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

特許第6233041号
(P6233041)

(45)発行日　平成29年11月22日(2017.11.22)　(24)登録日　平成29年11月2日(2017.11.2)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 673D
G06F 21/55 (2013.01)　　G06F 21/55

請求項の数 9　(全 10 頁)

(21)出願番号　特願2014-8107(P2014-8107)
(22)出願日　平成26年1月20日(2014.1.20)
(65)公開番号　特開2015-139011(P2015-139011A)
(43)公開日　平成27年7月30日(2015.7.30)
審査請求日　平成28年5月6日(2016.5.6)

(73)特許権者　000003207
トヨタ自動車株式会社
愛知県豊田市トヨタ町１番地
(74)代理人　100100549
弁理士　川口　嘉之
(74)代理人　100085006
弁理士　世良　和信
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100123319
弁理士　関根　武彦
(74)代理人　100123098
弁理士　今堀　克彦
(74)代理人　100143797
弁理士　宮下　文徳

最終頁に続く

(54)【発明の名称】無線通信装置および無線通信方法

(57)【特許請求の範囲】
【請求項１】
車両に搭載される無線通信装置であって、
前記無線通信装置または当該無線通信装置が搭載される車両の挙動を表す情報である挙動情報を取得する挙動情報取得手段と、
前記挙動情報取得手段から取得される挙動情報の履歴を格納する挙動情報記憶手段と、
前記挙動情報記憶手段に格納された直近の所定期間の挙動情報が、所定の種類の車両における挙動に合致しているか否かを判定する判定手段と、
前記判定手段によって、前記直近の所定期間の挙動情報が前記所定の種類の車両における挙動に合致していると判定された場合のみ、メッセージ送信を行う送信手段と、
を備える、無線通信装置。
【請求項２】
前記挙動情報は、加速度情報または位置情報であり、
前記挙動情報取得手段は、加速度センサまたは位置情報取得手段である、
請求項１に記載の無線通信装置。
【請求項３】
前記挙動情報は、車両の制御情報であり、
前記挙動情報取得手段は、車両制御装置から通信により車両の制御情報を取得する、
請求項１に記載の無線通信装置。
【請求項４】

前記判定手段は、前記送信手段によるメッセージ送信が要求された場合に、直近の所定期間の挙動情報の履歴が、車両の挙動に合致しているか否かを判定する、
請求項１から３のいずれか１項に記載の無線通信装置。
【請求項５】
前記判定手段は、車両の挙動を表す挙動情報に基づいて機械学習された識別器である、
請求項１から４のいずれか１項に記載の無線通信装置。
【請求項６】
あらかじめ格納された暗号鍵でメッセージを暗号化する暗号処理手段を更に備え、
前記送信手段は、前記暗号処理手段により暗号化されたメッセージを送信する、
請求項１から５のいずれか１項に記載の無線通信装置。
【請求項７】
前記挙動情報取得手段、前記挙動情報記憶手段、前記判定手段、前記送信手段は、いずれも耐タンパ装置によって構成される、
請求項１から６のいずれか１項に記載の無線通信装置。
【請求項８】
前記所定の種類の車両は、四輪以上の自動車である、
請求項１から７の何れか１項に記載の無線通信装置。
【請求項９】
車両に搭載され挙動情報取得手段と判定手段と送信手段とを有する無線通信装置が行う無線通信方法であって、
前記挙動情報取得手段が、前記無線通信装置または当該無線通信装置が搭載される車両の挙動を表す情報である挙動情報を取得して当該挙動情報の履歴を挙動情報記憶手段に格納するステップと、
前記判定手段が、前記挙動情報記憶手段に格納された直近の所定期間の挙動情報が所定の種類の車両における挙動に合致しているか否かを判定するステップと、
前記送信手段が、前記直近の所定期間の挙動情報が車両の挙動に合致していると判定された場合のみ、メッセージ送信を行うステップと、
を含む、無線通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信装置に関し、特に、車両になりすましたメッセージ送信を防止可能な無線通信装置に関する。
【背景技術】
【０００２】
近年の情報通信技術の発展に伴い、車両に情報処理装置および無線通信装置を搭載し、車両間あるいは車両と路側機等との間で無線通信を行うシステムが活発に検討されている。このような車車間通信や路車間通信等は、例えば交通安全システムや隊列走行システムなどに応用されるため、通信のセキュリティを確保することが必要である。
【０００３】
システムに対する攻撃として、攻撃者が車両になりすまして偽の情報を送信することが考えられる。例えば、走行中の車両が位置情報や走行方向などを互いに交換し、接触の危険がある場合に自動的にステアリングやブレーキやアクセルを操作して回避動作を行う交通安全システムにおいて、攻撃者が車両になりすまして通信すると、通信相手車両の運転に対して本来の状況に合致しない操作を誘発してしまう。このような攻撃がされると交通安全システムの機能低下が生じるので、第三者によるなりすましを防止することが必要である。
【０００４】
非特許文献１は、ＰＫＩ（公開鍵暗号基盤）とデジタル署名を使った認証を行って、通信相手が信頼できるかどうか判断している。特に、通信を行う車両同士は認証局の署名付

き公開鍵と秘密鍵のセットを用いて相互に認証を行うことが開示されている。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】M. Raya, J. P. Hubaux, "The security of vehicular ad hoc networks", 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks 2005, pp. 11-21, 2005
【発明の概要】
【発明が解決しようとする課題】
【０００６】
非特許文献１の手法では、通信を行う主体が車両であるという前提のもとに認証を行って、信頼できる相手であるかどうかを確認している。しかしながら、車載無線通信装置を車両から取り外して通信に用いたり、同等の機能を有する無線通信装置を新たに作成して通信に用いたりする場合には、他の車両は不正な利用に基づく通信であることを検知できない。
【０００７】
本発明は、攻撃者が車両になりすましてメッセージ送信することを防止可能な無線通信技術を提供することを目的とする。
【課題を解決するための手段】
【０００８】
本発明の一態様に係る無線通信装置は、挙動情報を取得する挙動情報取得手段と、前記挙動情報取得手段から取得される挙動情報の履歴を格納する挙動情報記憶手段と、前記挙動情報記憶手段に格納された挙動情報の履歴が、車両の挙動に合致しているか否かを判定する判定手段と、前記判定手段によって、前記挙動情報の履歴が車両の挙動に合致していると判定された場合のみ、メッセージ送信を行う送信手段と、を備える。
【０００９】
このような構成によれば、挙動情報の履歴が車両の挙動と一致する場合のみメッセージ送信が行われるため、本発明に係る無線通信装置を車両から取り外して使用した場合などにはメッセージ送信が行われない。したがって、攻撃者が車両になりすましてメッセージ送信することを防止可能となる。
【００１０】
本発明における挙動情報は、本発明に係る無線通信装置あるいは当該無線通信装置が搭載される装置の挙動を表す情報であれば任意の情報を採用可能である。挙動情報は、典型的には、装置の運動、姿勢、位置、制御状態などの少なくともいずれかを表す情報である。例えば、挙動情報として、加速度、速度、位置、向きの少なくともいずれかを採用可能である。それぞれに対応して、挙動情報取得手段として、加速度センサ、速度センサ、位置情報取得手段、ジャイロセンサを採用可能である。また、挙動情報として、本発明に係る無線通信装置が搭載される装置の制御情報を採用可能である。本発明に係る無線通信装置は車両に搭載されることが好ましいので、制御情報として、エンジン、アクセル、ブレーキ、ステアリングなどの車両機器の状態を表す情報を採用可能である。挙動情報取得手段は、このような車両の制御情報を、車両を制御する車両制御装置から通信により取得すればよい。
【００１１】
本発明の無線通信装置は、送信手段からのメッセージ送信が要求された場合に、判定手段が、直近の所定期間の挙動情報の履歴に基づいて、当該履歴が車両の挙動に合致するか否かを判定し、合致する場合のみ送信手段によるメッセージ送信を許可するように構成することができる。このようにすれば、最新の履歴情報に基づいて車両の挙動に合致するかどうかを判定することができ、また、メッセージ送信を行わない場合には判定処理を省略できる。ただし、判定手段は、定期的に挙動情報の履歴が車両の挙動に合致するか否かを判定し、送信手段は直近の判定結果に基づいてメッセージ送信を行うか否かを決定しても

構わない。このように構成すれば、メッセージ送信の度に判定処理を行わなくてよいので、判定処理の処理負荷を軽減することが可能となる。

【００１２】

本発明における判定手段は、車両の挙動を表す挙動情報を用いてあらかじめ機械学習された識別器を採用することができる。識別器は、入力された挙動情報の履歴が、車両の挙動に合致するか否か、あるいは車両の挙動である確からしさを出力する。ただし、判定手段は、機械学習を用いた識別器以外であってもよく、例えば、あらかじめ定められた条件を満足するか否かを判定する規則ベースの判定を行うものであってもよい。

【００１３】

また、本発明の無線通信装置は、あらかじめ格納された暗号鍵でメッセージを暗号化する暗号化処理手段を更に備え、送信手段は、暗号化処理手段により暗号化されたメッセージを送信することが好ましい。暗号化の方式は特に限定されず、公開鍵暗号方式であっても共通鍵暗号方式であっても構わない。メッセージ送信を暗号化することにより、攻撃者によるなりすましやメッセージの改ざんを防止したり、メッセージ内容の秘匿化が行える。

【００１４】

また、本発明の無線通信装置の挙動情報取得手段、挙動情報記憶手段、判定手段、送信手段はいずれも耐タンパ装置によって構成されることが好ましい。これらの要素を耐タンパ装置で構成することにより、情報内容を改ざんしたり、処理内容を改変したりする攻撃を防止することができる。なお、上記の各手段を１つの耐タンパ装置で構成してもよいし、複数の耐タンパ装置で構成してもよい。複数の耐タンパ装置で構成する場合は、装置間の通信を暗号化するなどして、不正な情報が入力されないようにすることが好ましい。

【００１５】

本発明は、上記の手段の少なくとも一部を備える無線通信装置として捉えることもできる。また、本発明は、上記の無線通信装置を搭載した車両として捉えることもできる。また、本発明は、上記処理の少なくとも一部を実行する無線通信方法として捉えることもできる。また、本発明は、この方法をコンピュータに実行させるためのコンピュータプログラム、あるいはこのコンピュータプログラムを非一時的に記憶したコンピュータ可読記憶媒体として捉えることもできる。上記手段および処理の各々は可能な限り互いに組み合わせて本発明を構成することができる。

【発明の効果】

【００１６】

本発明によれば、攻撃者が車両になりすましてメッセージ送信することを防止可能となる。

【図面の簡単な説明】

【００１７】

【図１】実施形態にかかる無線通信装置の構成を示す図である。

【図２】実施形態にかかる無線通信装置の送信時の処理の流れを示すフローチャートである。

【図３】変形例にかかる無線通信装置の構成を示す図である。

【発明を実施するための形態】

【００１８】

［構成］

本発明の実施形態は、車両に搭載され、他の車両あるいは路側通信機などとの通信に用いられる無線通信装置である。図１（ａ）は、車両１に搭載された無線通信装置１０から、車両２に搭載された無線通信装置２０へ、メッセージを送信する例を示している。送信側の無線通信装置１０の機能ブロックを図１（ｂ）に、受信側の無線通信装置２０の機能ブロックを図１（ｃ）にそれぞれ示している。なお、以下では、無線通信装置１０および２０がそれぞれ送信機能および受信機能のみを有するものとして説明するが、無線通信装置１０および２０のいずれも送信機能と受信機能の両方を有することが一般的である。

【００１９】
送信側の無線通信装置１０は、図１（ｂ）に示すように、加速度センサ１１ａ、ＧＰＳ装置１１ｂ、センシング履歴保存部１２、メッセージ送信部１３、挙動判定部１４、鍵保存部１５、暗号化部１６、無線通信部１７の各機能部を有する。無線通信装置１０のこれらの機能部は、プロセッサ（ＭＰＵ）とコンピュータプログラムの組合せによって実現してもよいし、ＡＳＩＣ等の専用のハードウェアによって実現してもよいし、ＦＰＧＡのような再構成可能なゲートアレイによって実現してもよいし、これらの組合せによって実現してもよい。
【００２０】
加速度センサ１１ａは、典型的には３軸の加速度センサであるが、２軸や１軸の加速度センサであってもよい。加速度センサ１１ａから得られる加速度情報によって、無線通信装置１０ひいては無線通信装置１０が搭載された車両１の動きが分かる。また、加速度情報を積分することによって、速度情報を得ることもできる。
【００２１】
ＧＰＳ装置１１ｂは、ＧＰＳ衛星信号から位置情報を取得する。ＧＰＳ装置によって、緯度、経度、高度の情報が分かる。なお、ＧＰＳ装置以外にも、ガリレオ、北斗、ＧＬＯＮＡＳＳなどの任意の衛星測位システムを用いて位置情報を取得する位置情報取得装置を採用することができる。また、衛星測位以外にも、携帯電話基地局や無線ＬＡＮアクセスポイントなどからの電波に基づく測位を採用しても構わない。
【００２２】
加速度センサ１１ａおよびＧＰＳ装置１１ｂは、無線通信装置１０の挙動を示す挙動情報を取得するセンサの一例である。したがって、加速度センサ１１ａやＧＰＳ装置１１ｂ以外にも、無線通信装置１０の挙動情報を取得可能なセンサであれば、任意のセンサを採用可能である。例えば、ジャイロセンサ（角速度センサ）、地磁気センサなどを用いることもできる。なお、本明細書中では、加速度センサ１１ａやＧＰＳ装置１１ｂを総称してセンサ１１と称する場合もある。
【００２３】
センシング履歴保存部１２は、センサ１１から取得されるセンサ情報（挙動情報）を格納する機能部であり、任意の種類のメモリ装置によって構成される。センサ１１は、定期的にセンサ情報を取得して、センシング履歴保存部１２に格納する。なお、センシング履歴保存部１２には、センサ１１の計測データをそのまま格納してもよいし、ノイズ除去などのフィルタ処理を施した後のデータを格納してもよいし、フーリエ解析などの信号解析処理後のデータを格納してもよい。
【００２４】
メッセージ送信部１３は、車車間通信を行う要求および送信すべきメッセージ（送信メッセージ）の内容を受け付ける。メッセージ送信部１３は、送信要求を受信すると、無線通信装置１０の挙動が車両の挙動に合致するかどうか判定するよう挙動判定部１４に指示し、車両の挙動に合致する場合には、送信メッセージの暗号化および送信を行う。
【００２５】
挙動判定部１４は、センシング履歴保存部１２に格納されているセンサ情報（挙動情報）が、車両の挙動に合致するか否かを判定する機能部である。挙動判定部１４は、例えば、あらかじめ用意された車両の挙動を表すセンサ情報と車両以外の挙動を表すセンサ情報を学習データとして機械学習を行って得られる識別器である。機械学習の手法としては、ニューラルネットワーク、決定木、サポートベクターマシンなど任意の手法を採用可能である。学習データは、実測に基づいて得られたデータであってもよいし、シミュレーションによって生成されたデータであっても構わない。本実施形態では、挙動判定部１４は、挙動情報を車両とそれ以外の挙動に分類することを目的とするが、車両の中でも四輪以上の自動車の挙動であるかどうかを判定するものとし、自動二輪車や原動機付き自転車などの挙動は判定に合格しないように構成してもよい。どのような挙動を識別するかは、実際の運用において要求される要件にしたがって決定すればよい。

【００２６】
なお、挙動判定部１４は、機械学習に基づく識別器以外の構成を採用することもできる。例えば、挙動判定部１４は、あらかじめ定められた規則を満足するか否かを判定する規則ベースの処理を行うものとして構成してもよい。あるいは規則ベースの判定と識別器による判定とを組み合わせて、最終的な判定結果を得るようにしても構わない。
【００２７】
鍵保存部１５は、通信相手との無線通信の際の暗号化に用いられる暗号鍵を保存する機能部である。本実施形態では公開鍵暗号方式を採用し、鍵保存部１５には、無線通信装置１０の秘密鍵および公開鍵と無線通信装置２０の公開鍵が保存される。
【００２８】
暗号化部１６は、送信メッセージの暗号化を行う。本実施形態では、なりすまし防止を目的とするため、無線通信装置１０の秘密鍵で送信メッセージの暗号化を行う。受信側では、無線通信装置１０の公開鍵で復号することにより、メッセージの送信者が無線通信装置１０であることを確認できる。なお、送信メッセージの内容を秘匿化するために、通信相手（ここでは無線通信装置２０）の公開鍵を用いて送信メッセージを暗号化してもよい。
【００２９】
無線通信部１７は、暗号化部１６によって暗号化された送信メッセージを送信する。無線通信方式は任意のものであってよく、無線ＬＡＮ（ＩＥＥＥ　８０２．１１）、ＩＥＥＥ　８０２．２０、ＩＥＥＥ　８０２．１６、ＤＳＲＣなど任意のものを採用可能である。
【００３０】
なお、無線通信装置１０の上記各機能部は、耐タンパ装置によって構成することが好ましい。耐タンパ化により、物理的に安全であり、外部から各機能部の処理内容や保存されている情報を改変したり入手したりすることは不可能あるいは非常に困難になる。
【００３１】
次に、受信側の車両２に搭載される無線通信装置２０の構成について説明する。無線通信装置２０は、図２（ｃ）に示すように、無線通信部２１、鍵保存部２２、暗号化部２３、メッセージ受信部２４の各機能部を有する。無線通信装置２０のこれらの機能部は、プロセッサ（ＭＰＵ）とコンピュータプログラムの組合せによって実現してもよいし、ＡＳＩＣ等の専用のハードウェアによって実現してもよいし、ＦＰＧＡのような再構成可能なゲートアレイによって実現してもよいし、これらの組合せによって実現してもよい。
【００３２】
無線通信部２１は、無線通信装置１０からの無線通信を受信する。無線通信部２１の無線通信方式は、無線通信装置１０と同様の方式が採用される。鍵保存部２２には、無線通信装置２０の秘密鍵および公開鍵と無線通信装置１０の公開鍵が保存される。暗号化部２３は、鍵保存部２２に格納された無線通信装置１０の公開鍵を用いて、無線通信装置１０から送信された暗号化送信メッセージを復号する。復号された送信メッセージは、メッセージ受信部２４を介して、メッセージ処理部（不図示）に送られる。
【００３３】
［処理］
次に、送信側の無線通信装置１０において送信時に行われる処理について、図２のフローチャートを参照して説明する。なお、フローチャートには記載していないが、加速度センサ１１ａやＧＰＳ装置１１ｂはセンサ情報を定期的に取得して、センシング履歴保存部１２に履歴として格納している。
【００３４】
まず、メッセージ送信部１３が、メッセージの送信を要求するリクエストと、送信すべきメッセージの内容を受け取る（Ｓ１）。メッセージ送信部１３が送信リクエストを受け取ると、挙動判定部１４に対して、センシング履歴保存部１２に格納されているセンサ情報（本実施形態では、加速度情報と位置情報）の履歴が車両の挙動に合致するかどうかの

判定を行うように指示する。挙動判定部１４は、センシング履歴保存部１２に格納されているセンサ情報のうち、直近の所定期間のセンサ情報を取得し、このセンサ情報が車両の挙動と合致するかを識別器を用いて判定する（Ｓ２）。

【００３５】

センシング履歴保存部１２に格納されたセンサ情報が車両の挙動に合致すると判断される場合（Ｓ３－ＹＥＳ）は、メッセージの送信が許可される。具体的には、暗号化部１６によって無線通信装置１０の秘密鍵を用いて送信メッセージの暗号化処理が施され（Ｓ４）、暗号化後のメッセージが無線通信部１７から送信される（Ｓ５）。

【００３６】

一方、センシング履歴保存部１２に格納されたセンサ情報が車両の挙動に合致しないと判断される場合（Ｓ３－ＮＯ）は、送信メッセージを破棄して（Ｓ６）、メッセージの送信処理を行わない。

【００３７】

［実施形態の有利な効果］

本実施形態によれば、無線通信装置１０が車両に搭載されている場合のみ、メッセージの送信が行える。したがって、攻撃者が無線通信装置１０を車両から取り外して、道路上等に設置して周囲の車両に対して攻撃目的でメッセージを送信しようとしても、そのようなメッセージは送信されず、攻撃を未然に防ぐことができる。暗号鍵による認証を採用することで、無線通信装置１０から送信された情報であるかどうかを受信側で判断することができるが、それだけでは上記のような無線通信装置１０を取り外して攻撃に用いる場合を検知できない。本実施形態のように、車両の挙動と合致することをメッセージ送信の条件とすることで、このような攻撃を防止することが可能となる。

【００３８】

また、無線通信装置１０の各機能部は、耐タンパ装置により構成されているので、攻撃者がセンシング履歴保存部１２に格納されているセンサ情報を改変して車両の挙動を表すものに置き換えたり、挙動判定部１４による判定結果を偽ってメッセージを送信させてしまうような攻撃も行えない。また、メッセージの改ざんや偽造も、暗号鍵を抽出することができないので、不可能である。したがって、車車間通信において、車両になりすましてメッセージを送信するという攻撃を防止することが可能である。

【００３９】

［変形例］

上記の説明は、本発明の実施形態を例示的に説明したものであり、本発明は上記の実施形態に限定して解釈されるべきではなく、本発明の技術的思想の範囲内で種々の変形が可能である。

【００４０】

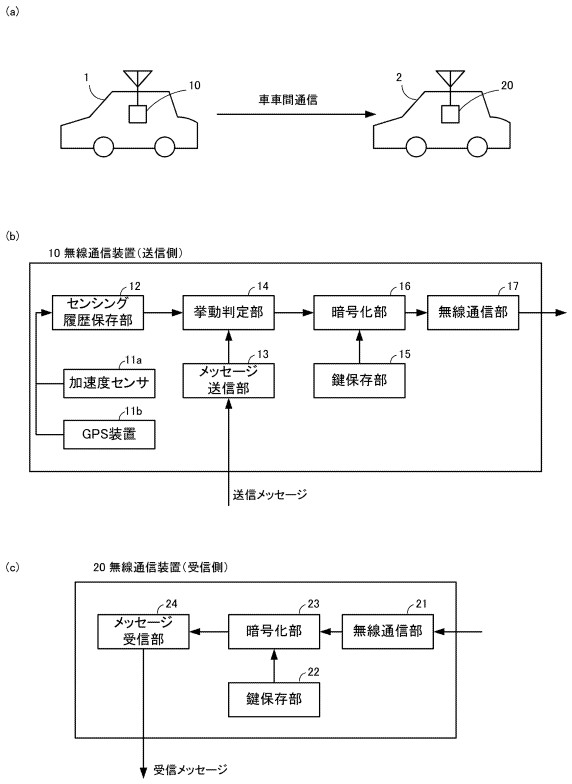
上記の説明では、加速度情報や位置情報などに基づいて、無線通信装置の挙動が車両の挙動に合致するか判断しているが、車両の挙動であるかどうかを判定するためにはセンサ情報以外の情報を用いることもできる。例えば、図３に示すように、無線通信装置１０に制御情報取得部１８を設け、制御情報取得部１８は車両制御装置３０から、車両の制御情報を取得するようにしてもよい。車両制御装置３０は、エンジン、ステアリング、ブレーキなどに対して制御指令を送信したり、これらの状態を表す情報を取得する装置である。制御情報取得部１８は、車両制御装置３０が送信する制御指令や、制御状態を表す情報を取得して、制御情報履歴保存部１９に格納する。この例では、挙動判定部１４は、制御情報に基づいて車両の挙動であるか否かを判定する。このような構成によって、上記の実施形態と同様の効果が得られる。

【００４１】

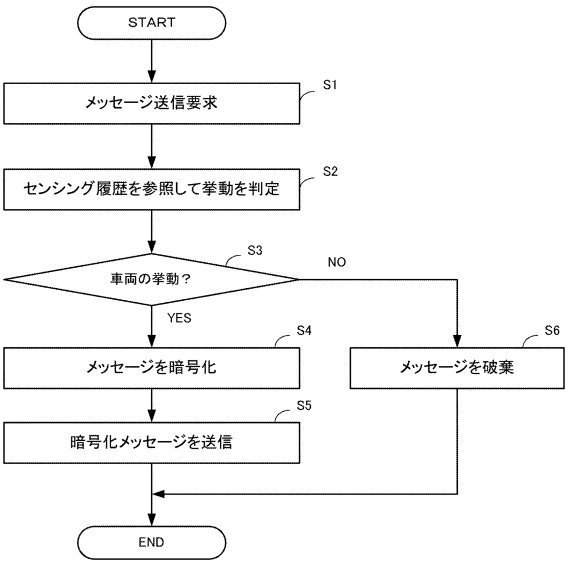
なお、上記のような構成を採用する場合は、制御情報取得部１８が偽の制御情報の誤って取得しないように構成することが望ましい。そのためには、車両制御装置３０を耐タンパ装置によって構成し、かつ、車両制御装置３０と制御情報取得部１８との間の通信を暗号化してメッセージの改ざんやなりすましを防止することが望ましい。

【００４２】
上記の説明では、無線通信装置１０の各機能部が１つの耐タンパ装置によって構成されるものとして説明したが、複数の耐タンパ装置で構成し、装置間の通信を暗号化するようにしても構わない。
【００４３】
上記の説明では、メッセージ送信要求を受けた後に、挙動の履歴が車両の挙動に合致するか判定してから送信を行っているが、処理の順序はこれ以外としてもよい。例えば、判定手段は、定期的に挙動情報の履歴が車両の挙動に合致するかを判定するようにしてもよい。そして、メッセージ送信の要求を受けた場合に、直近の挙動判定結果が車両の挙動に一致していれば、要求されたメッセージの送信を行うようにしてもよい。このようにすれば、メッセージ送信の度に判定処理を行わなくてよくなるので、メッセージの送信要求を受けてからより即座に送信を行えるようになる。
【００４４】
上記の説明では、無線通信装置１０は送信機能のみを有するものとして説明したが、無線通信装置２０が有する受信機能も備えることで、メッセージの送受信が可能となる。また、上記の説明では、無線通信装置１０の通信相手は車載の無線通信装置２０であったが、通信相手は路側通信装置やその他任意の無線通信装置であって構わない。
【符号の説明】
【００４５】
１０：無線通信装置
１１ａ：加速度センサ　１１ｂ：ＧＰＳ装置　１２：センシング履歴保存部
１３：メッセージ送信部　１４：挙動判定部　１６：暗号化部　１７：無線通信部

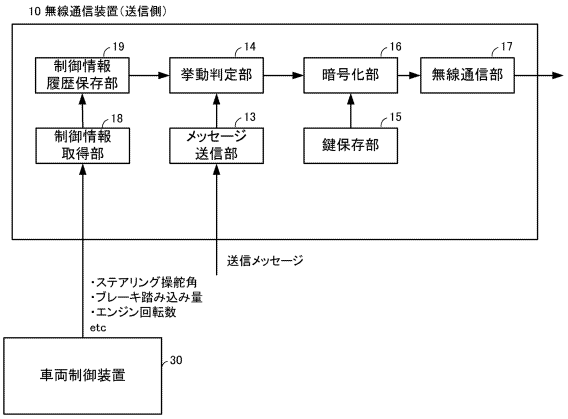
【図１】



【図２】



【図３】


10 無線通信装置（送信側）
19
制御情報
履歴保存部
14
挙動判定部
16
暗号化部
17
無線通信部
18
制御情報
取得部
13
メッセージ
送信部
15
鍵保存部
送信メッセージ
・ステアリング操舵角
・ブレーキ踏み込み量
・エンジン回転数
etc
車両制御装置
30

フロントページの続き

(74)代理人　100138357
弁理士　矢澤　広伸
(72)発明者　遠山　毅
東京都港区赤坂６丁目６番２０号　株式会社トヨタＩＴ開発センター内
(72)発明者　前川　陽介
東京都港区赤坂６丁目６番２０号　株式会社トヨタＩＴ開発センター内
(72)発明者　後藤　英樹
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内
(72)発明者　守谷　友和
愛知県豊田市トヨタ町１番地　トヨタ自動車株式会社内

審査官　行田　悦資

(56)参考文献　特開２００５－２２９４７８（ＪＰ，Ａ）
特開平１０－１５４９７６（ＪＰ，Ａ）
特開２０１３－１２０１４３（ＪＰ，Ａ）
特開２００６－２５１９１８（ＪＰ，Ａ）
特開２００５－２４２８７１（ＪＰ，Ａ）
特開２００３－０８７２３４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　　２１／５５