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

特許第6454614号
(P6454614)

(45)発行日　平成31年1月16日(2019.1.16)　(24)登録日　平成30年12月21日(2018.12.21)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	650B
B60R	16/023	(2006.01)	B60R	16/023	P
H04L	12/28	(2006.01)	H04L	12/28	100A
			H04L	12/28	200Z

請求項の数 6　(全 17 頁)

(21)出願番号　特願2015-139116(P2015-139116)
(22)出願日　平成27年7月10日(2015.7.10)
(65)公開番号　特開2017-21219(P2017-21219A)
(43)公開日　平成29年1月26日(2017.1.26)
審査請求日　平成29年12月12日(2017.12.12)

(73)特許権者　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　110001689
青稜特許業務法人
(72)発明者　吉田　博隆
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　萱島　信
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　大和田　徹
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

最終頁に続く

(54)【発明の名称】車載システム、その制御装置および制御方法

(57)【特許請求の範囲】
【請求項１】
複数の制御装置を通信可能に接続する車載システムであって、
前記複数の制御装置の中の第１の制御装置は、
複数のベース乱数を格納する第１のベース乱数記憶部と、
パケット識別子に紐づくマスク値を、パケット識別子に対応させてマスク値テーブルとして格納する第１のマスク値記憶部と、
前記第１のベース乱数記憶部のベース乱数の格納場所を示す第1のインデックスを用いて、前記第１のベース乱数記憶部からパケット乱数の長さ分だけのベース乱数を取得し、送信するパケットの識別子から前記第1のマスク値記憶部に格納されたマスク値を取得し、取得したベース乱数とマスク値の排他的論理和によりパケット乱数を生成する第１のパケット乱数生成部と、
通信するデータに前記第１のパケット乱数生成部により生成されたパケット乱数を付加した通信パケットを送信する第１の通信部と、を有し、
前記複数の制御装置の中の第２の制御装置は、
前記第１のベース乱数記憶部と同一のベース乱数を格納する第２のベース乱数記憶部と、
前記第１のマスク値記憶部と同一のマスク値テーブルを格納する第２のマスク値記憶部と、
前記第１の通信部から通信パケットを受信する第２の通信部と、

前記第２の通信部により受信した通信パケットからパケット乱数とパケット識別子を取得し、取得したパケット識別子と前記第２のマスク値記憶部に格納されたマスク値に基づいて、パケットの識別子に対応するマスク値を取得し、前記第１のインデックスと同一の第２のインデックスを用いて、前記第２のベース乱数記憶部からパケット乱数の長さ分だけのベース乱数を取得し、取得したベース乱数とマスク値の排他的論理和によりパケット乱数を生成する第２のパケット乱数生成部と、

前記第２のパケット乱数生成部によって生成されたパケット乱数と前記第２の通信部より受信されたパケット乱数とにより通信パケットの検証を行う通信パケット検証部とを有することを特徴とする車載システム。

【請求項２】

前記第１の制御装置は、複数のベース乱数を生成するベース乱数生成部と、パケット識別子毎にパケット識別子に紐づくマスク値を生成するマスク値生成部とを有し、

前記第１の通信部は、

車両のエンジン起動時に、前記ベース乱数生成部の生成したベース乱数と前記マスク値生成部の生成したマスク値を前記第２の制御装置へ送信し、

前記第２の通信部は、

前記ベース乱数生成部の生成したベース乱数と前記マスク値生成部の生成したマスク値を前記第１の制御装置から受信し、

前記第２のベース乱数記憶部は、前記第２の通信部が受信したベース乱数が格納される

前記第２のマスク値記憶部は、前記第２の通信部が受信したマスク値が格納されることを特徴とする請求項１に記載の車載システム。

【請求項３】

前記第１の制御装置は、

前記第１のベース乱数記憶部に格納された複数のベース乱数の取得位置を特定するベース乱数インデックスに基づき同期情報を生成する同期情報生成部をさらに備え、

前記第１の通信部は、

前記生成された同期情報を前記第２の制御装置へ送信し、

前記第２の通信部は、

前記生成された同期情報を前記第１の制御装置から受信し、

前記第２の制御装置は、

前記第２のベース乱数記憶部に格納された複数のベース乱数の取得位置を特定するベース乱数インデックスを前記第２の通信部が受信した同期情報に基づき同期する同期部を備えたことを特徴とする請求項２に記載の車載システム。

【請求項４】

第１の制御装置が第２の制御装置へ制御情報を送信する車載システムの制御方法であって、

前記第１の制御装置は、

第１のＣＰＵと、

複数のベース乱数と、パケットの複数の識別子それぞれに紐づけてマスク値を格納する第１のメモリを備え、

前記第１のＣＰＵは、

前記第１のメモリのベース乱数の格納場所を示す第1のインデックスを用いて、前記第１のメモリからパケット乱数の長さ分だけのベース乱数を取得し、送信するパケットの識別子から前記第1のメモリに格納されたマスク値に基づいて、送信するパケットの識別子に対応するマスク値を取得し、取得したベース乱数とマスク値の排他的論理和により第１のパケット乱数を生成し、

通信するデータに前記第１のパケット乱数を付加した通信パケットを前記第２の制御装置に送信し、

前記第２の制御装置は、

第２のＣＰＵと、

前記第１のメモリと同一の複数のベース乱数と、前記第１のメモリと同一のパケットの複数の識別子それぞれに紐づけてマスク値を格納する第２のメモリを備え、
前記第２のＣＰＵは、
前記第１の制御装置から受信した通信パケットからパケット乱数とパケット識別子を取得し、取得したパケット識別子に基づいて前記第２のメモリに格納されたパケット識別子に対応するマスク値を取得し、前記第１のインデックスと同一の第２のインデックスを用いて、前記第２のメモリからパケット乱数の長さ分だけのベース乱数を取得し、取得したベース乱数とマスク値の排他的論理和により第２のパケット乱数を生成し、
前記第２のパケット乱数と前記第１のパケット乱数とにより通信パケットの検証を行うことを特徴とする車載システムの制御方法。

【請求項５】
前記第１の制御装置は、複数のベース乱数を生成するベース乱数生成部と、パケット識別子毎にパケット識別子に紐づくマスク値を生成するマスク値生成部とを有し、
車両のエンジン起動時に、前記ベース乱数生成部の生成したベース乱数と前記マスク値生成部の生成したマスク値を前記第２の制御装置へ送信し、
前記第２の制御装置は、
前記ベース乱数生成部の生成したベース乱数と前記マスク値生成部の生成したマスク値を前記第１の制御装置から受信する第２の通信部を有し、
前記第２のメモリは、前記第２の通信部が受信したベース乱数が格納され、
前記第２のメモリは、前記第２の通信部が受信したマスク値が格納されることを特徴とする請求項４に記載の車載システムの制御方法。

【請求項６】
前記第１の制御装置は、
前記第１のメモリに格納された複数のベース乱数の取得位置を特定するベース乱数インデックスに基づき同期情報を生成し、
前記生成された同期情報を前記第２の制御装置へ送信し、
前記第２の制御装置は、
前記生成された同期情報を前記第１の制御装置から受信し、
前記第２のメモリに格納された複数のベース乱数の取得位置を特定するベース乱数インデックスを前記第２の通信部が受信した同期情報に基づき同期することを特徴とする請求項５に記載の車載システムの制御方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、車載システム、その制御装置および制御方法に関するものである。
【背景技術】
【０００２】
自動車の制御を支える車載システムでは、ＥＣＵ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｎｔｒｏｌ　Ｕｎｉｔ）と呼ばれる組み込みシステムが制御装置として制御を行っている。例えば、エンジン制御の場合、ＥＣＵがエンジン等の状態をセンサによって観測し、燃料噴射量を算出し、適切なタイミングで点火させるための制御を行う。さらに、制御処理は、周期的動作であり、かつ実行周期は短い。したがって、データの更新頻度が高い。
【０００３】
自動車の車載ネットワークにおける代表的な標準プロトコルとしてＣｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（以下、ＣＡＮ）が広く使用されており、さらに今後はＣＡＮを拡張したＣＡＮ　ＦＤ（Ｆｌｅｘｉｂｌｅ　Ｄａｔａ－Ｒａｔｅ）も普及が進むことが予想されている。
【０００４】
このような車載ネットワークを用いた車載システムについても、一般的な情報システムと同様に、脅威が指摘されつつある。例えば、ＯＢＤ２（Ｏｎ－Ｂｏａｒｄ－Ｄｉａｇｎ

ｏｓｔｉｃｓ　２）ポートのような車載ネットワークに直接繋がっているインタフェースに不正な機器を接続し、リプレイ攻撃（再送攻撃）が行なわれる脅威等がある。ここで、リプレイ攻撃とは、攻撃者が通信路上を流れるパケットを盗聴して事前に取得し、取得したパケットを再送することで自動車の不正な動作を引き起こす攻撃である。

【０００５】

第三者による受信者のシステムのリプレイ攻撃に対する対策手段として、パケットごとに値が変わるシーケンス番号（順序番号）を付与することが知られている。シーケンス番号によるリプレイ攻撃対策技術は、ネットワーク層での認証および暗号化を行うプロトコルとしてＩＥＴＦで標準化されたＩＰＳｅｃにおいても採用されている。

【０００６】

また、予測困難性を確保するために、パケットごとに値が変わる乱数を生成し、シーケンス番号として採用することが知られており、特許文献１には、暗号化側において、まず、演算器Aで、疑似乱数生成器の出力Ｘiと、ｍ遅延器Bから得られるそのｍステップ前の疑似乱数生成器の出力Ｘi-mとのビットごとの排他的論理和をとり、次に、演算器Cで上記排他的論理和の結果と平文のブロックMiとのビットごとの排他的論理和をとることにより暗号文を作成する技術が開示されている。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開２００３－１５８５１５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

特許文献１に開示された技術によれば、複数のブロックからなる長文を疑似乱数生成器により暗号化するシステムにおいて、単独のブロックを暗号化するのと同程度の処理量と安全度で長文の各ブロックを効率的に暗号化できるようになる。

【０００９】

しかしながら、車載システムにおける制御装置は低コストであることを要求されることが多く、暗号処理で使える計算リソースが限られるため、特許文献１に開示された技術でも負担が大きく、計算リソースが枯渇して車両の制御へ影響する可能性がある。また、車載システムでは１つの制御装置が他の複数の制御装置へ制御情報を送信する場合も多く、送信先の複数の制御装置ごとに独立な乱数列を生成することも大きな負担となる。

【００１０】

そこで、本発明の目的は、車両システムの通信に適した乱数処理を提供することにある。

【課題を解決するための手段】

【００１１】

本発明に係る代表的な制御装置は、車載システムにおいて制御情報を送信する制御装置であって、複数のベース乱数が格納される乱数記憶部と、パケットの複数の識別子それぞれに紐づけてマスク値が格納されるマスク値記憶部と、前記乱数記憶部に格納された複数のベース乱数の中から１つのベース乱数を取得し、前記マスク値記憶部に格納された複数のマスク値の中から、前記制御情報を送信するためのパケットの識別子に紐づくマスク値を取得し、前記取得したベース乱数と前記取得したマスク値とに基づきパケット乱数を生成するパケット乱数生成部と、前記制御情報と前記生成したパケット乱数を含むパケットを送信する通信部とを備えたことを特徴とする。

【発明の効果】

【００１２】

本発明によれば、車両システムの通信に適した乱数処理が可能になる。

【図面の簡単な説明】

【００１３】

【図１】車載システムの構成の例を示す図である。
【図２】制御装置のハードウェアの構成の例を示す図である。
【図３】通信の全体フローの例を示す図である。
【図４】秘匿共有処理のフローの例を示す図である。
【図５】パケット送信処理のフローの例を示す図である。
【図６】パケット受信処理のフローの例を示す図である。
【図７】マスク値テーブルの構成の例を示す図である。
【図８】通信パケットの構成の例を示す図である。
【図９】複数の受信制御装置を含む車載システムの構成の例を示す図である。
【図１０】同期補正を含む車載システムの構成の例を示す図である。
【図１１】同期補正を含む通信の全体フローの例を示す図である。
【図１２】送信制御装置の同期補正処理のフローの例を示す図である。
【図１３】受信制御装置の同期補正処理のフローの例を示す図である。
【発明を実施するための形態】
【００１４】
以下、本発明の実施形態について、実施例を用い、図面を参照しながら詳細に説明する。
【実施例１】
【００１５】
（車載システムの構成）
図１を参照して、車載システムの構成の例を説明する。図１において、車載システム１００は、送信制御装置１１０、受信制御装置１３０、通信バス１９０を含んで構成される。車載システム１００では、送信制御装置１１０がパケット乱数を生成し、通信バス１９０を介して、データとともにパケット乱数を格納したパケットを送信する。受信制御装置１３０は受信したパケットの乱数の真正性を検証し、真正性の検証された受信パケットに格納されたデータの取得を行なう。
【００１６】
なお、以下では、送信制御装置１１０と受信制御装置１３０の送信と受信を区別せずに単に制御装置と呼ぶことがある。また、送信制御装置１１０と受信制御装置１３０のそれぞれは、送信と受信の両方の構成を有する制御装置であってもよい。
【００１７】
（送信制御装置）
通信バス１９０には、一つまたは複数の制御装置が接続される。ここでは、送信制御装置１１０と受信制御装置１３０の二つの制御装置が接続される例を示す。送信制御装置１１０は、通信部１１１、通信パケット生成部１１２、パケット乱数生成部１１３、マスク値テーブル生成部１１４、ベース乱数生成部１１５、鍵管理部１１７、ベース乱数記憶部１１８、マスク値テーブル記憶部１１９を含んで構成されている。
【００１８】
通信部１１１は、通信パケット生成部１１２が生成した通信パケットを通信バス１９０経由で受信制御装置１３０へ送信する。通信パケット生成部１１２は通信パケットを生成する。パケット乱数生成部１１３はパケット乱数を生成する。マスク値テーブル生成部１１４はマスク値のテーブルを生成する。ベース乱数生成部１１５はベース乱数を生成する。
【００１９】
鍵管理部１１７は、パケット乱数生成部１１３やベース乱数生成部１１５がそれぞれの乱数データを生成するための暗号処理を行う際に用いる鍵を管理する。ベース乱数記憶部１１８は、ベース乱数生成部１１５が生成したベース乱数を記憶する。マスク値テーブル記憶部１１９は、マスク値テーブル生成部１１４が生成したマスク値のテーブルを記憶する。
【００２０】

（受信制御装置）
受信制御装置１３０は、通信部１３１、通信パケット検証部１３２、パケット乱数生成部１３３、ベース乱数生成部１３５、鍵管理部１３７、ベース乱数記憶部１３８、マスク値テーブル記憶部１３９を含んで構成されている。なお、ベース乱数生成部１３５は含まれなくてもよい。通信部１３１は、制御装置１１０の通信パケット生成部１１２が生成した通信パケットを通信バス１９０経由で受信する。通信パケット検証部１３２は、制御装置１１０から送信された通信パケットに含まれるパケット乱数を検証する。
【００２１】
パケット乱数生成部１３３は、通信パケット検証部１３２が通信パケットの検証を行うために、マスク値テーブルとベース乱数とを入力とした処理を行い、パケット乱数を生成する。ベース乱数生成部１３５は、暗号処理によりベース乱数を生成する。鍵管理部１３７は、パケット乱数生成部１３３やベース乱数生成部１３５がそれぞれのデータを生成するための暗号処理を行う際に用いる鍵を管理する。ベース乱数記憶部１３８は、ベース乱数を記憶する。
【００２２】
マスク値テーブル記憶部１３９は、パケット乱数生成部１３３がパケット乱数を生成するために入力として使用するマスク値テーブルを記憶する。なお、記憶されるマスク値テーブルは、送信制御装置１１０のマスク値テーブル生成部１３４が生成したものを受信するか、もしくは、受信制御装置１３０自体が生成してもよい。送信制御装置１１０から受信したパケットに格納されたパケット乱数を通信パケット検証部１３２が検証して、正規と判断されたパケットのデータが受信制御装置１３０に格納される。
【００２３】
（制御装置のハードウェア構成）
図２を参照して、制御装置のハードウェアの構成の例を説明する。この例では、送信制御装置１１０と受信制御装置１３０のハードウェアは同じであるので、まとめて説明する。図２において、制御装置は、通信装置１１、入出力装置１２、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１４、メモリ１５を含んで構成されている。
【００２４】
ＣＰＵ１４はメモリ１５に格納されたプログラムにしたがって、通信装置１１、入出力装置１２、メモリ１５から情報を読み出し、読み出した情報に演算を行い、通信装置１１、入出力装置１２、メモリ１５へ情報を書き込む。メモリ１５は、ＣＰＵ１４のプログラムが格納されたり、ＣＰＵ１４の処理結果が一時的に格納されたりする。入出力装置１２は、車両の図示を省略したセンサまたはアクチュエータと通信する。通信装置１１は、他の制御装置と通信バス１９０を介して通信する。
【００２５】
ＣＰＵ１４がメモリ１５に格納されたプログラムを実行することにより、ＣＰＵ１４とメモリ１５とは、図１に示した例えば通信パケット生成部１１２などの各部となってもよい。通信部１１１、１３１は通信装置１１を含んでもよい。ベース乱数記憶部１１８、１３８とマスク値テーブル記憶部１１９、１３９はメモリ１５であってもよい。そして、ＣＰＵ１４、メモリ１５、通信装置１１以外の図示を省略したハードウェアを含めて、図１に示した各部を形成してもよい。
【００２６】
なお、ＣＰＵ１４とメモリ１５は低コストなものであってもよい。このため、例えばＣＰＵ１４は性能の高くないものであってもよいし、メモリ１５は大容量なものでなくてもよい。
【００２７】
（送信制御装置と受信制御装置の通信処理の全体概要）
図３を参照して、送信制御装置１１０と受信制御装置１３０の間の通信処理の全体概要の例について説明する。送信制御装置１１０は、通信パケットのシーケンス番号の代わりとなるパケット乱数を通信パケットに格納する。パケット乱数は、各パケットＩＤと、そ

のパケットＩＤに対応して秘密かつランダムに選択されたマスク値というデータを格納するテーブルであるマスク値テーブルを用いて生成される。ここで、秘密とは、制御装置１１０と制御装置１３０のみに格納されている値であるという意味である。

【００２８】

マスク値テーブルの例については後で図９を用いて説明する。ベース乱数を暗号化処理（例えばＡＥＳ：Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）に含まれる擬似乱数生成器等の利用により暗号学的に生成し、送信制御装置１１０と受信制御装置１３０が、ベース乱数とマスク値テーブルを共有し、それらを用いたパケット乱数の生成を行うことを特徴とする。

【００２９】

送信制御装置１１０と受信制御装置１３０は、車両のエンジン起動時と実利用時にフェーズを分けて、それぞれのフェーズに応じた処理を行う。まずエンジン起動時に、送信制御装置１１０と受信制御装置１３０の間で、秘匿共有処理（Ｓ２０１）を実施する。そして、実利用時に、送信制御装置１１０がパケット乱数送信処理（Ｓ２０２）を繰り返し、これに対応して、受信制御装置１３０がパケット乱数受信処理（Ｓ２０３）を繰り返すことにより、パケット乱数通信を安全に実施する。

【００３０】

エンジン起動時等の秘匿共有処理（Ｓ２０１）は、ベース乱数共有処理（Ｓ３１１）とマスク値テーブル共有処理（Ｓ３１２）を含み、ベース乱数とマスク値テーブルの事前共有を行う。ベース乱数共有処理（Ｓ３１１）とマスク値テーブル共有処理（Ｓ３１２）の詳細については、図４を用いて説明する。

【００３１】

実利用時には、送信制御装置１１０がマスク値テーブルを参照し（Ｓ３１５）、パケット乱数生成し（Ｓ３１６）、パケット乱数送信する（Ｓ２０２）。受信制御装置１３０がマスク値テーブルを参照し（Ｓ３２４）、パケット乱数生成（Ｓ３２６）し、パケット検証する（Ｓ３２６）。パケット乱数送信処理（Ｓ２０２）とパケット乱数受信処理（Ｓ２０３）については、図５と図６を用いて後でさらに説明する。

【００３２】

（秘匿共有処理）

図４は、エンジン起動時の秘匿共有処理（Ｓ２０１）の例を示す図である。既に説明したように秘匿共有処理（Ｓ２０１）はベース乱数共有処理（Ｓ３１１）とマスク値テーブル共有処理（Ｓ３１２）とからなる。

【００３３】

まず、ベース乱数共有処理（Ｓ３１１）に関して説明する。受信制御装置１３０は、ベース乱数生成のために必要な乱数生成量（乱数の個数）等のパラメータを送信制御装置１１０に送信する（Ｓ４２１）。送信制御装置１１０のベース乱数生成部１１５は、受信制御装置１３０からのパラメータを受信し（Ｓ４１０）、ベース乱数の生成に必要なパラメータを決定する（Ｓ４１１）。ここで、決定するパラメータは例えば乱数生成量に応じたパラメータであってもよい。

【００３４】

決定したパラメータに基づき、ベース乱数生成部１１５はベース乱数の生成を行い、ベース乱数記憶部１１８に格納する（Ｓ４１２）。なお、ベース乱数生成部１１５は、鍵管理部１１７に格納された鍵情報が入力された暗号処理において使用される疑似乱数生成を用いてベース乱数を生成する。

【００３５】

ここで、ベース乱数は複数生成され、所定系列の疑似乱数となってもよい。１つのベース乱数の長さ（ビット長）は十分に長くてもよく、決定したパラメータに応じた個数が生成されてもよい。生成したベース乱数は受信制御装置１３０に送信され（Ｓ４１３）、受信制御装置１３０は、送信されたベース乱数を受信する（Ｓ４２２）。

【００３６】

次に、マスク値テーブル共有処理（Ｓ３１２）に関して説明する。送信制御装置１１０のマスク値テーブル生成部１１４は、パケットＩＤに依存するデータであるマスク値をパケットＩＤごとに生成し（Ｓ４１４）、パケットＩＤをインデックスとして、このインデックスに対応する値をマスク値とするマスク値テーブルを生成し、マスク値テーブル記憶部１１９に格納する（Ｓ４１５）。

【００３７】

生成したマスク値テーブルは、受信制御装置１３０に送信され（Ｓ４１６）、受信制御装置１４０は、送信されたマスク値テーブルを受信し（Ｓ４２３）、受信時点までにマスク値テーブルが設定されていなければ、受信したマスク値テーブルをマスク値テーブル記憶部１３９に格納し、そうでなければ、受信したマスク値テーブルでマスク値テーブル記憶部１３９を更新する（Ｓ４２４）。

【００３８】

なお、マスク値自体は、パケットＩＤに依存するデータであれば、暗号処理に用いられる擬似乱数生成器等により生成されてもよい。また、マスク値テーブル更新（Ｓ４２４）のタイミングはエンジン起動時とし、車両実利用時の期間は、同じマスク値テーブルを使い続ける。また、ベース乱数の生成とマスク値テーブルの生成は、送信制御装置１１０と受信制御装置１３０の両方で行ってもよい。

【００３９】

（送信制御装置のパケット乱数送信）

図５を参照して、パケット乱数送信処理（Ｓ２０２）の例を説明する。この例では、複数のベース乱数がベース乱数記憶部１１８に格納され、各ベース乱数をインデックスにより指し示される。各ベース乱数は固定長のデータであってもよい。まず、ベース乱数記憶部１１８の中でベース乱数の使用箇所を指すインデックスであるベース乱数インデックスが初期化される。

【００４０】

送信制御装置１１０は、ベース乱数記憶部１１８の中のベース乱数インデックスが指し示す場所から、パケット乱数の長さ分だけのベース乱数を取得し、ベース乱数インデックスの値を１つのベース乱数の長さ分だけインクリメントする（Ｓ５０１）。そして、送信するパケットのＩＤを取得し（Ｓ５０２）、マスク値テーブル記憶部１１９に格納されたマスク値テーブルを参照し（Ｓ５０３）、取得したパケットＩＤに対応するマスク値を取得する（Ｓ５０４）。

【００４１】

パケット乱数生成部１１５は、取得したベース乱数と取得したマスク値の排他的論理和により、パケット乱数を生成する（Ｓ５０５）。通信パケット生成部１１２は、送信制御装置１１０の上で動作する図示を省略した制御アプリケーションから取得するデータに、生成したパケット乱数を付加し、通信パケットを生成する（Ｓ５０６）。通信部１１１は、通信パケット生成部１１２で生成した通信パケットを受信制御装置１３０へバス１９０を介して送信する（Ｓ５０７）。そして、ベース乱数の取得（Ｓ５０１）へ戻る。

【００４２】

なお、通信パケットの構成については、図８を用いて後で説明する。また、ベース乱数インデックスの値のインクリメントは、ベース乱数の取得時とベース乱数の取得時以外を含めて所定のタイミングであってもよい。この所定のタイミングは例えば１０ｍＳごとの予め設定された時間の間隔でもよいし、例えば０時０分０秒を起点に１０ｍＳごとの予め設定された時刻の間隔であってもよい。また、１回のベース乱数の取得（Ｓ５０１）に対して、予め設定された期間内は、パケットＩＤの取得（Ｓ５０２）から通信パケットの送信（Ｓ５０７）までを複数実行してもよい。

【００４３】

（受信制御装置のパケット乱数受信）

図６を参照して、パケット乱数受信処理（Ｓ２０３）を説明する。ベース乱数記憶部１３８の中でベース乱数の使用箇所を指すインデックスであるベース乱数インデックスの初

期化を行う。受信制御装置１３０は、ベース乱数記憶部１３８の中のベース乱数インデックスが指し示す場所から、パケット乱数の長さ分だけのベース乱数を取得し、ベース乱数インデックスの値を前記乱数の長さ分だけインクリメントする（Ｓ６０１）。

【００４４】

通信部１３１は、通信バス１９０を介して通信パケットを受信し（Ｓ６０２）、パケット乱数を取得し、パケットＩＤを取得する（Ｓ６０３）。マスク値テーブル記憶部１３９に格納されたマスク値テーブルを参照し（Ｓ６０４）、取得したパケットＩＤに対応するマスク値を取得する（Ｓ６０５）。パケット乱数生成部１３２は、取得したベース乱数と取得したマスク値の排他的論理和により、パケット乱数を生成する（Ｓ６０６）。

【００４５】

通信パケット検証部１３２は、通信パケットから取得したパケット乱数と生成したパケット乱数が等しいか否かを判定して通信パケットを検証し（Ｓ６０７）、２つのパケット乱数が等しいと判定された場合（Ｓ６０８）、通信パケットは真正なものとして、図示を省略した記憶部に通信パケットのデータを格納する（Ｓ６０９）。２つのパケット乱数が等しくないと判定された場合（Ｓ６０８）、通信パケット検証部１３２は、受信した通信パケットを破棄する。そして、ベース乱数の取得（Ｓ６０１）へ戻る。

【００４６】

なお、ベース乱数インデックスの値のインクリメントは、ベース乱数の取得時とベース乱数の取得時以外を含めて所定のタイミングであってもよい。この所定のタイミングは例えば１０ｍＳごとの予め設定された時間の間隔でもよいし、例えば０時０分０秒を起点に１０ｍＳごとの予め設定された時刻の間隔であってもよい。送信制御装置１１０からの信号に基づいてもよい。このため、１回のベース乱数の取得（Ｓ６０１）に対して、パケット受信（Ｓ６０２）からパケットデータ格納（Ｓ６０９）までを複数実行してもよい。

【００４７】

次に、送信制御装置１１０と受信制御装置１３０との間で、どのような構成を持つ情報を処理または通信すれば、パケット乱数を用いた通信を行うことができるかを示すために、各種情報の構成を説明する。

【００４８】

（マスク値テーブルの構成）

図７を参照して、マスク値テーブル９００の構成の例を説明する。マスク値テーブル９００は、マスク値テーブル生成部１１４により生成され、マスク値テーブル記憶部１１９、１３９に格納される。マスク値テーブル９００は、パケットＩＤ欄９０１とマスク値欄９０２から成る。この例では、パケットＩＤ欄９０１の「ＩＤ＿１」とマスク値欄９０２の「ＭＡＳＫ＿ＩＤ１」とが対応する、すなわち紐づくことを表す。以下、マスク値テーブル９００のパケットＩＤ欄９０１の「ＩＤ＿２」と「ＩＤ＿３」のそれぞれはマスク値欄９０２の「ＭＡＳＫ＿ＩＤ２」と「ＭＡＳＫ＿ＩＤ３」のそれぞれに紐づくテーブルである。

【００４９】

マスク値欄９０２の各マスク値は、マスク値テーブル生成部１１４が、鍵管理部１１７に格納された鍵情報とパケットＩＤ欄９０１のパケットＩＤを入力とする暗号処理の疑似乱数生成により生成されてもよい。マスク値欄９０２のマスク値は、パケットＩＤ欄９０１のパケットＩＤを使用した乱数とすることにより、パケットＩＤに依存する。なお、マスク値の生成はこのような処理に限定されるものではない。また、マスク値テーブル９００の構成も図７に示した例に限定されるものではない。

【００５０】

（通信パケットの構成）

図８を参照して、通信パケット１０００の構成の例を説明する。この通信パケット１０００は、通信パケット生成部１１２により生成される通信パケットであり、例えば図３を用いて説明したパケット送信（Ｓ３１７）にて通信部１１１から通信バス１９０に送信され、パケット受信（Ｓ３２３）にて通信部１３１で受信される通信パケットである。

【００５１】
通信パケット１０００は、ヘッダ情報１０１１、データ１０１２、パケット乱数１０１３、フッタ情報１０１５から成る。ヘッダ情報１０１１は、例えば車載ネットワークである通信バス１９０のＣＡＮ　ＦＤにおけるアービトレーションフィールドやコントロールフィールドを示すが、他の通信プロトコルにおいては、通信先、通信元、データ長等を示す情報を含むものであればよい。なお、ヘッダ情報はパケットＩＤを含んでもよい。
【００５２】
データ１０１２は、車両を制御するためのデータなどであり、受信制御装置１３０で真正なものと判定されれば使用される。パケット乱数１０１３はパケット乱数生成部１１３、１３３で生成される既に説明したパケット乱数であり、一定の長さの乱数であってもよい。また、パケット乱数１０１３は検証情報であるとみなしてもよい。フッタ情報１０１４は、例えば車載ネットワークである通信バス１９０のＣＡＮ　ＦＤにおける周期的冗長性チェックフィールドやアクノレッジフィールドを示す。
【００５３】
通信パケット１０００を構成する情報は図８の例に限定されるものではなく、情報の順序も図８の例に限定されるものではなく、各情報の内容は図８を用いて説明した内容に限定されるものではない。
【００５４】
以上のように、排他的論理和という単純な演算により、パケットＩＤごとに異なる乱数の系列を生成することができる。
【００５５】
（複数の受信制御装置へのパケット乱数送信）
図９を参照して、複数の受信制御装置１３０へのパケット乱数送信処理の例を説明する。図９は、１つの送信制御装置１１０から、パケットＩＤが「ＩＤ＿１」の通信パケット１１０４を受信制御装置１３０に送信し、パケットＩＤが「ＩＤ＿２」の通信パケット１１０５を受信制御装置１４０に送信する例を示す図である。
【００５６】
送信制御装置１１０は、受信制御装置１３０と受信制御装置１４０のそれぞれへ通信パケット１１０４と通信パケット１１０５を送信するために、ベース乱数記憶部１１８の中のベース乱数インデックスで指定された箇所から、パケット乱数と同じ長さのベース乱数１１０１－１の値「ＩＶ＿ＩＤ１」を取得する。また、マスク値テーブル記憶部１１９を参照し、パケットＩＤが「ＩＤ＿１」に対応するマスク値１１０２－１の値「ＭＡＳＫ＿ＩＤ１」と、パケットＩＤが「ＩＤ＿２」に対応するマスク値１１０３－１の値「ＭＡＳＫ＿ＩＤ２」を取得する。
【００５７】
次に、値「ＩＶ＿ＩＤ１」と値「ＭＡＳＫ＿ＩＤ１」を排他的論理和して乱数「ｒ１」を算出し、パケットＩＤの「ＩＤ＿１」と乱数「ｒ１」を含む通信パケット１１０４を生成し、受信制御装置１３０へ送信する。また、値「ＩＶ＿ＩＤ２」と値「ＭＡＳＫ＿ＩＤ２」を排他的論理和して乱数「ｒ２」を算出し、パケットＩＤの「ＩＤ＿２」と乱数「ｒ２」を含む通信パケット１１０５を生成し、受信制御装置１４０へ送信する。
【００５８】
受信制御装置１３０は、受信した通信パケット１１０４から乱数「ｒ１」を取得する。ベース乱数記憶部１３８の中のベース乱数インデックスで指定された箇所から、パケット乱数と同じ長さのベース乱数１１０１－２の値「ＩＶ＿ＩＤ１」を取得し、マスク値テーブル記憶部１３９を参照し、パケットＩＤが「ＩＤ１」に対応するマスク値１１０２－２の値「ＭＡＳＫ＿ＩＤ１」を取得する。
【００５９】
次に、値「ＩＶ＿ＩＤ１」と値「ＭＡＳＫ＿ＩＤ１」を排他的論理和して乱数「ｒ１」を算出し、通信パケット１１０４から取得した乱数「ｒ１」と比較する。この例では、ベース乱数１１０１－１とベース乱数１１０１－２の値が「ＩＶ＿ＩＤ１」で等しく、マス

ク値１１０２－１とマスク値１１０２－２の値が「ＭＡＳＫ＿ＩＤ１」で等しいため、乱数「ｒ１」も等しく、比較の結果は等しいと判定される。このように等しいと判定されると、通信パケット１１０４は真正なものであると検証されたことになる。

【００６０】

受信制御装置１４０は、受信した通信パケット１１０５から乱数「ｒ２」を取得する。ベース乱数記憶部１４８の中のベース乱数インデックスで指定された箇所から、パケット乱数と同じ長さのベース乱数１１０１－３の値「ＩＶ＿ＩＤ１」を取得し、マスク値テーブルを参照し、パケットＩＤが「ＩＤ２」に対応するマスク値１１０３－３の値「ＭＡＳＫ＿ＩＤ２」を取得する。

【００６１】

次に、値「ＩＶ＿ＩＤ１」と値「ＭＡＳＫ＿ＩＤ２」を排他的論理和して乱数「ｒ２」を算出し、通信パケット１１０４から取得した乱数「ｒ２」と比較する。この例では、ベース乱数１１０１－１とベース乱数１１０１－３の値が「ＩＶ＿ＩＤ１」で等しく、マスク値１１０３－１とマスク値１１０３－３の値が「ＭＡＳＫ＿ＩＤ２」で等しいため、乱数「ｒ２」も等しく、比較の結果は等しいと判定される。このように等しいと判定されると、通信パケット１１０５は真正なものであると検証されたことになる。

【００６２】

なお、パケット１１０４とパケット１１０５に含まれるデータは同じであっても、異なっていてもよい。

【００６３】

以上で説明したように、１つの送信制御装置から複数の異なる受信制御装置へパケットを送信する場合であっても、複数の異なる受信制御装置それぞれに使用するパケットＩＤごとに排他的論理和という単純な演算により、乱数を生成できる。このため、車載システムのような低コストの制御装置であっても、車両制御への悪影響を与えることなく、車載システムのセキュリティを確保できる。

【００６４】

特に車載システムのように同じ周期、例えば１０ｍＳ間隔で制御情報がそろって送信されることの多いシステムでは、共通のベース乱数を多く利用することができるため、制御装置の計算リソースの節約度が高い。

【００６５】

また、同じ周期で多くのパケットが送信されるシステムへ適用する方が、乱数生成のための計算リソースの節約度が高いため、好ましい。

【００６６】

１つの系列のベース乱数は例えば１ＭＢであるため、複数の系列のベース乱数が格納され、セキュリティ向上のために定期的に更新されると、車載システムとしては更新コストの高いものとなるが、ベース乱数記憶部１１８、１３８、１４８は１つの系列のベース乱数が格納されるだけであるので、ベース乱数の更新コストを低くできる。また、ベース乱数記憶部１１８、１３８、１４８の記憶容量も小さくなるため、小容量のメモリ１５を採用できる。

【実施例２】

【００６７】

（同期補正を行う通信保護システム）

実施例１で説明した構成では、ベース乱数の使用箇所を指すインデックスであるベース乱数インデックスが、送信制御装置１１０と受信制御装置１３０の両方で一致している必要がある。通信エラー等により、両方のベース乱数インデックスが一致しなくなった状態（同期ずれ状態）が生じる可能性もある。

【００６８】

実施例２では、同期ずれ状態が生じたときに、送信制御装置１１０が同期を補正するための情報を送信し、元の同期が取れた状態、即ち、ベース乱数インデックスが送信制御装置１１０と受信制御装置１３０で一致する状態に補正する例を説明する。図２を用いて説

明したハードウェア構成、図３～８を用いて説明した秘匿共有処理（Ｓ２０１）、パケット乱数送信処理（Ｓ２０２）、パケット乱数受信処理（Ｓ２０３）などについて、実施例２は実施例１と同じであるので説明を省略し、実施例２で差分となる構成についいて説明する。

【００６９】

図１０を参照して、同期補正を含む車載システム１００の構成の例を説明する。送信制御装置１１０は、同期補正情報生成部１１６を備え、同期補正情報を生成する。また、受信制御装置１３０は、同期補正部１３６を備え、送信制御装置１１０から受信した同期補正情報を基に、パケット乱数に関する同期補正を行う。

次に図１１を参照して、送信制御装置１１０と受信制御装置１３０の間の同期処理を含む通信処理の全体概要の例について説明する。秘匿共有処理（Ｓ２０１）、パケット乱数送信処理（Ｓ２０２）、パケット乱数受信処理（Ｓ２０３）は図３を用いて既に説明したとおりである。同期補正時には、送信側同期処理（Ｓ２０４）として、送信制御装置１１０は、同期補正情報を生成し（Ｓ３１８）、生成した同期補正情報を送信する（Ｓ３１９）。

【００７０】

これに対して、受信制御装置１３０は、受信側同期処理（Ｓ２０５）として、送信制御装置１１０から同期補正情報を受信し（Ｓ３２７）、受信した同期補正情報に基づき同期補正する（Ｓ３２８）。送信側同期処理（Ｓ２０４）と受信側同期処理（Ｓ２０５）について、それぞれ図１２と図１３を用いてさらに説明する。

【００７１】

図１１の例では、同期補正時の後にエンジン起動時へ戻っているが、実利用時へ戻ってもよい。また、予め設定された回数あるいは時間だけ実利用時が経過すると同期補正時へ移ってもよい。また、図示を省略した複数の受信制御装置へ送信制御装置１１０は１つの同期補正情報を送信してもよい。

【００７２】

（送信側同期処理）

図１２を参照し、送信側同期処理（Ｓ２０４）の例を説明する。送信側同期処理（Ｓ２０４）は、同期補正時に送信制御装置１１０によって行われる。まず、送信制御装置１１０の同期補正情報生成部１１６は、ベース乱数インデックスを取得し（Ｓ７１１）、取得したベース乱数インデックスを適切な量だけインクリメントした値を、同期補正後のベース乱数インデックスとして、同期補正後のベース乱数インデックスを同期補正情報として格納した通信パケットを生成する（Ｓ７１２）。

【００７３】

ここで、インクリメントする適切な量とは、例えば送信制御装置１１０が既に消費した乱数の量であってもよいし、この既に消費した乱数の量と取得したベース乱数インテックスの値との差分であってもよいし、予め設定された値であってもよい。制御装置１１０の通信部１１１は、生成した通信パケットを通信バス１９０経由で制御装置１３０へ送信する（Ｓ７１３）。

【００７４】

（受信側同期処理）

図１３を参照して、受信側同期処理（Ｓ２０５）の例を説明する。受信側同期処理（Ｓ２０５）は、同期補正時に受信制御装置１３０によって行われる。受信制御装置１３０の通信部１３１は、通信バス１９０を介して、送信制御装置１１０が送信した同期補正情報を格納した通信パケットを受信する（Ｓ８１１）。同期補正部１３６は、受信した通信パケットから同期補正情報を取得し（Ｓ８１２）、取得した同期補正情報を同期補正後のベース乱数インデックスとして設定することにより、同期補正を行う（Ｓ８１３）。

【００７５】

以上で説明したように、送信制御装置１１０と受信制御装置１３０との間で通信エラーや真正でない通信パケット等により、両方のベース乱数インデックスが一致しなくなった

同期ずれ情報が生じても、同期補正情報により、両方のベース乱数インデックスを一致させることができる。そして、送信制御装置１１０と受信制御装置１３０の通信を継続できる。

【００７６】

なお、本発明は、上述した実施例に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。そのような場合においてもシステム全体において行う処理に本質的な変化はない。

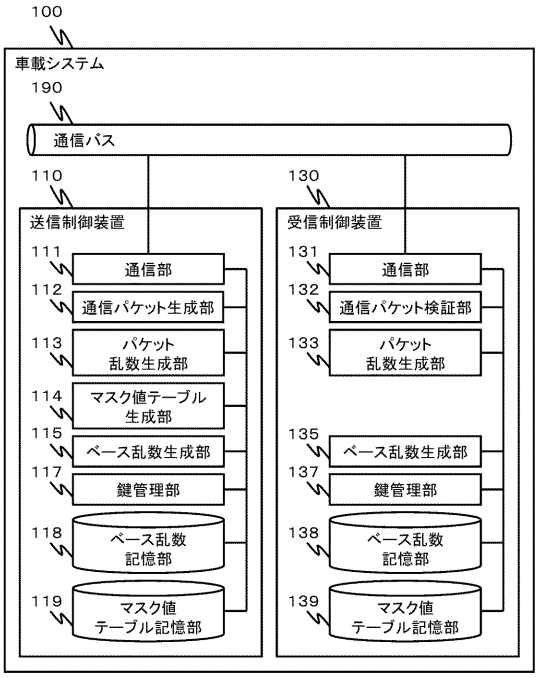
【符号の説明】

【００７７】

１１…通信装置、１２…入出力装置、１４…ＣＰＵ、１５…メモリ、１００…車載システム、１１０…送信制御装置、１１１…通信部、１１２…通信パケット生成部、１１３…パケット乱数送信制御部、１１４…マスク値テーブル記憶部、１１５…ベース乱数生成部、１１６…同期補正情報生成部、１１７…鍵管理部、１１８…ベース乱数記憶部、１１９…マスク値テーブル記憶部、１３０…受信制御装置、１３１…通信部、１３２…通信パケット検証部、１３３…パケット乱数生成部、１３５…ベース乱数生成部、１３６…同期補正部、１３７…鍵管理部、１３８…ベース乱数記憶部、１３９…マスク値テーブル記憶部、１４０…受信制御装置

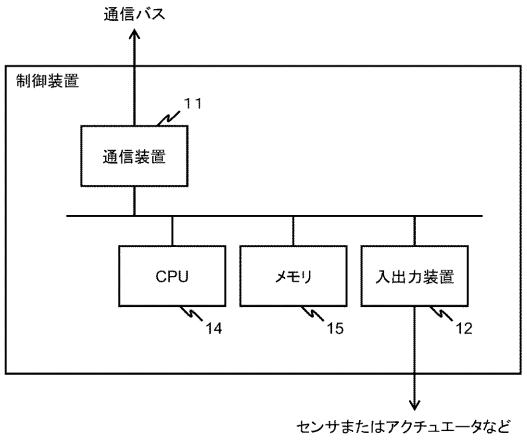
【図１】

図1



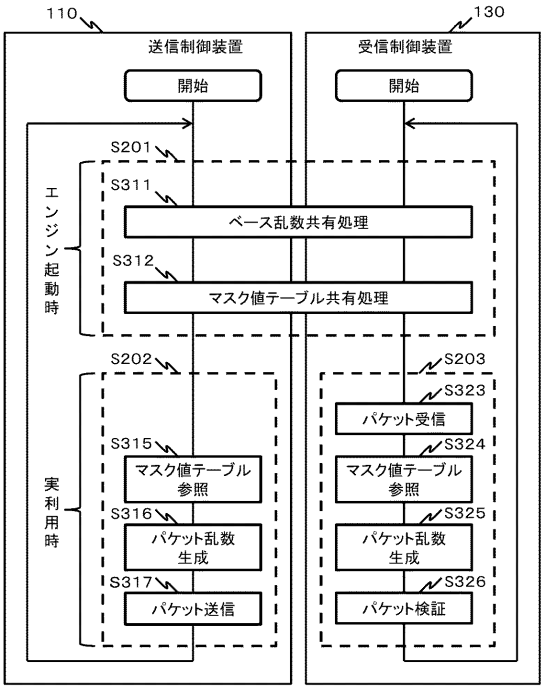
【図２】

図2



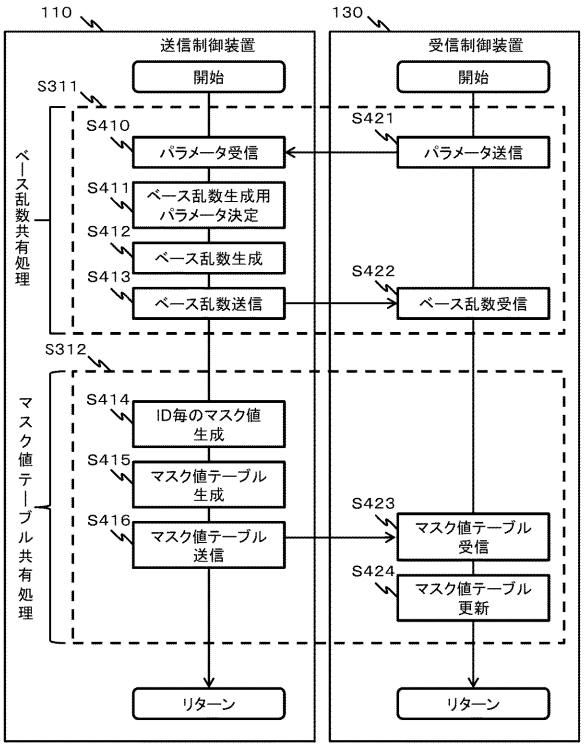
【図３】

図3



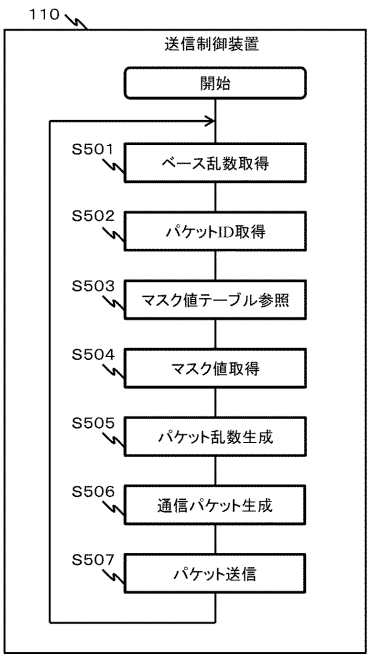
【図４】

図4



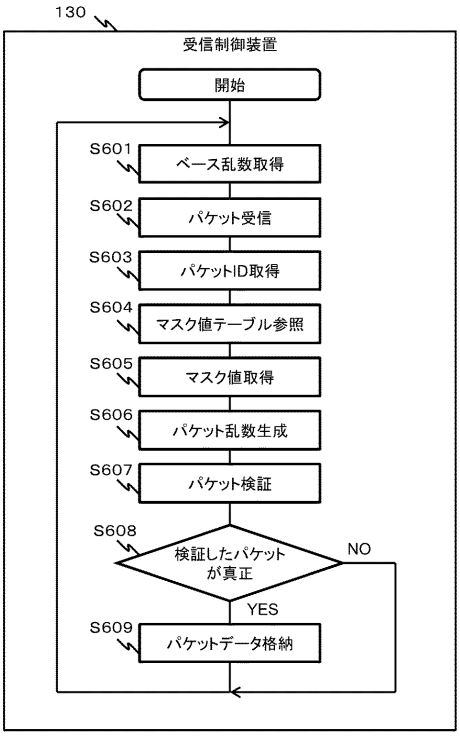
【図５】

図5



【図６】

図6



【図７】

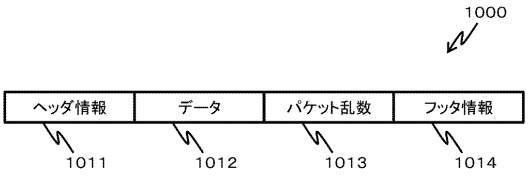
図7

900
マスク値テーブル

901 パケットID	902 マスク値
ID_1	MASK_ID1
ID_2	MASK_ID2
ID_3	MASK_ID3
…	…

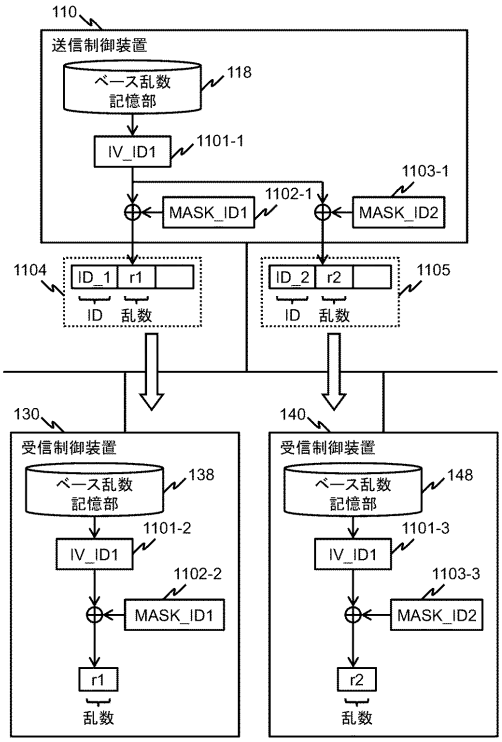
【図８】

図8



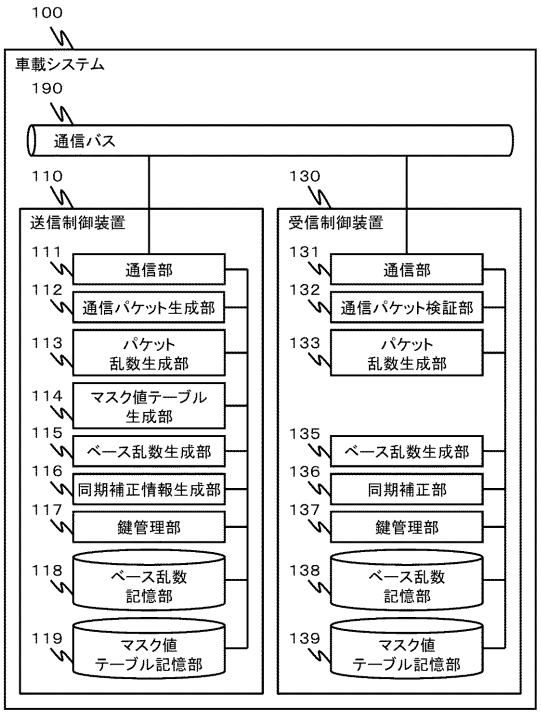
【図９】

図9



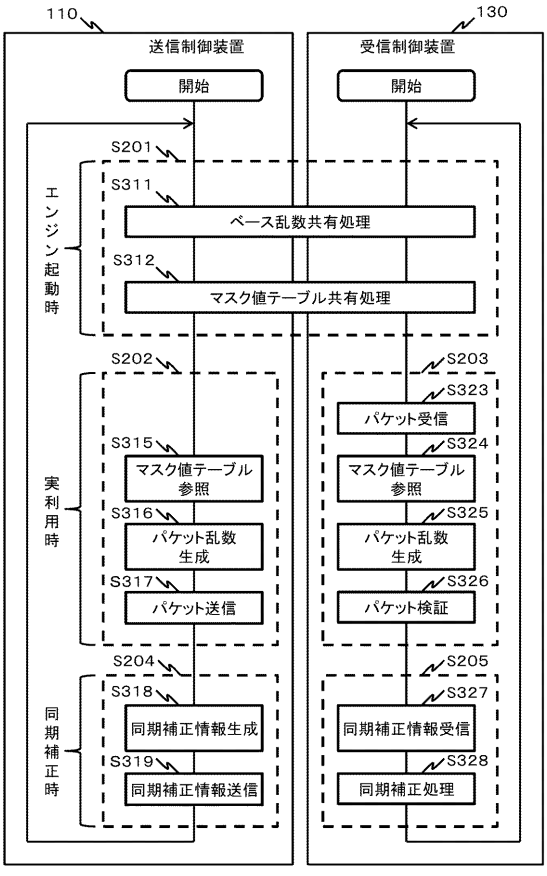
【図１０】

図10



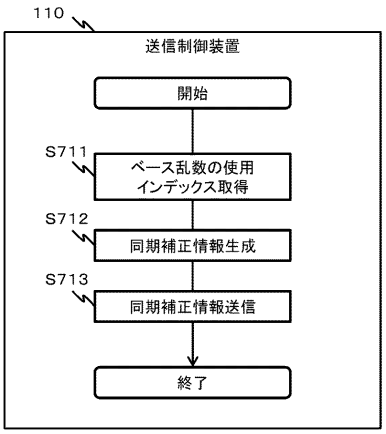
【図１１】

図11



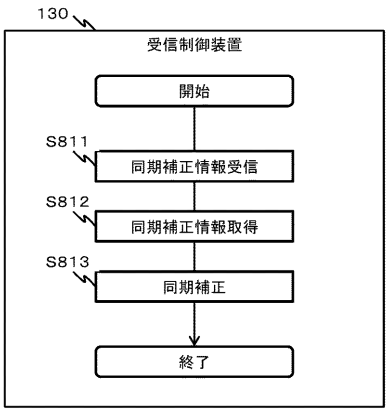
【図１２】

図12



【図１３】

図13



フロントページの続き

(72)発明者　森田　伸義
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　伯田　恵輔
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

審査官　金沢　史明

(56)参考文献　特開２００３－２８３４８９（ＪＰ，Ａ）
特開２００３－００８５９３（ＪＰ，Ａ）
国際公開第０２／０８２７１５（WO，Ａ１）
国際公開第２００８／０３５４５０（WO，Ａ１）
特開２０１６－１５８２０４（ＪＰ，Ａ）
吉岡顕，他，構成証明機能を持つ車内通信プロトコルの提案，マルチメディア，分散，協調とモバイル（ＤＩＣOMO２００８）シンポジウム論文集，日本，情報処理学会，２００８年　7月2日，Vol.2008，No.1，pp.1270-1275

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／３２
Ｂ６０Ｒ　１６／０２３
Ｈ０４Ｌ　１２／２８