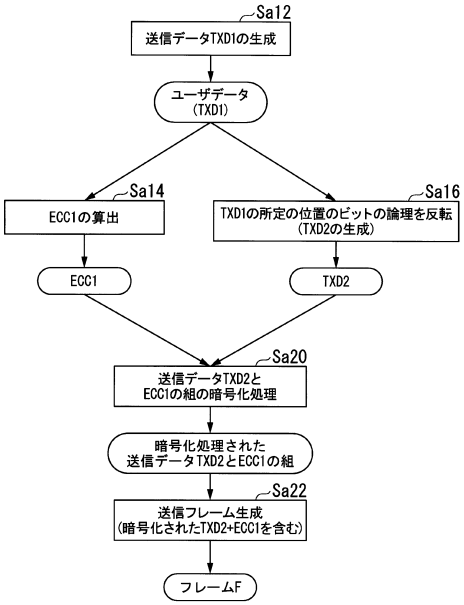
【図６Ａ】



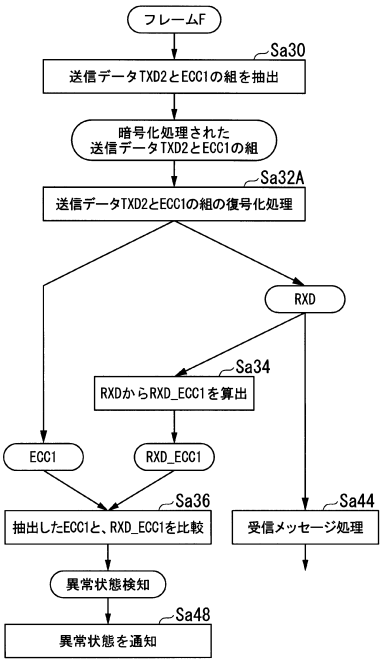
【図６Ｂ】



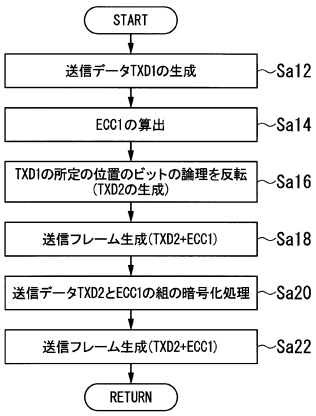
【図７】


Sa12
送信データTXD1の生成
ユーザデータ
(TXD1)
Sa14
ECC1の算出
Sa16
TXD1の所定の位置のビットの論理を反転
(TXD2の生成)
ECC1
TXD2
Sa20
送信データTXD2と
ECC1の組の暗号化処理
暗号化処理された
送信データTXD2とECC1の組
Sa22
送信フレーム生成
(暗号化されたTXD2+ECC1を含む)
フレームF

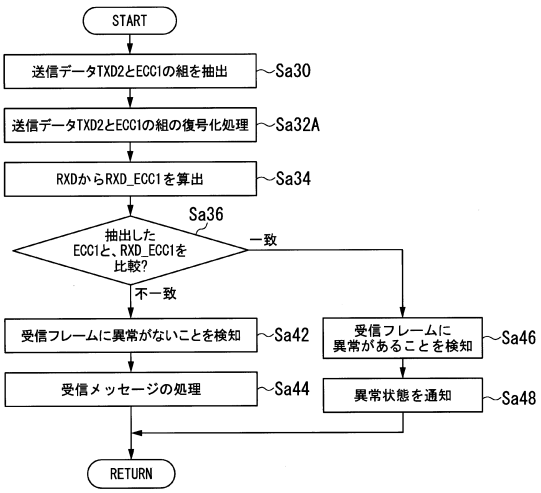
【図８】


フレームF
Sa30
送信データTXD2とECC1の組を抽出
暗号化処理された
送信データTXD2とECC1の組
Sa32A
送信データTXD2とECC1の組の復号化処理
RXD
Sa34
RXDからRXD_ECC1を算出
ECC1
RXD_ECC1
Sa36
抽出したECC1と、RXD_ECC1を比較
Sa44
受信メッセージ処理
異常状態検知
Sa48
異常状態を通知

【図９】


START
送信データTXD1の生成
Sa12
ECC1の算出
Sa14
TXD1の所定の位置のビットの論理を反転
(TXD2の生成)
Sa16
送信フレーム生成(TXD2+ECC1)
Sa18
送信データTXD2とECC1の組の暗号化処理
Sa20
送信フレーム生成(TXD2+ECC1)
Sa22
RETURN

【図１０】


START
送信データTXD2とECC1の組を抽出
Sa30
送信データTXD2とECC1の組の復号化処理
Sa32A
RXDからRXD_ECC1を算出
Sa34
Sa36
抽出した
ECC1と、RXD_ECC1を
比較?
一致
不一致
受信フレームに異常がないことを検知
Sa42
受信フレームに
異常があることを検知
Sa46
受信メッセージの処理
Sa44
異常状態を通知
Sa48
RETURN

フロントページの続き

(74)代理人 100175802
弁理士 寺本 光生
(74)代理人 100094400
弁理士 鈴木 三義
(72)発明者 境 裕樹
埼玉県和光市中央１丁目４番１号 株式会社本田技術研究所内

審査官 平井 嗣人

(56)参考文献 特開２００７－３１８２４７（ＪＰ，Ａ）
欧州特許出願公開第００５６４８２５（ＥＰ，Ａ２）
特開２００２－１５８６７８（ＪＰ，Ａ）
Ying Li, et al., IEEE 802.16m Identifying Femtocells Subscriber Groups, IEEE C802.16m-09/1965, ２００９年 ８月
中野 将志 MASASHI NAKANO, 先進運転支援システムを搭載した自動車に対する制御乗っ取り攻撃の脅威分析 Threat analysis of spoofing attacks on vehicles equipped with the Advanced Driving Assistant System, 電子情報通信学会技術研究報告 Ｖｏｌ．１１５ Ｎｏ．５１９ IEICE Technical Report, 日本, 一般社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers, 第115巻
北村 健太 Kenta Kitamura, ＳＣＩＳ２０１６ ［ＵＳＢ］ ＳＣＩＳ２０１６ ２０１６ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ １２／２８
Ｈ０４Ｌ １／００
Ｈ０４Ｌ １２／４０