(19)日本国特許庁(JP)

再公表特許(A1)

(11)国際公開番号
WO2017/110056

発行日　平成30年10月11日(2018.10.11)

(43)国際公開日　平成29年6月29日(2017.6.29)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/40	(2006.01)	H04L	12/40	M	5K032

審査請求 未請求　予備審査請求 未請求　（全 23 頁）

出願番号	特願2017-557692 (P2017-557692)
(21)国際出願番号	PCT/JP2016/005116
(22)国際出願日	平成28年12月13日(2016.12.13)
(31)優先権主張番号	特願2015-255420 (P2015-255420)
(32)優先日	平成27年12月25日(2015.12.25)
(33)優先権主張国	日本国(JP)

(71)出願人　314012076
パナソニックＩＰマネジメント株式会社
大阪府大阪市中央区城見２丁目１番６１号
(74)代理人　100109210
弁理士　新居　広守
(74)代理人　100137235
弁理士　寺谷　英作
(74)代理人　100131417
弁理士　道坂　伸一
(72)発明者　藤原　睦
日本国京都府長岡京市神足焼町１番地　パナソニックセミコンダクターソリューションズ株式会社内

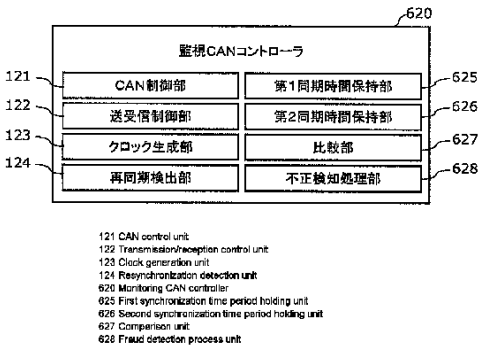
Ｆターム(参考)　5K032 AA08　BA06　CC11　CC13　CD05
DB28　EA02

最終頁に続く

(54)【発明の名称】不正メッセージ検知装置、不正メッセージ検知装置を備える電子制御装置、不正メッセージ検知方法、及び不正メッセージ検知プログラム

(57)【要約】

バスに送出された不正メッセージを検知する不正メッセージ検知装置は、１ビット期間においてバス上の信号の論理値を取得するためのサンプリングポイントを調整するために、信号のエッジとのずれを検知して再同期を実行するか否かを判定する再同期検出部（１２４）と、再同期検出部（１２４）によってエッジが検知された後の１ビット期間において、当該検知前に用いられていたサンプリングポイントにおけるバスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおけるバスの論理値である第２論理値とを取得する送受信制御部（１２２）と、第１論理値及び第２論理値を比較する比較部（６２７）と、第１論理値及び第２論理値が一致しない場合に不正検知時処理を実行する不正検知処理部（６２８）とを備える。



【特許請求の範囲】
【請求項１】
バス型ネットワークにおけるバスに送出された不正メッセージを検知する不正メッセージ検知装置であって、
１ビット期間において前記バス上の信号の論理値を取得するために前記バスの電圧が読み出される時点であるサンプリングポイントを調整するために、前記信号のエッジを検出し、前記エッジに基づく再同期を実行するか否かを判定する再同期検出部と、
前記再同期検出部によって再同期を実行すると判定された後の１ビット期間において、当該エッジが検出される前に用いられていたサンプリングポイントにおける前記バスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおける前記バスの論理値である第２論理値とを取得する受信部と、
前記受信部で取得された前記第１論理値及び前記第２論理値を比較する比較部と、
前記比較部によって前記第１論理値及び前記第２論理値が一致しないと判断された場合に、不正メッセージが検知された場合に対応付けられた不正検知時処理を実行する不正検知処理部と
を備える不正メッセージ検知装置。
【請求項２】
さらに、
前記再同期検出部によって前記エッジが検出される前に用いていたサンプリングポイントを保持する第１同期時間保持部と、
前記再同期検出部によって検出された前記エッジに基づく再同期による調整後のサンプリングポイントを保持する第２同期時間保持部とを備え、
前記受信部は、前記第１同期時間保持部に保持されたサンプリングポイントにおいて前記第１論理値を取得し、前記第２同期時間保持部に保持されたサンプリングポイントにおいて前記第２論理値を取得する
請求項１記載の不正メッセージ検知装置。
【請求項３】
前記不正検知処理部は、前記不正検知時処理として、前記バス型ネットワークにおける通信時にエラーが発生したことを通知するフレームを前記バスに送信する
請求項１又は２記載の不正メッセージ検知装置。
【請求項４】
前記バス型ネットワークは、ＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）である
請求項１～３のいずれか１項に記載の不正メッセージ検知装置。
【請求項５】
当該不正メッセージ検知装置は、前記バス型ネットワークに接続された電子制御装置の一部として装備されている
請求項１～４のいずれか１項に記載の不正メッセージ検知装置。
【請求項６】
請求項１～４のいずれか１項に記載の不正メッセージ検知装置を備え、バス型ネットワークで接続される通信機器からなる車載通信システムに接続される電子制御装置。
【請求項７】
バス型ネットワークにおけるバスに送出された不正メッセージを検知する不正メッセージ検知方法であって、
１ビット期間において前記バス上の信号の論理値を取得するために前記バスの電圧が読み出される時点であるサンプリングポイントを調整するために、前記信号のエッジを検出し、前記エッジに基づく再同期を実行するか否かを判定する再同期検知ステップと、
前記再同期検知ステップで再同期を実行すると判定された後の１ビット期間において、当該エッジが検知される前に用いられていたサンプリングポイントにおける前記バスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおける

前記バスの論理値である第２論理値とを取得する受信ステップと、
前記受信ステップで取得された前記第１論理値及び前記第２論理値を比較する比較ステップと、
前記比較ステップにおいて前記第１論理値及び前記第２論理値が一致しないと判断された場合に、不正メッセージが検知された場合に対応付けられた不正検知時処理を実行する不正検知処理ステップと
を含む不正メッセージ検知方法。
【請求項８】
請求項７に記載の不正メッセージ検知方法をプロセッサに実行させるための不正メッセージ検知プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、ＣＳＭＡ／ＣＡ（Ｃａｒｒｉｅｒ Ｓｅｎｓｅ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ／Ｃｏｌｌｉｓｉｏｎ Ａｖｏｉｄａｎｃｅ、搬送波感知多重アクセス／衝突回避）方式等の通信プロトコルを用いて通信可能な複数の装置が接続されるネットワークでの不正なメッセージを検知する装置に関する。
【背景技術】
【０００２】
車載ネットワークに用いられるＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ Ａｒｅａ Ｎｅｔｗｏｒｋ）には、ＣＡＮへの接続端子としてのデータリンクコネクタ（Ｄａｔａ Ｌｉｎｋ Ｃｏｎｎｅｃｔｏｒ、以下ＤＬＣと表記する）を介して、メーカやカーディーラ等により用意された車両診断装置や電子制御ユニット（Ｅｌｅｃｔｒｏｎｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ、以下ＥＣＵと表記する）のプログラムをアップデートさせる装置などを接続することができる。特許文献１の通信システムでは、規定の通信間隔でメッセージがネットワークの通信線上に送信され、メッセージを受信した通信装置はこのメッセージの受信間隔を検出し、この受信間隔を上記の通信間隔との差を基準範囲に照らしてこの受信したメッセージの正当性を判定する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】国際公開第１３／０９４０７２号
【非特許文献】
【０００４】
【非特許文献１】松本勉、他４名、「ＣＡＮにおける再同期を利用した電気的データ改ざん」、２０１５年、第３２回　暗号と情報セキュリティシンポジウム（ＳＣＩＳ　２０１５）
【発明の概要】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１に開示される手法によるメッセージの正当性の判定では、通信間隔と受信間隔との差が基準範囲内であれば、不正なメッセージであっても正当であると誤判定されるという問題がある。また、この問題を回避しようとより狭い基準範囲を用いれば、正当なメッセージを不正なメッセージとする誤判定が増加し、通信効率が低下する。
【０００６】
本発明は、電気的な攻撃によるメッセージの改ざんの有無を検知して高い精度でメッセージの正当性を判定し、通信効率を低下させることなく、安全性の高いＣＡＮを実現する不正メッセージ検知装置等を提供する。
【課題を解決するための手段】

【０００７】
本発明の一態様に係る不正メッセージ検知装置は、バス型ネットワークにおけるバスに送出された不正メッセージを検知する不正メッセージ検知装置であって、１ビット期間において前記バス上の信号の論理値を取得するために前記バスの電圧が読み出される時点であるサンプリングポイントを調整するために、前記信号のエッジを検出し、前記エッジに基づく再同期を実行するか否かを判定する再同期検出部と、前記再同期検出部によって再同期を実行すると判定された後の１ビット期間において、当該エッジが検出される前に用いられていたサンプリングポイントにおける前記バスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおける前記バスの論理値である第２論理値とを取得する受信部と、前記受信部で取得された前記第１論理値及び前記第２論理値を比較する比較部と、前記比較部によって前記第１論理値及び前記第２論理値が一致しないと判断された場合に、不正メッセージが検知された場合に対応付けられた不正検知時処理を実行する不正検知処理部とを備える。

【０００８】
また、本発明の一態様に係る不正メッセージ検知方法は、バス型ネットワークにおけるバスに送出された不正メッセージを検知する不正メッセージ検知方法であって、１ビット期間において前記バス上の信号の論理値を取得するために前記バスの電圧が読み出される時点であるサンプリングポイントを調整するために、前記信号のエッジを検出し、前記エッジに基づく再同期を実行するか否かを判定する再同期検知ステップと、前記再同期検知ステップで再同期を実行すると判定された後の１ビット期間において、当該エッジが検知される前に用いられていたサンプリングポイントにおける前記バスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおける前記バスの論理値である第２論理値とを取得する受信ステップと、前記受信ステップで取得された前記第１論理値及び前記第２論理値を比較する比較ステップと、前記比較ステップにおいて前記第１論理値及び前記第２論理値が一致しないと判断された場合に、不正メッセージが検知された場合に対応付けられた不正検知時処理を実行する不正検知処理ステップとを含む。

【０００９】
また、本発明の一態様に係る不正メッセージ検知プログラムは、上記の不正メッセージ検知方法をプロセッサに実行させるためのプログラムである。

【００１０】
なお、これらの包括的又は具体的な態様は、システム、方法、集積回路、コンピュータプログラム又はコンピュータ読み取り可能なＣＤ－ＲＯＭなどの記録媒体で実現されてもよく、システム、方法、集積回路、コンピュータプログラム及び記録媒体の任意な組み合わせで実現されてもよい。

【発明の効果】

【００１１】
本発明の不正メッセージ検知装置、不正メッセージ検知方法、及び不正メッセージ検知プログラムは、高い精度でメッセージの正当性を判定し、通信効率を低下させることなく、安全性の高いＣＡＮを実現する。

【図面の簡単な説明】

【００１２】
【図１Ａ】図１Ａは、ＣＡＮを用いた車載通信システムのハードウェア構成例を示すブロック図である。
【図１Ｂ】図１Ｂは、ＣＡＮコントローラの機能構成図である。
【図１Ｃ】図１Ｃは、攻撃ＣＡＮコントローラの機能構成図である。
【図２】図２は、ＣＡＮの規格に定められているデータフレームの標準フォーマットを示す図である。
【図３】図３は、ＣＡＮの規格に定められている、１ビット期間を構成する４つの論理的なセグメントを示す図である。
【図４】図４は、信号のエッジと１ビット期間とのずれのパターンと、１ビット期間の調

整の例を示す図である。
【図５】図５は、ＣＡＮにおける、ＥＣＵによるメッセージの受信の動作のフロー図である。
【図６】図６は、攻撃ＣＡＮコントローラによる攻撃のタイミング及び電圧の操作を示す図である。
【図７Ａ】図７Ａは、実施の形態における不正メッセージ検知装置を備える車載通信システムのハードウェア構成例を示すブロック図である。
【図７Ｂ】図７Ｂは、実施の形態における不正メッセージ検知装置の機能構成図である。
【図８】図８は、実施の形態における不正メッセージ検知装置を備えるＥＣＵによるＣＡＮバスの監視及び不正メッセージの検知の動作のフロー図である。
【図９】図９は、攻撃ＣＡＮコントローラによる攻撃があった場合に２つのサンプリングポイントで取得される論理値を示す図である。
【発明を実施するための形態】
【００１３】
［本発明の基礎となった知見］
本発明者は、背景技術の欄において記載した通信システムでは検知できない不正なメッセージによるＣＡＮへの攻撃手法があることを指摘する文献（非特許文献１）を得た。まず、ＣＡＮを用いた車載通信システムを例に、ＣＡＮの構成及びこの攻撃手法の概要について図を参照しながら説明する。
【００１４】
（ＣＡＮの構成の概要）
図１ＡはＣＡＮを用いた車載通信システム１０のハードウェア構成例を示すブロック図である。
【００１５】
車載通信システム１０は、通信線であるＣＡＮバス２００と、このＣＡＮバス２００に接続される複数のノードであるＥＣＵ１０１～１０ｎ（以下、これらを区別しない場合はＥＣＵ１００ともいう）及び５０１とを含むバス型ネットワークである。なお、ＥＣＵ５０１は攻撃手法について説明する目的でこの構成に含めたものであり、正常な車載通信システムには含まれない。ただし本図に示されるような、ＣＡＮバス２００に接続される、ＥＣＵをそれぞれ含む複数の車載装置のひとつが悪意のある装置であるという構成、及びこの構成において、この悪意のある車載装置がＣＡＮバス２００上に不正なメッセージを流して他の車載装置をかく乱させるという攻撃は、現実に起こり得る例としての想定である。
【００１６】
ＥＣＵ１００及び５０１（以下、これらを区別しない場合に単にノードともいう）は、それぞれ例えばエンジン制御システムのＥＣＵであったり、ブレーキシステムのＥＣＵであったり、空調システムのＥＣＵであったり、カーナビゲーションシステムのＥＣＵであったりする。ここに挙げたのは今日の自動車が備える車載通信システムに接続される通信機器のＥＣＵの例のごく一部であり、このようなＥＣＵは各種の制御系統に含まれている。ＥＣＵ同士はＣＡＮバス２００を介して通信可能であり、いずれも受信側にも送信側にもなることができる。なお、ＥＣＵ５０１は、もっぱら攻撃を目的とする機器である場合も想定される。なお、図示しないが、各ＥＣＵの先に、ＣＡＮバス２００とは別のインターフェースで、センサーやアクチュエータが接続されてもよい。
【００１７】
ＣＡＮバス２００は２本の信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈからなり、信号を安定させるための終端抵抗（図示なし）を信号線上に備える。なお、本図では各信号線は模式的に直線で示されているが、耐ノイズ性のあるツイストペア線を用いて実現される。
【００１８】
ＣＡＮではこれらの信号線ＣＡＮ＿ＬとＣＡＮ＿Ｈとの間の電圧差の大小（以下では簡便に差の有無とも表現する）でデジタル信号の各ビットの論理値（０または１の数値デー

タ）が示され、ＮＲＺ（Ｎｏｎ－Ｒｅｔｕｒｎ－ｔｏ－Ｚｅｒｏ方式）で逐次的に各ビットの値が送信されるシリアル通信が行われる。具体的には、電圧の差が大きい状態で０が、小さい状態で１が示される。ノードはそれぞれ信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈの両方に接続されており、信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈに電圧を印加することで信号を送信し、信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈの電圧を読み取ってその差分を取ることで信号を受信する。なお、ＣＡＮの規格では、０の値はドミナント（ｄｏｍｉｎａｎｔ、優性の意）、１の値はリセッシブ（ｒｅｃｅｓｓｉｖｅ、劣性の意）と呼ばれ、ＣＡＮバス２００上では０の値が優先される。具体的には、複数のノードから０の値と１の値とが当時にＣＡＮバス２００に送信された場合は０が優先されてＣＡＮバス２００は０の値を示す電圧の状態におかれる。また、あるノードが１の値を送信した後で他のノードが０の値を送信した場合もＣＡＮバス２００上の信号は０の値で上書きされる、つまりＣＡＮバス２００は０の値を示す電圧の状態におかれる。以下では、ＣＡＮバス２００の電圧が信号の０の値を示す状態をドミナント状態、１の値を示す状態をリセッシブ状態ともいう。

【００１９】

なお、ＣＡＮでは全体の通信を制御する特定のマスターデバイスは存在しない（マルチマスター方式）。また、メッセージの衝突を回避するために、ＣＡＮバス２００上に同時に複数のメッセージを存在させず、各ノードはＣＡＮバス２００がアイドルなときに送信を開始する。各ノードから送信されたメッセージはＣＡＮバス２００に接続されるすべてのノードにブロードキャストされる。このメッセージはＣＡＮの規格に定められているフレームというフォーマットに従って送信される。

【００２０】

各フレームには、送信ノードを示す識別子（ｉｄｅｎｔｉｆｉｅｒ、以下ＩＤと表記する）が含まれる。図２は、ＣＡＮの規格に定められているフレームの１つである、データフレームの標準フォーマットを示す。本図では左がフレームの先頭であり、データフレームの前後はＣＡＮバス２００がアイドルな状態である。データフレームは時系列に並ぶ用途別のスロットからなり、本図内の数値は各スロットに使用されるビット数（長さ）を示す。また、上下の横線は各スロットに含まれうる信号の論理値を示す。つまり、上記のＩＤのスロットは、フレームの先頭から２ビット目から始まり、論理値０及び１の両方を含みうる１１ビット長のデータである。複数のノードが送信のために同時にＣＡＮバス２００にアクセスした場合は、各フレームが含むＩＤに基づくフレーム間の優先順位に従って衝突が回避され、優先順位の高い方のフレームから送信される（ＣＳＭＡ／ＣＡ）。ＩＤはまた、各ノードにおいて、受信したフレームは使用するフレームか否かの判断に用いられる。

【００２１】

なお、ＣＡＮの規格では上記のデータフレームを含めて全部で４種類のフレームが用意されており、その中のひとつに、エラーを検知したノードが送信するエラーフレームがある。エラーフレームは本発明で解決される課題とは直接関係しないためその概要のみ記載すると、エラーフレームが送信されると、送信側のノードによる直近の送信は中断され、他に同じメッセージを受信していたノードはこのメッセージを破棄する。その後送信側のノードは再送信を実行する。

【００２２】

各ノードの基本的な構成は共通している。図１Ａの例では、各ノードは処理部１１０、ＣＡＮコントローラ１２０又は攻撃ＣＡＮコントローラ５２０、及びＣＡＮトランシーバ１３０を備える。ＥＣＵ１０２～１０ｎではこれらの参照符号を省略している。ＣＡＮコントローラ１２０と攻撃ＣＡＮコントローラ５２０とは機能が一部異なるためここでは区別しているが、共通の基本構成を有している。まずはＣＡＮコントローラ１２０及び攻撃ＣＡＮコントローラ５２０に共通する構成及びその動作について説明する。

【００２３】

処理部１１０は、例えば中央処理装置であり、各ノードを含むシステムの機能に応じた演算処理を実行する。

【００２４】
ＣＡＮコントローラ１２０及び攻撃ＣＡＮコントローラ５２０は、例えばマイクロコントローラを用いて実現され、通信処理を実行する。ＣＡＮコントローラ１２０及び攻撃ＣＡＮコントローラ５２０についてはその違いを含めて詳細を後述する。
【００２５】
ＣＡＮトランシーバ１３０は、各ＥＣＵのＣＡＮコントローラ１２０とＣＡＮバス２００との間のインターフェース用集積回路であって、ＣＡＮバス２００上の電圧差の値と、ＣＡＮコントローラ１２０が扱う論理値との間の変換を実行する。
【００２６】
ＣＡＮコントローラ１２０及び攻撃ＣＡＮコントローラ５２０の詳細について、図１Ｂ及び図１Ｃを用いて説明する。図１ＢはＣＡＮコントローラ１２０の機能構成図であり、図１Ｃは攻撃ＣＡＮコントローラ５２０の機能構成図である。共通の構成要素については共通の参照符号を付している。ＣＡＮコントローラ１２０及び攻撃ＣＡＮコントローラ５２０は、ＣＡＮ制御部１２１、送受信制御部１２２、クロック生成部１２３、再同期検出部１２４、及び同期時間保持部１２５を備える。いずれも上記のＣＡＮのプロトコルに準じた通信処理を実行するための機能を実現する。
【００２７】
ＣＡＮ制御部１２１は、ＣＡＮコントローラ１２０の動作全体を制御する。
【００２８】
送受信制御部１２２は、処理部１１０及びＣＡＮトランシーバ１３０とのメッセージの入出力のインターフェースである。ＣＡＮバス２００上の信号の論理値の読み出し及び書き込みは、送受信制御部１２２によってＣＡＮトランシーバ１３０を介して実行される。送受信制御部１２２は、例えば処理部１１０から入力されたデジタル信号の値に応じて、ＣＡＮトランシーバ１３０に所定の電圧を信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈのそれぞれに印加させる送信部として機能する。また、ＣＡＮトランシーバ１３０を介してＣＡＮバス２００の信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈのそれぞれの電圧を読み取り、その差の大きさ（有無）に基づいてＣＡＮバス２００上の信号の論理値を取得する受信部として機能する。
【００２９】
クロック生成部１２３は発振回路であり、データの処理及びメッセージの送受信のタイミングの基準となるシステムクロックを生成する。このシステムクロックにより、上記の信号の１ビットの時間長（以下、１ビット期間という）が決まる。この１ビット期間の長さは、ＣＡＮバス２００に接続されるノード間で共通の長さに設定される。
【００３０】
なお、ＣＡＮにおいてノード間で通信を適切に行うには、各ノード間での１ビット期間の長さが等しいことに加え、ビットの切り替わりのタイミングについて同期がとれている必要がある。しかし、仮に初期状態で同期がとれていても、ノード間でのシステムクロックの誤差などが原因で、このタイミングに許容できない大きさのずれが生じることがある。ＣＡＮにおけるこのずれの解消は、送信側のノードの信号送信によるＣＡＮバス２００上の信号のリセッシブからドミナントへの切り替わり（以下、エッジという）が発生した場合に、受信側のノードでの再同期と呼ばれる動作によって実行される。より具体的には、エッジが発生すると、このエッジに基づく再同期を実行するか否かについて受信側のノードの再同期検出部１２４によって判定された上で実行される。
【００３１】
再同期は本願で想定されている攻撃に関与するため、ここで概要を説明しておく。再同期には、上記の１ビット期間をＴｉｍｅ ｑｕａｎｔｕｍ（以下、Ｔｑと表記する）という単位で表わされる４つの論理的なセグメントに分割して扱う、ビットタイミングと呼ばれるタイミング制御の仕組みが用いられる。図３は、これらの４つのセグメントを示す図である。それぞれ、同期セグメント（Ｓｙｎｃｈｒｏｎｉｚａｔｉｏｎ Ｓｅｇｍｅｎｔ、図ではＳＳとも表記）、伝播時間セグメント（Ｐｒｏｐａｇａｔｉｏｎ Ｔｉｍｅ Ｓ

ｅｇｍｅｎｔ、図ではＰＴＳとも表記）、位相バッファセグメント１（Ｐｈａｓｅ Ｂｕｆｆｅｒ Ｓｅｇｍｅｎｔ １、図ではＰＢＳ１とも表記）、位相バッファセグメント２（Ｐｈａｓｅ Ｂｕｆｆｅｒ Ｓｅｇｍｅｎｔ ２、図ではＰＢＳ２とも表記）という名前がＣＡＮの規格において付けられている。なお、本図中のサンプリングポイント（Ｓａｍｐｌｉｎｇ Ｐｏｉｎｔ、図ではＳＰとも表記）とは１ビット期間におけるある時点であり、この１ビット期間においてＣＡＮバス２００上の信号の論理値を１ビットのデータとしてＣＡＮコントローラ１２０が取得するために、ＣＡＮトランシーバ１３０を介して信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈの電圧を読み出す（サンプリングする）時点である。サンプリングポイントは、例えば１ビット期間の先頭を基準（始期）とする時間（Ｔｑ）で設定され、同期時間保持部１２５に保持される。位相バッファセグメント１の終端はサンプリングポイントである。再同期検出部１２４は、ＣＡＮトランシーバ１３０を介してＣＡＮバス２００上の信号のエッジを検出し、このエッジに基づく再同期を実行するか否か判定する。より具体的には、エッジが発生したセグメントに基づいて、再同期を実行するか否か判定し、また、実行する場合はその再同期の内容を決定する。４つのセグメントのうちの同期セグメントはいわば許容時間差であり、エッジがこの１Ｔｑのセグメントで発生した場合には再同期が実行されない。つまり、それ以外のセグメントでエッジが発生した場合、再同期検出部１２４は再同期を実行すると判定する。再同期は、ずれの検知後の１ビット期間の長さの調整によって行われ、再同期の内容とは、長さを変更するセグメントとその変更の程度である。この１ビット期間の調整について図を用いて説明する。図４は、信号のエッジと１ビット期間とのずれのパターンと、１ビット期間の調整の例を示す図である。

【００３２】

図４の（ａ）に示される受信側のノードの１ビット期間は、信号のエッジからのずれがない、つまり受信側のノードと送信側のノードとは同期がとれている。この場合、１ビット期間は調整されない。

【００３３】

図４の（ｂ）に示される受信側のノードの場合、信号のエッジは受信側のノードの同期セグメントより後であって、サンプリングポイントよりも前のセグメントで発生している。この場合、送信側のノードに対して受信側のノードが進んでいるとして、位相バッファセグメント１（本図中、横縞の区間）が延長される。これにより、信号のエッジ（送信側のノードの１ビット期間の始期）とサンプリングポイントとの時間差が調整される。また、この調整によって１ビット期間が延長された分、この受信側のノードの次の１ビット期間の始期は遅れ、結果として送信側のノードとの同期がとられる。

【００３４】

図４の（ｃ）に示される受信側のノードの場合、信号のエッジは受信側のノードのサンプリングポイントより後のセグメントで発生している。この場合、送信側のノードに対して受信側のノードが遅れているとして、位相バッファセグメント２（本図中、縦縞の区間）が短縮される。これにより、次の１ビット区間では信号のエッジ（送信側のノードの１ビット期間の始期）とサンプリングポイントとの時間差が調整される。また、この調整によって１ビット期間が短縮された分、この受信側のノードの次の１ビット期間の始期が早まり、結果として送信側のノードとの同期がとられる。

【００３５】

このように再同期によって１ビット期間の長さを調整することによって、サンプリングポイントが送信側のノードによる信号の送信タイミングに対して適切に調整される。なお、上記の位相バッファセグメント１及び位相バッファセグメント２の長さの変更の程度は、ずれの程度に応じて所定の範囲内で適宜決定される。

【００３６】

上記の構成を有するＣＡＮコントローラ１２０を備えるＥＣＵ１００は、それぞれ図５のフロー図に示される動作を実行してメッセージを受信する。

【００３７】

まずＥＣＵ１００では、サンプリングポイントが同期時間保持部１２５に保存される（ステップＳ１０）。これは初期設定のサンプリングポイントであり、例えばＥＣＵ１００を含む各車載システムの設計時に設定される。サンプリングポイントは上述のとおり位相バッファセグメント１の終端に位置し、例えば上記の１ビット内の各セグメントの長さがＴｑ単位で設定されることでその先頭からの位置が決定される。このように、サンプリングポイントの設定自体はＥＣＵ１００の動作ではないが、同期時間保持部１２５に保存されるデータの存在を示す説明の便宜上このフロー図に含めている。

【００３８】

ＥＣＵ１００は、このサンプリングポイントを用いての、ＣＡＮコントローラ１２０及びＣＡＮトランシーバ１３０を介するメッセージの受信を開始する（ステップＳ２０）。このメッセージの受信の動作について別の表現をすれば、ＣＡＮコントローラ１２０の送受信制御部１２２によって、連続する１ビット期間（クロック生成部１２３が生成するシグナルクロックに基づく）のそれぞれにおけるサンプリングポイントで、ＣＡＮトランシーバ１３０を介してＣＡＮバス２００の信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈの電圧が読みとられる。そして読み取られたこれらの電圧の差に基づいて、ＣＡＮバス２００上の信号の論理値が取得される。送受信制御部１２２が取得したこの論理値は、メッセージのデータとしてＥＣＵ１００の処理部１１０に渡される。

【００３９】

ＥＣＵ１００はこのように各１ビット期間におけるサンプリングポイントで電圧を読み取って論理値を逐次に取得しながら、さらにこれらの論理値の変化に基づいてエッジを検出し（ステップＳ３０）、再同期の実行をするか否かについて判定する（ステップＳ４０）。この判定について別の表現をすれば、ＣＡＮコントローラ１２０の再同期検出部１２４によって、エッジを検出した時点が１ビット期間のどのセグメントであるかに基づいて再同期の実行をするか否かについて判定される。

【００４０】

再同期を実行しないと判定された場合（ステップＳ４０でＮＯ）、ＥＣＵ１００は初期設定のサンプリングポイントを継続して使用してメッセージを受信する（ステップＳ５０）。再同期を実行すると判定された場合（ステップＳ４０でＹＥＳ）、次のサンプリングポイントの適切なタイミングが例えば送受信制御部１２２によって算出される。そしてこの算出された新たなサンプリングポイントのタイミングに応じて位相バッファセグメント１又は位相バッファセグメント２の長さが変更される（再同期の実行、ステップＳ６０）。これによりＥＣＵ１００は、調整後の新たなサンプリングポイントをして使用してメッセージを受信する（ステップＳ７０）。

【００４１】

その後もＣＡＮバス２００にメッセージがあれば（ステップＳ８０でＹＥＳ）ＥＣＵ１００はこれを受信し（ステップＳ２０）、なければ（ステップＳ８０でＮＯ）受信動作を終了する。なお、ＥＣＵ５０１もメッセージの受信をする場合は、この図５に示されるフロー図の動作を実行してもよい。

【００４２】

（攻撃手法の概要）

次に、攻撃ＣＡＮコントローラ５２０の構成のＣＡＮコントローラ１２０と異なる点及び攻撃ＣＡＮコントローラ５２０による攻撃の動作について説明する。

【００４３】

攻撃ＣＡＮコントローラ５２０は、攻撃タイミング生成部１２６を備える点がＣＡＮコントローラ１２０と異なる。車載通信システム１０において、攻撃ＣＡＮコントローラ５２０は以下の動作を実行して、ＥＣＵ１００が送信したメッセージを改ざんする。

【００４４】

まず、送信側であるＥＣＵ１００は、ＣＡＮバス２００上で逐次に示される論理値としてメッセージを送信し、受信側のＥＣＵ１００は送信側のＥＣＵ１００による論理値の送信のタイミングに対して１ビット期間以内の所定の時間差の時点（サンプリングポイント

）でＣＡＮバス２００上の信号の論理値を逐次に取得することによってメッセージを受信する。

【００４５】

悪意のあるＥＣＵであるＥＣＵ５０１の攻撃ＣＡＮコントローラ５２０は、あるタイミングで１Ｔｑ程度のごく短い時間、ＣＡＮバス２００上の信号の論理値を電気的に操作することで送信側のＥＣＵ１００によるメッセージの送信のタイミングを受信側のＥＣＵ１００に誤認させる（第１攻撃）。

【００４６】

送信のタイミングを誤認している受信側のＥＣＵ１００は、ＣＡＮバス２００上の信号の論理値を取得するのに、正しい送信のタイミングに対しては不適切な時間差のサンプリングポイントを用いる。攻撃ＣＡＮコントローラ５２０はその不適切なサンプリングポイントに合わせたタイミングでもう一度ＣＡＮバス２００上の信号の論理値を電気的に操作する（第２攻撃）。この結果、受信側のＥＣＵ１００は、送信側のＥＣＵ１００が発したメッセージとは異なるメッセージを受信する。

【００４７】

攻撃タイミング生成部１２６は、攻撃ＣＡＮコントローラ５２０が上記の電気的な操作（電圧操作）によって第１攻撃と第２攻撃を実行するタイミングを生成する。次に、このタイミング及び電圧操作について説明する。

【００４８】

図６は、上述した攻撃ＣＡＮコントローラ５２０による攻撃のタイミング及び電圧の操作を示す図である。

【００４９】

まず、送信側のＥＣＵ１００による論理値０の送信が実行される。一方、攻撃ＣＡＮコントローラ５２０が、このＥＣＵ１００による論理値０の送信のタイミングにかぶせるように論理値１をごく短い時間送信する（第１攻撃）。これにより、ＣＡＮバス２００上の信号の論理値の１から０への変化、つまりＣＡＮバス２００のリセッシブ状態からドミナント状態への変化が遅れる。なお、上述のとおりＣＡＮではドミナントである０はリセッシブである１に優先されるが、この攻撃ＣＡＮコントローラ５２０とＣＡＮバス２００とを接続するＣＡＮトランシーバ１３０は、ＥＣＵ１００のＣＡＮトランシーバ１３０とＣＡＮバス２００との接続の仕方と逆の接続がされている。つまり、ＣＡＮ＿Ｈに接続されるべき線がＣＡＮ＿Ｌに接続され、ＣＡＮ＿Ｌに接続されるべき線がＣＡＮ＿Ｈに接続されている。これにより、ＣＡＮバス２００のドミナント状態からリセッシブ状態への変更も、各信号線上で逆方向の電圧同士で互いに打ち消すことで可能にしている。

【００５０】

上記の第１攻撃によるＣＡＮバス２００のリセッシブ状態からドミナント状態への変化の遅延は、すなわちエッジの発生の遅延である。本図の（ｃ）において、第１攻撃がなければエッジは破線の矢印で示す時点で発生する。しかし第１攻撃の影響で、エッジの発生は実線の矢印で示す時点に遅延する。受信側のＥＣＵはこのエッジを検出すると、上記で説明したようにこのエッジがどのセグメントで発生したかに応じて再同期を実行する。本図で示される例では、エッジは伝播時間セグメントで発生しているので、受信側のＥＣＵは位相バッファセグメント１を延長することで再同期を実行する（本図の（ｄ）参照）。これにより、第１攻撃がなければ破線の三角形で示す時点であったサンプリングポイントが、黒の三角形で示すサンプリングポイントに遅延する。

【００５１】

次に攻撃ＣＡＮコントローラ５２０は、受信側のＥＣＵのサンプリングポイントにあわせて論理値１をごく短い時間送信する（第２攻撃）。これにより、受信側のＥＣＵは、送信側のＥＣＵが送信した０の値ではなく、１の値をこの１ビット期間における信号の論理値として取得する。このように、攻撃ＣＡＮコントローラ５２０による２段階の攻撃によってメッセージは改ざんされ、受信側のＥＣＵは不正なメッセージを受信する。

【００５２】

なお、送信側のＥＣＵは、自身のサンプリングポイント（本図の（ａ）参照）でＣＡＮバス２００上の電圧をモニタする。しかし攻撃ＣＡＮコントローラ５２０による第２攻撃はこの時点を外して論理値を変更しているため、送信側のＥＣＵではこの改ざんを検知することができない。

【００５３】

以下では、悪意のあるＥＣＵによるこのような攻撃によって改ざんされた不正メッセージを検知する装置の一実施の形態について図面を参照しながら説明する。

【００５４】

なお、以下で説明する実施の形態は、包括的又は具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素は任意の構成要素である。

【００５５】

［実施の形態］

図７Ａは、実施の形態における不正メッセージ検知装置を備える車載通信システム１０Ａのハードウェア構成例を示すブロック図である。車載通信システム１０Ａは、車載通信システム１０と同じく、通信線であるＣＡＮバス２００と、このＣＡＮバス２００に接続される複数のノードであるＥＣＵ１００を含むバス型ネットワークである。

【００５６】

また、車載通信システム１０ＡはＥＣＵ５０１及びＥＣＵ６００を備える。ＥＣＵ５０１は上述の悪意のあるＥＣＵであり、以下で攻撃の発生について説明する目的でこの構成に含めたものである。

【００５７】

ＥＣＵ６００は車載通信システム１０Ａに他のＥＣＵ１００及び５００と同様に、ひとつのＥＣＵとしてＣＡＮバス２００に接続される。ＥＣＵ６００は他のＥＣＵと同様に処理部１１０及びＣＡＮトランシーバ１３０を備えるが、ＣＡＮコントローラ１２０に代えて本実施の形態における不正メッセージ検知装置である監視ＣＡＮコントローラ６２０を備える点がＥＣＵ１００と異なる。次に、この監視ＣＡＮコントローラ６２０について図７Ｂを参照して説明する。

【００５８】

図７Ｂは、本実施の形態における不正メッセージ検知装置である監視ＣＡＮコントローラ６２０の機能構成図である。

【００５９】

ＣＡＮバス２００に送出された不正メッセージを検知する不正メッセージ検知装置である監視ＣＡＮコントローラ６２０は、ＣＡＮ制御部１２１、送受信制御部１２２、クロック生成部１２３、及び再同期検出部１２４を備える。これらは上記のＣＡＮのプロトコルに準じた通信処理を実行するための機能を実現するための構成要素であり、ＥＣＵ１００と共通の構成要素であるため、詳細な説明は省略する。

【００６０】

監視ＣＡＮコントローラ６２０はさらに、第１同期時間保持部６２５、第２同期時間保持部６２６、比較部６２７、及び不正検知処理部６２８を備える。

【００６１】

第１同期時間保持部６２５及び第２同期時間保持部６２６は、それぞれ同期時間保持部１２５と同じくサンプリングポイントを保持する。ただし第１同期時間保持部６２５は、再同期検出部１２４によってエッジが検出され、このエッジに基づく再同期を実行すると判定されたときに、このエッジが検出される前に用いられていたサンプリングポイント（以下、旧サンプリングポイントともいう）を保持し続ける。一方、第２同期時間保持部６２６は、再同期検出部１２４によってエッジが検出されたとき、このエッジに基づく再同期を実行すると判定されたときに、この再同期による調整後のサンプリングポイント（以

下、新サンプリングポイントともいう）を保持する。そして送受信制御部１２２は、再同期が実行されるときには新旧両方のサンプリングポイントでＣＡＮバス２００の論理値（以下ではそれぞれ第１論理値及び第２論理値ともいう）を取得する。

【００６２】

比較部６２７は、上記の新旧サンプリングポイントで取得された第１論理値及び第２論理値を比較してこれらが一致するか否かを判断する。

【００６３】

不正検知処理部６２８は、比較部６２７が第１論理値と第２論理値とが一致しないと判断した場合に、不正メッセージが検知された場合に対応付けられた処理である不正検知時処理を実行する。

【００６４】

上記の構成を有する監視ＣＡＮコントローラ６２０を備えるＥＣＵ６００は、図８のフロー図に示される動作を実行してＣＡＮバス２００を監視し、不正メッセージを検知する。図８は、本実施の形態における監視ＣＡＮコントローラ６２０を備えるＥＣＵ６００によるＣＡＮバス２００の監視及び不正メッセージの検知の動作のフロー図である。なお図８では、図５に示されるＥＣＵ１００によるメッセージの受信の動作と共通のステップは共通の参照符号で示している。

【００６５】

まずＥＣＵ６００では、初期設定のサンプリングポイントが第１同期時間保持部６２５に保持される（ステップＳ１０）。このサンプリングポイントの設定自体はＥＣＵ６００の動作ではないが、第１同期時間保持部６２５に保持されるデータの存在を示す説明の便宜上このフロー図に含めている。

【００６６】

ＥＣＵ６００は、このサンプリングポイントを用いての、監視ＣＡＮコントローラ６２０及びＣＡＮトランシーバ１３０を介するメッセージの受信を開始する（ステップＳ２０）。このメッセージの受信の動作について別の表現をすれば、監視ＣＡＮコントローラ６２０の送受信制御部１２２によって、連続する１ビット期間（クロック生成部１２３が生成するシグナルクロックに基づく）のそれぞれにおけるサンプリングポイントで、ＣＡＮトランシーバ１３０を介してＣＡＮバス２００の信号線ＣＡＮ＿Ｌ及びＣＡＮ＿Ｈの電圧が読み取られる。そして読み取られたこれらの電圧の差に基づいて、ＣＡＮバス２００上の信号の論理値が取得される。送受信制御部１２２が取得したこの論理値は、メッセージのデータとしてＥＣＵ６００の処理部１１０に渡される。

【００６７】

ＥＣＵ６００はこのように各１ビット期間におけるサンプリングポイントで電圧を読み取って論理値を逐次に取得しながら、さらにこれらの論理値の変化に基づいてエッジを検出し（ステップＳ３０）、このエッジに基づく再同期の実行をするか否かについて判定する（ステップＳ４０）。この判定について別の表現をすれば、監視ＣＡＮコントローラ６２０の再同期検出部１２４によって、エッジを検出した時点が１ビット期間のどのセグメントであるかに基づいて再同期の実行をするか否かについて判定される。

【００６８】

再同期を実行しないと判定された場合（ステップＳ４０でＮＯ）、ＥＣＵ６００は初期設定のサンプリングポイントを継続して使用してメッセージを受信する（ステップＳ５０）。再同期を実行すると判定された場合（ステップＳ４０でＹＥＳ）、次のサンプリングポイントの適切なタイミングが例えば送受信制御部１２２によって算出される。そしてこの算出された新たなサンプリングポイントは第２同期時間保持部６２６に保持される。この結果、監視ＣＡＮコントローラ６２０では、初期設定のサンプリングポイント、つまり旧サンプリングポイントと、算出された新サンプリングポイントとの両方が保持される。一方で、この算出された新たなサンプリングポイントのタイミングに応じて位相バッファセグメント１又は位相バッファセグメント２の長さが変更される（再同期の実行Ｓ６６０）。

【００６９】
ここでＥＣＵ６００はメッセージを受信するが、監視ＣＡＮコントローラ６２０の送受信制御部１２２は、旧サンプリングポイントと新サンプリングポイントとの両方でＣＡＮバス２００の論理値をそれぞれ第１論理値及び第２論理値として取得する（ステップＳ６７０）。
【００７０】
取得された第１論理値及び第２論理値は、比較部６２７によって比較され、一致するか否かについて判断される（Ｓ６７５）。ここで第１論理値と第２論理値との一致について判断する理由について説明する。図９は、攻撃ＣＡＮコントローラ５２０による攻撃があった場合に２つのサンプリングポイントで取得される論理値を示す図である。
【００７１】
まず、（ａ１）に示される、送信側のＥＣＵ１００と受信側のＥＣＵであるＥＣＵ６００とで同期がとれている場合に、攻撃ＣＡＮコントローラ５２０によって（ｂ）に示される第１攻撃の結果、ＥＣＵ６００が再同期を実行する場合を想定する。この場合、受信側のＥＣＵ６００は、（ｄ）に示される旧サンプリングポイントと新サンプリングポイントとでステップＳ６７０のメッセージの取得を実行する。ここでＣＡＮバス２００上の信号の論理値は、（ｃ）に示されるように推移する。具体的には、旧サンプリングポイントでは、攻撃ＣＡＮコントローラ５２０による第２攻撃開始前であり、ＣＡＮバス２００上の信号の論理値は改ざんされず、送信側のＥＣＵ１００による出力どおり０である。これは、旧サンプリングポイントは送信側のＥＣＵ１００がビットモニタリングを実行するため、攻撃ＣＡＮコントローラ５２０はこの時点を避けて第２攻撃を実行するためである。一方、新サンプリングポイントでは、図６を参照して説明したように攻撃ＣＡＮコントローラ５２０によってＣＡＮバス２００上の値が０から１に改ざんされている。したがって、攻撃ＣＡＮコントローラ５２０による攻撃によって再同期が実行された場合には、ＣＡＮバス２００上の信号の論理値は旧サンプリングポイントと新サンプリングポイントとで一致しない。したがって、新旧のサンプリングポイントでＥＣＵ６００の送受信制御部１２２が取得する論理値は一致しない。
【００７２】
これに対し、（ａ２）に示されるように、ＥＣＵ１００とＥＣＵ６００とで同期がとれていないために再同期が実行される場合には、ＣＡＮバス２００上の信号の論理値は、ＥＣＵ１００が出力したとおりに推移する。したがって、新旧のサンプリングポイントでＥＣＵ６００の送受信制御部１２２が取得する論理値は一致する。
【００７３】
このように、旧サンプリングポイント及び新サンプリングポイントのそれぞれで取得された論理値が一致するかしないかを判断することで、悪意のあるＥＣＵによる攻撃があったか否かを判定することができる。
【００７４】
第１論理値と第２論理値とが一致すると判断された場合（ステップＳ６７５でＹＥＳ）、ＥＣＵ６００は通常の動作、つまり次のメッセージがＣＡＮバス２００にあるか否かの判断に移る。ＣＡＮバス２００にメッセージがあれば（ステップＳ８０でＹＥＳ）、ＥＣＵ６００はこれを受信し（ステップＳ２０）、なければ（ステップＳ８０でＮＯ）メッセージ受信の動作を終了する。
【００７５】
第１論理値と第２論理値とが一致しないと判断された場合（ステップＳ６７５でＮＯ）、ＥＣＵ６００では、不正メッセージが検知された場合に対応付けられた処理である不正検知時処理が不正検知処理部６２８によって実行される。この不正検知時処理としては、ネットワークにおける通信時にエラーが発生したことを通知するフレーム、例えば上述のようなエラーフレームがＣＡＮバス２００に送信されてもよい。これにより車載通信システム１０Ａにおいて改ざんされたメッセージを受信していたＥＣＵ１００ではこのメッセージが破棄され、送信側のＥＣＵ１００は再送信を実行することができる。または、車載

通信システム１０Ａが備える画面などの図示しないユーザインターフェースを介してユーザに警告がされてもよい。これにより、ユーザは悪意のあるＥＣＵが車載通信システム１０Ａに接続されていることを知って対処することができる。

【００７６】

このように、本実施の形態における不正メッセージ検知装置は、バス型ネットワークにおけるバスに送出された不正メッセージを検知する不正メッセージ検知装置であって、１ビット期間において前記バス上の信号の論理値を取得するために前記バスの電圧が読み出される時点であるサンプリングポイントを調整するために、前記信号のエッジを検出し、前記エッジに基づく再同期を実行するか否かを判定する再同期検出部と、前記再同期検出部によって再同期を実行すると判定された後の１ビット期間において、当該エッジが検出される前に用いられていたサンプリングポイントにおける前記バスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおける前記バスの論理値である第２論理値とを取得する受信部と、前記受信部で取得された前記第１論理値及び前記第２論理値を比較する比較部と、前記比較部によって前記第１論理値及び前記第２論理値が一致しないと判断された場合に、不正メッセージが検知された場合に対応付けられた不正検知時処理を実行する不正検知処理部とを備える。この不正メッセージ検知装置は、ネットワーク上の悪意のあるＥＣＵによるメッセージの改ざんを確実に検知して高い精度でメッセージの正当性を判定し、このネットワークを備える機器、本実施の形態として記載された例であれば、自動車の安全な動作を確保することができる。

【００７７】

なお、上記の実施の形態において記載されたＥＣＵ６００を備える機器又はシステムについては特に限定されない。上記ではＥＣＵ６００がメッセージの受信の動作においてメッセージの改ざんを検知する例を説明したが、ＥＣＵ６００はエラーフレーム以外のメッセージの送信も行う通信機器が備えるＥＣＵであってもよい。例えば車載通信システムに接続される任意のシステムのＥＣＵ、例えば空調システムのＥＣＵやカーナビゲーションシステムのＥＣＵであってもよい。また、ネットワークの監視専用の機器として接続される機器が備えるＥＣＵであってもよい。また、監視ＣＡＮコントローラ６２０は、ＣＡＮバスどうしを接続するゲートウェイのＥＣＵに装備されてもよい。この場合、この監視ＣＡＮコントローラ６２０はゲートウェイが接続する複数のＣＡＮバスを監視してもよい。

【００７８】

（効果）

上述のとおり、上記の構成を有する不正メッセージ検知装置は、ネットワーク上の悪意のあるＥＣＵによるメッセージの改ざんを確実に検知して高い精度でメッセージの正当性を判定する。

【００７９】

上記の構成を有する不正メッセージ検知装置以外でこのような攻撃に対処する手段としては、１ビット期間内のＣＡＮバス上の電気的な変化の回数に基づく方法が考えられる。これには、例えばサンプリングポイント間の周期を短くして、１ビットの間で何度もＣＡＮバス上の電気的な変化をスキャンするように読み取る方法が考えられる。しかしこの方法では、サンプリングとサンプリングとの間で電圧の操作を攻撃することで、電気的な変化の検知を回避することができる。このような検知の回避を困難にするためにサンプリングポイント間の周期をより短くすることは論理的には可能であるが、消費電力の増加や取得する論理値の記憶のためのメモリのコストの増加を招く。一方、本実施の形態における不正メッセージ検知装置であれば、従来のＣＡＮコントローラに比べてサンプリング間の周期が短縮されるのは、再同期が実行される場合であって、悪意のある装置による電圧の操作が起こり得るタイミングに限られる。したがって、消費電力やメモリのコストの増加は限定的である。

【００８０】

また、受信側のＥＣＵがデータの改ざんを検知できるように、送信側のＥＣＵがメッセージにＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を含めると

いう方法も考えられる。この方法の場合、ＣＡＮの規格ではデータフレームの各スロットの用途が図２に示されるように規定されているため、その中でデータフィールドにＭＡＣが挿入される。しかしながら、十分な安全性を担保するために用いられるＭＡＣは一般的に１２８ビット長であり、データフィールドの既定の最大長である６４ビットに収まらない。より短い簡易的なＭＡＣを用いることも考えられるが、ＭＡＣを短くすることは安全性の高さとのトレードオフである。仮に短いＭＡＣを用いたとしても、その分データフィールドに含めることができる情報量が制限され、通信効率が低下する。また、ＭＡＣによって安全性を確保するためには、ＭＡＣを扱うための回路をネットワーク上のすべてのＥＣＵに装備させる必要があり、コストの増加を招き、また、普及までに時間がかかる。一方、本実施の形態における不正メッセージ検知装置であれば、ネットワーク上で１台のＥＣＵがこれを備え、ＣＡＮバス上の電圧の操作の変化を監視することでデータの改ざんを検知することができる。したがって、既存のネットワークにも容易に適用することができる。また、本実施の形態における不正メッセージ検知装置では、データフィールドを不正メッセージの検知のためには消費しないため、通信効率への影響は生じない。

【００８１】

ここまで、バス型ネットワークで接続される通信機器からなる車載通信システムにおいて、このバスに送出された不正メッセージを検知する不正メッセージ検知装置として、ＥＣＵの一部に装備される監視ＣＡＮコントローラについて説明した。なお、例えばＣＡＮの規格が利用されるネットワークであれば、上述した再同期の仕組みを利用する攻撃は車載のネットワークに限らず実行することができる。したがって、例えばＣＡＮの規格が利用されるネットワークで制御される工作機械などにも上記の実施の形態における不正メッセージ装置は有用に適用される。また、ＣＡＮの規格が利用されないネットワークであっても、複数の通信機器から送信される信号の衝突の問題を、上述した再同期のような方法を用いて解消しているネットワークであれば同様の攻撃が可能であるため、上記の実施の形態における不正メッセージ装置は有用に適用される。

【００８２】

以上、一つの態様に係る不正メッセージ検知装置について、実施の形態に基づいて説明したが、本発明はこの実施の形態に限定されるものではない。例えば上記の実施の形態において、監視ＣＡＮコントローラ６２０の各構成要素によって実行される、ＣＡＮバス２００の監視及び不正メッセージの検知の動作のフローにおける処理をステップとして含む不正メッセージ検知方法として実現されてもよい。また、各構成要素は専用のハードウェアで構成されてもよいし、十分な処理速度が確保されるのであれば、各構成要素に適したソフトウェアプログラムをＣＰＵなどのプロセッサが実行することによって実現されてもよい。例えばプロセッサが、ハードディスク又は半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。ここで、上記実施の形態の不正メッセージ検知装置を実現するソフトウェアプログラムとは次のようなプログラムである。

【００８３】

本発明の一態様に係る不正メッセージ検知プログラムは、プロセッサに、バス型ネットワークにおけるバスに送出された不正メッセージを検知する不正メッセージ検知方法であって、１ビット期間において前記バス上の信号の論理値を取得するために前記バスの電圧が読み出される時点であるサンプリングポイントを調整するために、前記信号のエッジを検出し、前記エッジに基づく再同期を実行するか否かを判定する再同期検知ステップと、前記再同期検知ステップで再同期を実行すると判定された後の１ビット期間において、当該エッジが検知される前に用いられていたサンプリングポイントにおける前記バスの論理値である第１論理値と、当該エッジに基づく再同期後のサンプリングポイントにおける前記バスの論理値である第２論理値とを取得する受信ステップと、前記受信ステップで取得された前記第１論理値及び前記第２論理値を比較する比較ステップと、前記比較ステップにおいて前記第１論理値及び前記第２論理値が一致しないと判断された場合に、不正メッセージが検知された場合に対応付けられた不正検知時処理を実行する不正検知処理ステッ

プとを含む方法を実行させるプログラムである。

【００８４】

また本発明は、上記で説明した不正メッセージ検知装置を備えるＥＣＵとして実現されてもよい。

【００８５】

以上、一つの態様に係る不正メッセージ検知装置について、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したものや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つ又は複数の態様の範囲内に含まれてもよい。

【００８６】

例えば上記の実施の形態として記載された例では、同期時間保持部は第１同期時間保持部６２５及び第２同期時間保持部６２６の２個のみであるが、同期時間保持部の個数は２個に限定されない。１台の監視ＣＡＮコントローラが、例えば３個以上の同期時間保持部を備えることで、複数の受信側のＥＣＵ１００に対する異なるタイミングの攻撃を検知することができる。

【産業上の利用可能性】

【００８７】

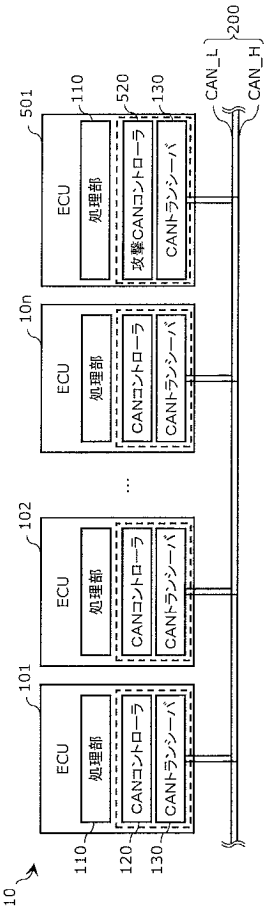
本発明は、ＣＤＭＡ／ＣＡ方式等の通信プロトコルを用いて通信可能な複数の装置が接続されるネットワーク、例えば車載ネットワーク等として利用されるＣＡＮ等に利用可能である。

【符号の説明】

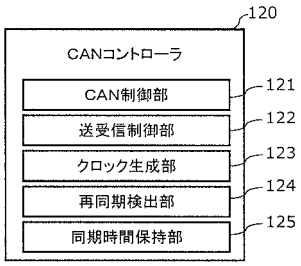
【００８８】

１０、１０Ａ　車載通信システム
１００、１０１、１０２、１０ｎ、５０１、６００　ＥＣＵ
１１０　処理部
１２０　ＣＡＮコントローラ
１２１　ＣＡＮ制御部
１２２　送受信制御部
１２３　クロック生成部
１２４　再同期検出部
１２５　同期時間保持部
１２６　攻撃タイミング生成部
１３０　ＣＡＮトランシーバ
２００　ＣＡＮバス
５２０　攻撃ＣＡＮコントローラ
６２０　監視ＣＡＮコントローラ
６２５　第１同期時間保持部
６２６　第２同期時間保持部
６２７　比較部
６２８　不正検知処理部

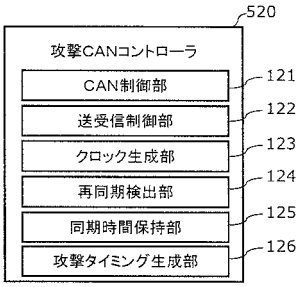
【図１Ａ】



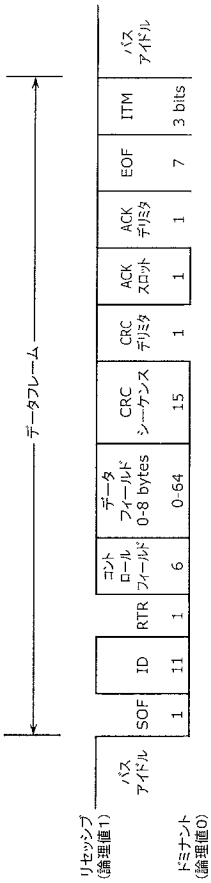
【図１Ｂ】



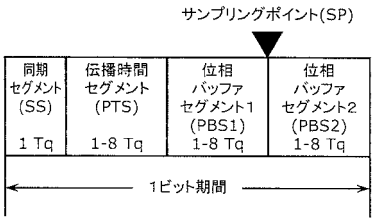
【図１Ｃ】



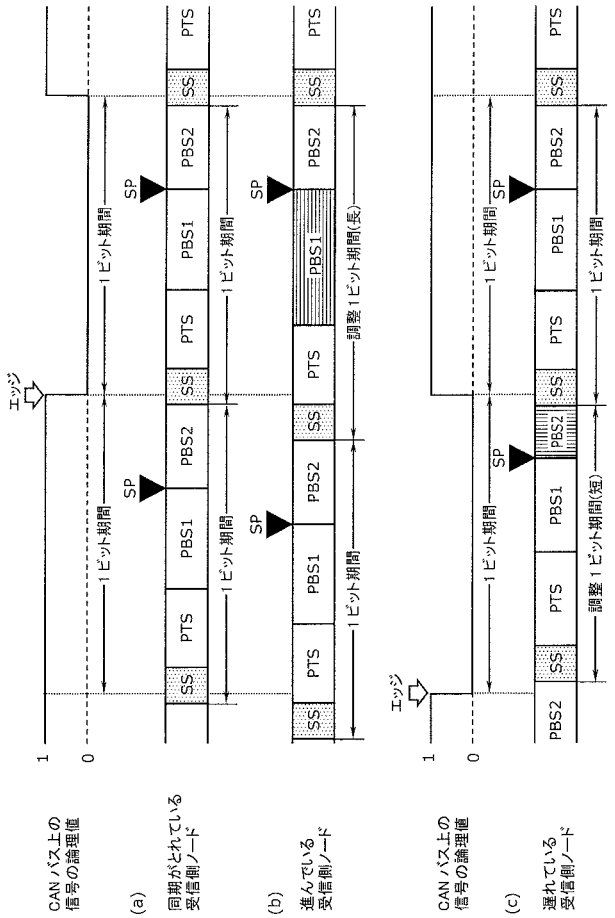
【図２】



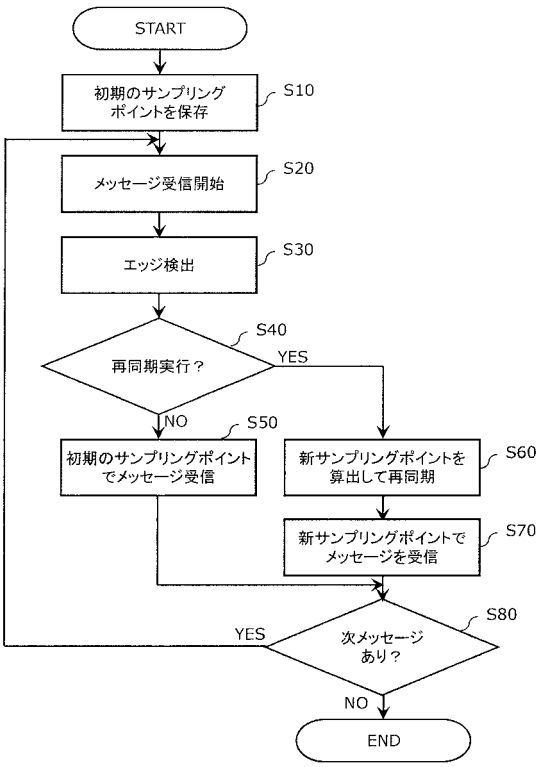
【図３】



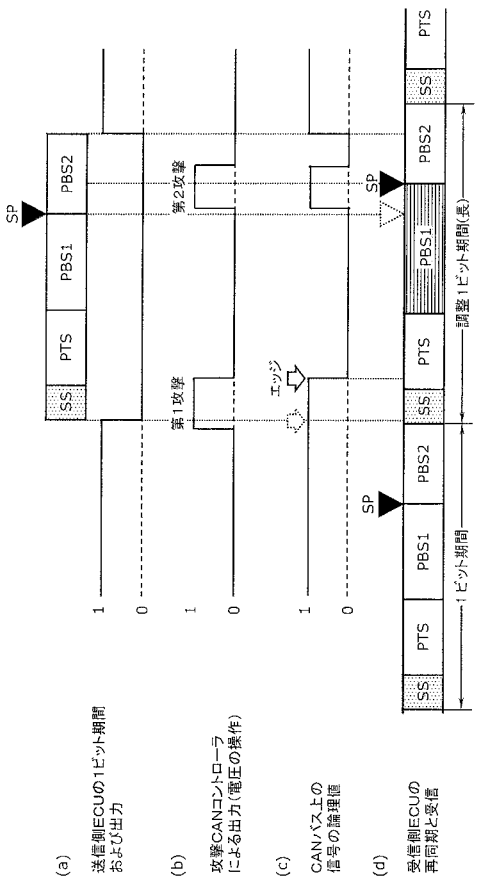
【図４】


エッジ
1ビット期間
SP
SS
PTS
PBS1
PBS2
調整1ビット期間(長)
調整1ビット期間(短)
CANバス上の信号の論理値
(a) 同期がとれている受信側ノード
(b) 進んでいる受信側ノード
(c) 遅れている受信側ノード

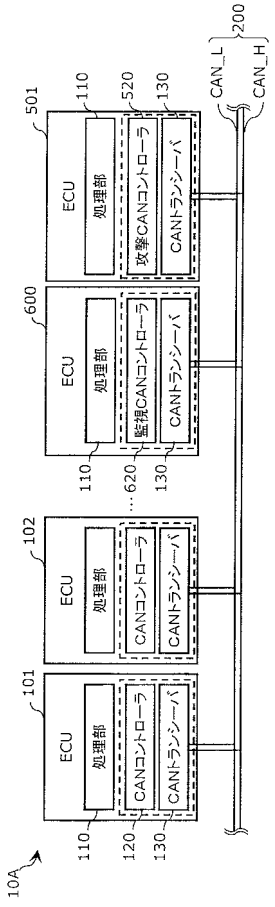
【図５】


START
初期のサンプリングポイントを保存
S10
メッセージ受信開始
S20
エッジ検出
S30
再同期実行？
S40
YES
NO
初期のサンプリングポイントでメッセージ受信
S50
新サンプリングポイントを算出して再同期
S60
新サンプリングポイントでメッセージを受信
S70
次メッセージあり？
S80
YES
NO
END

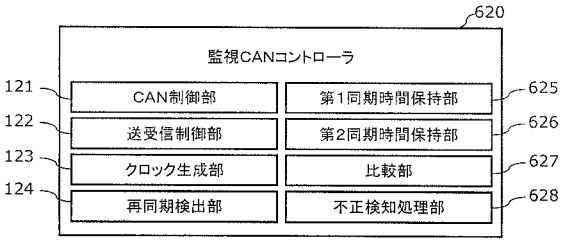
【図６】


(a) 送信側ECUの1ビット期間および出力
(b) 攻撃CANコントローラによる出力(電圧の操作)
(c) CANバス上の信号の論理値
(d) 受信側ECUの再同期と受信
第1攻撃
第2攻撃
エッジ
SP
SS
PTS
PBS1
PBS2
1ビット期間
調整1ビット期間(長)

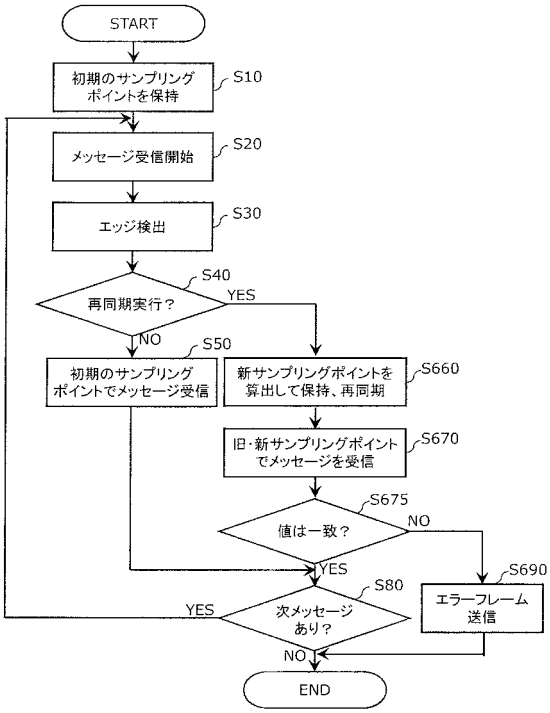
【図７Ａ】


10A
ECU
処理部
CANコントローラ
攻撃CANコントローラ
監視CANコントローラ
CANトランシーバ
CAN_L
CAN_H
101
102
110
120
130
200
501
520
600
620

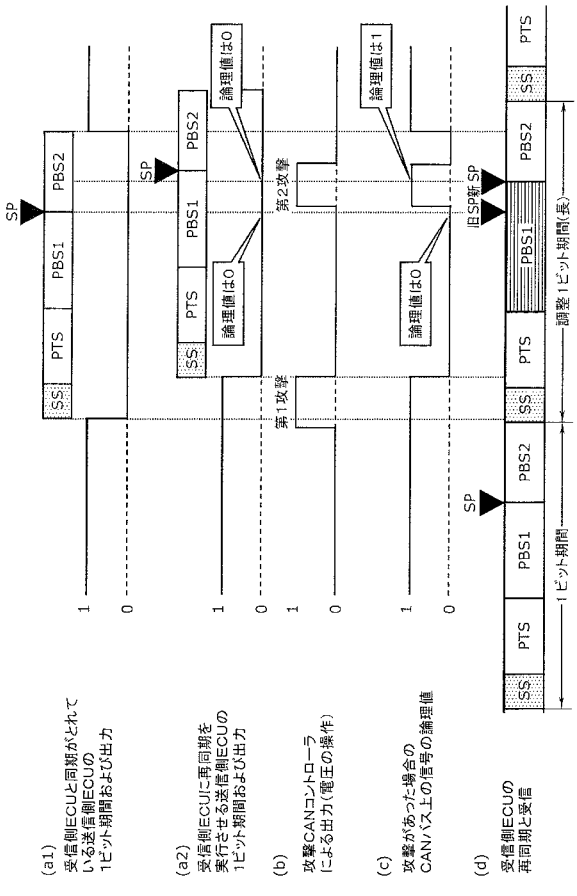
【図７Ｂ】


620
監視CANコントローラ
121
CAN制御部
第1同期時間保持部
625
122
送受信制御部
第2同期時間保持部
626
123
クロック生成部
比較部
627
124
再同期検出部
不正検知処理部
628

【図８】


START
初期のサンプリング ポイントを保持
S10
メッセージ受信開始
S20
エッジ検出
S30
再同期実行？
S40
YES
NO
初期のサンプリング ポイントでメッセージ受信
S50
新サンプリングポイントを 算出して保持、再同期
S660
旧・新サンプリングポイント でメッセージを受信
S670
値は一致？
S675
NO
YES
次メッセージ あり？
S80
YES
エラーフレーム 送信
S690
NO
END

【図９】


SP
PBS2
PBS1
PTS
SS
論理値は0
論理値は1
第2攻撃
第1攻撃
旧SP
新SP
調整1ビット期間(長)
1ビット期間
(a1) 受信側ECUと同期がとれている送信側ECUの1ビット期間および出力
(a2) 受信側ECUに再同期を実行させる送信側ECUの1ビット期間および出力
(b) 攻撃CANコントローラによる出力(電圧の操作)
(c) 攻撃があった場合のCANバス上の信号の論理値
(d) 受信側ECUの再同期と受信

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/005116

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/40(2006.01)i, *H04L12/413*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/40, H04L12/413

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2017
Kokai Jitsuyo Shinan Koho 1971-2017 Toroku Jitsuyo Shinan Koho 1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Tsutomu MATSUMOTO et al., "CAN ni Okeru Saidoki o Riyo shita Denkiteki Data Kaizan", 2015 Symposium on Cryptography and Information Security SCIS2015, 2015.01	1-8
A	US 2014/0334314 A1 (FREDRIKSSON, LB), 13 November 2014 (13.11.2014), & US 8737426 B1 & WO 2014/143717 A1	1-8
A	AL-MEKKAWY, M K et al., Reliable design of the CAN bit synchronization block, Proceedings of the WSEAS Conference: Information Science, Communications and Applications (ISCA 2005), 2005	1-8

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 February 2017 (24.02.17)	07 March 2017 (07.03.17)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２０１６／００５１１６

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/40(2006.01)i, H04L12/413(2006.01)i

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L12/40, H04L12/413

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	松本勉ほか，ＣＡＮにおける再同期を利用した電気的データ改ざん，２０１５年　暗号と情報セキュリティシンポジウム　ＳＣＩＳ２０１５，2015.01	1-8
A	US 2014/0334314 A1 (FREDRIKSSON, LB) 2014.11.13, & US 8737426 B1 & WO 2014/143717 A1	1-8

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２４．０２．２０１７	０７．０３．２０１７

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5X	3365
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	速水　雄太 電話番号　０３－３５８１－１１０１　内線　３５９６		

国際調査報告 国際出願番号 PCT／JP2016／005116

C（続き）. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	AL-MEKKAWY, M K et al., Reliable design of the CAN bit synchronization block, Proceedings of the WSEAS Conference: Information Science, Communications and Applications (ISCA 2005), 2005	1-8

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。