

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2011-164729

(P2011-164729A)

(43) 公開日 平成23年8月25日(2011.8.25)

(51) Int.Cl.
G06F 21/20 (2006.01)F I
G06F 15/00 330Bテーマコード (参考)
5B285

審査請求 未請求 請求項の数 6 O L (全 71 頁)

(21) 出願番号 特願2010-23805 (P2010-23805)
(22) 出願日 平成22年2月5日 (2010.2.5)

(特許庁注：以下のものは登録商標)

1. VICS

(71) 出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番
1号
(74) 代理人 100074099
弁理士 大菅 義之
(74) 代理人 100133570
弁理士 ▲徳▼永 民雄
(72) 発明者 林 洋輝
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(72) 発明者 志手 和彦
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 プログラム、車載装置および情報処理装置

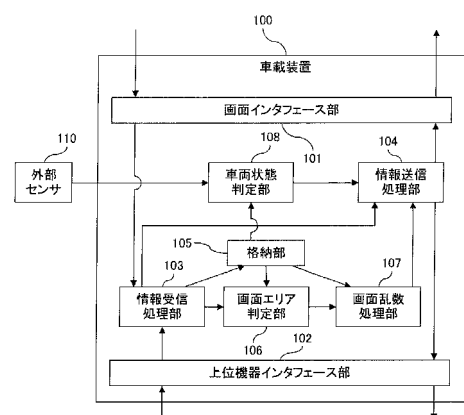
(57) 【要約】

【課題】車載装置に好適な認証用情報の生成技術を提供する。

【解決手段】画面エリア判定部106は、画面インタフェース部101と情報受信処理部103を介した入力から、軌跡情報を得る。また、格納部105には、予め鍵情報が記憶されている。そして、画面エリア判定部106と画面乱数処理部107により、軌跡情報と鍵情報から認証用情報が生成され、認証用情報は無線通信により送信される。また、情報送信処理部104と上位機器インタフェース部102により、鍵情報の更新を要求する更新要求が生成され、送信される。送信のタイミングは、車載装置100を搭載した車両の状態に基づいたタイミングである。そして、更新要求に応じて無線通信により送信される新たな鍵情報は、上位機器インタフェース部102と情報受信処理部103を介して受信され、格納部105に記憶される。

【選択図】 図1

車載装置の構成図



【特許請求の範囲】

【請求項 1】

コンピュータに、
ユーザからの入力から得られる第 1 の情報を記憶する第 1 の記憶ステップと、
前記第 1 の情報と、予め記憶装置に記憶されている第 2 の情報とを用いて、認証用の第 3 の情報を生成する第 1 の生成ステップと、
無線通信により前記第 3 の情報を送信する第 1 の送信ステップと、
前記第 2 の情報の更新を要求する更新要求を生成する第 2 の生成ステップと、
前記コンピュータを搭載した車両の状態に基づいたタイミングで前記無線通信により前記更新要求を送信する第 2 の送信ステップと、
前記更新要求に応じて前記無線通信により送信される新たな第 2 の情報を受信する受信ステップと、
受信した前記新たな第 2 の情報を前記記憶装置に記憶する第 2 の記憶ステップと、
を実行させるプログラム。

10

【請求項 2】

前記第 2 の送信ステップは、
前記車両が信号機から所定の範囲内で停止していると見なせる停止状態のときに前記更新要求を送信するよう、前記タイミングを決定する決定ステップを含む
ことを特徴とする請求項 1 に記載のプログラム。

20

【請求項 3】

前記第 1 の情報は、
前記ユーザからの入力が描く軌跡の形状、
時間の経過にともなう前記軌跡の変化、または
空間内の複数の位置が前記ユーザからの入力により指定される順序、間隔、もしくは前記順序と前記間隔の組み合わせ
を示し、
前記第 2 の情報は、
前記ユーザからの入力になされる入力領域を第 1 の個数の分割領域に分割する第 1 のパターンに対応する前記第 1 の個数のランダムな値、
前記入力領域を第 2 の個数の分割領域に分割する第 2 のパターン、または
前記入力領域を第 3 の個数の分割領域に分割する第 3 のパターンと前記第 3 のパターンに対応する前記第 3 の個数のランダムな値との組み合わせ
を示す
ことを特徴とする請求項 1 または 2 に記載のプログラム。

30

【請求項 4】

前記第 2 の送信ステップが前記第 1 の送信ステップを兼ねており、前記第 3 の情報が前記更新要求とともに送信される
ことを特徴とする請求項 1 から 3 のいずれか 1 項に記載のプログラム。

【請求項 5】

車載装置であって、
ユーザからの入力から得られる第 1 の情報を記憶する第 1 の記憶手段と、
第 2 の情報を記憶する第 2 の記憶手段と、
前記第 1 の情報と前記第 2 の情報を用いて、認証用の第 3 の情報を生成する第 1 の生成手段と、
第 2 の情報の更新を要求する更新要求を生成する第 2 の生成手段と、
無線通信により前記第 3 の情報を送信し、前記車載装置を搭載した車両の状態に基づいたタイミングで前記無線通信により前記更新要求を送信する送信手段と、
前記更新要求に応じて前記無線通信により送信される新たな第 2 の情報を受信する受信手段とを備え、
前記受信手段が受信した前記新たな第 2 の情報を前記第 2 の記憶手段に記憶する

40

50

ことを特徴とする車載装置。

【請求項6】

車両に搭載された車載装置から前記車両の位置を示す位置情報を受信する受信手段と、複数の送信機にそれぞれ対応する複数の範囲のいずれかに前記車両の前記位置が含まれるか否かを、前記位置情報に基づいて判断する判断手段と、

前記車両の前記位置が前記複数の範囲のいずれかに含まれると前記判断手段が判断した場合に、前記複数の送信機のうち前記車両の前記位置を含むと判断された当該範囲に対応する送信機に対して、前記車載装置が認証用情報を生成するのに用いる情報である鍵情報を送信する送信手段と、

を備えることを特徴とする情報処理装置。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は認証用情報の生成に関する。

【背景技術】

【0002】

多くのサービスにおいて、識別情報とパスワードの組み合わせによる認証が行われている。サービスを提供するシステムによって、パスワードが文字列で表されることもあるし、図形や画像などの文字以外の要素を利用したパスワードが使われることもある。

【0003】

20

例えば、あるパスワード方式は、グリッド表示されるディスプレイと、このディスプレイ上に表示された任意のグリッドを位置座標として入力する位置入力手段と、この位置入力手段により入力されたグリッド座標を基準点として記憶する基準位置記憶部を備える。

【0004】

また、当該パスワード方式は、基準点とされたグリッド座標が入力された後に位置入力手段より入力されたグリッド座標の、基準位置記憶部に記憶された基準点に対する相対座標を計算する相対位置計算部を備える。そして、当該パスワード方式は、この相対位置計算部により計算された相対座標を、位置入力手段により入力されたグリッド座標の入力順序にしたがって、順序列として記憶する読みとり図形一時記憶部を備える。

【0005】

30

さらに、当該パスワード方式は、ディスプレイ上に表示されたグリッドの1つを基準点として、この基準点に対するグリッドの相対座標の順序列を予め記憶しておく図形パスワード登録部も備える。そして、当該パスワード方式は、この図形パスワード登録部に記憶された相対座標の順序列と、読みとり図形一時記憶部に記憶された相対座標の順序列とが一致するか否かを判定する照合検索部を備える。

【0006】

また、ある個人認証システムでは、情報処理システムの使用者が身近な空間をモデル化した格子状の場面に、その身近な空間内に存在するような物体をモデル化した複数の図柄イメージを格子に沿って配置し、その配置の組み合わせ情報を暗証データとする。

【0007】

40

そして、パスワード入力操作を簡素化し、誤操作を防ぐための個人認証方法も提案されている。当該個人認証方法では、情報処理システムの使用者の個人認証を行うために、表示装置の表示画面に表示された複数のイメージの中で、使用者に割り当てられた複数のイメージを選択し、選択された複数のイメージが正規か否かを判定することにより個人認証を行う。

【0008】

具体的には、当該個人認証方法では、複数のイメージが複数のグループに分けられ、複数のグループごとに1つのイメージを選択するためのGraphical User Interface (GUI)が表示画面に表示される。そして、GUIにより選択された複数のイメージの組み合わせがパスワードを示す文字列に変換され、正規か否かが判定される。

50

【0009】

また、利用者に複数の表示画像の所定部分を順次指定させ、当該表示画像に対する指定情報を認証用のパスワードとして入力するパスワード入力装置も知られている。当該パスワード入力装置において、画像表示制御部は、利用者によってパスワード入力用の画像として予め選択された標準画像および当該標準画像のように見せかけたダミー画像をタッチパネル部に表示するように制御する。そして、パスワード入力制御部は、標準画像に対する指定情報を認証用のパスワードとして入力し、ダミー画像に対する指定情報を認証用のパスワードとして入力しないように制御する。

【0010】

以上のように、認証技術に関する観点の1つとして、パスワードを表すのに図形や画像などの文字以外の要素を利用するか否かという点が挙げられる。また、別の観点としては、パスワードを安全に送信する方法が挙げられる。

10

【0011】

例えば、セキュリティを高めることを目的としたある通信システムにおいては、第1送受信者と第2送受信者との間が、物理的に離間された第1回線および第2回線で接続される。そして、第1送受信者が乱数を発生して第1回線を用いて第2送受信者に送信し、乱数を受信した第2送受信者は、乱数に対して秘密情報を加工し、第2回線を用いて第1送受信者に秘密情報の加工情報を送信する。すると、第1送受信者は、乱数を基に加工情報を解読する。

20

【先行技術文献】

【特許文献】

【0012】

【特許文献1】特開昭60-171560号公報

【特許文献2】特開2003-345757号公報

【特許文献3】特開2001-282738号公報

【特許文献4】国際公開WO03/079204号公報

【特許文献5】特開2002-92499号公報

【発明の概要】

【発明が解決しようとする課題】

【0013】

30

ところで、近年の情報化社会の進展にともなうサービスの車載装置を介した提供も広まってゆくと予想される。そして、車載装置を介したサービスの提供において行われる認証では、車載装置ならではの特性が考慮されることが好ましい。

【0014】

例えば、車載装置を介したサービスの提供においては、認証にかかる時間は短いことが好ましい。また、車載装置を介したサービスは無線通信を利用して提供されるので、セキュリティ強化の対策を取ることが好ましい。

【0015】

そこで本発明は、車載装置に好適な認証用情報の生成技術を提供することを目的とする。

40

【課題を解決するための手段】

【0016】

一態様によるプログラムは、コンピュータに、第1の記憶ステップ、第1の生成ステップ、第1の送信ステップ、第2の生成ステップ、第2の送信ステップ、受信ステップ、および第2の記憶ステップを実行させる。

【0017】

前記第1の記憶ステップは、ユーザからの入力から得られる第1の情報を記憶するステップである。また、前記第1の生成ステップは、前記第1の情報と、予め記憶装置に記憶されている第2の情報とを用いて、認証用の第3の情報を生成するステップである。そして、前記第1の送信ステップは、無線通信により前記第3の情報を送信するステップであ

50

る。

【0018】

また、前記第2の生成ステップは、前記第2の情報の更新を要求する更新要求を生成するステップであり、前記第2の送信ステップは、前記コンピュータを搭載した車両の状態に基づいたタイミングで前記無線通信により前記更新要求を送信するステップである。

【0019】

そして、前記受信ステップは、前記更新要求に応じて前記無線通信により送信される新たな第2の情報を受信するステップであり、前記第2の記憶ステップは、受信した前記新たな第2の情報を前記記憶装置に記憶するステップである。

【発明の効果】

10

【0020】

上記のプログラムによれば、コンピュータは、第2の記憶ステップで記憶した新たな第2の情報を、再び上記プログラムを実行するときの第1の生成ステップにおいて用いることができる。よって、上記プログラムは、第2の情報の事前の取得を可能とすることで1回の認証にかかる時間を短縮する効果がある。つまり、上記プログラムによれば、第1の情報を得るためのユーザからの入力が行われてから認証が終わるまでにかかる時間が、認証用の第3の情報を生成する直前に第2の情報を取得する場合と比較して、第2の情報の取得にかかる時間の分、短縮される。

【0021】

また、上記のプログラムによれば、上記のプログラムをコンピュータが再度実行する際には、新たな第2の情報をを用いて認証用の第3の情報が生成されるので、生成される第3の情報の内容も異なる。よって、上記のプログラムによれば、いつも同じ内容の第3の情報を送信する場合と比べて高いセキュリティが実現される。

20

【0022】

したがって、上記のプログラムによれば、車載装置に好適な仕方で認証情報の生成が行われる。

【図面の簡単な説明】

【0023】

【図1】車載装置の構成図である。

【図2】システム構成図である。

30

【図3】システムが適用される環境の例を示す図である。

【図4】第1実施形態における車載装置の動作のフローチャートである。

【図5】第1実施形態において、認証サーバが車載装置から情報を受信したときの処理のフローチャートである。

【図6】乱数とエリアの対応づけの例を示す図（その1）である。

【図7】乱数とエリアの対応づけの例を示す図（その2）である。

【図8A】フレームの例を説明する図（その1）である。

【図8B】フレームの例を説明する図（その2）である。

【図9】第2実施形態における車載装置の動作のフローチャートである。

【図10】第2実施形態で認証に成功する場合のタイミングチャートの例である。

40

【図11】第3実施形態における車載装置の動作のフローチャートである。

【図12】第3実施形態において、認証サーバが車載装置から情報を受信したときの処理のフローチャートである。

【図13】コンピュータの構成図である。

【発明を実施するための形態】

【0024】

以下、実施形態について、図面を参照しながら詳細に説明する。説明の順序は次のとおりである。

まず、第1～3実施形態の共通点について図1～3を参照して説明する。次に、図4～5を参照して第1実施形態における装置の動作について説明し、図6～8Bを参照して第

50

1 実施形態で使われる情報の具体例を説明する。なお、図示の都合上、図 8 B には一部、第 2 ～ 3 実施形態で使われる情報も含まれる。

【0025】

その後、第 1 実施形態との違いを中心に、図 9 ～ 10 を参照して第 2 実施形態について説明し、図 11 ～ 12 を参照して第 3 実施形態について説明する。なお、第 1 実施形態と同様の点については説明を適宜省略する。最後に、第 1 ～ 3 実施形態に関連するコンピュータのハードウェア構成について図 13 を参照して説明し、第 1 ～ 3 実施形態に関するいくつかの変形例についても説明する。

【0026】

さて、図 1 は車載装置の構成図である。図 1 の車載装置 100 は、自動車に搭載され、例えば何らかのサービスを受けるにあたっての認証のために用いられる端末装置である。車載装置 100 は、認証用情報を送信し、認証に成功したか否かの結果を受信する。以下ではまず車載装置 100 の用途と動作の概要を説明し、その後で図 1 を参照しながら車載装置 100 の具体的な構成を説明する。

【0027】

近年では Electronic Toll Collection (ETC) システムや Vehicle Information and Communication System (VICS) など、Intelligent Transport System (ITS) サービスの普及が進みつつある。今後も、各種の ITS サービスの利用が広まってゆくと予想され、サービスの種類によってはユーザ認証をとまなう。

【0028】

車載装置 100 は、ITS サービスにおけるユーザ認証に使われる。例えば、警察車両などの緊急車両に対して進路上の信号機を青に設定するサービスや、カーシェアリングにおける課金のために、車載装置 100 を介したユーザ認証が利用可能である。

【0029】

ところで、コンピュータシステムにおけるユーザ認証では、キーボードやテンキーなどから入力される文字によるユーザ名とパスワードの組み合わせが使われることが多い。しかし、ユーザの入力の手間と時間を削減するために、図形的な情報（換言すれば空間的な情報）を利用したパスワードが使われることもある。図形的な情報としては、例えばユーザの手書き署名などが利用可能である。

【0030】

一般に、セキュリティを高めるためには、他者に類推されにくいパスワードを利用することが有効だが、文字によるパスワードでは、他者に類推されにくいパスワードは得てしてユーザ本人も記憶しにくく、忘れやすい。それに対して、図形的な情報を利用したパスワードは、ユーザ本人にとって覚えやすく、他者には真似しにくい。また、図形的な情報は、例えばタッチスクリーンを介して簡便に入力することができる。

【0031】

そして、ITS サービスの受益者たるユーザは、車両の運転者でもあるので、車両の運転以外の操作であるパスワード入力操作などは、なるべく簡便に済ませられることが好ましい。よって、入力の簡便性とパスワードの安全性を両立させるため、車載装置 100 では、図形的な情報を利用したパスワードが利用される。

【0032】

なお、車載装置 100 には予め一意な Identification (ID) が割り当てられている。以下では当該 ID を「車載装置 ID」という。そして、第 1 ～ 3 実施形態では、車載装置 ID が認証対象のアカウントの識別に用いられる。また、車載装置 100 が送信する上記「認証用情報」とは、図形的な情報を利用したパスワードに対応する情報であって、パスワードを加工することで得られる。

【0033】

また、車載装置 100 と他の装置（具体的には路側機）との間の通信は、当然ながら無線通信により行われる。そして、無線通信は傍受可能なので、車載装置 100 を介したユーザ認証のためには、セキュリティ向上のための工夫を行うことが望ましい。具体的には

10

20

30

40

50

、ワンタイム・パスワードのように認証のたびに異なる情報を用いる手法が、リプレイ攻撃によるなりすましの防止に役立ち、高いセキュリティ実現のために有効である。

【0034】

そこで、車載装置100は、認証のたびに異なる認証用情報を生成することで高いセキュリティを実現する。具体的には、車載装置100は、認証用情報の生成のたびに異なる情報（以下、説明の便宜上「鍵情報」という）を用いて認証用情報を生成することで、認証のたびに異なる認証用情報が使われるようにする。

【0035】

ところで、認証用情報の生成のたびに異なる鍵情報を用いるには、2つの方法が考えられる。1つ目の方法は、チャレンジ・レスポンス方式でのワンタイム・パスワードの生成と同様に、認証を行う装置（以下「認証サーバ」という）から車載装置100が認証のたびに新たな鍵情報を取得する方法である。そして、2つ目の方法は、タイム・シンクロナス方式でのワンタイム・パスワードの生成と同様に、認証サーバと車載装置100が同期して認証のたびに同じ新たな鍵情報をそれぞれ生成する方法である。

【0036】

車載装置100は、具体的には1つ目の方法をとることで、認証用情報の生成のたびに異なる鍵情報を用いることを可能とする。しかし、もし「車載装置100が認証を要求しようとする段になってから、新たな鍵情報を認証サーバに要求し、認証サーバが要求に応じて新たな鍵情報を送信する」と仮定すれば、ユーザからの入力を受け付けから認証の完了までの時間が長くなるおそれがある。その理由は、車載装置100が、高速に移動可能な移動体である車両に搭載されており、車載装置100の無線通信環境が急激に変わることがあるためである。

【0037】

つまり、上記の仮定のもとでは、認証に際して、新たな鍵情報の要求、新たな鍵情報の通知、新たな鍵情報を用いて生成された認証情報による認証の要求、および認証結果の通知という一連の通信が、車載装置100と認証サーバとの間で行われる。換言すれば、認証のために2往復の通信が行われる。

【0038】

しかし、車載装置100を搭載する車両は、車載装置100が路側機を介して認証サーバと通信している間にも高速に移動しているかもしれない。すると、通信断が生じ、その結果、通信のリトライが生じるかもしれない。

【0039】

また、道路上には他の多くの車両が存在するかもしれないので、車載装置100が路側機を介して認証サーバと通信している最中に、車載装置100を搭載した車両と路側機の間が他の車両により遮蔽されるかもしれない。すると、やはり通信断が生じ、その結果、通信のリトライが生じるかもしれない。

【0040】

さらに、「通信環境の悪化を防ぐために、あらゆる道路において通信不可領域が生じないように、大量の路側機を設置する」といった対策は非現実的であり、路側機同士の間はある程度離れている。よって、車載装置100を搭載している車両自体の走行や他の車両による遮蔽などの影響で通信断が生じた場合、次の路側機と車載装置100の間で通信のリトライが行われるまでには、ある程度の時間が経過してしまう。

【0041】

以上のような理由から、車載装置100と認証サーバの間の通信は、場合によっては時間がかかることがある。つまり、認証に比較的長い時間がかかってしまう可能性がある。他方で、ITSサービスの中には、車両のエンジンがかけられてすぐにでもサービスを開始することが好ましいものもあり、認証はなるべく短時間で終わることが好ましい。

【0042】

そこで、車載装置100は、上記の仮定のように認証を要求しようとする段になってから認証サーバとの間で2往復の通信を行う代わりに、最初の1往復の通信を予め済ませて

10

20

30

40

50

おくことで、認証にかかる時間を短縮する。つまり、車載装置１００は、予め新たな鍵情報を認証サーバに要求し、認証サーバから新たな鍵情報を取得して記憶しておく。そして、車載装置１００は、ユーザから図形的な情報の入力を受け付けて認証を要求するときには、予め記憶しておいた新たな鍵情報（すなわち、認証用情報の生成には未使用の鍵情報）を用いて認証用情報を生成する。

【００４３】

すると、車載装置１００がユーザから入力を受け付けてから認証が完了するまでの間に、車載装置１００と認証サーバとの間で行われる通信は、新たな鍵情報を用いて生成された認証情報による認証の要求と認証結果の通知という１往復の通信のみでよい。よって、上記の仮定のように２往復の通信を行う場合と比べて、車載装置１００は認証にかかる時間を短縮することができる。

10

【００４４】

また、新たな鍵情報の要求と新たな鍵情報の通知という１往復の通信が行われるタイミングは、当該新たな鍵情報を使って生成される認証用情報による認証より前であれば任意である。しかし、好適なタイミングは、「当該新たな鍵情報を使って生成される認証用情報による認証の直前の認証が完了した直後、『通信品質が良好であろう』という判定が得られ次第」というタイミングか、「直前の認証と同時に」というタイミングである。

【００４５】

その理由の１つは、いつ認証が行われるかが予測不能なためであり、もう１つの理由は、車載装置１００の無線通信環境は変動が大きいからである。よって、車載装置１００は、現在の鍵情報を用いて生成した認証用情報による認証が完了した直後、「通信品質が良好であろう」という判定が得られ次第、次の認証のための新たな鍵情報を認証サーバに要求する。あるいは、車載装置１００は、現在の鍵情報を用いて生成した認証用情報による認証と同時に、次の認証のための新たな鍵情報を認証サーバに要求する。

20

【００４６】

換言すれば、車載装置１００は、現在の鍵情報を使用した直後に、「通信品質が悪そうだ」といった障害要因さえなければすぐに、次の認証のための新たな鍵情報を認証サーバに要求する。すると、たとえすぐに次の認証を行うことになったとしても、車載装置１００は既に未使用の新たな鍵情報を保持しているので、認証は短時間で完了する。

【００４７】

以上のとおり、車載装置１００は、車両に搭載される装置に適した様々な利点を有する。続いて、図１を参照しながら車載装置１００の具体的構成について説明する。なお、各部の具体的動作については、実施形態ごとにフローチャートを参照して後述する。

30

【００４８】

図１の車載装置１００は、外部とのインタフェースとして、画面インタフェース部１０１と上位機器インタフェース部１０２を有する。また、車載装置１００は、情報受信処理部１０３と情報送信処理部１０４と格納部１０５と画面エリア判定部１０６と画面乱数処理部１０７と車両状態判定部１０８をさらに有する。そして、車載装置１００は、同じ車両に搭載されている外部センサ１１０と接続されている。

【００４９】

画面インタフェース部１０１は、タッチスクリーンを含むユーザインタフェース装置である。画面インタフェース部１０１は、車載装置１００のユーザからのタッチスクリーンへの入力を受け取り、入力された内容を情報受信処理部１０３へ出力する。つまり、画面インタフェース部１０１は、画面への接触を感知し、接触を感知した画面上の位置を表す情報を情報受信処理部１０３へ出力する。さらに、画面インタフェース部１０１は、画面上に入力プロンプトなどを表示してもよい。なお、ユーザからの入力は、タッチスクリーンの種類に応じて、ユーザの指による入力でもよいし、スタイラスペンなどの装置を介した入力でもよい。

40

【００５０】

また、以下ではタッチスクリーンを単に「画面」ということがある。そして、以下では

50

説明の便宜上、画面インタフェース部 101 が接触を感知した位置を表す情報とは、具体的には画面上の位置を表す 2 次元座標であるものとする。

【0051】

上位機器インタフェース部 102 は、無線通信インタフェース装置であり、アナログ・デジタル変換、変復調、符号化・復号化などの各種処理を行う回路や、アンテナなどのハードウェアを含む。なお、「上位機器」とは、具体的には、図 2 を参照して後述する路側機 201、認証サーバ 202 および交通管制サーバ 203 のことである。

【0052】

上位機器インタフェース部 102 は、無線フレームを受信し、無線フレームにおいて暗号化されているペイロードの復号などの処理を適宜行い、受信した無線フレームのデータ（例えばヘッダと復号されたペイロードの内容）を情報受信処理部 103 に出力する。また、上位機器インタフェース部 102 は、情報送信処理部 104 から出力されるデータに対して、無線フレームのヘッダの設定、ペイロードの暗号化、同期用プリアンプルの追加などの処理を行うことで無線フレームを生成し、生成した無線フレームを送信する。

【0053】

なお、上位機器インタフェース部 102 が無線通信に用いる無線通信プロトコルは実施形態に応じて任意である。例えば、Institute of Electrical and Electronics Engineers (IEEE) 802.11p 規格にしたがって無線通信が行われてもよい。IEEE 802.11p 規格は、Wireless Access in Vehicular Environments (WAVE) 方式と呼ばれる無線 Local Area Network (LAN) 規格である。また、記載の簡略化のため、以下では「無線フレーム」を単に「フレーム」という。

【0054】

情報受信処理部 103 は、画面インタフェース部 101 または上位機器インタフェース部 102 から出力される情報を受け取り、情報の種類に応じて、受け取った情報を格納部 105 に格納するか、または画面エリア判定部 106 に出力する。また、詳しくは図 4 とともに説明するが、情報受信処理部 103 は、上位機器インタフェース部 102 を介したフレームの受信をトリガとして検出し、トリガの検出を情報送信処理部 104 に通知することがある。

【0055】

他方、情報送信処理部 104 は、画面インタフェース部 101 に対して、画面に出力する情報を指示する。また、情報送信処理部 104 は、上位機器インタフェース部 102 に対して、上位機器インタフェース部 102 から送信するフレームに含める情報を指示する。情報送信処理部 104 は、上記のような指示を、情報受信処理部 103、画面乱数処理部 107 または車両状態判定部 108 からの入力に応じて行う。

【0056】

格納部 105 は、情報を格納するための不揮発性の記憶装置を含む。例えば、ハードディスク装置や、フラッシュメモリなどの不揮発性の半導体メモリ装置などが、格納部 105 として利用可能である。

【0057】

なお、格納部 105 として使われる記憶装置は、耐タンパ性を備えたものでもよい。また、格納部 105 は、不揮発性の記憶装置に格納された情報を一時的に格納するための、Random Access Memory (RAM) などの揮発性の記憶装置をさらに含んでもよい。

【0058】

詳しくは後述するが、格納部 105 は、画面をメッシュ状に複数のエリアに細分化する仕方を規定する細分化エリア情報と、複数のエリアにそれぞれランダムな値を対応づける乱数情報を格納する。なお、細分化エリア情報は、予め固定的に決められた情報でもよいし、更新可能な可変の情報でもよい。

【0059】

乱数情報と細分化エリア情報は、認証用情報の生成のために使われる情報である。すなわち、上記の鍵情報とは、具体的には乱数情報と細分化エリア情報を含む情報である。

乱数情報は、上位機器インタフェース部102において受信されるフレームに含まれ、上位機器インタフェース部102から情報受信処理部103に出力され、情報受信処理部103によって格納部105に書き込まれる。そして、乱数情報は画面乱数処理部107により読み出される。

【0060】

固定的な場合の細分化エリア情報は、予め格納部105に格納される。他方、可変な場合の細分化エリア情報は、上位機器インタフェース部102において受信されるフレームに含まれ、上位機器インタフェース部102から情報受信処理部103に出力され、情報受信処理部103によって格納部105に書き込まれる。そして、固定的であるにしろ可変であるにしろ、細分化エリア情報は、画面エリア判定部106により読み出される。

10

【0061】

さらに、格納部105は、信号機の位置などを表す地図情報も格納する。地図情報は、予め用意されて格納部105に格納され、車両状態判定部108により参照される。

画面エリア判定部106は、画面インタフェース部101を介して入力される図形を描く軌跡が、画面（厳密には、画面内においてユーザからの入力を受け付ける入力領域）を細分化する複数のエリアのうち、どのエリアを通るのかを判定する。あるいは、実施形態によっては、画面エリア判定部106は、画面インタフェース部101を介して順次指定される複数の位置のそれぞれが、複数のエリアのうちどのエリアにあるのかを判定してもよい。画面エリア判定部106は、細分化エリア情報を参照して上記のような判定を行う。

20

【0062】

また、画面エリア判定部106は、時間の経過と入力の進行との間の関係をさらに判定してもよい。時間の経過と入力の進行との間の関係としては、例えば、時間の経過にともなう軌跡の変化が利用可能であり、具体的にはエリアの通過順や各エリアの通過にかかる時間により表すことができる。あるいは、時間の経過と入力の進行との間の関係は、画面上の複数の位置が指定される順序、間隔、または順序と間隔の組み合わせにより表すこともできる。

【0063】

画面乱数処理部107は、画面エリア判定部106による判定結果と、格納部105に格納されている乱数情報とを用いて、車載装置100のユーザの認証に使うための認証用情報を生成する。そして、画面乱数処理部107は、生成した認証用情報を情報送信処理部104に出力する。

30

【0064】

車両状態判定部108は、車載装置100と接続された外部センサ110からの入力と格納部105に格納された地図情報に基づいて、車載装置100が搭載されている車両の状態を判定する。そして、車両状態判定部108は、上位機器インタフェース部102からの送信のタイミングを車両の状態に応じて制御するためのタイミング制御情報を情報送信処理部104に出力する。

【0065】

なお、車両状態判定部108は、第3実施形態では省略されてもよい。また、外部センサ110は、第1～2実施形態では、具体的には、車速センサと位置センサを含む。第3実施形態では、外部センサ110は、なくてもよいし、車速センサと位置センサの一方のみを含んでもよいし、車速センサと位置センサの双方を含んでもよい。

40

【0066】

位置センサとしては、具体的には、Global Positioning System (GPS) 受信機や、GPS受信機とその他のセンサ（例えばジャイロセンサや加速度センサ）を含むカーナビゲーション装置などが利用可能である。

【0067】

車速センサからの車両状態判定部108への入力は、例えば車速パルスでもよいし、車速パルスから計算された車速を示す数値でもよい。また、位置センサから車両状態判定部

50

108への入力、例えば、車載装置100が搭載された車両が位置する緯度と経度を表す測位情報でもよい。車両状態判定部108は、車速と車両の位置と地図情報を用いて車両の状態を判定する。なお、外部センサ110または車両状態判定部108は、マップマッチングなどの手法を用いて、車両の位置を示す情報を補正してもよい。

【0068】

図2はシステム構成図である。図2に示すシステム200は、複数の車載装置100a～100c、複数の路側機201a～201c、認証サーバ202、および交通管制サーバ203を含む。また、システム200において、路側機201a～201cと認証サーバ202と交通管制サーバ203は、ネットワーク204に接続されている。

【0069】

なお、本実施形態において複数の路側機201a～201cは互いに同様の構成を有するので、以下の説明において路側機一般について述べるときは、「201」という参照符号を使う。また、図2の複数の車載装置100a～100cは図1の車載装置100と同様の構成を有するので、以下の説明において車載装置一般について述べるときは、図1に示した「100」という参照符号を使う。

【0070】

路側機201は、道路の近傍に設置される中継装置である。なお、「道路の近傍」には路面上空の空間を含むものとする。路側機201は車載装置100との間で無線通信を行うことで、車載装置100と認証サーバ202の間または車載装置100と交通管制サーバ203の間の通信を中継する。

【0071】

認証サーバ202は、車載装置100からいずれかの路側機201を介して送信された認証用情報を、ネットワーク204を介して受信し、受信した認証用情報を用いて車載装置100の認証を行う。そして、認証サーバ202は、ネットワーク204と路側機201を介して、認証結果を車載装置100に送信する。さらに、認証に成功した場合は、認証サーバ202は、ネットワーク204を介して交通管制サーバ203にも認証結果を送信する。

【0072】

また、認証サーバ202は、鍵情報の更新を要求する鍵情報更新要求を、路側機201とネットワーク204を介して、車載装置100から受信する。そして、認証サーバ202は、新たな鍵情報を生成し、ネットワーク204と路側機201を介して、新たな鍵情報を車載装置100に送信する。

【0073】

交通管制サーバ203は、認証サーバ202から通知された認証結果を利用して、車載装置100に各種サービスを提供する。例えば、車載装置100が搭載されている車両が救急車、消防車、警察車両などの緊急車両である場合、認証サーバ202による認証が成功すると、交通管制サーバ203は車載装置100に対して、進路上の信号機を青にするといったサービスを提供してもよい。あるいは、交通管制サーバ203は、緊急車両に搭載された車載装置100に対して「この経路上の信号機は青に設定してあるのでこの経路を通るとよい」と経路を指定する情報を提供してもよい。

【0074】

ネットワーク204は、例えば、LAN、Wide Area Network (WAN)、インターネット、またはそれらの任意の組み合わせである。また、ネットワーク204は有線ネットワークでもよいし、一部に無線通信路を含むネットワークであってもよい。

【0075】

また、第1～3実施形態において、ネットワーク204はInternet Protocol (IP) ネットワークである。また、上記のとおり、上位機器インタフェース部102が無線通信に用いる無線通信プロトコルは実施形態に応じて任意である。

【0076】

よって、中継装置である路側機201は、車載装置100からフレームを受信した場合

10

20

30

40

50

は、フレームから適宜のフィールドのデータを取り出し、取り出したデータをペイロードに含む I P パケットを生成する。例えば、路側機 2 0 1 は、車載装置 1 0 0 から受信したフレームのヘッダとペイロードの全体をカプセル化して I P パケットのペイロードに含めてもよい。そして、路側機 2 0 1 は、生成した I P パケットを、ネットワーク 2 0 4 を介して認証サーバ 2 0 2 または交通管制サーバ 2 0 3 に送信する。

【0077】

なお、車載装置 1 0 0 と路側機 2 0 1 の間の通信は暗号化される。そこで、路側機 2 0 1 は、車載装置 1 0 0 から受信したフレーム（すなわち暗号化されたペイロードを含むフレーム）の適宜の範囲（例えばヘッダとペイロードの全体）をそのままカプセル化した I P パケットを生成してもよい。あるいは、路側機 2 0 1 は、車載装置 1 0 0 から受信した暗号化フレームを一旦復号して適宜のフィールドのデータを取り出し、取り出したデータを再度暗号化して I P パケットのペイロードに含めてもよい。

10

【0078】

なお、I P パケットの生成にあたり、路側機 2 0 1 は、フレームの種別を示す種別情報を I P パケットに設定する。路側機 2 0 1 は、車載装置 1 0 0 から受信したフレーム内にもともと含まれているフィールドを、そのまま種別情報として利用して I P パケットに含めてもよい。

【0079】

また、路側機 2 0 1 は、自らの I P アドレスを送信元 I P アドレスとして設定する。また、路側機 2 0 1 は、車載装置 1 0 0 から受信したフレームの種別に応じて宛先を認証サーバ 2 0 2 または交通管制サーバ 2 0 3 と決め、決めた宛先の I P アドレスを送信先 I P アドレスとして設定する。

20

【0080】

逆に、路側機 2 0 1 は、認証サーバ 2 0 2 または交通管制サーバ 2 0 3 からネットワーク 2 0 4 を介して I P パケットを受信した場合は、I P パケットのペイロードから適宜のデータを取り出し、取り出したデータを使ってフレームを生成して送信する。

【0081】

なお、I P パケットのペイロードも適宜暗号化されている。例えば、認証サーバ 2 0 2 または交通管制サーバ 2 0 3 から路側機 2 0 1 へ送信される I P パケットには、路側機 2 0 1 が送信する無線フレームで使われるヘッダと、同じく無線フレームで使われる暗号化されたペイロードがカプセル化されているデータを取り出し、無線通信の同期用プリアンブルを付加することでフレームを生成することができる。あるいは、路側機 2 0 1 は、受信した I P パケットにおいて暗号化されているデータを一旦復号し、復号したデータを再度暗号化してフレームのペイロードに設定してもよい。

30

【0082】

以上のように、路側機 2 0 1 における中継時に、中継されるデータの形式は変更され、必要に応じてヘッダの設定などが行われる。しかし、中継されるデータの内容自体は変わらない。よって、以下では形式の違いに取り立てて注目する場合以外は、「認証要求」のようなデータの内容を示す名前によってデータを名指すこととし、形式の違いを明示的に示す場合に「認証要求のフレーム」のように表現することにする。また、車載装置 1 0 0 における暗号化と復号の処理と、路側機 2 0 1 において実施形態に応じて行われることがある復号と再暗号化の処理については、以下では説明の簡略化のため特に明記しないこともある。

40

【0083】

なお、図 2 において、車載装置 1 0 0 a の矩形と路側機 2 0 1 a の矩形の間の直線は、車載装置 1 0 0 a と路側機 2 0 1 a の間の無線通信路を示す。しかし、車載装置 1 0 0 a は車両の走行にともなって移動し、路側機 2 0 1 a は路側に固定的に設置されているので、車載装置 1 0 0 a と路側機 2 0 1 a の間の無線通信路は恒久的なものではない。つまり、車載装置 1 0 0 a と路側機 2 0 1 a の間の無線通信路は、路側機 2 0 1 a と無線通信可

50

能な位置に車載装置 100a が存在する間だけ一時的に確立されるものである。

【0084】

同様に、図 2 に示した車載装置 100b と路側機 201b の間の無線通信路も、一時的に確立されるものであり、車載装置 100c と路側機 201c の間の無線通信路も、一時的に確立されるものである。このように、システム 200 内においてどの車載装置 100 とどの路側機 201 の間に無線通信路が存在するかは、時々刻々と動的に変化する。

【0085】

さて、図 3 は、システムが適用される環境の例を示す図である。図 3 には、紙面縦方向に延びる道路 301a ～ 301b と紙面横方向に延びる道路 301c ～ 301g が図示されている。

10

【0086】

道路 301a と 301c は交差点 302a において丁字路をなしており、道路 301a と 301d は交差点 302b において丁字路をなしている。また、道路 301a と 301e は交差点 302c で十字路をなしており、道路 301e と 301b は交差点 302d で丁字路をなしている。そして、道路 301a と 301f は交差点 302e で丁字路をなしており、道路 301a と 301g は交差点 302f で十字路をなしている。

【0087】

また、交差点 302a には、道路 301c 上に設置された信号機 303a と道路 301a 上に設置された信号機 303b がある。そして、信号機 303b には路側機 201b が取り付けられている。さらに、交差点 302b には、道路 301a 上に設置された信号機 303c があり、信号機 303c には路側機 201c が取り付けられている。

20

【0088】

そして、道路 301e 上には、交差点 302c のところに信号機 303d が、交差点 302d のところに信号機 303e が、それぞれ設置されている。また、交差点 302c には、道路 301a 上に設置された信号機 303f もある。しかし、これらの信号機 303d、303e および 303f には、路側機 201 は取り付けられていない。

【0089】

また、交差点 302d には、道路 301b 上に設置された信号機 303g もある。信号機 303g には路側機 201g が取り付けられている。

そして、交差点 302e には、道路 301f 上に設置された信号機 303h と道路 301a 上に設置された信号機 303i がある。なお、信号機 303h には路側機 201h が取り付けられているが、信号機 303i には路側機 201 は取り付けられていない。

30

【0090】

また、交差点 302f には、道路 301g 上に設置された信号機 303j と道路 301a 上に設置された信号機 303k がある。信号機 303k には路側機 201k が取り付けられているが信号機 303j には路側機 201 は取り付けられていない。

【0091】

以上例示したように、路側機 201 は、例えば信号機に取り付けられてもよいが、すべての信号機に必ず路側機 201 が取り付けられているわけではない。また、路側機 201 は、信号機に取り付けられるのでなくともよく、例えば歩道上に設置されてもよいし、道路沿いの建物の壁面などに設置されてもよい。

40

【0092】

また、図 3 には、道路 301d 沿いに存在する駐車場 304 と、駐車場 304 に駐車中の車両 305 も図示してある。以下では特に断らない限り、図 1 の車載装置 100 が車両 305 に搭載されている場合を例にして説明する。

【0093】

以上、図 1 ～ 3 を参照して第 1 ～ 3 実施形態の共通点について説明したので、続いて、第 1 ～ 3 実施形態についてそれぞれ具体的に説明する。

図 4 は、第 1 実施形態における車載装置の動作のフローチャートである。図 4 の処理は、車載装置 100 に電源が入れられると開始される。なお、車載装置 100 は、車載装置

50

100が搭載される車両305のエンジンがかけられると自動的に電源が入れるように設定されていてもよい。

【0094】

さて、ステップS101で情報受信処理部103は、画面インタフェース部101を介した図形の入力を受け付ける。ステップS101で受け付けられる図形は、予めユーザごとに決められて認証サーバ202に登録された図形である。例えば、ユーザの手書き署名などがステップS101での図形として好適だが、署名以外の図形もちろん利用可能である。また、第1実施形態では、説明の簡単化のため、ユーザと車載装置100が1対1に対応し、車載装置IDによりユーザが識別されるものとする。

【0095】

具体的には、画面インタフェース部101は、画面上で接触を感知すると、接触を感知した位置の2次元座標を情報受信処理部103に出力する。すると、情報受信処理部103は、画面インタフェース部101から出力された2次元座標と、2次元座標が画面インタフェース部101から情報受信処理部103に入力されたタイミングの組み合わせから軌跡情報を生成する。軌跡情報は、時間の経過とともに入力がどのような軌跡を描いていくのかを示す情報である。情報受信処理部103は、軌跡情報を画面エリア判定部106に出力する。

【0096】

つまり、ステップS101は、ユーザからの入力から得られる軌跡情報を、画面エリア判定部106の一部としてのRAMに記憶するステップである。そして、画面エリア判定部106が軌跡情報を受け取ってRAMに記憶すると、処理はステップS101からS102へ移行する。

【0097】

なお、ステップS101における入力の完了は、ユーザから明示的に指示されてもよいし、暗黙的な状況の変化に応じて情報受信処理部103が自動的に判断してもよい。

例えば、情報送信処理部104は、終了ボタンを画面上に表示するよう画面インタフェース部101に指示してもよい。そして、情報受信処理部103は、画面インタフェース部101から入力された2次元座標が終了ボタンの範囲内に含まれるか否かを判断してもよい。この場合、情報受信処理部103は、入力された2次元座標が終了ボタンの範囲内に含まれれば、「ステップS101における入力が完了した」と判断することができる。

【0098】

あるいは、情報受信処理部103は、画面インタフェース部101からの2次元座標の入力が一旦始まった後、所定の時間以上にわたって2次元座標の入力が途切れたとき、「ステップS101における入力が完了した」と判断してもよい。入力される図形は必ずしも一筆書きが可能な図形とは限らないので、図形の入力の途中で画面インタフェース部101からの2次元座標の入力が途切れることもある。しかし、例えば2秒間などの所定の時間以上の中断が生じれば、情報受信処理部103は、「図形の入力の途中でスタイルスペン（あるいは指）が一時的に画面から離れたのではなく、図形の入力が終了した」と判断してもよい。

【0099】

いずれにせよ、情報受信処理部103は上記のようにして図形の入力の完了を検知することができる。よって、情報受信処理部103は、入力の完了を検知した段階で軌跡情報を完成させ、完成させた軌跡情報を画面エリア判定部106に出力することができる。

【0100】

そして、ステップS102では、以上のようにして入力された図形から得られる軌跡情報と、格納部105に予め記憶されている鍵情報とを使って、車載装置100が認証用情報を生成する。

【0101】

なお、上記のとおり、第1実施形態において鍵情報は細分化エリア情報と乱数情報を含む。認証用情報の生成は、具体的には以下のようにして行われる。まず、画面エリア判定

10

20

30

40

50

部106が、細分化エリア情報と軌跡情報に基づいて、下記(a1)、(a2)、または(a1)と(a2)の双方を判定する。

【0102】

(a1)入力された軌跡を描いて移動する点が、細分化エリア情報により規定される複数のエリアのうち、どのエリアをどういう順序で通過していったか。

(a2)入力された軌跡を描いて移動する点が、細分化エリア情報により規定される各エリアを通過するのにかかった時間。

【0103】

なお、(a1)は入力された軌跡が描く形状と書き順(描き順)を表し、(a2)はユーザの入力スピードとユーザの入力癖を表す。例えば、入力する図形として手書きの署名が登録されているユーザの場合、ユーザ本人が書きなれた自分の署名を入力する時間と、悪意のある他人が真似をしながら慎重に当該ユーザの署名を入力する時間とでは差がある。よって、(a2)の時間は、ユーザ認証に利用するのに好適な情報である。

【0104】

そして、画面エリア判定部106は、判定結果を画面乱数処理部107に出力する。すると、画面乱数処理部107は、格納部105から乱数情報を読み出し、画面エリア判定部106による判定結果と乱数情報から、認証用情報を作成する。あるいは、画面乱数処理部107は、乱数情報を使わずに画面エリア判定部106による判定結果から、認証用情報を作成してもよい。いずれにせよ、ステップS102では画面エリア判定部106と画面乱数処理部107が協働して、軌跡情報と鍵情報を用いて認証用情報を生成する第1の生成手段として機能する。

【0105】

認証用情報の作成のためのアルゴリズムは任意である。ここで、認証用情報の作成のためのアルゴリズムについて説明するため、以下の(b1)～(b4)のような記法を導入することにする。

【0106】

(b1)細分化エリア情報により規定される複数のエリアを、 $area_1, area_2, \dots, area_n$ とする($n > 1$)。細分化エリア情報は、画面においてユーザからの入力となされる入力領域をn個の分割領域(つまりn個のエリア)に分割するパターンを表す情報であれば、形式は任意である。

【0107】

例えば、各エリアが矩形の場合は、細分化エリア情報は、各エリア $area_j$ ($1 \leq j \leq n$)についての、上端、下端、左端および右端の座標の組により表されていてもよい。あるいは、「画面を水平方向に何等分し、垂直方向に何等分するか」という分割の数によって細分化エリア情報が表されていてもよい。

【0108】

あるいは、画面を何行・何列に細分化するかということが固定的に決められていてもよい。その場合、細分化エリア情報は、各行の高さと各列の幅を指定する情報であってもよい。すると、行ごとに高さが異なっていたり、列ごとに幅が異なっていたりする細分化の仕方を細分化エリア情報により規定することができる。もちろん、行の高さと列の幅の一方のみが可変という実施形態も可能である。

【0109】

さらに、エリアの形状は実施形態に応じて任意であり、エリアは例えば三角形や六画形でもよい。また、細分化エリア情報において各エリアは、頂点の座標により表されてもよいし、重心の座標と大きさにより表されてもよい。

【0110】

(b2)乱数情報において、エリア $area_j$ に対応づけられているランダムな値を $rand_j$ とする($1 \leq j \leq n$)。ランダムな値 $rand_j$ は、数値でもよいし、文字列でもよい。乱数情報は、画面においてユーザからの入力となされる入力領域をn個の分割領域に分割するパターンに対応するn個のランダムな値を表現することができる情報であれ

10

20

30

40

50

ば、どのような形式でもよい。

【0111】

例えば、エリア $area_j$ とランダムな値 $rand_j$ は、ランダムな値 $rand_j$ の乱数情報内での順序を介して対応づけられていてもよい。例えば、エリア $area_j$ の頂点の座標の組によりエリア $area_j$ を定義する情報が細分化エリア情報内で j 番目にあり、ランダムな値 $rand_j$ が乱数情報内で同じく j 番目にあるのもよい。

【0112】

または、エリア $area_j$ とランダムな値 $rand_j$ は、エリア $area_j$ に割り当てられる ID を介して対応づけられていてもよい。例えば、細分化エリア情報においてはエリア $area_j$ を定義する座標などの情報がエリア $area_j$ の ID と対応づけられており、乱数情報においてはランダムな値 $rand_j$ がエリア $area_j$ の ID と対応づけられていてもよい。

【0113】

(b3) 入力された軌跡は、重複も含めて延べ m 個のエリアを通過したとする。このとき、入力された軌跡を描いて移動する点が k 番目 ($1 \leq k \leq m$) に通過したエリアを $area_{t(k)}$ とする。

【0114】

この表記によれば、細分化エリア情報と軌跡情報に基づいて得られる上記 (a1) の判定結果は、 $\langle area_{t(1)}, area_{t(2)}, \dots, area_{t(m)} \rangle$ というエリアの並びとして表すことができる。なお、エリア $area_{t(k)}$ に対応づけられているランダムな値は、上記 (b2) より、 $rand_{t(k)}$ と表記することができる。

【0115】

(b4) 入力された軌跡を描いて移動する点が、 k 番目のエリア $area_{t(k)}$ を通過するのにかった時間を $pass_{t(k)}$ とする。

この表記によれば、細分化エリア情報と軌跡情報に基づいて得られる上記 (a2) の判定結果は、 $\langle pass_{t(1)}, pass_{t(2)}, \dots, pass_{t(m)} \rangle$ という時間の並びとして表すことができる。

【0116】

さてここで、認証用情報を α と記すことにして、以上の (b1) ~ (b4) の記法を用いて説明すると、ステップ S102 において画面乱数処理部 107 は、実施形態に応じて下記の式 (1) ~ (3) のいずれかにしたがって認証用情報 α を生成する。

$$\alpha = f_A(rand_{t(1)}, \dots, rand_{t(m)}) \quad (1)$$

$$\alpha = f_B(pass_{t(1)}, \dots, pass_{t(m)}) \quad (2)$$

$$\alpha = f_C(rand_{t(1)}, pass_{t(1)}, \dots, rand_{t(m)}, pass_{t(m)}) \quad (3)$$

【0117】

式 (1) の関数 f_A と式 (2) の f_B はいずれも、例えば、 m 個の引数を文字列としてそのまま連結する関数でもよいし、所定のデリミタで区切りながら m 個の引数を文字列として連結する関数でもよい。あるいは、関数 f_A と f_B は、 m 個の各引数を所定の関数 g で変換した結果を、文字列としてそのまま（あるいは所定のデリミタで区切りながら）連結する関数でもよい。なお、関数 g には逆関数 g^{-1} が存在するものとする。

【0118】

また、関数 f_A と f_B はいずれも、所定の規則にしたがって m 個の引数の順序を入れ換えてから、上記いずれかの連結を行う関数でもよい。所定の規則による順序の入れ換えは、逆変換が存在する変換であれば任意であり、例えば、「順序を逆にする」、「最初から 2 個ずつ組にして組の中で順序を逆にする」などの入れ換えが利用可能である。

【0119】

同様に、式 (3) の関数 f_C は、 $2m$ 個の引数を、文字列としてそのまま（あるいは所定のデリミタで区切りながら）連結する関数でもよい。あるいは、関数 f_C は、奇数番目の各引数を所定の関数 g_A で変換してから連結を行う関数であってもよいし、偶数番目の

各引数を所定の関数 g_B で変換してから連結を行う関数であってもよい。なお、関数 g_A と g_B にはそれぞれ逆関数 g_A^{-1} と g_B^{-1} が存在するものとする。また、関数 f_C は、所定の規則にしたがって $2m$ 個の引数の順序を入れ換えてから、上記いずれかの連結を行う関数でもよい。

【0120】

また、関数 f_A 、 f_B および f_C は、認証用情報 α から元の引数を一意に求めることができるように定義される。デリミタを使うことにより、あるいは各引数（もしくは引数を関数 g などによって変換した結果）を固定長の文字列とすることにより、認証用情報 α から元の引数を一意に求めることができるように関数 f_A 、 f_B および f_C を定義することが可能である。

10

【0121】

さて、画面乱数処理部 107 は、ステップ S102 において以上のようにして式 (1) ~ (3) のいずれかにしたがって認証用情報 α を生成すると、生成した認証用情報 α を情報送信処理部 104 に出力する。

【0122】

すると、次のステップ S103 で情報送信処理部 104 は、認証用情報と車載装置 100 自身の車載装置 ID を含む認証要求のフレーム用のデータ（例えばヘッダと、暗号化する前のペイロードのデータ）を生成する。そして、情報送信処理部 104 は、生成したデータを上位機器インタフェース部 102 に出力し、フレームの送信を上位機器インタフェース部 102 に命じる。

20

【0123】

すると、上位機器インタフェース部 102 は命令にしたがって、ペイロードを暗号化したりフレームの先頭にプリアンプルを付加したりする適宜の処理を行い、認証要求のフレームを生成する。そして、上位機器インタフェース部 102 は認証要求のフレームを送信する。

【0124】

また、情報送信処理部 104 は、タイマをタイムアウト検出用の所定の時間に設定する。なお、認証要求の再送に備えて、情報送信処理部 104 は、認証用情報 α か、または生成した認証要求のフレーム用のデータを保持する。

【0125】

なお、車載装置 100 のユーザである運転者は、ステップ S101 における図形の入力を行った後は運転に専念してよい。例えば、図 3 のように駐車場 304 に駐車されている車両 305 にエンジンがかけられ、車載装置 100 に電源が入れられたとすると、ステップ S103 の時点で車両 305 は、まだ駐車場 304 内で停止したままかもしれないし、既に走り出しているかもしれない。

30

【0126】

続いて、ステップ S104 で情報送信処理部 104 は、後続の処理を行うためのトリガとなるイベントの発生を待つ。そして、トリガとなるイベントが発生すると、処理はステップ S105 に移行する。本実施形態ではステップ S104 でトリガとなるイベントには、認証通知の受信と、拒否通知の受信と、タイムアウトの 3 種類があり、具体的には以下のようにして検出される。

40

【0127】

ステップ S103 で上位機器インタフェース部 102 から送信された認証要求のフレームは、車載装置 100 と路側機 201 との間の通信品質が良好であれば、路側機 201 に受信される。そして、認証要求は、路側機 201 からネットワーク 204 を介して、認証サーバ 202 に送信され、認証サーバ 202 に到達する。

【0128】

例えば、駐車場 304 を出た車両 305 が信号機 303c 付近で徐行あるいは停止しているときにステップ S103 が実行されるとする。この場合、大型車両などの遮蔽物によって車両 305 と路側機 201c との間が遮られていなければ、上位機器インタフェース

50

部 1 0 2 と、信号機 3 0 3 c に取り付けられた路側機 2 0 1 c との間の通信品質は良好であることが多い。

【0 1 2 9】

上位機器インタフェース部 1 0 2 と路側機 2 0 1 c との間の通信品質が良好なとき、認証要求のフレームは、路側機 2 0 1 c において成功裡に受信される。すると、認証要求は路側機 2 0 1 c により中継され、ネットワーク 2 0 4 を介して認証サーバ 2 0 2 に送信される。

【0 1 3 0】

そして、認証要求が認証サーバ 2 0 2 に到達すると、詳しくは図 5 とともに後述するように、認証サーバ 2 0 2 は認証要求に含まれる認証用情報と車載装置 I D に基づいて認証処理を行う。

10

【0 1 3 1】

認証サーバ 2 0 2 は、認証処理の結果、認証用情報が正当な情報か不正な情報かを判断する。そして、認証用情報が正当な情報であると判断した場合、認証サーバ 2 0 2 は認証通知を送信する。他方、認証用情報が不正な情報であると判断した場合、認証サーバ 2 0 2 は拒否通知を送信する。そして、認証通知または拒否通知は、ネットワーク 2 0 4 と路側機 2 0 1 を介して車載装置 1 0 0 に到達し、上位機器インタフェース部 1 0 2 において受信される。

【0 1 3 2】

例えば、上記のように路側機 2 0 1 c を介して認証要求が送信された場合、車両 3 0 5 は認証要求の送信後にもまだ路側機 2 0 1 c の付近に位置しているかもしれないし、既に路側機 2 0 1 c から離れているかもしれない。そこで、詳しくは図 5 とともに後述するように、認証サーバ 2 0 2 は、路側機 2 0 1 c だけでなく、路側機 2 0 1 c から所定の範囲内にある他の路側機 2 0 1 （例えば路側機 2 0 1 b など）にも宛てて、認証通知または拒否通知を送信する。

20

【0 1 3 3】

そして、認証サーバ 2 0 2 から認証通知または拒否通知を受信した路側機 2 0 1 c や路側機 2 0 1 b などは、所定の長さの期間にわたり、認証通知または拒否通知のフレームの送信を適宜の間隔で繰り返す。

【0 1 3 4】

例えば、上記の「所定の範囲」を規定する距離あるいは道のりを、適宜に想定された平均的な車速で移動するのにかかる時間が、30 秒であるとする。すると、上記「所定の長さ」とは、30 秒間でもよいし、30 秒に適宜のマージンを加えた長さでもよい。また、上記「適宜の間隔」とは、例えば、1 台の路側機 2 0 1 の通信可能範囲を、上記の適宜に想定された平均的な車速で端から端まで移動するのにかかる時間よりも短い時間である。

30

【0 1 3 5】

よって、認証サーバ 2 0 2 が宛先に路側機 2 0 1 を適切に選択し、かつ上記の期間と間隔が適切に設定されていれば、車載装置 1 0 0 の上位機器インタフェース部 1 0 2 は、認証通知または拒否通知のフレームを受信することができる。例えば、上位機器インタフェース部 1 0 2 は、車両 3 0 5 が信号機 3 0 3 b の付近で停止したとき、あるいは信号機 3 0 3 b の付近を通過するときに、路側機 2 0 1 b から認証通知または拒否通知のフレームを受信するかもしれない。

40

【0 1 3 6】

すると、上位機器インタフェース部 1 0 2 は、受信した認証通知または拒否通知のフレームに対して、例えば同期用のプリアンプルを除いたり、ペイロードにおいて暗号化されている部分を復号したりする処理を行う。そして、上位機器インタフェース部 1 0 2 は、認証通知または拒否通知のフレームの処理後のデータを情報受信処理部 1 0 3 に出力する。

【0 1 3 7】

また、情報受信処理部 1 0 3 は、上位機器インタフェース部 1 0 2 からのデータの入力

50

を、認証通知または拒否通知の受信というトリガの発生として検出し、トリガの検出を情報送信処理部104に通知する。すると、情報送信処理部104は、ステップS103で設定したタイマを無効化し、再送用に保持していた認証用情報または認証要求のフレーム用のデータを破棄する。

【0138】

なお、タイマに設定される上記所定の時間は、ネットワーク204の構成、認証サーバ202のスループット、もしくは路側機201の設置間隔などに応じて適切に決められているものとする。ネットワーク204の構成と認証サーバ202のスループットは、認証のためのラウンドトリップタイムに影響する。

【0139】

また、例えば、認証サーバ202が宛先の路側機201を決めるのに用いる上記の「所定の範囲」を規定する距離あるいは道のりは、路側機201の設置間隔を考慮して決められてもよい。そして、上記の「所定の範囲」を規定する距離あるいは道のりを、適宜に想定された平均的な車速で移動するのにかかる時間が、例えば30秒であるとする。すると、タイマに設定されるのに適切な時間は、30秒以上の時間である。つまり、タイマに設定されるのに適切な時間は、路側機201の設置間隔を間接的に考慮に入れて決められてもよい。

【0140】

タイマに適切な時間が設定されれば、認証通知または拒否通知の受信というトリガは、もし発生するならば、例外的な場合を除いて、タイマがタイムアウトする前に発生することになる。以下では、タイマに設定される時間は予め適切に決められているものとする。

【0141】

他方、ステップS103において車載装置100と路側機201との間の通信品質が良好でなければ、ステップS103で上位機器インタフェース部102から送信された認証要求のフレームは、どの路側機201にも受信されず、認証サーバ202にも到達しない。この場合、当然、認証サーバ202が認証処理を行うこともなく、認証通知または拒否通知が認証サーバ202から車載装置100へと送信されることもない。

【0142】

例えば、車両305がまだ駐車場304に位置しているときにステップS103が実行された場合、車両305の付近（つまり車両305に搭載された車載装置100と無線通信が可能な範囲内）には路側機201が存在しない。よって、車載装置100はどの路側機201との間の通信品質も良好とは言えず、送信された認証要求は認証サーバ202に到達しない。

【0143】

よって、この場合は、情報送信処理部104がステップS103でタイマに設定した時間以内に認証通知のフレームも拒否通知のフレームも受信されずに、タイマがタイムアウトする。そして、情報送信処理部104はタイムアウトをトリガの発生として検出する。例えば、タイムアウトが検出された時点で、車両305は、既に駐車場304から出て交差点302e付近を走行しているかもしれない。

【0144】

以上のようにして、情報送信処理部104がトリガの発生を、情報受信処理部103からの通知またはタイマのタイムアウトにより認識すると、処理はステップS105に移行する。

【0145】

そして、ステップS105で情報送信処理部104は、トリガとして検出されたイベントの種類を判断する。検出されたトリガが拒否通知の受信であれば、図4の処理が終了し、検出されたトリガが認証通知の受信であれば、処理はステップS106に移行する。また、検出されたトリガがタイムアウトであれば、処理はステップS103に戻る。

【0146】

以上のステップS103～S105の処理により、通信環境が悪ければ必要に応じて認

10

20

30

40

50

証要求のフレームの再送が繰り返される。よって、いずれは結局、認証通知と拒否通知のいずれかの受信がトリガとして検出される。

【0147】

つまり、ステップS101で入力された図形が正当な図形であれば、遅かれ早かれ認証通知の受信がトリガとして検出され、処理がステップS106に移行する。また、ステップS101で入力された図形が不正な図形であれば、遅かれ早かれ拒否通知の受信がトリガとして検出され、図4の処理が終了する。

【0148】

ステップS106～S111の処理は、次回の認証に備えて鍵情報の更新を認証サーバ202に要求し、鍵情報を更新するための処理である。

ステップS106で情報送信処理部104は、地図情報と車速から推測される通信品質が良好であるか否かを判断する。なお、第1実施形態では、車両状態判定部108が地図情報と車速から車両305の状態を判定し、通信品質は車両305の状態から推測される。

【0149】

具体的には、車載装置100が搭載されている車両305が信号機の付近で停車していると見なせる状態か否かを車両状態判定部108が判定する。

つまり、車両状態判定部108は、格納部105から地図情報を読み出し、外部センサ110からの出力が示す車両305の位置との距離が閾値D以下の範囲に信号機があるか否かを、地図情報から判定する。そして、車両状態判定部108は、車両305の位置との距離が閾値D以下の範囲に信号機があれば、「車両305は信号機の付近にある」と判定し、車両305の位置との距離が閾値D以下の範囲に信号機がなければ、「車両305は信号機の付近にはない」と判定する。閾値Dは、上位機器インタフェース部102が良好な通信品質で路側機201との間で無線通信を行うことが可能な距離に基づいて決められる。

【0150】

なお、この例に限らず、閾値との比較は、実施形態により「閾値を超えるか、それとも閾値以下か」でもよいし、「閾値以上か、それとも閾値未満か」でもよく、適宜方針を定めることができる。

【0151】

また、車両状態判定部108は、外部センサ110からの出力が示す車速と閾値Vを比較し、車速が閾値V以下であれば「車両305は停止している」と判定し、車速が閾値Vを超えていれば「車両305は停止しているとは見なせない」と判定する。なお、閾値Vはゼロでもよいし、小さな正の値でもよい。

【0152】

そして、車両状態判定部108は、「車両305は信号機の付近にあり、かつ停止している」と見なせる」という条件が成立するか否かを判定し、判定結果を情報送信処理部104に出力する。車両状態判定部108による判定結果は、以下の説明から明らかなように、ある種のフレームの送信のタイミングを車両305の状態に応じて制御するためのタイミング制御情報として利用される。

【0153】

なお、車両状態判定部108は、例えば定期的に車両305の状態を判定し、判定のたびに判定結果を情報送信処理部104に出力してもよい。あるいは、ステップS106において、車両305の状態の判定を行うよう情報送信処理部104が車両状態判定部108に明示的な指示を与え、車両状態判定部108が指示にしたがって車両305の状態を判定してもよい。いずれにしろ、車両状態判定部108は、車両305が信号機の付近で停止している」と見なせる状態か否かを示す情報を、情報送信処理部104に出力する。

【0154】

そして、車両状態判定部108から「車両305が信号機の付近で停止している」と見なせる状態である」と示す情報が入力された場合、情報送信処理部104は、「通信品質が

10

20

30

40

50

良好だろう」と推測する。逆に、車両状態判定部 108 から「車両 305 は信号機の付近で停止していると見なせる状態ではない」と示す情報が入力された場合、情報送信処理部 104 は、「通信品質が良好ではないだろう」と推測する。情報送信処理部 104 がこのような推測を行う理由は次のとおりである。

【0155】

第 1 に、例えば図 3 の例のように、路側機 201 は信号機に取り付けられることが多い。よって、車両 305 が信号機の付近にあれば車両 305 の付近に路側機 201 が存在するが多い。つまり、車両 305 が信号機の付近にあれば、車載装置 100 と路側機 201 との間に通信品質の良い無線通信路を確立することができる蓋然性が高い。

【0156】

第 2 に、無線通信においては、移動局の移動速度が速いほど通信路は不安定であり、通信断などが発生しやすい。他方、移動局が停止していれば、通信路は安定した通信品質を保ちやすい。しかも、車両 305 が信号機の付近で停止していれば、車両 305 は、赤信号のために停止している蓋然性が高く、信号機が赤の間しばらくは動かないと推測される。つまり、通信が途中で切断されるおそれがない。

【0157】

したがって、上記の第 1 と第 2 の理由から、車両 305 が信号機の付近で停車した状態であれば、車両 305 と路側機 201 との間に、フレームの受信が完了するまでにかかる時間の間、通信品質の良好な無線通信路が安定的に確立される蓋然性が高い。つまり、車載装置 100 と路側機 201 の間の通信が成功する蓋然性が高い。

【0158】

また、付加的な第 3 の理由として、カーナビゲーション装置などのための既存の地図情報は信号機の位置を示す情報を含むことが多いことが挙げられる。つまり、車両 305 が信号機の付近に存在するか否かという判定のためには、既存の地図情報を流用することが可能であり、地図情報作成のための初期コストは不要である。コストの抑制は車載装置 100 の普及にとって有利な点である。

【0159】

さて、以上のようにしてステップ S106 において情報送信処理部 104 は、通信品質を推測する。そして、情報送信処理部 104 は、通信が成功する蓋然性の高いタイミングを見計らって通信を行うために、推測される通信品質が良好になるまで待機する。推測される通信品質が良好であれば、処理はステップ S107 に移行する。

【0160】

ステップ S107 の処理は、推測される通信品質が良好なとき、すなわち路側機 201 との通信に成功する蓋然性の高いときに実行される。

具体的には、ステップ S107 で情報送信処理部 104 は、鍵情報の更新を認証サーバ 202 に要求するための鍵情報更新要求のフレーム用のデータ（例えばヘッダとペイロード）を生成し、生成したデータを上位機器インタフェース部 102 に出力する。そして、情報送信処理部 104 は、フレームの送信を上位機器インタフェース部 102 に命じる。すると、上位機器インタフェース部 102 は命令にしたがって、必要に応じてフレームの先頭にプリアンプルを付加するなどの処理を行い、鍵情報更新要求のフレームを送信する。

【0161】

このように、ステップ S107 において情報送信処理部 104 と上位機器インタフェース部 102 は、協働して、更新要求を生成する第 2 の生成手段として機能する。また、車両状態判定部 108 と情報送信処理部 104 と上位機器インタフェース部 102 は、協働して、車載装置 100 を搭載した車両 305 の状態に基づいたタイミングで無線通信により更新要求を送信する送信手段としても機能する。つまり、車両状態判定部 108 と情報送信処理部 104 は、送信手段の一部としてタイミングの制御を行い、上位機器インタフェース部 102 は、送信手段の一部としてフレームの送信を実現する。

【0162】

また、情報送信処理部 104 は、フレームの送信を上位機器インタフェース部 102 に命じた後、タイマをタイムアウト検出用の所定の時間に設定する。なお、フレームの再送に備えて、情報送信処理部 104 は、生成した鍵情報更新要求のフレーム用のデータを保持してもよい。

【0163】

また、ステップ S107 でタイマに設定される値は、ステップ S103 でタイマに設定される値と同じでもよいし、違っていてもよいが、適切な値が定められているものとする。つまり、ステップ S107 でタイマに設定される値も、ネットワーク 204 の構成、認証サーバ 202 のスループット、路側機 201 の設置間隔などに応じて適切に決められているものとする。

10

【0164】

続いて、ステップ S108 で情報送信処理部 104 は、後続の処理を行うためのトリガとなるイベントの発生を待つ。そして、トリガとなるイベントが発生すると、処理はステップ S109 に移行する。本実施形態ではステップ S108 でトリガとなるイベントには、鍵情報更新通知の受信とタイムアウトの 2 種類があり、具体的には以下のようにして検出される。

【0165】

ステップ S107 で上位機器インタフェース部 102 から送信された鍵情報更新要求は、車載装置 100 と路側機 201 との間の通信品質が良好であれば、路側機 201 とネットワーク 204 を介して、認証サーバ 202 に到達する。その場合、詳しくは図 5 とともに後述するが、認証サーバ 202 は車載装置 100 用の新たな鍵情報を生成し、新たな鍵情報を含む鍵情報更新通知を車載装置 100 に返信する。

20

【0166】

そして、鍵情報更新通知は、ネットワーク 204 と路側機 201 を介して車載装置 100 に到達し、上位機器インタフェース部 102 において受信される。

すると、上位機器インタフェース部 102 は受信した鍵情報更新通知のフレームのデータ（例えばヘッダとペイロード）を情報受信処理部 103 に出力する。つまり、上位機器インタフェース部 102 と情報受信処理部 103 は、協働して、更新要求に応じて無線通信により送信される新たな鍵情報を受信する受信手段として機能する。また、情報受信処理部 103 は、上位機器インタフェース部 102 からのデータの入力を、鍵情報更新通知の受信というトリガの発生として検出し、トリガの検出を情報送信処理部 104 に通知する。

30

【0167】

すると、情報送信処理部 104 は、ステップ S107 で設定したタイマを無効化する。また、情報送信処理部 104 は、もし再送用に鍵情報更新要求のフレーム用のデータを保持しているのであれば、鍵情報更新要求のフレーム用のデータを破棄する。

【0168】

例えば、ステップ S106 において、「車両 305 が信号機 303 h の付近で停止していると見なせる」と車両状態判定部 108 が判定したとする。すると、特に遮蔽物などがなければ、ステップ S107 で送信された鍵情報更新要求のフレームは、信号機 303 h に取り付けられた路側機 201 h において成功裡に受信される。

40

【0169】

すると、鍵情報更新要求が路側機 201 h からネットワーク 204 を介して認証サーバ 202 に送信されるので、認証サーバ 202 は、新たな鍵情報を生成し、路側機 201 h に鍵情報更新通知を送信する。よって、車両 305 がしばらく信号機 303 h の付近にとどまっていれば、車載装置 100 は路側機 201 h から鍵情報更新通知のフレームを受信することができる。

【0170】

あるいは、車載装置 100 が鍵情報更新要求のフレームを送信した直後に車両 305 が動き出してしまい、鍵情報更新通知を受信しないうちに（あるいは受信の途中で）路側機

50

201hと無線通信が可能な範囲から車載装置100が出てしまうこともありうる。しかし、そのような場合にも、車載装置100は鍵情報更新通知のフレームを受信することができる。

【0171】

なぜなら、第1に、認証サーバ202は、路側機201hだけでなく、例えば路側機201kなどの路側機201hの近くの他の路側機201にも、鍵情報更新通知を送信するからである。そして、第2に、路側機201は、認証通知または拒否通知のフレームの場合と同様に他の種別のフレームの場合でも、所定の長さの期間にわたり適宜の間隔でフレームの送信を繰り返すからである。例えば、車両305が信号機303kの付近まで来たときに、ステップS108で上位機器インタフェース部102が鍵情報更新通知のフレームを路側機201kから受信することもある。

10

【0172】

他方、ステップS106における「通信品質が良好であろう」という推測にもかかわらず、実際の通信品質が良好ではない場合、ステップS107で送信された鍵情報更新要求のフレームは、どの路側機201にも受信されない。よって、鍵情報更新要求は認証サーバ202に到達しない。

【0173】

例えば、車両305が交差点302cで停止しているとき、車両状態判定部108は、「車両305は信号機303dの付近で停止していると見なせる」と判定する。その結果、情報送信処理部104は、「通信品質は良好であろう」と推測する。しかし、図3のように信号機303dには路側機201が取り付けられていないので、ステップS107で送信された鍵情報更新要求のフレームは、どの路側機201にも受信されない。

20

【0174】

よって、この場合は、情報送信処理部104がステップS107でタイマに設定した時間以内に鍵情報更新要求のフレームが受信されることなく、タイマがタイムアウトする。そして、ステップS108において情報送信処理部104はタイムアウトをトリガの発生として検出する。

【0175】

以上のようにして、情報送信処理部104がトリガの発生を、情報受信処理部103からの通知またはタイマのタイムアウトにより認識すると、処理はステップS109に移行する。

30

【0176】

そして、ステップS109で情報送信処理部104は、トリガとして検出されたイベントの種類を判断する。検出されたトリガが鍵情報更新通知の受信であれば、処理はステップS110に移行する。また、検出されたトリガがタイムアウトであれば、処理はステップS106に戻る。

【0177】

以上のステップS106～S109の処理により、情報送信処理部104は、通信環境が良さそうなタイミングを見計らって鍵情報更新要求のフレームを送信するための制御を行う。そして、たとえ情報送信処理部104による通信品質の推測が間違っていたとしても、必要に応じて鍵情報更新要求のフレームの再送が繰り返される。よって、いずれは結局、鍵情報更新通知の受信がトリガとして検出される。

40

【0178】

なお、ほとんどの信号機に路側機201が取り付けられているような、路側機201が十分に整備された環境においては、ステップS106における推測が当たる確率が高い。そして、ステップS106における推測が正しい場合、タイムアウト用の時間が適切に設定されていれば、ステップS108でトリガとしてタイムアウトが検出されることはほとんどない。よって、路側機201が十分に整備された環境においては、フレームの再送はあまり生じず、ステップS106の処理により無線リソースの無駄な消費を抑えることができる。

50

【0179】

さて、次のステップS110では、情報受信処理部103が、ステップS108で上位機器インタフェース部102から出力された鍵情報更新通知から新たな鍵情報を取り出し、格納部105に格納されている現在の鍵情報を新たな鍵情報で上書き更新する。

【0180】

具体的には、新たな鍵情報には新たな乱数情報が含まれるので、情報受信処理部103は格納部105内の乱数情報を新たな乱数情報で上書きする。また、細分化エリア情報が可変の場合は、新たな鍵情報には新たな細分化エリア情報が含まれるので、情報受信処理部103は格納部105内の細分化エリア情報を新たな細分化エリア情報で上書きする。

【0181】

そして、次のステップS111で情報送信処理部104は、鍵情報を更新したことを認証サーバ202に通知するための鍵情報受領通知のフレーム用のデータ（例えばヘッダとペイロード）を生成し、生成したデータを上位機器インタフェース部102に出力する。さらに、情報送信処理部104は、フレームの送信を上位機器インタフェース部102に命じる。

【0182】

すると、上位機器インタフェース部102は命令にしたがって必要に応じてフレームの先頭にプリアンプルを付加するなどの処理を行い、鍵情報受領通知のフレームを送信する。そして、図4の処理は終了する。

【0183】

なお、ステップS110とS111の実行順は逆でもよい。あるいは、ステップS110とS111の処理が並行して行われてもよい。

また、鍵情報更新通知のフレームが受信可能ということは、上位機器インタフェース部102がいずれかの路側機201と通信可能ということである。そして、鍵情報更新通知のフレームの受信からステップS111の実行までの時間は非常に短い。さらに、一種の制御フレームである鍵情報更新通知のフレーム長は短いので、より長いフレームの送受信には失敗する場合であっても、鍵情報更新通知のフレームの送受信は成功することも大いにありうる。

【0184】

よって、第1実施形態では、「鍵情報更新通知のフレームの受信の直後に送信される鍵情報受領通知のフレームは、成功裡に路側機201において受信され、認証サーバ202に鍵情報受領通知が届く」と仮定している。まれにこの仮定が成立しない場合の対策については、後述の（f12）の観点からの変形例として述べる。

【0185】

続いて、第1実施形態における認証サーバ202の動作を説明する。認証サーバ202は、任意のタイミングで任意の車載装置100から任意の路側機201を介して情報を受信する可能性があり、情報の受信を契機として各種処理を行う。

【0186】

図5は、第1実施形態において、認証サーバ202が車載装置100から情報を受信したときの処理のフローチャートである。なお、図5に関する説明においては、図5の処理の開始の契機となった情報の送信元の車載装置100を「送信元の車載装置100」という。

【0187】

ステップS201で認証サーバ202は、送信元の車載装置100から路側機201とネットワーク204を介して受信した情報の内容が、認証要求、鍵情報更新要求、鍵情報受領通知のいずれであるかを判断する。

【0188】

上記のとおり、路側機201は、認証サーバ202に送信するIPパケットのペイロードに、送信元の車載装置100から路側機201が受信したフレームの種別を示す種別情報を含める。よって、認証サーバ202は、ネットワーク204を介して路側機201か

10

20

30

40

50

ら受信したIPパケットから種別情報を取り出して、種別情報に基づいてステップS201の判断を行うことができる。

【0189】

認証要求が受信された場合、処理はステップS202に移行する。鍵情報更新要求が受信された場合、処理はステップS208に移行する。また、鍵情報受領通知が受信された場合、処理はステップS211に移行する。

【0190】

ステップS202で認証サーバ202は、認証要求に含まれる認証用情報からパスワードを取り出す。

具体的には、認証サーバ202は、ネットワーク204を介して路側機201から受信した認証要求のIPパケットから、送信元の車載装置100の車載装置IDと認証用情報を取り出す。また、認証サーバ202は、必要に応じて、送信元の車載装置100の車載装置IDと対応づけて「認証利用版」として記憶している鍵情報を読み出す。

【0191】

なお、後述のステップS208およびS211とも関連するが、認証サーバ202は、各車載装置100の車載装置IDと対応づけて、「最新送信版」と「認証利用版」の鍵情報を記憶する。その理由は、認証サーバ202が単に新たな鍵情報を含む鍵情報更新通知を送信するだけでは、「鍵情報更新通知が車載装置100で正常に受信されて、認証サーバ202と車載装置100の間で新たな鍵情報が共有される」とは保証されないからである。

【0192】

そこで、認証サーバ202は、車載装置100との間での共有が確認された鍵情報を認証利用版として記憶するとともに、車載装置100に送信済みだが車載装置100との間での共有がまだ確認されていない鍵情報を最新送信版として記憶する。よって、ステップS202で認証サーバ202が参照するのは、認証利用版の鍵情報である。

【0193】

ステップS202において認証サーバ202はさらに、必要に応じて鍵情報を使い、認証用情報からパスワードを取り出す。なお、「パスワード」とは、具体的には下記(c1)～(c3)いずれかの情報のことである。

【0194】

(c1)画面乱数処理部107が式(1)により認証用情報 α を生成することに決められている場合は、パスワードは、上記(b3)に示した $\langle area_{t(1)}, area_{t(2)}, \dots, area_{t(m)} \rangle$ というエリアの並びを示す情報である。例えば、パスワードは、各エリア $area_{t(1)}, area_{t(2)}, \dots, area_{t(m)}$ を識別するID(あるいは行と列の組)の並びとして表されてもよい。

【0195】

この場合、認証サーバ202は、認証要求のIPパケットから認証用情報 α を取り出し、送信元の車載装置100の車載装置IDと対応づけて認証利用版として記憶している鍵情報を読み出す。ここで、上記のとおり、式(1)の関数 f_A は、認証用情報 α から元の引数を一意に求めることができるように定義されている。よって、認証サーバ202は、認証用情報 α から関数 f_A の m 個の引数(すなわち m 個のランダムな値) $rand_{t(1)}, \dots, rand_{t(m)}$ を求めることができる。

【0196】

そして、認証サーバ202は、読み出した鍵情報を用いて、求めた m 個のランダムな値 $rand_{t(1)}, \dots, rand_{t(m)}$ にそれぞれ対応するエリア $area_{t(1)}, area_{t(2)}, \dots, area_{t(m)}$ を特定する。以上の処理により、認証サーバ202はパスワードを得ることができる。

【0197】

(c2)画面乱数処理部107が式(2)により認証用情報 α を生成することに決められている場合は、パスワードは、上記(b4)に示した $\langle pass_{t(1)}, pass_{t(2)}, \dots, pass_{t(m)} \rangle$ というパスワードの並びを示す情報である。

10

20

30

40

50

(2), ..., pass_{t(m)} > という時間の並びである。

【0198】

この場合、認証サーバ202は、認証要求のIPパケットから認証用情報αを取り出す。上記のとおり、式(2)の関数 f_B は、認証用情報αから元の引数を一意に求めることができるように定義されている。よって、認証サーバ202は、認証用情報αから関数 f_B のm個の引数pass_{t(1)}, pass_{t(2)}, ..., pass_{t(m)}を求めることができる。つまり、認証サーバ202はパスワードを得ることができる。

【0199】

(c3)画面乱数処理部107が式(3)により認証用情報αを生成することに決められている場合は、パスワードは、上記(c1)と(c2)の組み合わせである。つまり、パスワードは上記(b3)に示した<area_{t(1)}, area_{t(2)}, ..., area_{t(m)}>というエリアの並びを示す情報と上記(b4)に示した<pass_{t(1)}, pass_{t(2)}, ..., pass_{t(m)}>という時間の並びの組み合わせである。

10

【0200】

上記のとおり、式(3)の関数 f_C は、認証用情報αから元の引数を一意に求めることができるように定義されている。よって、認証サーバ202は、認証用情報αから関数 f_C の2m個の引数rand_{t(1)}, pass_{t(1)}, ..., rand_{t(m)}, pass_{t(m)}を求めることができる。そして、認証サーバ202は、求めた2m個の引数のうちで奇数番目に当たるm個のランダムな値rand_{t(1)}, ..., rand_{t(m)}にそれぞれ対応するエリアarea_{t(1)}, area_{t(2)}, ..., area_{t(m)}を、読み出した鍵情報を用いて特定する。以上の処理により、認証サーバ202はパスワードを得ることができる。

20

【0201】

以上のように、パスワードが(c1)~(c3)のいずれの情報であれ、認証サーバ202はステップS202でパスワードを取り出すことができる。そして、次のステップS203で認証サーバ202は、受信した情報が経由してきた路側機201(以下「送信元路側機」という)とその近傍の路側機201(以下「送信元近傍路側機」という)を、返信時の中継点として選択する。

【0202】

具体的には、認証サーバ202は、受信した認証要求のIPパケットのヘッダから、送信元IPアドレスを取り出す。送信元IPアドレスには、車載装置100からの認証要求を中継した送信元路側機のIPアドレスが設定されているので、こうして認証サーバ202は送信元路側機を特定することができる。

30

【0203】

また、認証サーバ202は、どの路側機201同士が近傍にあるのかを表す路側機配置情報を保持している。よって、認証サーバ202は、路側機配置情報を参照することで、送信元近傍路側機を特定することができる。なお、送信元近傍路側機は複数台のこともある。路側機配置情報は、例えば下記(d1)~(d3)のいずれかであってもよい。

【0204】

(d1)路側機配置情報は、路側機201のIPアドレスに対応づけて、各路側機201の位置を、例えば緯度と経度の組により示す情報でもよい。その場合、認証サーバ202は、送信元路側機の位置からの距離が所定の閾値以下の位置にある路側機201を送信元近傍路側機として特定し、送信元近傍路側機のIPアドレスを得ることができる。例えば、送信元路側機が図3の路側機201cであり、路側機201cからの距離が所定の閾値以下の位置にあるのが路側機201bのみであれば、認証サーバ202は、路側機201bのみを送信元近傍路側機として特定する。

40

【0205】

(d2)路側機配置情報は、上記(d1)の情報に加えてさらに、道路地図の情報を含んでいてもよい。その場合、認証サーバ202は、送信元路側機からの道路沿いの道のり

50

が所定の閾値以下となる路側機 201 を送信元近傍路側機として特定してもよい。例えば、送信元路側機が図 3 の路側機 201 c であり、路側機 201 c からの道のりが所定の閾値以下となるのが路側機 201 b のみであれば、認証サーバ 202 は、路側機 201 b のみを送信元近傍路側機として特定してもよい。

【0206】

または、認証サーバ 202 は、「送信元路側機からの道路に沿った経路上に通信可能範囲が重なる他の路側機 201 の個数が所定の閾値 Q 以下」という条件を満たす路側機 201 を、送信元近傍路側機として特定してもよい。例えば、送信元路側機が図 3 の路側機 201 c であり、 $Q = 0$ とする。その場合、図 3 が示すように、送信元近傍路側機の条件を満たすのは、路側機 201 b、201 g、および 201 h である。

10

【0207】

例えば、路側機 201 c から路側機 201 h までの経路上には、他の路側機 201 が設置されておらず、他の路側機 201 の通信可能範囲も重なっていない。よって、路側機 201 h は上記の条件を満たす。

【0208】

また、道路 301 a 上には、路側機 201 c と路側機 201 k の間に他の路側機 201 はない。しかし、交差点 302 e 付近の路側機 201 h の通信可能範囲が、路側機 201 c から路側機 201 k までの経路上に一部重なるので、路側機 201 k は上記の条件を満たさない。

【0209】

(d3) 路側機配置情報は、任意の 2 つの路側機 201 について互いに近傍にあるか否かを示す情報であってもよい。また、路側機配置情報において、各路側機 201 は IP アドレスにより識別されていてもよい。各路側機 201 は固定されているので、任意の 2 つの路側機 201 について互いに近傍にあるか否かを示す情報を、例えば認証サーバ 202 が予め作成することも可能である。

20

【0210】

つまり、認証サーバ 202 は、任意の 2 つの路側機 201 間の距離もしくは道のり、または 2 つの路側機 201 間の道路沿いの経路上に通信可能範囲が重なる他の路側機 201 の個数を所定の閾値と比較してもよい。そして、認証サーバ 202 は比較結果に基づいて、当該 2 つの路側機 201 同士が近傍にあるか否かを判断し、判断の結果を路側機配置情報として記憶してもよい。

30

【0211】

以上の (d1) ~ (d3) に例示したように、路側機配置情報は実施形態によって様々であってもよいが、いずれにせよ認証サーバ 202 は、路側機配置情報を参照することで送信元近傍路側機を特定することができる。そして、認証サーバ 202 は、送信元路側機と送信元近傍路側機を、返信時の中継点として選択する。

【0212】

なお、ステップ S202 と S203 は実行順が逆でもよい。あるいは、認証サーバ 202 はステップ S202 と S203 の処理を並行して行ってもよい。

続いて、次のステップ S204 で認証サーバ 202 は、ステップ S202 で取り出したパスワードが正しいか否かを判断する。パスワードが正しい場合、処理はステップ S205 に移行し、パスワードが正しくない場合、処理はステップ S207 に移行する。認証サーバ 202 は、例えば適宜のパターンマッチングアルゴリズムを用いてパスワード照合を行うこともできる。

40

【0213】

すなわち、認証サーバ 202 は、各車載装置 100 の車載装置 ID に対応づけて、当該車載装置 100 のユーザにより予め登録された図形の軌跡情報を記憶している。よって、認証サーバ 202 は、記憶している軌跡情報と、車載装置 ID に対応づけて認証利用版として記憶している鍵情報内の細分化エリア情報から、正しいパスワードを認識することができる。

50

【0214】

つまり、認証サーバ202は、ステップS202で取り出した車載装置IDに対応づけてそれぞれ記憶している軌跡情報と細分化エリア情報から、当該軌跡情報が表す軌跡上を移動する点が、どのエリアをどういう順序で通過するのかを認識することができる。また、認証サーバ202は、当該軌跡情報が表す軌跡上を移動する点が、各エリアを通過するのにかかる時間も、軌跡情報と細分化エリア情報から認識することができる。したがって、認証サーバ202は、正しいパスワードを表すエリアの並び、時間の並び、またはその組み合わせを取得することができる。

【0215】

そこで、認証サーバ202はステップS204において、正しいパスワードと、ステップS202で取り出したパスワードを比較する。比較に際しては、認証サーバ202は適宜のパターンマッチングアルゴリズムを用いることができる。

【0216】

図形的な情報の入力においては、図形の描き出し位置が入力のたびに少々ずれたり、入力される図形の大きさに揺れがあったり、入力スピードに揺れがあったりするのが普通である。よって、認証サーバ202は、一定範囲内のずれまたは揺れを誤差として許容するために、適宜のパターンマッチングアルゴリズムを用いることができる。つまり、認証サーバ202は、パスワード同士をパターン同士として、適宜のパターンマッチングアルゴリズムにより比較する。

【0217】

比較の結果、両パスワードが許容範囲内の誤差で一致すれば、認証サーバ202は、「ステップS202で取り出したパスワードが正しい」と判断する。逆に、両パスワードが許容範囲内の誤差で一致しなければ、認証サーバ202は、「ステップS202で取り出したパスワードは不正である」と判断する。

【0218】

なお、実施形態によっては、書き順を反映した軌跡ではなく、図形の形状だけに基づいて認証サーバ202がパスワード照合を行ってもよい。つまり、式(1)によって認証情報 α を得る実施形態において、パスワードは、 $\{area_{t(1)}, area_{t(2)}, \dots, area_{t(m)}\}$ というエリアの集合(正確には重複を許す多重集合)を示す情報であってもよい。すると、軌跡が各エリアを通過する順序は無視され、形状のみがパスワード照合において考慮される。なぜなら、集合を示す情報では要素の並び順が無視されるからである。

【0219】

さて、ステップS204において「パスワードは正しい」と判断した場合、次のステップS205で認証サーバ202は、送信元の車載装置100へのサービス提供者である交通管制サーバ203に、ネットワーク204を介して、認証結果を知らせる。すなわち、認証サーバ202は、「送信元の車載装置100の車載装置IDについて認証が成功した」ということを交通管制サーバ203に通知する。

【0220】

そして、次のステップS206で認証サーバ202は、ネットワーク204とステップS203で選択した路側機201とを介して、送信元の車載装置100へ認証通知を返信する。

【0221】

具体的には、認証サーバ202は、ステップS203で中継点として選択した送信元路側機と送信元近傍路側機のそれぞれについて、以下の処理を行う。すなわち、認証サーバ202は、当該中継点となる路側機201のIPアドレスを送信先IPアドレスとして設定し、送信元の車載装置100の認証に成功したことを示す情報をペイロードに設定したIPパケットを生成する。そして、認証サーバ202は、生成したIPパケットをネットワーク204へ送出する。なお、送信元の車載装置100の認証に成功したことを示す情報は、送信元の車載装置100の車載装置IDを含む。

【0222】

以上のようにして、中継点として選択した送信元路側機と送信元近傍路側機それぞれへのIPパケットの送信が完了すると、図5の処理も終了する。

また、ステップS204において「パスワードが不正である」と判断した場合、認証サーバ202は、ステップS207において、ネットワーク204とステップS203で選択した路側機201とを介して、送信元の車載装置100へ拒否通知を返信する。つまり、認証サーバ202は、送信元の車載装置100の認証に失敗したことを示す情報をペイロードに設定する以外はステップS206と同様の処理を行う。なお、送信元の車載装置100の認証に失敗したことを示す情報も、送信元の車載装置100の車載装置IDを含む。

10

【0223】

そして、ステップS207において、以上のようにして、中継点として選択した送信元路側機と送信元近傍路側機それぞれへのIPパケットの送信が完了すると、図5の処理は終了する。

【0224】

また、受信したIPパケットが鍵情報更新要求のIPパケットであった場合、認証サーバ202はステップS208において、新たな鍵情報を作成する。そして、認証サーバ202は、送信元の車載装置100の車載装置IDと対応づけて、作成した鍵情報を最新送信版として記憶する。なお、認証サーバ202は、鍵情報更新要求のIPパケットのペイロードから車載装置IDを取り出し、認識することができる。

20

【0225】

また、実施形態に応じて、認証サーバ202は、ステップS208において細分化エリア情報と乱数情報の双方を新たに作成してもよいし、一方のみを新たに作成してもよい。例えば、認証サーバ202が細分化エリア情報のみを新たに作成する場合、新たな鍵情報とは、現在認証利用版として記憶している乱数情報と、新たに作成した細分化エリア情報の組み合わせである。また、認証サーバ202が乱数情報のみを新たに作成する場合、新たな鍵情報とは、現在認証利用版として記憶している細分化エリア情報と、新たに作成した乱数情報の組み合わせである。

【0226】

続いて、次のステップS209で認証サーバ202は、ステップS203と同様に、受信した情報が経由してきた路側機201とその近傍の路側機201を、返信時の中継点として選択する。

30

【0227】

さらに、続くステップS210で認証サーバ202は、ネットワーク204とステップS209で選択した路側機201とを介して、最新送信版の鍵情報を送信元の車載装置100に返信する。つまり、認証サーバ202は、最新送信版の鍵情報と送信元の車載装置100の車載装置IDを含む情報をペイロードに設定する以外はステップS206と同様の処理を行う。

【0228】

そして、ステップS210において、以上のようにして、中継点として選択した送信元路側機と送信元近傍路側機それぞれへのIPパケットの送信が完了すると、図5の処理は終了する。

40

【0229】

また、受信したIPパケットが鍵情報受領通知のIPパケットであった場合、認証サーバ202はステップS211において、送信元の車載装置100の車載装置IDに対応する認証利用版の鍵情報を更新する。つまり、認証サーバ202は、送信元の車載装置100の車載装置IDに対応する最新送信版の鍵情報を、当該車載装置IDに対応する認証利用版の鍵情報としてコピーする。なお、認証サーバ202は、鍵情報受領通知のIPパケットのペイロードから車載装置IDを取り出し、認識することができる。

【0230】

50

ステップ S 2 1 1 の処理により、認証サーバ 2 0 2 は、「送信元の車載装置 1 0 0 に対して認証サーバ 2 0 2 が最新送信版として以前送信した鍵情報を、送信元の車載装置 1 0 0 が確かに受信した」と認識することができる。つまり、認証サーバ 2 0 2 は、「送信元の車載装置 1 0 0 が将来再度認証要求を送信してくる場合に、認証のためには、認証利用版の鍵情報としてコピーした最新送信版の鍵情報を使えばよい」と認識することができる。そして、最新送信版の鍵情報のコピーの後、図 5 の処理は終了する。

【0 2 3 1】

続いて、図 6 ～ 8 B を参照して、上記の車載装置 1 0 0 と認証サーバ 2 0 2 の動作の説明における各種情報の具体例を説明する。

さて、図 6 と 7 は、乱数とエリアの対応づけの例を示す図である。図 6 と 7 では、「鍵情報に含まれる細分化エリア情報と乱数情報が、エリアを介してどのように対応づけられるのか」ということが模式的に示されている。図 6 と 7 ではさらに、「画面と鍵情報がエリアを介してどのように対応づけられるのか」ということも、模式的に示されている。

【0 2 3 2】

図 6 には、鍵情報 4 0 1 を模式的に図示した説明図と、画面と鍵情報の対応づけ 4 0 2 の例が示されている。

鍵情報 4 0 1 は、乱数情報のバージョンを示す “ R 2 0 0 9 1 2 3 1 1 0 3 5 4 7 ” という値と、細分化エリア情報のバージョンを示す “ S 2 0 0 9 1 2 3 1 1 0 3 5 4 7 ” という値を含む。なお、乱数情報と細分化エリア情報のバージョンは、認証サーバ 2 0 2 が図 5 のステップ S 2 0 8 で鍵情報 4 0 1 を生成するときに割り当てられる。例えば生成日時に基づく値を使うことで、認証サーバ 2 0 2 は鍵情報の生成のたびに異なる値をバージョンとして割り当てることができる。また、実施形態によっては、乱数情報と細分化エリア情報のバージョンとして共通の値が使われてもよい。

【0 2 3 3】

さらに、鍵情報 4 0 1 は、水平方向に 5 列、垂直方向に 8 行の、計 4 0 (= 5 × 8) 個のエリアに画面を等分することを示す細分化エリア情報と、4 0 個の 4 桁の乱数を 4 0 個のエリアそれぞれに対応づける乱数情報を含む。鍵情報 4 0 1 によれば、例えば 3 行目の 2 列目のエリアには、1 8 8 2 という乱数に対応づけられている。

【0 2 3 4】

また、図 4 のステップ S 1 0 1 において、以上のように 4 0 個のエリアに細分化される画面上で、軌跡 4 0 3 を描くように三角形が入力されたとする。図 6 によれば、軌跡 4 0 3 は、1 行目の 1 列目のエリアから始まり、2 行目の 1 列目のエリア、3 行目の 1 列目のエリア、3 行目の 2 列目のエリア、2 行目の 2 列目のエリア、2 行目の 1 列目のエリアを経由し、1 行目の 1 列目のエリアで終わる。よって、画面エリア判定部 1 0 6 は、軌跡 4 0 3 を示す軌跡情報と、鍵情報 4 0 1 に含まれる細分化エリア情報から、「軌跡 4 0 3 を描いて移動する点は、上記の延べ 7 つのエリアを順に通過する」と判定することができる。

【0 2 3 5】

そして、軌跡 4 0 3 が通過する上記の延べ 7 つのエリアにそれぞれ乱数情報において対応づけられている延べ 7 つの乱数は、図 6 によれば、順に、2 6 1 5、3 6 7 3、5 7 3 2、1 8 8 2、9 4 3 3、3 6 7 3、2 6 1 5 である。

【0 2 3 6】

なお、以下では説明の便宜上、入力された軌跡を描いて移動する点が上記の延べ 7 つのエリアの各々を通過するのににかかった時間が、順に、0. 3 秒、0. 4 秒、0. 6 秒、1. 0 秒、0. 4 秒、0. 2 秒、0. 1 秒であったとする。よって、画面エリア判定部 1 0 6 は、軌跡 4 0 3 を示す軌跡情報と、鍵情報 4 0 1 に含まれる細分化エリア情報から、軌跡 4 0 3 を描いて移動する点が上記の延べ 7 つのエリアをそれぞれ通過するのににかかった時間が上記のとおりであったことも認識する。

【0 2 3 7】

もちろん、画面上には 4 0 個のエリアに細分化する分割線や各乱数は表示されないが、

10

20

30

40

50

図 6 では説明の便宜上、画面上の軌跡 4 0 3 と鍵情報 4 0 1 との対応づけを、画面と鍵情報の対応づけ 4 0 2 として図示してある。

【0 2 3 8】

以上の図 6 の例を、(b 1) ~ (b 4) の表記を用いて表すと、以下の式 (4) ~ (18) のとおりである。

$$\begin{array}{ll}
 m = 7 & (4) \\
 rand_{t(1)} = 2615 & (5) \\
 rand_{t(2)} = 3673 & (6) \\
 rand_{t(3)} = 5732 & (7) \\
 rand_{t(4)} = 1882 & (8) \\
 rand_{t(5)} = 9433 & (9) \\
 rand_{t(6)} = 3673 & (10) \\
 rand_{t(7)} = 2615 & (11) \\
 pass_{t(1)} = 0.3 & (12) \\
 pass_{t(2)} = 0.4 & (13) \\
 pass_{t(3)} = 0.6 & (14) \\
 pass_{t(4)} = 1.0 & (15) \\
 pass_{t(5)} = 0.4 & (16) \\
 pass_{t(6)} = 0.2 & (17) \\
 pass_{t(7)} = 0.1 & (18)
 \end{array}$$

【0 2 3 9】

例えば、画面乱数処理部 1 0 7 が式 (1) の関数 f_A により認証用情報 α を求める実施形態において、関数 f_A が、所定のデリミタ “-” で区切りながら m 個の引数を連結する関数であるとする。この場合、式 (4) ~ (11) より、図 6 の鍵情報 4 0 1 と軌跡 4 0 3 から得られる認証用情報 α は、式 (19) のとおりである。

$$\alpha = “ 2615 - 3673 - 5732 - 1882 - 9433 - 3673 - 2615 ” \quad (19)$$

【0 2 4 0】

なお、式 (19) から明らかなとおり、認証サーバ 2 0 2 は、式 (19) で表される認証用情報 α から、認証用情報 α を得るのに用いた関数 f_A の 7 つの引数の値を一意に得ることができる。具体的には、認証サーバ 2 0 2 は、認証用情報 α を所定のデリミタ “-” で分割するだけで、関数 f_A の 7 つの引数の値（すなわち式 (5) ~ (11) に示した 7 つの値）を得ることができる。

【0 2 4 1】

また、画面乱数処理部 1 0 7 が式 (2) の関数 f_B により認証用情報 α を求める実施形態において、関数 f_B が、 m 個の各引数を所定の関数 g で変換した結果を、所定のデリミタ “-” で区切りながら連結する関数であるとする。そして、関数 g は、秒単位で表された数値を 1 0 0 倍して切り捨てにより整数に変換し、得られた整数を 4 桁の数字で表す関数であるとする。この場合、式 (4)、(12) ~ (18) より、図 6 の鍵情報 4 0 1 と軌跡 4 0 3 から得られる認証用情報 α は、式 (20) のとおりである。

$$\alpha = “ 0030 - 0040 - 0060 - 0100 - 0040 - 0020 - 0010 ” \quad (20)$$

【0 2 4 2】

なお、式 (20) から明らかなとおり、認証サーバ 2 0 2 は、式 (20) で表される認証用情報 α から、認証用情報 α を得るのに用いた関数 f_B の 7 つの引数の値を一意に得ることができる。具体的には、認証サーバ 2 0 2 は、認証用情報 α を所定のデリミタ “-” で分割し、分割により得られる 7 つの文字列を関数 g の逆関数 g^{-1} で変換することで、関数 f_B の 7 つの引数の値（すなわち式 (12) ~ (18) に示した 7 つの値）を得るこ

とができる。

【0243】

また、画面乱数処理部107が式(3)の関数 f_C により認証用情報 α を求める実施形態において、関数 f_C が、奇数番目の引数はそのままの文字列として、偶数番目の引数は関数 g_B で変換してから、デリミタ“－”で区切りながら連結する関数であるとする。そして、関数 g_B は、秒単位で表された数値を100倍して切り捨てにより整数に変換し、得られた整数を4桁の数字列で表す関数であるとする。この場合、式(4)～(18)より、図6の鍵情報401と軌跡403から得られる認証用情報 α は、式(21)のとおりである。

$$\alpha = \text{“ } 2615 - 0030 - 3673 - 0040 - 5732 - 0060 - 1882 - 0100 - 9433 - 0040 - 3673 - 0020 - 2615 - 0010 \text{”}$$

(21)

【0244】

なお、式(21)から明らかなとおり、認証サーバ202は、式(21)で表される認証用情報 α から、認証用情報 α を得るのに用いた関数 f_C の14個の引数の値を一意に得ることができる。具体的には、認証サーバ202は、認証用情報 α を所定のデリミタ“－”で分割し、分割により得られる14個の値のうち偶数番目の文字列をそれぞれ関数 g_B の逆関数 g_B^{-1} で変換する。すると、認証サーバ202は、関数 f_C の14個の引数の値(すなわち式(5)～(18)に示した14個の値)を得ることができる。

【0245】

また、上記の式(19)～(21)の例から容易に理解されるように、認証用情報 α は、人間が見ても一貫性を感じにくく覚えにくい内容となっており、かつ、適切な鍵情報と適切な関数 f_A 、 f_B または f_C を使うことで、十分に長くすることができる。このような認証用情報 α の性質は、セキュリティの観点から見て好ましい性質である。そして、ユーザ自身は、長くて複雑かつ不規則な認証用情報 α そのものを記憶する必要がないので、ユーザにとっての利便性が損なわれることはない。

【0246】

続いて、図7に示す別の具体例についても説明する。図7には、水平方向に5列、垂直方向に4行の、計20(=5×4)個のエリアに画面を細分化することを示す細分化エリア情報が使われる場合の例が示されている。図7の例では、乱数情報により、例えば3行目の4列目のエリアには、9496という乱数が対応づけられている。

【0247】

図7に示すように、「水平方向に5列、垂直方向に4行の、計20(=5×4)個のエリアに画面を細分化する」という点では同じでも、細分化エリア情報の具体的内容によって、20個のエリアの大きさが違うことがある。

【0248】

例えば、図7の上半分に示した画面と鍵情報の対応づけ404の図では、細分化エリア情報が、20個のエリアをすべて同じ大きさに定義している。よって、画面と鍵情報の対応づけ404によれば、軌跡405は、4行目の4列目、3行目の4列目、4行目の4列目、4行目の5列目、3行目の5列目、3行目の4列目、4行目の4列目、4行目の5列目、3行目の5列目という延べ9個のエリアを通過する。

【0249】

他方、図7の下半分に示した画面と鍵情報の対応づけ406の図では、20個のエリアの間で大きさの違いがあるように、細分化エリア情報が細分化の仕方を規定している。具体的には、細分化エリア情報により、1～2行目の高さは3～4行目の高さより高く定義され、1列目の幅は2～5列目より広く定義されている。換言すれば、細分化エリア情報は、3～4行目の2～5列目の8個のエリアが他の12個のエリアよりも小さくなるように画面の細分化の仕方を規定している。

【0250】

そして、画面と鍵情報の対応づけ406によれば、軌跡405と同じ軌跡407が通過

10

20

30

40

50

するエリアは、4行目の3列目、3行目の3列目、3行目の4列目、4行目の4列目、3行目の4列目、4行目の4列目、4行目の5列目、3行目の5列目という延べ8個である。

【0251】

すなわち、細分化エリア情報が異なれば、同じ軌跡405と407でも、画面エリア判定部106による判定結果が異なり、したがって、得られる認証用情報αも異なる。そして、図7の例では行数と列数は変わらないが、もちろん、行数、列数、またはエリアの形状が異なる細分化エリア情報が使われれば、同じ軌跡でも画面エリア判定部106による判定結果が異なる。

【0252】

例えば、あるユーザに対応して登録されている図形が、軌跡405や407のように、画面の右下に固まっているとする。あるいは、あるユーザに対応して登録されている図形が、画面の右下以外の部分にも広がってはいるが、画面の右下において相対的に複雑な形状であり、右下以外の部分において相対的に簡単な形状であるとする。

【0253】

その場合、例えば画面と鍵情報の対応づけ406として図7に例示されているような、画面の右下のエリアを小さく定義する細分化エリア情報が好適である。なぜなら、もし逆に画面の右下のエリアが大きいとすれば、他の図形との区別がつかなくなる（あるいは区別がつきづらくなる）からである。

【0254】

例えば、画面の右下のエリアを大きく定義する細分化エリア情報が使われると、軌跡407は、最下行の最右列にある1つのエリアしか通過しないかもしれない。すると、画面の最下行の最右列にある1つのエリアの範囲内に収まる図形であれば、たとえ軌跡407とはまったく異なる形状の図形が入力されても、「入力される軌跡はどのエリアを通過したか」という点ではまったく軌跡407と区別がつかない。そのため、画面乱数処理部107が認証用情報αを例えば式(1)によって求める場合は、軌跡407を描く図形が入力されるか軌跡407とはまったく異なる図形が入力されるかにかかわらず、まったく同じ認証用情報αが得られるおそれがある。

【0255】

よって、あるユーザに対応して登録されている図形が、画面内の特定の部分（例えば右下の部分）に固まっていたり、特定の部分において他の部分よりも複雑であったりする場合には、特定の部分のエリアを小さく定義する細分化エリア情報が好ましい。つまり、ユーザごとの図形の特徴を判別するのに十分な程度に細かな粒度で、特定の部分においてエリアを細分化する細分化エリア情報が使われることが好ましい。

【0256】

続いて、車載装置100と路側機201との間で送受信されるフレームの具体例を説明する。

図8Aと8Bは、フレームの例を説明する図である。図示の便宜のため、図8Aと8Bの双方に、第1実施形態におけるフレーム500一般の形式が示されている。フレーム500は、プリアンブルと、プリアンブルに続くヘッダと、ヘッダに続くペイロードを有する。

【0257】

また、以下では、車載装置100から路側機201へ送信される方向を「UpLink(UL)方向」といい、逆方向を「DownLink(DL)方向」という。図8Aと8Bには、各フレームの横に、どちらの方向に送信されるフレームなのかを示す文字が示されている。

【0258】

プリアンブルは、無線通信路で送受信されるフレーム500の先頭に同期用に付加される所定パターンのビット列である。

また、ヘッダには、データマップ情報と車載装置IDが含まれる。データマップ情報は、フレーム500のどの位置に何のフィールドのデータがあるかを示す情報である。

10

20

30

40

50

【0259】

例えば、ペイロード内の各フィールドの長さがフレーム500の種別ごとに固定されている実施形態では、データマップ情報としては、フレーム500の種別を示す値が利用可能である。あるいは、可変長のフィールドがペイロードに含まれる実施形態では、フレーム500の種別を示す値と、可変長のフィールドの長さを示す値がデータマップ情報に含まれてもよい。

【0260】

車載装置IDは、フレーム500がDL方向に送信される場合は送信先の車載装置100を指定するフィールドとして使われる。また、フレーム500がUL方向に送信される場合は、車載装置IDは送信元の車載装置100を表すフィールドとして使われる。

10

【0261】

そして、ペイロードには、平文の部分と暗号化された部分があり、フレーム500の種別に応じて一部のフィールドは省略可能である。平文の部分には公開DL情報が含まれ、暗号化された部分には、認証フラグと、秘密DL情報と、乱数情報と、細分化エリア情報と、秘密UL情報が含まれる。なお、実施形態によっては、ペイロードのすべてのフィールドが暗号化されていてもよい。

【0262】

また、暗号化方式は任意だが、例えば車載装置100ごとに固有の暗号化鍵を利用した対称鍵暗号化方式が利用可能である。車載装置100ごとに固有の暗号化鍵は、予め決められた固定されたものでもよいし、適宜の鍵交換アルゴリズムにしたがって適宜のタイミ

20

【0263】

公開DL情報は、DL方向に送信されるフレーム500の場合に使われる。公開DL情報は、車載装置100宛の、秘密にする必要のないオープンな情報である。公開DL情報の具体的内容は実施形態に応じて任意だが、例えば、公開DL情報は、渋滞が生じている地点に関する情報、交通規制に関する情報、天気予報に関する情報などを含んでもよい。

【0264】

認証フラグは2ビットのフィールドである。1ビット目は、認証プロセス自体と関係のあるフレーム500か否かを示し、認証プロセス自体と関係がある場合の値は“0”、認証プロセス自体と関係がない場合の値は“1”である。例えば、認証に成功した後に、認証済みの車載装置100に対して送信されるフレーム500では、認証フラグの1ビット目の値は“1”である。また、認証フラグの2ビット目は、“0”のとき、認証が済んでいないか認証に失敗したことを示し、“1”のとき、認証に成功したことを示す。なお、フレーム500の種別は、データマップ情報と認証フラグの一方または双方から判別可能である。

30

【0265】

ペイロード内のその他のフィールドは、フレーム500の種類に応じて具体的な内容が異なるので、詳細は後述する。また、図8Aと8Bでは省略されているが、実施形態によっては、ペイロードの後にさらに、例えば誤り検出のためのFrame Check Sequence (FCS) あるいは電子署名などのトレイラがあってもよい。

40

以上のようなフレーム500には、具体的には以下のような様々な種類がある。なお、図8Aと8Bにおいて、使われないフィールドは斜線で示されている。

【0266】

さて、図8Aの認証要求501は、例えば、図4のステップS103で送信される。認証要求501は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、認証要求501におけるフィールドの配置を示すデータマップ情報と、車載装置IDを含む。また、図8Aの認証要求501は、“123456789”という車載装置IDを持つ車載装置100から送信される場合の例である。

【0267】

認証要求501はUL方向に送信されるフレーム500なので、認証要求501におい

50

て公開DL情報は使われない。また、図8Aの認証要求501では、暗号化されるフィールドのうちでは、認証フラグと秘密UL情報以外のフィールドは使われない。

【0268】

なお、認証要求501は、認証プロセス自体に関係があり、まだ認証が済んでいないときに認証を要求するために送信されるので、認証要求501における認証フラグの値は“00”である。そして、秘密UL情報には、秘密の情報である認証用情報が設定される。

【0269】

また、認証通知502は、認証に成功したときに、認証に対する肯定応答(acknowledgment; ACK)としてDL方向に送信され、例えば図4のステップS104で受信される。認証通知502は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、認証通知502におけるフィールドの配置を示すデータマップ情報と、車載装置IDを含む。また、図8Aの認証通知502は、“123456789”という車載装置IDを持つ車載装置100の認証に成功した場合の例である。

10

【0270】

認証通知502は、DL方向に送信されるフレーム500なので、公開DL情報を含んでいてもよい。もちろん、公開DL情報は省略されてもよい。

なお、認証通知502は、認証プロセス自体に関係があり、認証に成功したときに送信されるので、認証通知502における認証フラグの値は“01”である。そして、ペイロード内の他のフィールドは、認証通知502では省略される。

【0271】

また、拒否通知503は、認証に失敗したときに、認証に対する否定応答(negative acknowledgement; NACK)としてDL方向に送信され、例えば図4のステップS104で受信される。拒否通知503は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、拒否通知503におけるフィールドの配置を示すデータマップ情報と、車載装置IDを含む。また、図8Aの拒否通知503は、“123456789”という車載装置IDを持つ車載装置100の認証に失敗した場合の例である。

20

【0272】

拒否通知503は、DL方向に送信されるフレーム500なので、公開DL情報を含んでいてもよい。もちろん、公開DL情報は省略されてもよい。

なお、拒否通知503は、認証プロセス自体に関係があり、認証に失敗したときに送信されるので、拒否通知503における認証フラグの値は“00”である。そして、ペイロード内の他のフィールドは、拒否通知503では省略される。

30

【0273】

また、鍵情報更新要求504は、例えば図4のステップS107において、鍵情報の更新を要求するためにUL方向に送信される。鍵情報更新要求504は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、鍵情報更新要求504におけるフィールドの配置を示すデータマップ情報と、車載装置IDを含む。また、図8Aの鍵情報更新要求504は、“123456789”という車載装置IDを持つ車載装置100が鍵情報の更新を要求する場合の例である。

【0274】

鍵情報更新要求504はUL方向に送信されるフレーム500なので、鍵情報更新要求504において公開DL情報は使われない。また、図8Aの鍵情報更新要求504では、認証フラグ以外のペイロード内のフィールドは使われない。

40

【0275】

なお、鍵情報更新要求504は、認証が成功した後に送信されるものであり、認証プロセス自体とは関係がない。よって、鍵情報更新要求504における認証フラグの値は“11”である。

【0276】

また、鍵情報更新通知505は、例えば図4のステップS108で受信される。鍵情報更新通知505は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダ

50

として、鍵情報更新通知 505 におけるフィールドの配置を示すデータマップ情報と、車載装置 ID を含む。また、図 8 A の鍵情報更新通知 505 は、“1 2 3 4 5 6 7 8 9”という車載装置 ID を持つ車載装置 100 に新たな鍵情報が通知される場合の例である。

【0277】

鍵情報更新通知 505 は、DL 方向に送信されるフレーム 500 なので、公開 DL 情報を含んでいてもよい。もちろん、公開 DL 情報は省略されてもよい。

なお、鍵情報更新通知 505 は、認証が成功した後に送信されるものであり、認証プロセス自体とは関係がない。よって、鍵情報更新通知 505 における認証フラグの値は“11”である。

【0278】

そして鍵情報更新通知 505 のペイロードのうち、乱数情報のフィールドには新たな乱数情報が設定され、細分化エリア情報のフィールドには新たな細分化エリア情報が設定される。ペイロード内の他のフィールドは、鍵情報更新通知 505 では省略される。

【0279】

また、鍵情報受領通知 506 は、例えば図 4 のステップ S111 において、新たな鍵情報を受領したことを認証サーバ 202 に通知するために UL 方向に送信される。鍵情報受領通知 506 は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、鍵情報受領通知 506 におけるフィールドの配置を示すデータマップ情報と、車載装置 ID を含む。また、図 8 A の鍵情報受領通知 506 は、“1 2 3 4 5 6 7 8 9”という車載装置 ID を持つ車載装置 100 が新たな鍵情報を受領した場合の例である。

【0280】

鍵情報受領通知 506 は UL 方向に送信されるフレーム 500 なので、鍵情報受領通知 506 において公開 DL 情報は使われない。

なお、鍵情報受領通知 506 は、認証が成功した後に送信されるものであり、認証プロセス自体とは関係がない。よって、鍵情報受領通知 506 における認証フラグの値は“11”である。

【0281】

そしてペイロードのうち、乱数情報のフィールドには、受領した新たな乱数情報のバージョンが設定され、細分化エリア情報のフィールドには受領した新たな細分化エリア情報のバージョンが設定される。ペイロード内の他のフィールドは、鍵情報受領通知 506 では省略される。

【0282】

なお、情報送信処理部 104 は、格納部 105 内の鍵情報を参照することで鍵情報のバージョンを認識することもできるし、情報受信処理部 103 が情報送信処理部 104 に新たな鍵情報のバージョンを通知してもよい。よって、情報送信処理部 104 は、図 4 のステップ S111 において、細分化エリア情報と乱数情報のバージョンを含むデータを、鍵情報受領通知 506 用のデータとして上位機器インタフェース部 102 に出力することができる。

【0283】

そして、鍵情報受領通知 506 が図 8 B の鍵情報受領通知 506 のように新たな鍵情報のバージョンを示す情報を含む場合は、図 5 のステップ S211 で認証サーバ 202 は、バージョンの確認を行ってもよい。

【0284】

つまり、認証サーバ 202 は、最新送信版として保持している鍵情報のバージョンと、受信した鍵情報受領通知 506 に含まれるバージョンが一致するか否かを確認してもよい。そして、認証サーバ 202 は、バージョンが一致すれば最新送信版の鍵情報を認証利用版の鍵情報としてコピーし、逆に、バージョンが不一致であれば適宜のエラー処理を行ってもよい。

【0285】

例えば、認証サーバ 202 は、エラー処理として、最新送信版の鍵情報を含む鍵情報更

10

20

30

40

50

新通知を車載装置 100 に再送してもよい。そして、車載装置 100 は、自ら送信した鍵情報更新要求 504 に対する直接の返信としてではなくエラー処理の結果として再送されてくる鍵情報更新通知 505 に関しても、受信を契機として図 4 のステップ S110 および S111 と同様の処理を行ってもよい。

【0286】

また、図 8 B サービス中通信 507 は、認証に成功した後に交通管制サーバ 203 から車両 305 が受けるサービスにおいて、DL 方向に送信されるフレーム 500 である。なお、サービスを受けるためのクライアントは、車載装置 100 に含まれていてもよいし、車載装置 100 と同じ車両 305 に搭載された車載装置 100 以外の装置であってもよい。後者の場合、サービス中通信 507 の受信とサービス中通信 508 の送信は、クライアントたる装置が行ってもよい。

10

【0287】

サービス中通信 507 は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、サービス中通信 507 におけるフィールドの配置を示すデータマップ情報と、車載装置 ID を含む。また、図 8 B のサービス中通信 507 は、“123456789”という車載装置 ID で識別されるアカウントに対するサービスにおいて送信されるフレーム 500 の例である。

【0288】

サービス中通信 507 は、DL 方向に送信されるフレーム 500 なので、サービス中通信 507 は公開 DL 情報を含んでいてもよい。図 8 B には、サービス中通信 507 における公開 DL 情報の例として、渋滞、事故、交通規制などについて示す一般的交通情報を示してある。

20

【0289】

なお、サービス中通信 507 は、認証が成功した後に送信されるものであり、認証プロセス自体とは関係がない。よって、サービス中通信 507 における認証フラグの値は“11”である。

【0290】

そして、ペイロードのうち秘密 DL 情報のフィールドには、交通管制サーバ 203 からのサービスに関する情報が含まれる。図 8 B のサービス中通信 507 は、具体的には、警察車両、消防車、救急車などの緊急車両向けのサービスにおいて送信されるフレーム 500 の例である。

30

【0291】

よって、サービス中通信 507 の秘密 DL 情報のフィールドには、交通管制サーバ 203 により信号が青に制御される経路を案内するための緊急車両用案内情報が設定されている。また、ペイロード内の他のフィールドは、サービス中通信 507 では省略される。もちろん、サービスの内容に応じて、秘密 DL 情報のフィールドの内容も様々であってもよい。

【0292】

また、サービス中通信 508 は、認証に成功した後に交通管制サーバ 203 から車両 305 がサービスを受けるために UL 方向に送信されるフレーム 500 である。サービス中通信 508 は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、サービス中通信 508 におけるフィールドの配置を示すデータマップ情報と、車載装置 ID を含む。また、図 8 B のサービス中通信 508 は、“123456789”という車載装置 ID で識別されるアカウントに対するサービスにおいて送信されるフレーム 500 の例である。

40

【0293】

サービス中通信 508 は、UL 方向に送信されるフレーム 500 なので、サービス中通信 508 において公開 DL 情報は使われない。

なお、サービス中通信 508 は、認証が成功した後に送信されるものであり、認証プロセス自体とは関係がない。よって、サービス中通信 508 における認証フラグの値は“1

50

1”である。

【0294】

そして、ペイロードのうち秘密UL情報のフィールドが使われ、他のフィールドは省略される。図8Bには、サービスを受けるにあたってユーザの個人情報（例えばクレジットカード番号などでもよい）が秘密UL情報として設定される場合の例が示されている。もちろん、秘密UL情報は個人情報以外の情報であってもよい。

【0295】

なお、図8Bの認証要求兼更新要求509と認証通知兼更新通知510は、第2実施形態で使われるフレーム500である。また、位置通知511は、第3実施形態で使われるフレーム500である。よって、これら3種類のフレーム500についての詳細な説明はここでは省略し、後述する。

10

【0296】

さて、続いて図9～10を参照して、第1実施形態との違いを中心に、第2実施形態について説明する。第2実施形態では、図8Aの認証要求501と鍵情報更新要求504の役割を兼ねる図8Bの認証要求兼更新要求509が使われ、図8Aの認証通知502と鍵情報更新通知505の役割を兼ねる図8Bの認証通知兼更新通知510が使われる。

【0297】

図9は、第2実施形態における車載装置の動作のフローチャートである。

ステップS301で情報受信処理部103は、図4のステップS101と同様にして、画面インタフェース部101を介した図形の入力を受け付け、軌跡情報を生成し、軌跡情報を画面エリア判定部106に出力する。

20

【0298】

そして、次のステップS302で車載装置100は、図4のステップS102と同様にして、入力された図形から得られる軌跡情報と、格納部105に予め記憶されている鍵情報とを使って、認証用情報を生成する。

【0299】

つまり、細分化エリア情報と軌跡情報に基づいて画面エリア判定部106は上記(a1)、(a2)、または(a1)と(a2)の双方を判定し、判定結果を画面乱数処理部107に出力する。そして、画面乱数処理部107は、格納部105から乱数情報を読み出し、画面エリア判定部106による判定結果と乱数情報から認証用情報を作成する。あるいは、画面乱数処理部107は、乱数情報を使わずに画面エリア判定部106による判定結果から、認証用情報を作成してもよい。いずれにせよ、画面乱数処理部107は生成した認証用情報を情報送信処理部104に出力する。

30

【0300】

すると、次のステップS303で情報送信処理部104は、図4のステップS106と同様に、地図情報と車速から推測される通信品質が良好であるか否かを判断する。具体的には、車両状態判定部108が「車載装置100が搭載されている車両305が信号機の付近で停止している」と見なせる状態か否か」ということを判定する。

【0301】

そして、車両状態判定部108から「車両305が信号機の付近で停止している」と見なせる状態である」と示す情報が入力された場合、情報送信処理部104は、「通信品質が良好だろう」と推測する。逆に、車両状態判定部108から「車両305は信号機の付近で停止している」と見なせる状態ではない」と示す情報が入力された場合、情報送信処理部104は、「通信品質が良好ではないだろう」と推測する。そして、情報送信処理部104は、推測される通信品質が良好になるまで待機する。推測される通信品質が良好であれば、処理はステップS304に移行する。

40

【0302】

ステップS304で情報送信処理部104は、認証と鍵情報の更新をあわせて認証サーバ202に要求するための認証要求兼更新要求のフレーム用のデータ（例えばヘッダとペイロード）を生成し、生成したデータを上位機器インタフェース部102に出力する。そ

50

して、情報送信処理部 104 は、フレームの送信を上位機器インタフェース部 102 に命じる。すると、上位機器インタフェース部 102 は命令にしたがって、必要に応じて暗号化やプリアンプルの付加などの処理を行い、認証要求兼更新要求のフレームを送信する。

【0303】

ステップ S 304 で送信される認証要求兼更新要求のフレームは、例えば、図 8 B の認証要求兼更新要求 509 のような形式である。認証要求兼更新要求 509 は、図 8 A の認証要求 501 と鍵情報更新要求 504 の役割を兼ねる。

【0304】

具体的には、認証要求兼更新要求 509 は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、認証要求兼更新要求 509 におけるフィールドの配置を示すデータマップ情報と、車載装置 ID を含む。図 8 B の認証要求兼更新要求 509 は、“123456789” という車載装置 ID を持つ車載装置 100 から送信される場合の例である。

【0305】

認証要求兼更新要求 509 は UL 方向に送信されるフレーム 500 なので、認証要求兼更新要求 509 において公開 DL 情報は使われない。また、図 8 B の認証要求兼更新要求 509 ではペイロードのフィールドのうちでは認証フラグと秘密 UL 情報以外のフィールドは使われない。

【0306】

なお、認証要求兼更新要求 509 は認証プロセス自体に関係があり、まだ認証が済んでいないときに送信されるので、認証要求兼更新要求 509 における認証フラグの値は、認証要求 501 と同様に“00”である。そして、秘密 UL 情報には、秘密の情報である認証用情報が認証要求 501 と同様に設定される。

【0307】

さて、ここで図 9 の説明に戻る。ステップ S 304 において、認証要求兼更新要求のフレームの送信を上位機器インタフェース部 102 に命じた後、情報送信処理部 104 は、タイマをタイムアウト検出用の所定の時間に設定する。なお、フレームの再送に備えて、情報送信処理部 104 は、認証用情報または認証要求兼更新要求のフレーム用のデータを保持する。また、第 1 実施形態における想定と同様に、第 2 実施形態においても、ステップ S 304 でタイマに設定される値は、ネットワーク 204 の構成、認証サーバ 202 のスループット、路側機 201 の設置間隔などに応じて適切に定められているものとする。

【0308】

続いて、ステップ S 305 で情報送信処理部 104 は、後続の処理を行うためのトリガとなるイベントの発生を待つ。そして、トリガとなるイベントが発生すると、処理はステップ S 306 に移行する。本実施形態ではステップ S 305 でトリガとなるイベントには認証通知兼更新通知の受信と、拒否通知の受信と、タイムアウトの 3 種類があり、具体的には以下のようにして検出される。

【0309】

ステップ S 304 で上位機器インタフェース部 102 から送信された認証要求兼更新要求のフレームは、車載装置 100 と路側機 201 との間の通信品質が良好であれば、路側機 201 に受信される。そして、認証要求兼更新要求は、路側機 201 からネットワーク 204 を介して、認証サーバ 202 に送信される。

【0310】

そして、認証要求兼更新要求が認証サーバ 202 に到達すると、認証サーバ 202 は認証要求兼更新要求に含まれる認証用情報と車載装置 ID に基づいて認証処理を行い、認証用情報が正当な情報か不正な情報かを判断する。認証サーバ 202 による認証処理と判断は、図 5 のステップ S 202 および S 204 と同様である。また、認証サーバ 202 は図 5 のステップ S 203 と同様に、返信時の中継点となる路側機 201 の選択も行う。

【0311】

そして、認証用情報が正当な情報であると判断した場合、認証サーバ 202 は、図 5 の

10

20

30

40

50

ステップ S 2 0 5 と同様に交通管制サーバ 2 0 3 に対して認証結果を知らせ、図 5 のステップ S 2 0 8 と同様に新たな鍵情報を作成して最新送信版として記憶する。そして、認証サーバ 2 0 2 は、認証通知兼更新通知を作成し、選択した路側機 2 0 1 に宛てて送信する。他方、認証用情報が不正な情報であると判断した場合、認証サーバ 2 0 2 は図 5 のステップ S 2 0 7 と同様に、選択した路側機 2 0 1 に宛てて拒否通知を送信する。

【0312】

そして、認証通知兼更新通知または拒否通知は、ネットワーク 2 0 4 と路側機 2 0 1 を介して車載装置 1 0 0 に到達し、上位機器インタフェース部 1 0 2 において受信される。例えば、上位機器インタフェース部 1 0 2 において受信される拒否通知は、第 1 実施形態における図 8 A の拒否通知 5 0 3 と同様である。また、上位機器インタフェース部 1 0 2 において受信される認証通知兼更新通知は、例えば図 8 B に示す認証通知兼更新通知 5 1 0 のような形式である。

10

【0313】

図 8 B の認証通知兼更新通知 5 1 0 は、図 8 A の認証通知 5 0 2 と鍵情報更新通知 5 0 5 の役割を兼ねる。具体的には、認証通知兼更新通知 5 1 0 は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、認証通知兼更新通知 5 1 0 におけるフィールドの配置を示すデータマップ情報と、車載装置 I D を含む。図 8 B の認証通知兼更新通知 5 1 0 は、“1 2 3 4 5 6 7 8 9 ” という車載装置 I D を持つ車載装置 1 0 0 の認証に成功し、当該車載装置 1 0 0 に新たな鍵情報を通知する場合の例である。

【0314】

認証通知兼更新通知 5 1 0 は、D L 方向に送信されるフレーム 5 0 0 なので、公開 D L 情報を含んでいてもよい。もちろん、公開 D L 情報は省略されてもよい。

20

なお、認証通知兼更新通知 5 1 0 は、認証プロセス自体に関係があり、認証に成功したときに送信されるので、認証通知兼更新通知 5 1 0 における認証フラグの値は認証通知 5 0 2 と同様に“0 1 ”である。

【0315】

そして、認証通知兼更新通知 5 1 0 では、鍵情報更新通知 5 0 5 と同様に、ペイロードのうち、乱数情報のフィールドには新たな乱数情報が設定され、細分化エリア情報のフィールドには新たな細分化エリア情報が設定される。ペイロード内の他のフィールドは、認証通知兼更新通知 5 1 0 では省略される。

30

【0316】

さて、認証通知兼更新通知または拒否通知を上位機器インタフェース部 1 0 2 が受信すると、上位機器インタフェース部 1 0 2 は認証通知兼更新通知または拒否通知のデータを情報受信処理部 1 0 3 に出力する。そして、情報受信処理部 1 0 3 は、上位機器インタフェース部 1 0 2 からのデータの入力を、認証通知兼更新通知または拒否通知の受信というトリガの発生として検出し、トリガの検出を情報送信処理部 1 0 4 に通知する。すると、情報送信処理部 1 0 4 は、ステップ S 3 0 4 で設定したタイマを無効化し、再送用に保持していた認証用情報または認証要求兼更新要求のフレーム用のデータを破棄する。

【0317】

他方、ステップ S 3 0 3 における「通信品質が良好であろう」という推測にもかかわらず、実際の通信品質が良好ではない場合、ステップ S 3 0 4 で送信された認証要求兼更新要求のフレームは、どの路側機 2 0 1 にも受信されない。よって、認証要求兼更新要求は認証サーバ 2 0 2 には到達しない。よって、この場合は、情報送信処理部 1 0 4 がステップ S 3 0 4 でタイマに設定した時間以内に認証通知兼更新通知のフレームが受信されることなく、タイマがタイムアウトする。そして、ステップ S 3 0 5 において情報送信処理部 1 0 4 はタイムアウトをトリガの発生として検出する。

40

【0318】

以上のようにして、情報送信処理部 1 0 4 がトリガの発生を、情報受信処理部 1 0 3 からの通知またはタイマのタイムアウトにより認識すると、処理はステップ S 3 0 6 に移行する。

50

【0319】

そして、ステップS306で情報送信処理部104は、トリガとして検出されたイベントの種類を判断する。検出されたトリガが拒否通知の受信であれば、図9の処理が終了し、検出されたトリガが認証通知兼更新通知の受信であれば、処理はステップS307に移行する。また、検出されたトリガがタイムアウトであれば、処理はステップS303に戻る。

【0320】

以上のステップS303～S306の処理により、通信環境が悪ければ必要に応じて認証要求兼更新要求のフレームの再送が繰り返される。よって、いずれは結局、認証通知兼更新通知と拒否通知のいずれかの受信がトリガとして検出される。

10

【0321】

つまり、ステップS301で入力された図形が正当な図形であれば、遅かれ早かれ認証通知兼更新通知の受信がトリガとして検出され、処理がステップS307に移行する。また、ステップS301で入力された図形が不正な図形であれば、遅かれ早かれ拒否通知の受信がトリガとして検出され、図9の処理が終了する。

【0322】

そして、認証通知兼更新通知の受信がトリガとして検出された場合、ステップS307で情報受信処理部103が、図4のステップS110と同様にして鍵情報の更新を行う。すなわち、情報受信処理部103は、ステップS305で上位機器インタフェース部102から出力された認証通知兼更新通知から新たな鍵情報を取り出し、格納部105に格納されている現在の鍵情報を新たな鍵情報で上書き更新する。

20

【0323】

そして、次のステップS308で車載装置100は、図4のステップS111と同様にして鍵情報受領通知のフレームを送信する。つまり、情報送信処理部104が鍵情報受領通知のフレーム用のデータ（例えばヘッダとペイロード）を生成し、生成したデータを上位機器インタフェース部102に出力し、上位機器インタフェース部102にフレームの送信を命じる。そして、上位機器インタフェース部102は命令にしたがって、必要に応じて暗号化やプリアンプルの付加などの処理を行い、鍵情報受領通知のフレームを送信し、図9の処理が終了する。

【0324】

なお、ステップS307とS308の実行順は逆でもよい。あるいは、ステップS307とS308の処理が並行して行われてもよい。また、鍵情報受領通知を受信したときに認証サーバ202が行う処理は第1実施形態と同様である。

30

【0325】

以上説明した第2実施形態では、第1実施形態と比較して車載装置100と認証サーバ202の間のトラフィックが少ない。よって、ネットワーク204の負荷が第1実施形態よりも軽くて済む。

【0326】

続いて、図9の処理の具体例について図10を参照して説明する。図10は、第2実施形態で認証に成功する場合のタイミングチャートの例である。

40

ステップS401において、ユーザが、図3の駐車場304に駐車されている車両305のエンジンをかけ、車載装置100の電源をオンにする。すると、車載装置100は図9の処理を開始する。

【0327】

続くステップS402は、図9のステップS301に相当する。ステップS402でユーザが予め決められた図形を入力し、車載装置100は画面インタフェース部101を介して図形の入力を受け付ける。

【0328】

そして、次のステップS403は図9のステップS302に相当し、車載装置100は認証用情報を生成する。

50

ところで、ユーザは、ステップ S 4 0 1 での図形の入力後は、運転に専念することができる。よって、車載装置 1 0 0 がステップ S 4 0 3 で認証用情報を生成するのと並行して、ユーザは車両 3 0 5 を運転して駐車場 3 0 4 から道路 3 0 1 d に向かっているかもしれない。

【0329】

具体的には、図 1 0 の例では、ユーザの運転操作にしたがって車両 3 0 5 は次の経路に沿って移動するものとする。すなわち、車両 3 0 5 は、駐車場 3 0 4 から道路 3 0 1 d に出た後、交差点 3 0 2 b に向かい、交差点 3 0 2 b を右折し、次の交差点 3 0 2 c も右折し、さらに次の交差点 3 0 2 d を左折するものとする。

【0330】

上記の経路に沿って車両 3 0 5 が移動する場合、図 3 に示すとおり、車両 3 0 5 にとって初めて近傍を通過することになる信号機は、交差点 3 0 2 b の信号機 3 0 3 c である。また、図 1 0 の例では、車両 3 0 5 が、交差点 3 0 2 b を右折する前に一時停止したとする。

【0331】

すると、車両 3 0 5 が停止した際に、図 9 のステップ S 3 0 3 において情報送信処理部 1 0 4 が「地図情報と車速から推測される通信品質が良好である」と判断する。よって、図 1 0 にステップ S 4 0 4 として示すように、車載装置 1 0 0 は図 9 のステップ S 3 0 4 で図 8 B の認証要求兼更新要求 5 0 9 を送信する。

【0332】

そして、図 3 に示すように交差点 3 0 2 b に設置された信号機 3 0 3 c には、路側機 2 0 1 c が取り付けられている。よって、ステップ S 4 0 4 で送信された認証要求兼更新要求 5 0 9 は、ステップ S 4 0 5 において路側機 2 0 1 c に無事に受信される。

【0333】

すると、路側機 2 0 1 c は、受信した認証要求兼更新要求 5 0 9 から、認証サーバ 2 0 2 宛の認証要求兼更新要求の I P パケットを生成し、生成した I P パケットをネットワーク 2 0 4 に送出する。具体的には、路側機 2 0 1 c は、認証要求兼更新要求 5 0 9 から車載装置 I D の値と秘密 U L 情報として設定された認証用情報を取り出して I P パケットのペイロードに含める。また、路側機 2 0 1 c は、送信元 I P アドレスに路側機 2 0 1 c 自身の I P アドレスを設定し、送信先 I P アドレスに認証サーバ 2 0 2 の I P アドレスを設定する。

【0334】

なお、路側機 2 0 1 c は、送信する I P パケットが認証要求兼更新要求であることを示すため、認証要求兼更新要求 5 0 9 からデータマップ情報を取り出して I P パケットのペイロードに含めてもよい。あるいは、路側機 2 0 1 c は、認証要求兼更新要求という種別を示す特定の値を I P パケットのペイロードに含めてもよい。

【0335】

以上のようにして路側機 2 0 1 c で生成された I P パケットは、ネットワーク 2 0 4 を介して認証サーバ 2 0 2 に送信され、ステップ S 4 0 6 で認証サーバ 2 0 2 において受信される。すると、認証サーバ 2 0 2 は I P パケットのペイロードから、車載装置 1 0 0 の車載装置 I D と認証用情報を取り出し、認証処理を行う。図 1 0 の例は、認証に成功する場合の例である。また、認証サーバ 2 0 2 は図 5 のステップ S 2 0 3 と同様に返信時の中継点となる路側機 2 0 1 の選択を行う。

【0336】

そして、次のステップ S 4 0 7 で認証サーバ 2 0 2 は、認証通知兼更新通知の I P パケットを生成し、送信する。

具体的には、認証サーバ 2 0 2 は、送信元路側機が路側機 2 0 1 c であると認識する。また、認証サーバ 2 0 2 は、上記 (d 1) ~ (d 3) に例示したような路側機配置情報を保持している。図 1 0 の例では、認証サーバ 2 0 2 が路側機配置情報から、路側機 2 0 1 b と 2 0 1 g と 2 0 1 h を送信元近傍路側機として特定したとする。すると、認証サーバ

10

20

30

40

50

202は、ステップS407で、送信元路側機と送信元近傍路側機のそれぞれに宛てて、認証通知兼更新通知のIPパケットを送信する。

【0337】

そして、ステップS408において、路側機201gは、認証通知兼更新通知のIPパケットを受信し、受信したIPパケットに基づいて図8Bの認証通知兼更新通知510を送信する。

【0338】

ここで、車両305は、上記の経路上を交差点302dの付近まで進んできたとする。すると、車両305に搭載されている車載装置100は、交差点302dに設置された信号機303gに取り付けられた路側機201gから送信された認証通知兼更新通知510を、ステップS409において受信する。つまり、ステップS409は、図9のステップS305においてトリガとして認証通知兼更新通知が検出される場合の例である。

【0339】

なお、ステップS407で認証サーバ202から送信された認証通知兼更新通知のIPパケットは、ステップS410において、送信元近傍送信機である路側機201bに受信される。そして、路側機201bは認証通知兼更新通知510を送信する。しかし、車載装置100を搭載した車両305は路側機201bの付近にはないので、路側機201bが送信した認証通知兼更新通知510は車載装置100に受信されない。

【0340】

同様に、ステップS407で認証サーバ202から送信された認証通知兼更新通知のIPパケットは、ステップS411において、送信元送信機である路側機201cに受信される。そして、路側機201cは認証通知兼更新通知510を送信する。

【0341】

しかし、図10の例では、ステップS411の時点で、車載装置100を搭載した車両305は既にステップS404にいた位置から離れており、路側機201cとの通信範囲から出てしまっている。そのため、路側機201cが送信した認証通知兼更新通知510は車載装置100に受信されない。

【0342】

また、ステップS407で認証サーバ202から送信された認証通知兼更新通知のIPパケットは、ステップS412において、送信元近傍送信機である路側機201hに受信される。そして、路側機201hは認証通知兼更新通知510を送信する。しかし、車載装置100を搭載した車両305は路側機201hの付近にはないので、路側機201hが送信した認証通知兼更新通知510は車載装置100に受信されない。

【0343】

さて、車載装置100においては、ステップS409での認証通知兼更新通知510の受信を契機として、ステップS413において図9のステップS307の処理が行われる。すなわち、ステップS413で車載装置100は鍵情報を更新する。

【0344】

そして、続くステップS414は図9のステップS308に相当し、ステップS414で車載装置100は、鍵情報受領通知506を送信する。なお、ステップS409からステップS414までの時間は、実際には非常に短いので、ステップS414の時点でも、車両305はまだ交差点302dの付近にあり、車載装置100は路側機201gの通信範囲内にある。

【0345】

よって、ステップS414で送信された鍵情報受領通知506は、ステップS415で無事に路側機201gに受信される。そして、路側機201gは、ネットワーク204を介して鍵情報受領通知のIPパケットを認証サーバ202に送信する。

【0346】

すると、ステップS416で認証サーバ202は、ステップS407で送信した認証通知兼更新通知に対する返信としての鍵情報受領通知を受信する。そして、認証サーバ20

10

20

30

40

50

2は図5のステップS211と同様に、最新送信版の鍵情報を認証利用版としてコピーする。

【0347】

したがって、車両305がいずれ走行を終えて車載装置100の電源が切られ、次に再び車載装置100の電源が入れられたとき、車載装置100は認証に使うための新たな鍵情報を既に格納部105に保持していることになる。よって、次の認証を行おうとする段になって改めて車載装置100が新たな鍵情報を要求する必要はない。

【0348】

つまり、次に再び車載装置100の電源が入れられたとき、車載装置100は、格納部105に格納済みの鍵情報を用いて図9の処理を行うことができる。換言すれば、車載装置100への電源投入から認証結果の受信までの時間は、鍵情報の更新にかかる時間が含まれない分だけ、短くて済む。なお、この時間短縮の効果は、他の実施形態においても同様に得られる。

【0349】

さて、続いて第3実施形態について、第1実施形態との違いを中心に説明する。第3実施形態は、無線通信路の通信品質に関して車載装置100ではなく認証サーバ202が推測を行う実施形態である。

【0350】

つまり、第3実施形態における車載装置100は、UL方向のフレームの送信に関して、特に通信品質を考慮することなく単純にフレームの送信を行い、認証サーバ202からの返信がなければタイムアウトしてフレームを再送するだけである。他方、認証サーバ202は、車載装置100の位置を把握し、把握した位置に基づいて、車載装置100がいずれかの路側機201との間で無線通信可能な状態か否かを推測する。

【0351】

具体的には、車載装置100は、車載装置100自身の位置を示す情報を位置通知として送信する。そして、認証サーバ202は、車載装置100から送信されてきた位置通知を利用して、車載装置100がいずれかの路側機201との間で無線通信可能な状態か否かを推測する。認証サーバ202は、推測結果にしたがい、車載装置100への鍵情報の送信のタイミングを決定し、送信時の中継点となる路側機201を選択する。

【0352】

なお、車載装置100からの位置通知の送信は、定期的に行われてもよいし、不定期に行われてもよい。以下では説明の便宜上、車載装置100が、電源投入後から、認証に関する処理とは独立して、位置通知の送信を繰り返すものとする。

【0353】

例えば、外部センサ110が位置センサを含む場合、車載装置100の情報送信処理部104は、位置センサから出力される位置情報（例えば緯度と経度の組）を含む位置通知のフレームのデータを定期的に作成してもよい。そして、情報送信処理部104は、上位機器インタフェース部102にフレームの送信を命じ、上位機器インタフェース部102が位置通知のフレームを送信してもよい。

【0354】

あるいは、路側機201がビーコンフレームをブロードキャストしてもよい。そして、車載装置100がビーコンフレームの受信に反応して返すフレームが位置通知として使われてもよい。

【0355】

なお、路側機201によるビーコンフレームの送信間隔は任意だが、路側機201は、例えば所定の間隔でビーコンフレームを送信してもよい。送信間隔は、例えば、信号機が赤の期間中に複数回の送信が行われる程度の間隔でもよい。

【0356】

また、ビーコンフレームには、送信元の路側機201を識別する路側機識別情報が含まれてもよい。路側機識別情報は、例えば下記(e1)～(e4)のような情報であり、認

10

20

30

40

50

証サーバ202にも予め登録されている。

(e1) 路側機201に予め割り当てられているID。

(e2) 路側機201のIPアドレス。

(e3) 路側機201の位置を示す緯度と経度の組。

(e4) 上記(e1)～(e3)のうち2つ以上の任意の組み合わせ。

【0357】

例えば、車載装置100を搭載した車両305が図3の交差点302bを通過するとき、車載装置100は、路側機201cからのビーコンフレームを受信するかもしれない。そして、車両305が道路301aを直進して交差点302fに至り、そのとき信号機303kが赤になっていれば、車両305はしばらく停止し、車載装置100は路側機201kからのビーコンフレームを複数回受信するかもしれない。車載装置100は、具体的には以下のようにして、ビーコンフレームの受信のたびに位置通知のフレームを送信することができる。

10

【0358】

すなわち、車載装置100において上位機器インタフェース部102は、ビーコンフレームを受信すると、ビーコンフレームに含まれる路側機識別情報を情報受信処理部103に出力する。すると、情報受信処理部103は路側機識別情報を情報送信処理部104に出力し、情報送信処理部104は路側機識別情報から位置通知のフレームのデータを生成する。そして、情報送信処理部104はフレームの送信を上位機器インタフェース部102に命じ、上位機器インタフェース部102はフレームを送信する。

20

【0359】

以上のように、外部センサ110である位置センサの出力または路側機201からのビーコンフレームに含まれる路側機識別情報に基づいて、車載装置100は位置通知のフレームを送信することができる。車載装置100が送信する位置通知のフレームの具体例は、例えば、図8Bの位置通知511である。

【0360】

位置通知511は、車載装置100の位置を認証サーバ202に通知するためにUL方向に送信される。位置通知511は、所定パターンのビット列が指定されたプリアンプルに続いて、ヘッダとして、位置通知511におけるフィールドの配置を示すデータマップ情報と、車載装置IDを含む。また、図8Bの位置通知511は、“123456789”という車載装置IDを持つ車載装置100が位置を通知する場合の例である。

30

【0361】

位置通知511はUL方向に送信されるフレーム500なので、位置通知511において公開DL情報は使われない。

なお、位置通知511は、認証とは独立して送信されるので、認証フラグの2ビット目の値は便宜的に“0”に設定され、認証フラグ全体の値は“10”である。また、ペイロードのうち、秘密UL情報のフィールドには、車両305の位置を示す位置情報が設定される。位置情報は、外部センサ110である位置センサから出力される緯度と経度の組でもよいし、車両305の位置を近似的に示す路側機識別情報でもよい。ペイロード内の他のフィールドは、位置通知511では省略される。

40

【0362】

以上のような位置情報を含む位置通知が路側機201により中継されると、認証サーバ202は位置情報から車載装置100の位置を把握することができる。あるいは、より単純に、認証サーバ202は次のようにして車載装置100の位置を把握してもよい。

【0363】

すなわち、路側機201はビーコンフレームを送信する。このビーコンフレームには路側機識別情報が含まれなくてもよい。車載装置100は、ビーコンフレームを受信すると、ビーコンフレームの受信を通知する受信通知のフレームを、位置通知のフレームとして送信する。この場合、位置通知のフレームは、図8Bの位置通知511とは異なり、秘密UL情報を持たなくてもよい。その理由は次のとおりである。

50

【0364】

もし位置通知のフレームが路側機201において無事受信されるならば、路側機201は位置通知を認証サーバ202に中継する。その際、位置通知のIPパケットの送信元IPアドレスとして、路側機201は路側機201自身のIPアドレスを設定する。すると、位置通知のIPパケットを受信した認証サーバ202は、送信元IPアドレスから、車載装置100がどの路側機201の近傍にいるときに位置通知のフレームを送信したのかを把握することができる。つまり、認証サーバ202は、送信元IPアドレスに基づいて、車載装置100の位置を路側機201の位置により近似して把握することができる。

【0365】

よって、車載装置100が位置通知として送信するフレームおよび路側機201が位置通知として中継するIPパケットには、図8Bの位置通知511に含まれるような位置情報があってもよいし、なくてもよい。いずれにしろ、認証サーバ202は位置通知から車載装置100の位置を把握することができる。

【0366】

以下、第3実施形態において車載装置100と認証サーバ202がそれぞれ行う処理について、図11～12を参照してさらに詳しく説明する。

図11は、第3実施形態における車載装置の動作のフローチャートである。

【0367】

ステップS501～S505は、図4のステップS101～S105とそれぞれ同じなので、説明を省略する。なお、検出されたトリガが拒否通知の受信であるとステップS505で判断されれば、図11の処理が終了し、検出されたトリガが認証通知の受信であれば、処理はステップS505からステップS506に移行する。また、検出されたトリガがタイムアウトであれば、処理はステップS505からステップS503に戻る。

【0368】

以上のステップS501～S505の処理により、通信環境が悪ければ必要に応じて認証要求のフレームの再送が繰り返される。よって、いずれは結局、認証通知と拒否通知のいずれかの受信がトリガとして検出される。

【0369】

ステップS506で情報送信処理部104は、図4のステップS107と同様に、鍵情報更新要求のフレーム用のデータを生成し、生成したデータを上位機器インタフェース部102に出力する。そして、情報送信処理部104は、フレームの送信を上位機器インタフェース部102に命じる。すると、上位機器インタフェース部102は命令にしたがって、必要に応じて暗号化やプリアンプルの付加などの処理を行い、鍵情報更新要求のフレームを送信する。

【0370】

また、情報送信処理部104は、フレームの送信を上位機器インタフェース部102に命じた後、タイマをタイムアウト検出用の所定の時間に設定する。なお、フレームの再送に備えて、情報送信処理部104は、鍵情報更新要求のフレーム用のデータを保持してもよい。また、タイムアウト検出用の時間の長さに関しては、ステップS508の説明の後で説明する。

【0371】

続いて、ステップS507で情報送信処理部104は、後続の処理を行うためのトリガとなるイベントの発生を待つ。そして、トリガとなるイベントが発生すると、処理はステップS508に移行する。本実施形態ではステップS507でトリガとなるイベントには、鍵情報更新通知の受信とタイムアウトの2種類がある。

【0372】

もしステップS506においていずれかの路側機201との間に良好な品質の無線通信路が確立されていれば、ステップS506で送信した鍵情報更新要求は認証サーバ202に到達する。その場合、タイムアウト検出用の所定の時間が適切に設定されていれば、タイマがタイムアウトする前に、上位機器インタフェース部102は鍵情報更新通知のフレ

10

20

30

40

50

ームを受信する。

【0373】

すると、上位機器インタフェース部102は受信した鍵情報更新通知のフレームのデータを情報受信処理部103に出力する。また、情報受信処理部103は、上位機器インタフェース部102からのデータの入力を、鍵情報更新通知の受信というトリガの発生として検出し、トリガの検出を情報送信処理部104に通知する。

【0374】

すると、情報送信処理部104は、ステップS506で設定したタイマを無効化する。また、情報送信処理部104は、もし再送用に鍵情報更新要求のフレーム用のデータを保持しているのであれば、鍵情報更新要求のフレーム用のデータを破棄する。

10

【0375】

他方、鍵情報更新通知の受信というトリガの発生が情報受信処理部103から通知される前にタイマがタイムアウトすると、情報送信処理部104は、ステップS507においてタイムアウトをトリガの発生として検出する。

【0376】

以上のようにして、情報送信処理部104がトリガの発生を、情報受信処理部103からの通知またはタイマのタイムアウトにより認識すると、処理はステップS508に移行する。

【0377】

ステップS508で情報送信処理部104は、トリガとして検出されたイベントの種類を判断する。検出されたトリガが鍵情報更新通知の受信であれば、処理はステップS509に移行する。また、検出されたトリガがタイムアウトであれば、処理はステップS506に戻る。

20

【0378】

以上のステップS506～S508の処理により、必要に応じて鍵情報更新要求のフレームの再送が繰り返される。よって、いずれは結局、鍵情報更新通知の受信がトリガとして検出される。なお、ステップS507でのタイムアウトの時間は、第1実施形態の図4のステップS107で設定されるタイムアウトの時間と同じでもよいし、それより長くてもよいし、それより短くてもよい。

【0379】

例えば、車両305が走行している最中に車載装置100がステップS506で鍵情報更新要求504を送信することがある。その場合でも、鍵情報更新要求504はペイロードが非常に短いフレームなので、たまたま近傍に路側機201があれば、路側機201が鍵情報更新要求504の受信に成功することがある。すると、認証サーバ202に鍵情報更新要求が到達する。

30

【0380】

他方、車両305はなかなか赤信号に遭遇せずに走行を続けるかもしれない。そして、鍵情報更新通知505のように、鍵情報更新要求504と比べてペイロードのデータ量が多く、フレーム長の長いフレームの受信が成功するのは、ある程度安定した良好な通信品質の通信環境においてである。よって、もし車両305が赤信号に遭遇せずに高速で走行し続けている場合、なかなか安定した良好な通信品質の通信環境にはならないかもしれない。

40

【0381】

以上のような場合を考慮に入れて重視するならば、ステップS506で設定されるタイムアウトの時間は、ステップS107で設定されるタイムアウトの時間より長くてもよい。

【0382】

逆に、「車両305が走行している最中に送信した鍵情報更新要求504を路側機201が偶然うまく受信するような場合は無視する」という方針も考えられる。この方針にしたがうならば、ステップS506で設定されるタイムアウトの時間は、ステップS107

50

で設定されるタイムアウトの時間より短くてもよい。

【0383】

ステップS506で設定されるタイムアウトの時間が適切に短ければ、鍵情報更新要求504の送信から鍵情報更新通知505の受信までの間、同じ路側機201との間で安定して良好な通信品質が保てるような環境でない限り、車載装置100はタイムアウトする。そして、車載装置100は、タイムアウトのたびに鍵情報更新要求504を再送する。

【0384】

さて、ステップS509では、情報受信処理部103が、図4のステップS110と同様にして鍵情報の更新を行う。また、第3実施形態においては鍵情報更新通知の送信タイミングを認証サーバ202が制御するために位置通知が使われるので、鍵情報の更新後は位置通知の送信は不要である。よって、情報受信処理部103は、位置通知の送信を停止させる。

【0385】

さらに、次のステップS510では、情報送信処理部104と上位機器インタフェース部102が協働して、図4のステップS111と同様にして鍵情報受領通知のフレームを送信する。そして、図11の処理は終了する。

なお、ステップS509とS510の実行順は逆でもよい。あるいは、ステップS509とS510の処理が並行して行われてもよい。

【0386】

続いて、第3実施形態における認証サーバ202の動作を説明する。第3実施形態においても、認証サーバ202は、任意のタイミングで任意の車載装置100から任意の路側機201を介して情報を受信する可能性があり、情報の受信を契機として各種処理を行う。

【0387】

図12は、第3実施形態において、認証サーバが車載装置から情報を受信したときの処理のフローチャートである。なお、図12に関する説明においては、図12の処理の開始の契機となった情報の送信元の車載装置100を「送信元の車載装置100」という。

【0388】

ステップS601で認証サーバ202は、送信元の車載装置100から受信した情報の内容が認証要求、鍵情報更新要求、位置通知、鍵情報受領通知のいずれであるかを判断する。認証要求が受信された場合、処理はステップS602に移行し、鍵情報更新要求が受信された場合、処理はステップS608に移行し、位置通知が受信された場合、処理はステップS612に移行し、鍵情報受領通知が受信された場合、処理はステップS613に移行する。

【0389】

ステップS602～S607はそれぞれ図5のステップS202～S207と同じなので説明を省略する。

また、受信したIPパケットが鍵情報更新要求のIPパケットであった場合、認証サーバ202はステップS608において、図5のステップS208と同様にして、新たな鍵情報を作成する。そして、認証サーバ202は、送信元の車載装置100の車載装置IDと対応づけて、作成した鍵情報を最新送信版として記憶する。

【0390】

続いて、次のステップS609で認証サーバ202は、送信元の車載装置100を搭載した車両305の位置から推測される通信品質が良好になるまで待機する。第3実施形態において認証サーバ202は、位置通知に基づいて送信元の車載装置100の位置（つまり車両305の位置）を認識しているので、位置から通信品質を推測することができる。

【0391】

例えば、位置通知に、位置センサの出力した緯度と経度により表される位置情報が含まれる場合、認証サーバ202は、車載装置100から直近に受信した位置通知に含まれる位置情報が示す位置と、鍵情報更新要求を中継した路側機201の位置を比較してもよい

10

20

30

40

50

。車載装置 100 による位置通知の送信間隔が適宜に定められていれば、認証サーバ 202 は、2 つの位置が所定の距離内にあるとき、通信品質が良好であると推測することができる。

【0392】

なぜなら、2 つの位置が所定の距離内にあれば、「車両 305 がしばらく 1 箇所で停止しているか、速度が遅いためにせいぜい上記の所定の距離しか移動することができない間に、直近の位置通知と今回受信した鍵情報更新要求が送信された」と見なせるからである。車両 305 が停止ないし徐行していれば通信環境が安定していると期待され、また、停止ないし徐行している最中に直近の位置通知と今回受信した鍵情報更新要求が送信されたとすれば、車載装置 100 はいずれかの路側機 201 と通信可能な位置にある。よって、10
認証サーバ 202 は、比較した 2 つの位置が所定の距離内にあるとき、通信品質が良好であると推測してもよい。なお、ここでの「所定の距離」は、例えば路側機 201 の通信可能範囲の大きさに応じて定められることが望ましい。

【0393】

あるいは、認証サーバ 202 は、送信元の車載装置 100 から直近の位置通知を受信した受信時刻と現在時刻の差から、通信品質を推測してもよい。すなわち、認証サーバ 202 は、受信時刻と現在時刻の差が所定の閾値以下のとき、通信品質が良好であると推測してもよい。

【0394】

例えば、車載装置 100 が 10 秒間隔で位置通知のフレームを送信する場合に、直近の位置通知を受信した受信時刻と現在時刻の差が 25 秒あったとする。この場合、車載装置 100 が位置通知のフレームを送信したにもかかわらず、いずれの路側機 201 によっても中継されず、認証サーバ 202 に到達しなかった位置通知が 2 回あったということである。20

【0395】

この場合、車載装置 100 を搭載した車両 305 は、例えば路側機 201 の存在しないところを走行中なのかもしれないし、他の車両によって路側機 201 との間が遮蔽されてしまったのかもしれない。いずれにせよ、車載装置 100 と路側機 201 との間の通信品質は良好でないと推測される。つまり、鍵情報更新要求は、通信品質が安定していて良好だったから受信可能だったというよりも、偶然、受信されたのかもしれない。30

【0396】

他方、直近の位置通知を受信した受信時刻と現在時刻の差が例えば 1 秒といった短い時間であれば、車載装置 100 はまだ路側機 201 の付近に位置していると推測される。つまり、車載装置 100 と路側機 201 との間に通信可能な状態がまだ持続していると推測される。そこで、認証サーバ 202 は、直近の位置通知を受信した受信時刻と現在時刻の差が所定の閾値以下のとき、通信品質が良好であると推測してもよい。

【0397】

あるいは、認証サーバ 202 は、受信した位置通知の履歴を使って通信品質を推測してもよい。例えば、直近の 2 回あるいはそれ以上の位置通知が同じ路側機 201 を介して認証サーバ 202 に中継された場合、車両 305 は、中継点の路側機 201 の付近で停止ないし徐行していると推測される。したがって、車載装置 100 と中継点の路側機 201 との間の無線通信路の通信品質は、安定した良好なものだと推測される。よって、認証サーバ 202 は、受信した直近の所定回数（例えば 2 回）の位置通知を中継した路側機 201 が同じとき、通信品質が良好であると推測してもよい。40

【0398】

また、認証サーバ 202 は、信号機の状態を表す信号機情報を交通管制サーバ 203 から受け取り、信号機情報と受信した位置通知の履歴を使って通信品質を推測してもよい。位置通知の送信間隔が適切に定められていれば、受信した位置通知の履歴から、認証サーバ 202 は、車両 305 の走行方向を認識することができる。よって、信号機情報を用いることで、認証サーバ 202 は、車両 305 が赤信号で停止するタイミングを推測するこ50

とができる。

【0399】

例えば、車両305が、図3の道路301aを交差点302aから交差点302fに向かって走行するとする。この場合、認証サーバ202は、順に、路側機201b、201c、201h、201kを介して位置通知を受信するかもしれない。そして、路側機201kを介した位置通知の受信と前後して、認証サーバ202は、同じく路側機201kを介して鍵情報更新要求を受信するかもしれない。

【0400】

この場合、認証サーバ202は、位置通知の受信履歴から、車両305は道路301a上を走行していることを認識することができる。また、認証サーバ202は、交通管制サーバ203から信号機情報を得て、車両305の走行方向の進行の可否を示す信号機303kの状態を認識することができる。

10

【0401】

もし信号機303kが赤信号であれば、認証サーバ202は、「車両305は、路側機201kの近傍で赤信号による停止中であるから、車載装置100と路側機201kとの間の通信路の通信品質は良好である」と推測する。他方、信号機303kが青信号であれば、認証サーバ202は、「たまたま路側機201kを介した通信が成功したが、車両305は停止中とは限らず、したがって、通信品質も良好であるとは限らない」と推測する。黄信号に関しては、実施形態に応じて認証サーバ202は「通信品質が良好」と推測することにしてもよいし、「通信品質が良好であるとは限らない」と推測することにしてもよい。

20

【0402】

以上、ステップS609における認証サーバ202の判断基準についていくつか例示したが、いずれの判断基準にしたがうにしろ、認証サーバ202は、送信元の車載装置100の位置から推測される通信品質が良好になるまで待機する。そして、通信品質が良好だという推測結果を認証サーバ202が得ると、処理はステップS610に移行する。

【0403】

そして、次のステップS610で認証サーバ202は、車両305の近傍の路側機201を、返信時の中継点として選択する。具体的には、認証サーバ202は、直近の位置通知を中継した路側機201を、返信時の中継点として選択する。

30

【0404】

続くステップS611では、認証サーバ202が、ネットワーク204とステップS610で選択した路側機201とを介して、最新送信版の鍵情報を送信元の車載装置100に返信する。そして、図12の処理は終了する。

【0405】

また、認証サーバ202は、位置通知を受信したとき、ステップS612において送信元の車載装置100の車載装置IDに対応づけて、受信した位置通知が示す位置情報を記憶する。上記のように、認証サーバ202が受信する位置通知は、実施形態に応じて、緯度と経度の組により車載装置100の位置を示す位置情報を含んでいることもある。あるいは、位置通知は、実施形態に応じて、当該位置通知を中継した路側機201のIDやIPアドレスなどにより近似的に車載装置100の位置を表していてもよい。

40

【0406】

よって、認証サーバ202は、ステップS612において、位置通知の形式に応じて、例えば、車載装置IDと緯度と経度を対応づけて記憶してもよい。あるいは、認証サーバ202は、車載装置IDと、位置通知を中継した路側機201のIPアドレスとを対応づけて記憶してもよい。また、認証サーバ202は、さらに、位置通知を受信した受信時刻を記憶してもよい。

【0407】

なお、緯度と経度の組により車載装置100の位置を示す位置情報を位置通知が含む場合、認証サーバ202は、マップマッチングを行うことで位置情報を補正し、補正した位

50

置情報を記憶してもよい。

【0408】

また、実施形態に応じて、認証サーバ202は各車載装置IDごとに最新の位置通知についてのみ記憶してもよいし、位置通知の履歴を取ってもよい。位置通知の履歴を取る場合、認証サーバ202は、必要に応じて古い履歴を削除する処理も行う。

【0409】

以上のようにして位置通知の受信を契機として認証サーバ202が車載装置100の位置を記憶すると、図12の処理も終了する。

なお、認証サーバ202が鍵情報受領通知を受信したときに行うステップS613の処理は、図5のステップS211の処理と同じなので、説明を省略する。

10

【0410】

ところで、上記のどの実施形態においても、車載装置100はコンピュータを使って実現することができる。また、認証サーバ202と交通管制サーバ203は、それぞれ、汎用的なコンピュータなどの適宜の情報処理装置により実現することができる。

【0411】

また、認証サーバ202と交通管制サーバ203が物理的には1台の同じコンピュータにより実現されていてもよい。あるいは逆に、複数のコンピュータにより認証サーバ202が実現されてもよいし、複数のコンピュータにより交通管制サーバ203が実現されてもよい。

【0412】

そこで、次に図13を参照してコンピュータの構成例について説明する。また、図1の車載装置100および図2の認証サーバ202と図13のコンピュータの各部との関係についても説明する。

20

【0413】

図13のコンピュータ600は、Central Processing Unit (CPU) 601、Read Only Memory (ROM) 602、RAM 603および通信インタフェース604を有する。また、コンピュータ600は、入力装置605、出力装置606、記憶装置607および可搬型記憶媒体610の駆動装置608を有する。そして、CPU 601、ROM 602、RAM 603、通信インタフェース604、入力装置605、出力装置606、記憶装置607および駆動装置608は、バス609により互いに接続されている。

30

【0414】

通信インタフェース604は、コンピュータ600がネットワーク204を介して他の装置と通信するためのインタフェースであり、有線通信インタフェース、無線通信インタフェース、またはその双方である。ネットワーク204には、プログラム提供者611である他のコンピュータがさらに接続されていてもよい。また、車載装置100に使われるコンピュータ600においては、通信インタフェース604は、ネットワーク204との間のインタフェースに加えて、路側機201との間の無線通信のためのインタフェースを含む。

【0415】

また、図13では入力装置605と出力装置606が別々に図示されているが、入力装置605と出力装置606は、タッチスクリーンとして統合されていてもよい。もちろん、コンピュータ600は、入力装置605としてさらに、キーボード、あるいはマウスなどのポインティングデバイスを有していてもよい。また、コンピュータ600は、出力装置606としてさらに、スピーカやプリンタを有していてもよいし、タッチスクリーンではないディスプレイ装置を出力装置606として有していてもよい。

40

【0416】

記憶装置607は、ハードディスク装置、フラッシュメモリなどの不揮発性の半導体メモリ装置、またはその組み合わせである。記憶装置607の少なくとも一部が耐タンパ性を有していてもよい。耐タンパ性の記憶装置607は、鍵情報の保持に好適である。

【0417】

50

また、可搬型記憶媒体 610 としては、Compact Disc (CD) や Digital Versatile Disk (DVD) などの光ディスク、光磁気ディスク、磁気ディスク、フラッシュメモリなどの不揮発性の半導体メモリカードなどが利用可能である。

【0418】

CPU 601 は、RAM 603 にプログラムをロードして RAM 603 をワークエリアとして用いながらプログラムを実行する。そして、CPU 601 が実行する上記プログラムは、予め ROM 602 または記憶装置 607 にインストールされていてもよいし、可搬型記憶媒体 610 に格納されて提供され、駆動装置 608 により読み取られて記憶装置 607 にコピーされてもよい。あるいは、上記プログラムは、プログラム提供者 611 からネットワーク 204 を介して記憶装置 607 にダウンロードされてもよい。

10

【0419】

そして、以上のようなコンピュータ 600 は、図 2 の認証サーバ 202 を実現することもできるし、交通管制サーバ 203 を実現することもできる。例えば、認証サーバ 202 がコンピュータ 600 により実現される場合、記憶装置 607 には、車載装置 ID と対応づけられた認証利用版と最新送信版の鍵情報や、路側機配置情報が記憶される。また、第 3 実施形態の場合はさらに、記憶装置 607 に、車載装置 ID と対応づけられた位置情報が記憶される。

【0420】

また、図 1 の車載装置 100 は、専用のハードウェアを使って実現することもできるが、少なくとも一部についてはプログラムを実行する汎用のコンピュータ 600 を用いて実現することができる。もちろん、車載装置 100 は、専用のハードウェアとコンピュータ 600 の両者によって実現されていてもよい。

20

【0421】

例えば、図 13 のコンピュータ 600 を用いて図 1 の車載装置 100 を次のように実現することが可能である。

画面インタフェース部 101 は、入力装置 605 と、出力装置 606 と、入力装置 605 と出力装置 606 を制御するプログラム（つまりデバイスドライバ）を実行する CPU 601 と、ワークエリアとしての RAM 603 によって実現することができる。また、上位機器インタフェース部 102 は、通信インタフェース 604 に対応する。

【0422】

そして、情報受信処理部 103 と、情報送信処理部 104 と、画面エリア判定部 106 と、画面乱数処理部 107 は、プログラムを実行する CPU 601 と、ワークエリアとしての RAM 603 により実現することができる。なお、RAM 603 は、ユーザからの入力から得られる第 1 の情報（具体的には例えば軌跡情報）を記憶する第 1 の記憶手段としても機能する。

30

【0423】

また、格納部 105 は、例えば鍵情報を格納する記憶装置 607 により実現されてもよい。あるいは、メモリカードなどの可搬型記憶媒体 610 に鍵情報が格納され、格納部 105 が可搬型記憶媒体 610 と駆動装置 608 により実現されてもよい。いずれにせよ、格納部 105 は、第 2 の情報（具体的には例えば鍵情報）を記憶する第 2 の記憶手段の一例である。

40

【0424】

なお、細分化エリア情報が固定されている場合、細分化エリア情報は、画面エリア判定部 106 を実現するためのプログラム内において各種定数として定義されていてもよい。その場合も、プログラムは ROM 602、記憶装置 607、または駆動装置 608 を介して参照される可搬型記憶媒体 610 に格納されているので、細分化エリア情報を格納する格納部 105 は、ROM 602、記憶装置 607、または可搬型記憶媒体 610 と駆動装置 608 により実現されていると言える。

【0425】

また、車両状態判定部 108 は、外部センサ 110 とコンピュータ 600 との間の不図

50

示のインタフェースと、当該インタフェースを介して受け取ったデータを使ってプログラムを実行するCPU601と、RAM603により実現することができる。外部センサ110とコンピュータ600との間のインタフェースは、専用のインタフェースカードなどを含んでもよいし、Universal Serial Bus (USB) などの汎用的なインタフェースでもよい。

【0426】

なお、上記実施形態は様々に変形可能である。以下に、上記実施形態を変形するいくつかの観点为例示する。例えば、上記実施形態は、下記(f1)～(f15)の観点から様々に変形することができ、上記実施形態および下記の変形は、相互に矛盾しない限り、任意に組み合わせることが可能である。

10

【0427】

(f1) 鍵情報の更新の契機に関する変形

上記第1～3実施形態では、鍵情報の更新は、車載装置100からの鍵情報更新要求（あるいは鍵情報更新要求の役割を兼ねている認証要求兼更新要求）の送信を契機として行われる。しかし、実施形態によっては、車載装置100から鍵情報の更新を要求することなく、認証サーバ202が鍵情報の更新のタイミングを制御してもよい。また、上記第1～3実施形態では、鍵情報の更新は、認証に成功したときにのみ行われるが、鍵情報の更新は、認証の成否とは独立していてもよい。

【0428】

例えば、第1実施形態は、次のように変形されてもよい。すなわち、車載装置100は、図4のステップS105において、検出されたトリガの種類が認証通知の受信であると判断した場合、図4の処理を終えてもよい。そして、車載装置100は、図4の処理とは独立して、認証サーバ202からの鍵情報更新通知の受信の有無を監視し、鍵情報更新通知を受信したら図4のステップS110とS111の処理を行ってもよい。

20

【0429】

また、この場合、認証サーバ202は、車載装置100の位置を考慮に入れずに鍵情報更新通知を送信してもよいし、車載装置100の位置を考慮に入れて鍵情報更新通知を送信してもよい。

【0430】

例えば、認証サーバ202は、車載装置100の位置を考慮に入れずに、システム200内のすべての路側機201に対して定期的に車載装置100に対する鍵情報更新通知を送信してもよい。すると、車載装置100は、もしいずれかの路側機201からたまたま鍵情報更新通知を受信することができれば、受信を契機として、図4のステップS110とS111のように鍵情報の更新と鍵情報受領通知の送信を行う。この場合、認証サーバ202は車載装置100の位置を考慮する必要がないので、車載装置100からの位置通知も不要である。

30

【0431】

あるいは、車載装置100が位置通知を送信し、認証サーバ202は鍵情報更新通知の送信のタイミングの制御および中継点となる路側機201の選択を位置通知に基づいて行い、鍵情報更新通知を送信してもよい。つまり、認証サーバ202は、図12のステップS608～S611の処理を、鍵情報更新要求の受信を契機として行うのではなく、例えば定期的なスケジュールにしたがって行ってもよい。

40

【0432】

なお、ステップS608～S611の処理を行う契機が何であれ、通信インタフェース604とCPU601とRAM603は、協働して、車載装置100から車両305の位置を示す位置情報を受信する受信手段として機能する。また、ステップS609において、CPU601とRAM603は、複数の送信機（すなわち複数の路側機201）にそれぞれ対応する複数の範囲のいずれかに車両305の位置が含まれるか否かを位置情報に基づいて判断する判断手段として機能する。そして、ステップS610とS611では、通信インタフェース604とCPU601とRAM603は、協働して、車両305の位置

50

を含むと判断された範囲に対応する送信機に対して鍵情報を送信する送信手段として機能する。なおここで、「車両 305 の位置を含むと判断された範囲に対応する送信機」とは、換言すれば、通信範囲内に車載装置 100 があると判断され、中継点として選択された路側機 201 のことである。

【0433】

(f2) 鍵情報の更新タイミングに関する変形

実施形態によっては、車載装置 100 に電源が入れられてから電源が切断されるまでの間に、1 回だけ認証が行われるかもしれないし、複数回の認証が行われるかもしれない。

【0434】

例えば、交通管制サーバ 203 が異なる種類の複数のサービスを提供し、複数のサービスの認証をいずれも認証サーバ 202 が担う場合、認証サーバ 202 はサービスごとに認証を行ってもよい。そして、車載装置 100 に電源が入れられてから電源が切断されるまでの間に、車両 305 が複数のサービスを受けることもありうる。また、例えば駐車場の料金支払いのようにユーザへの課金をともなうサービスの場合は、課金のたびに認証が行われてもよい。

【0435】

このように、車載装置 100 に電源が入れられてから電源が切断されるまでの間に複数回の認証が行われる場合、ユーザからの入力や車載装置 100 への電源投入直後の最初の 1 回だけに限ることがユーザビリティの観点から好ましい。しかし、鍵情報の更新は、認証が済むたびに行われることが望ましい。そのために、画面乱数処理部 107 は、画面エリア判定部 106 から出力された判定結果を、車載装置 100 の電源が切断されるまでの間、RAM 603 に保持し続けてもよい。

【0436】

また、複数回の認証のために、上記実施形態は次のように変形されてもよい。例えば、車載装置 100 は、図 4 のステップ S101 と S102 の処理を行った後、ステップ S103 ～ S111 の処理を認証のたびに繰り返してもよい。あるいは、車載装置 100 は、図 9 のステップ S301 と S302 の処理を行った後、ステップ S303 ～ S308 の処理を認証のたびに繰り返してもよい。また、車載装置 100 は、図 11 のステップ S501 と S502 の処理を行った後、ステップ S503 ～ S510 の処理を認証のたびに繰り返してもよい。

【0437】

ただし、車載装置 100 が拒否通知を受信した場合は、ステップ S101、S301、または S501 での入力が不正だったと認証サーバ 202 により判断されたということである。よって、拒否通知を受信した場合、たとえ車載装置 100 がステップ S103 ～ S111、S303 ～ S308、または S503 ～ S510 の処理を繰り返したとしても、認証は再度失敗することが明らかである。したがって、車載装置 100 は、拒否通知を受信した場合は上記の繰り返しを行うことなく、処理を終えてよい。

【0438】

また、上記 (f1) でも述べたが、鍵情報の更新のタイミングは、認証の成否とは独立していてもよい。あるいは、1 回認証が成功した後で、車載装置 100 の電源がオンになっている間は、車載装置 100 は鍵情報の更新を繰り返し行ってもよい。

【0439】

例えば、車載装置 100 は、図 4 のステップ S101 ～ S105 の処理を行った後、認証が成功したか否かによらず、ステップ S106 ～ S111 の処理を繰り返してもよい。ステップ S106 ～ S111 の処理の繰り返しは、所定の間隔で行われてもよいし、ステップ S111 の処理の直後にステップ S106 の処理が行われてもよい。

【0440】

同様に、車載装置 100 は、図 11 のステップ S501 ～ S505 の処理を行った後、認証が成功したか否かによらず、ステップ S506 ～ S510 の処理を繰り返してもよい。ステップ S506 ～ S510 の処理の繰り返しは、所定の間隔で行われてもよいし、ス

テップ S 5 1 0 の処理の直後にステップ S 5 0 6 の処理が行われてもよい。

【0 4 4 1】

あるいは、車載装置 1 0 0 は、認証が成功した場合に、図 4 のステップ S 1 1 1 または図 9 のステップ S 3 0 8 の送信を行った後に、ステップ S 1 0 6 ~ S 1 1 1 の処理を繰り返してもよい。ステップ S 1 0 6 ~ S 1 1 1 の処理の繰り返しは、所定の間隔で行われてもよいし、ステップ S 1 1 1 の処理の直後にステップ S 1 0 6 の処理が行われてもよい。

【0 4 4 2】

例えば上記のように鍵情報を繰り返し更新することにより、ある認証から次の認証までの時間が比較的長い場合にも、できるだけ新しい鍵情報が次の認証用情報の生成において使われることになる。このように、古い情報の使用をできるだけ避けることで、古い情報が盗まれることによるセキュリティ低下のリスクを減らすことができる。

【0 4 4 3】

このように、上記実施形態は様々に変形することができるが、図 4 のステップ S 1 0 6 と S 1 0 7 は、いずれの変形例においても、車両 3 0 5 の状態に基づいたタイミングで無線通信により更新要求を送信するステップに相当する。より詳しくは、ステップ S 1 0 6 が、車両 3 0 5 が信号機から所定の範囲内で停止していると見なせる停止状態のときに更新要求を送信するよう、タイミングを決定する決定ステップに相当する。

【0 4 4 4】

同様に、図 9 のステップ S 3 0 3 と S 3 0 4 も、いずれの変形例においても、車両 3 0 5 の状態に基づいたタイミングで無線通信により更新要求（具体的には認証要求兼更新要求）を送信するステップに相当する。より詳しくは、ステップ S 3 0 3 がステップ S 1 0 6 と同様に上記決定ステップに相当する。

また、ステップ S 1 0 8 と S 3 0 5 は、いずれも、更新要求に応じて無線通信により送信される新たな鍵情報を受信する受信ステップを含む。

【0 4 4 5】

（f 3）更新対象の鍵情報に関する変形

鍵情報のうち、細分化エリア情報と乱数情報の双方が更新対象でもよいし、細分化エリア情報のみが更新対象でもよいし、乱数情報のみが更新対象でもよい。図 7 から明らかなように、細分化エリア情報のみが更新されるだけでも、細分化エリア情報の更新に応じて異なる認証用情報 α が生成されることになる。また、式（1）と（3）から明らかなように、乱数情報のみが更新されるだけでも、画面乱数処理部 1 0 7 が例えば関数 f_A または f_C を用いて認証用情報 α を生成する場合には、乱数情報の更新に応じて異なる認証用情報 α が生成されることになる。

【0 4 4 6】

（f 4）認証サーバ 2 0 2 による中継点の路側機 2 0 1 の選択に関する変形

認証サーバ 2 0 2 は、車載装置 1 0 0 への通信の中継点となる路側機 2 0 1 を選択する際に、路側機は位置情報と車載装置 1 0 0 の位置の双方を考慮に入れてもよい。

【0 4 4 7】

例えば、車載装置 1 0 0 からの位置通知を何回か認証サーバ 2 0 2 が受信している場合、認証サーバ 2 0 2 は、車載装置 1 0 0 を搭載した車両 3 0 5 がどの道路をどの方向に走行中かを認識することができる。つまり、認証サーバ 2 0 2 は、位置通知により通知された車載装置 1 0 0 の位置を必要に応じてマップマッチングなどの処理により補正し、複数の位置通知でそれぞれ通知された位置の変化から、車両 3 0 5 が走行中の道路と走行方向を認識することができる。そこで、認証サーバ 2 0 2 は、複数の送信元近傍路側機のうち、送信元路側機から見て車両 3 0 5 の走行方向と逆側にあるものは、IP パケットの送信先から除外してもよい。

【0 4 4 8】

（f 5）認証要求の送信タイミングに関する変形

第 1 実施形態において車載装置 1 0 0 は、図 4 に示すように、認証要求 5 0 1 に関しては通信品質の良さの推測を行わずに単に送信を行い、鍵情報更新要求 5 0 4 に関しては通

10

20

30

40

50

信品質の良さの推測を行って送信タイミングを調整する。しかし、実施形態によっては、車載装置 100 は、認証要求 501 に関しても図 4 のステップ S106 と同様に通信品質の良さの推測を行って送信タイミングを調整してもよい。それにより、結果的に失敗に終わる無駄な送信を減らすことができる。

【0449】

(f6) 入力支援に関する変形

画面インタフェース部 101 がユーザからの入力を受け付けるにあたり、情報送信処理部 104 は、入力支援のための情報を画面に表示するよう、画面インタフェース部 101 を制御してもよい。入力支援により、ユーザビリティが向上する。

【0450】

例えば、情報送信処理部 104 は、図形の入力を開始する位置を、矢印や丸などによりハイライト表示するよう、画面インタフェース部 101 を制御してもよい。すると、「入力位置のずれが原因で、正しい入力が不正な入力と判断される」といった事態が避けやすくなる。

【0451】

なお、ハイライト表示する対象となる入力開始位置が、ユーザが図形を認証サーバ 202 に登録したときの入力開始位置に固定される場合は、格納部 105 には予め、固定される当該入力開始位置を示す情報が登録されるものとする。そして、情報送信処理部 104 は、格納部 105 に登録された情報を読み出して、上記のように画面インタフェース部 101 にハイライト表示の指示を与える。

【0452】

逆に、情報送信処理部 104 は、ユーザからの入力の受け付けのたびにランダムな位置を選び、選んだ位置をハイライト表示するよう、画面インタフェース部 101 を制御してもよい。このようにハイライト表示する対象となる入力開始位置が可変の場合は、情報受信処理部 103 は、入力開始位置として選んだ位置の座標を、認証用情報とあわせて認証要求のフレームに含め、認証サーバ 202 に通知する。

【0453】

また、「入力位置のずれが原因で、正しい入力が不正な入力と判断される」といった事態を避けるためには、情報受信処理部 103 は、ガイド表示として画面上に例えば格子を表示するよう、画面インタフェース部 101 を制御してもよい。すると、ユーザは、格子を頼りに、ユーザが図形を認証サーバ 202 に登録したときの入力開始位置に近い位置から入力を開始することができるようになるので、ユーザビリティが向上する。

【0454】

(f7) ユーザからの入力の内容に関する変形

上記実施形態においては、ユーザから入力される図形的な情報として、手書きの署名、図 6 の軌跡 403、図 7 の軌跡 405、および軌跡 407 を例示した。しかし、実施形態によっては、ユーザから入力される図形的な情報は、上記の例が示すような連続的な軌跡を描くものでなくてもよい。

【0455】

例えば、画面インタフェース部 101 はソフトウェアキーボード機能を有していてもよい。なお、画面インタフェース部 101 は、キーの位置を固定して画面に表示してもよいし、表示のたびにキーの位置をランダムに入れ換えて画面上にキーボードあるいはテンキーなどを表示してもよい。

【0456】

具体的には、画面インタフェース部 101 は、画面上にキーボードあるいはテンキーなどを表示し、画面上に表示されたどのキーをユーザが指定したか、そして、キーが指定された順序と間隔はどうだったかを検出してもよい。つまり、画面インタフェース部 101 は、空間内の複数の位置がユーザからの入力により指定される順序、間隔、またはその組み合わせを情報受信処理部 103 に出力してもよい。

【0457】

この場合、細分化エリア情報は各キーが表示されるエリアを規定する情報であり、乱数情報は、各キーが表示されるエリアにそれぞれランダムな値を対応づける情報である。また、画面乱数処理部107は、認証用情報αの生成にあたり、エリアの通過にかかった時間の代わりに、キーが指定される間隔またはキーに接触されていた時間を使うことができる。

【0458】

例えば、ソフトウェアキーボード機能により画面上に表示される“X”と“Y”と“Z”という3つのキーがこの順で指定され、“X”と“Y”の指定の間隔は1.0秒、“Y”と“Z”の指定の間隔は0.7秒であったとする。また、“X”と“Y”と“Z”という3つのキーが表示されるエリアにそれぞれ対応する乱数が、1935と4018と6253であるとする。

10

【0459】

すると、画面乱数処理部107は、実施形態に応じて、1935と4018と6253という3つの乱数を引数とする関数により認証用情報αを生成してもよいし、1.0と0.7という2つの時間を引数とする関数により認証用情報αを生成してもよい。あるいは、画面乱数処理部107は、1935と1.0と4018と0.7と6253という計5つの値を引数とする関数により認証用情報αを生成してもよい。

【0460】

また、画面乱数処理部107は、認証用情報αの生成において、キーが指定される間隔の代わりに、またはキーが指定される間隔とともに、キーが表示されるエリア内での画面への接触が持続していた時間を用いてもよい。

20

【0461】

そして、上記のソフトウェアキーボードに関する変形例と同様に、画面インタフェース部101がハードウェアキーボードを介してユーザから文字による入力を受け付ける変形例も可能である。この場合、鍵情報は細分化エリア情報を含まなくてよい。そして、乱数情報は、各キーにそれぞれランダムな値を対応づける情報である。また、画面乱数処理部107は、認証用情報αの生成にあたり、エリアの通過にかかった時間の代わりに、キーの押されていた時間、キーが押される間隔、またはその組み合わせを使うことができる。

【0462】

(f8) 鍵情報に関する変形

30

例えば、認証サーバ202は、あるとき、画面を8行・5列に40分割する図6の鍵情報401を車載装置100に通知してもよい。そして、車載装置100の画面エリア判定部106は、いくつかのエリアを併合することで、鍵情報401が規定する細分化よりも粗く画面を細分化するパターンを作成し、作成したパターンにおいて定義したエリアに基づいて、上記(a1)と(a2)の判定を行ってもよい。

【0463】

例えば、画面エリア判定部106は、1～4行目を併合し、5～8行目を併合することで、画面を2行・5列に10分割するパターンを作成してもよい。すると、図6の軌跡403は、併合後の1行目の1列目のエリア、併合後の1行目の2列目のエリア、併合後の1行目の1列目のエリア、という延べ3つのエリアを通ると判定される。

40

【0464】

そして、軌跡403が併合後の1行目の1列目のエリアを最初に通過するときの通過時間は、式(12)～(14)によれば1.3(=0.3+0.4+0.6)秒である。また、併合後の1行目の2列目のエリアの通過時間は、式(15)と(16)によれば1.4(=1.0+0.4)秒である。そして、軌跡403が併合後の1行目の1列目のエリアを最後に通過するときの通過時間は、式(17)と(18)によれば0.3(=0.2+0.1)秒である。

【0465】

また、画面エリア判定部106は、併合後の各エリアに対応する乱数を、併合前のエリアの乱数を連結することで求めることができる。例えば、元の鍵情報401における1列

50

目において1～4行目の4つのエリアを併合したエリアに対応する乱数は、元の4つのエリアに対応する4つの乱数を文字列として連結した2615367357320044である。同様に、併合後の1行目の2列目のエリアに対応する乱数は、5499943318825812である。

【0466】

したがって、この場合、画面乱数処理部107は下記の式(22)～(28)を用いて認証用情報 α を求める。

$$\begin{aligned} m &= 3 & (22) \\ \text{rand}_{t(1)} &= 2615367357320044 & (23) \\ \text{rand}_{t(2)} &= 5499943318825812 & (24) \\ \text{rand}_{t(3)} &= 2615367357320044 & (25) \\ \text{pass}_{t(1)} &= 1.3 & (26) \\ \text{pass}_{t(2)} &= 1.4 & (27) \\ \text{pass}_{t(3)} &= 0.3 & (28) \end{aligned}$$

【0467】

また、画面乱数処理部107は、「1～4行目を併合し、5～8行目を併合することで、画面を2行・5列に10分割するパターンを用いた」ということを示す情報（以下「細分化変更情報」という）を、認証用情報 α とあわせて、情報送信処理部104に出力する。すると、情報送信処理部104は、認証用情報 α だけでなく細分化変更情報も認証要求501の秘密UL情報のフィールドに設定する。

【0468】

その結果、認証サーバ202も細分化変更情報を認識することができ、細分化変更情報を考慮に入れて、パスワードを抽出することができる。なお、以上のように、認証サーバ202から通知された細分化エリア情報に対して、車載装置100が粗い分割の仕方を定めることには、次のような効果がある。すなわち、「細分化エリア情報によって定義されているエリアが小さいために、ユーザの入力の微妙なずれが原因で、認証に失敗してしまう」といった事態が防ぎやすくなる。

【0469】

また、この場合、認証のたびに鍵情報の更新を行うのではなく、鍵情報の更新は何回かの認証ごとに1度でもよい。その代わりに、エリアの併合の仕方（換言すれば細分化変更情報の内容）を認証のたびに適宜変えれば、認証のたびに異なる認証用情報 α が生成される。

【0470】

あるいは、実施形態によっては、上記とは逆に、認証サーバ202が細分化変更情報を指定してもよい。

例えば、認証サーバ202は、ある鍵情報更新要求の受信を契機に、鍵情報401のような40分割の鍵情報401とともに細分化変更情報も含む鍵情報更新通知を車載装置100に返信してもよい。そして、認証サーバ202は、次の鍵情報更新要求の受信したときは、エリアの併合の仕方を変えた細分化変更情報のみを車載装置100に返信してもよい。さらに次の鍵情報更新要求を受信したときも、認証サーバ202は同様にエリアの併合の仕方を変えた細分化変更情報のみを車載装置100に返信してもよい。そして、さらに次の鍵情報更新要求を受信したとき、認証サーバ202は新たな鍵情報を生成し、新たな細分化変更情報とともに車載装置100に通知してもよい。

【0471】

以上の例は、「鍵情報自体の更新が3回の認証ごとに1回だけ行われ、残りの2回は細分化変更情報の更新のみが行われる」という例である。もちろん、この「3回」という数値は単なる例示であり、実施形態に応じて適宜変更されてよい。

【0472】

(f9) 画面インタフェース部101に関する変形

第1～3実施形態の画面インタフェース部101はタッチスクリーンを用いて実現され

る。しかし、実施形態によっては、タッチスクリーン以外の、空間的情報の入力用の他のユーザインタフェース装置により、画面インタフェース部101が実現されてもよい。

【0473】

例えば、画面インタフェース部101が、ペンタブレットやマウスなどのポインティングデバイスと、ディスプレイとを含んでもよい。そして、画面インタフェース部101は、ディスプレイ上にカーソルを表示し、ポインティングデバイスからの入力に応じてカーソルを移動させてもよい。そして、画面インタフェース部101は、ポインティングデバイスを介して指定される画面上の位置を表す2次元座標を、情報受信処理部103に出力してもよい。

【0474】

また、ポインティングデバイスとしては、データグローブなどの3次元の空間的情報の入力用の装置が使われてもよい。その場合は、画面インタフェース部101が情報受信処理部103に出力する情報は3次元座標を含み、細分化エリア情報は3次元空間を複数のエリアに細分化する仕方を表し、各エリアは2次元ではなく3次元のエリアである。

【0475】

(f10) フレーム500に関する変形

図8Aと8Bに示した各種フレームの形式と、“123456789”や“00”などの値は、例示に過ぎない。各種情報は、実施形態に応じたその他の任意の形式の無線通信フレームとして送受信されてもよい。また、図8Aと8Bに例示した2ビットの認証フラグは、データマップ情報によりフレーム500の種別が一意に特定可能な場合は省略されてもよい。

【0476】

また、第3実施形態に関連して、位置通知のフレームは位置通知511の形式に限らず、位置通知のフレームに位置情報が明示的に含まれていなくてもよいと説明したが、逆に、位置通知のフレームは、車両305の速度を示す速度情報をさらに含んでもよい。この場合、路側機201を介して認証サーバ202に速度情報も通知されるので、認証サーバ202は図12のステップS612で速度情報も記憶することができる。

【0477】

すると、認証サーバ202はステップS609において、直近に受信した位置通知に含まれていた速度情報に基づいて、車両305が停止しているか否かを判断することができる。そこで、認証サーバ202は、車両305の位置（あるいは位置の履歴）だけからステップS609の判断を行う代わりに、車両305が停止しているか否かに鍵情報を送信するよう、送信タイミングを制御してもよい。

【0478】

(f11) 路側機201の配置と車両状態判定部108に関する変形

例えば、高速道路など、信号機が存在しない区間が長い道路においては、路側機201は信号機とは無関係に適宜の間隔で道路沿いに設置されてもよい。その場合も、車両状態判定部108は、路側機201が設置された位置に関する情報を含む地図情報を参照することにより、車載装置100が搭載されている車両305が路側機201の近傍に位置しているか否かを判断することができる。

【0479】

また、車両状態判定部108は車両305の状態を判定するのに車速を用いなくてもよい。つまり、実施形態によっては、車両状態判定部108は、路側機201の近傍に車両305が位置しているか否かだけを判定してもよい。

【0480】

あるいは、外部センサ110が電波受信状態を感知することができる場合、車両状態判定部108は、位置と車速から無線通信路の通信品質を推測する代わりに、電波受信状態から直接的に通信品質を判定してもよい。例えば、外部センサ110が、スペクトラムアナライザを含んでいたり、路側機201との間の通信に使われる特定の周波数の電波の受信強度を感知するセンサを含んでいたりする場合、外部センサ110は電波受信状態を感

10

20

30

40

50

知することができる。

【0481】

(f12) 鍵情報受領通知と鍵情報の版管理に関する変形

まれに、「路側機201から送信される鍵情報更新通知のフレームが車載装置100に受信されるにもかかわらず、車載装置100から送信される鍵情報受領通知のフレームを路側機201が受信することができない」という場合が起こりうる。

【0482】

そこで、認証サーバ202は、図5のステップS204または図12のステップS604において認証利用版の鍵情報を使って認証に失敗した場合は、最新送信版の鍵情報を使って認証を再度試してもよい。そして、最新送信版の鍵情報を使った認証に成功すれば、認証サーバ202は「パスワードは正しい」と判断してもよい。

10

【0483】

なお、車載装置100と認証サーバ202との間での鍵情報の同期を確実にするために、例えば、認証サーバ202は、最新送信版の鍵情報を使った認証に成功した場合は、図5のステップS211や図12のステップS613と同様の処理を行ってもよい。あるいは、認証サーバ202は、鍵情報更新通知または認証通知兼更新通知の送信後、一定時間が経過しても鍵情報受領通知を受信することができなければ、最新送信版の鍵情報を再度車載装置100に送信してもよい。

【0484】

(f13) 認証処理において用いられる情報に関する変形

20

図8Aと8Bに例示した各種フレームのヘッダには、車載装置IDが指定されている。しかし、実施形態に応じて、車載装置IDの代わりに、あるいは車載装置IDとともに、ユーザID、車両ID、またはその双方がフレームに含まれていてもよい。

【0485】

ユーザと車載装置100と車両305は、実施形態によって1対1対1に対応することもあるし、n対1対1など、それ以外の対応関係の場合もある。ユーザと車載装置100と車両305の対応関係に応じて、適宜のIDが認証対象のアカウントの識別のために利用可能である。

【0486】

つまり、画面インタフェース部101は、必要に応じて、ユーザからユーザIDの入力をさらに受け付けてもよい。また、格納部105は、必要に応じて、車載装置100が搭載される車両305に予め割り当てられている車両IDを格納していてもよい。

30

【0487】

(f14) 装置の種類に関する変形

車載装置100は、例えばカーナビゲーション装置を兼ねていてもよい。その場合、格納部105が格納する地図情報は、カーナビゲーション装置で使われる既存の地図情報であってよい。また、図1では車載装置100の外部に外部センサ110があるが、もちろん、実施形態によっては、車載装置100が外部センサ110を含んでいてもよい。

【0488】

また、上記の各種実施形態に関して、車載装置100における鍵情報の更新について詳細に説明したが、車載装置100以外の装置に上記の各種実施形態を適用することもできる。例えば、認証をとまなう何らかのサービスを受けようとする携帯端末装置は、上記の実施形態における車載装置100と同様にして、認証の前に予め新たな鍵情報を取得することで認証にかかる時間を短縮することができる。なお、その場合、携帯端末装置は、鍵情報更新要求または認証要求兼更新要求を送信するタイミングを決めるのに、地図情報と移動速度から通信品質を推測する代わりに、受信電波強度から直接的に通信品質を判断すればよい。

40

【0489】

また、他の装置と有線接続される有線端末装置に対しても、上記の各種実施形態を適用することができる。その場合も、認証時に認証サーバとの間で2往復の通信が生じるので

50

はなく 1 往復の通信で済む分だけ、時間短縮の効果が得られる。

【0490】

(f15) 認証の結果通知を契機とする車載装置 100 の動作に関する変形

認証通知、拒否通知、または認証通知兼更新通知を受信したとき、車載装置 100 は、さらに、何らかの処理を行ってもよい。例えば、サービスを受けるためのクライアントが、認証の成否を外部から受け取る仕様になっている場合、情報受信処理部 103 は、認証通知、拒否通知、または認証通知兼更新通知の受信を契機として、認証の成否をクライアントに通知してもよい。あるいは、情報受信処理部 103 は、認証通知または認証通知兼更新通知の受信を契機として、サービスを受けるためのクライアントを起動してもよい。

【0491】

以上、(f1)～(f15)の観点から様々な変形を例示したが、いずれにしろ、車載装置 100 がユーザからの入力を受け付けた段階では既に、まだ認証用情報の生成に用いていない新たな鍵情報が格納部 105 に格納されている。よって、車載装置 100 は、ユーザからの入力を受け付けてから改めて鍵情報の更新を行う必要なしに、すぐさま認証用情報を生成することができる。なお、例えば車載装置 100 の製造時に製造工場において格納部 105 に初回用の鍵情報を格納することで、ユーザが車載装置 100 の購入後に初めて認証を行う場合にも、「未使用の鍵情報が格納部 105 に格納されている」という条件を成立させることができる。

【0492】

したがって、上記の各種の実施形態によれば、ユーザからの入力の受け付けから認証の完了までの時間が短くて済む。このように短時間で認証が終了すると、車両 305 あるいはそこに搭載されている機器は、車両 305 のエンジン始動からできるだけすぐに交通管制サーバ 203 からのサービスの提供が受けられるようになる。そのため、エンジン始動からサービス開始までの時間が短いほど好ましい ITS システムにとって、上記の各種の実施形態による鍵情報の更新と認証は有益である。

【0493】

また、上記の各種の実施形態によれば認証のたびに異なる鍵情報が使われ、認証サーバ 202 に送られる認証用情報も認証のたびに異なる。認証用情報が認証のたびに異なることは、無線通信を介した認証を行う車載装置 100 にとって、セキュリティ強度の向上のために有益である。

【0494】

最後に、上記の種々の実施形態に関して、さらに下記の付記を開示する。

(付記 1)

コンピュータに、

ユーザからの入力から得られる第 1 の情報を記憶する第 1 の記憶ステップと、

前記第 1 の情報と、予め記憶装置に記憶されている第 2 の情報とを用いて、認証用の第 3 の情報を生成する第 1 の生成ステップと、

無線通信により前記第 3 の情報を送信する第 1 の送信ステップと、

前記第 2 の情報の更新を要求する更新要求を生成する第 2 の生成ステップと、

前記コンピュータを搭載した車両の状態に基づいたタイミングで前記無線通信により前記更新要求を送信する第 2 の送信ステップと、

前記更新要求に応じて前記無線通信により送信される新たな第 2 の情報を受信する受信ステップと、

受信した前記新たな第 2 の情報を前記記憶装置に記憶する第 2 の記憶ステップと、
を実行させるプログラム。

(付記 2)

前記第 2 の送信ステップは、

前記車両が信号機から所定の範囲内で停止していると見なせる停止状態のときに前記更新要求を送信するよう、前記タイミングを決定する決定ステップを含む

ことを特徴とする付記 1 に記載のプログラム。

10

20

30

40

50

(付記 3)

前記第 1 の情報は、

前記ユーザからの入力が描く軌跡の形状、

時間の経過にともなう前記軌跡の変化、または

空間内の複数の位置が前記ユーザからの入力により指定される順序、間隔、もしくは前記順序と前記間隔の組み合わせ

を示し、

前記第 2 の情報は、

前記ユーザからの入力になされる入力領域を第 1 の個数の分割領域に分割する第 1 のパターンに対応する前記第 1 の個数のランダムな値、

前記入力領域を第 2 の個数の分割領域に分割する第 2 のパターン、または

前記入力領域を第 3 の個数の分割領域に分割する第 3 のパターンと前記第 3 のパターンに対応する前記第 3 の個数のランダムな値との組み合わせ

を示す

ことを特徴とする付記 1 または 2 に記載のプログラム。

(付記 4)

前記第 2 の送信ステップが前記第 1 の送信ステップを兼ねており、前記第 3 の情報が前記更新要求とともに送信される

ことを特徴とする付記 1 から 3 のいずれか 1 項に記載のプログラム。

(付記 5)

車載装置であって、

ユーザからの入力から得られる第 1 の情報を記憶する第 1 の記憶手段と、

第 2 の情報を記憶する第 2 の記憶手段と、

前記第 1 の情報と前記第 2 の情報を用いて、認証用の第 3 の情報を生成する第 1 の生成手段と、

第 2 の情報の更新を要求する更新要求を生成する第 2 の生成手段と、

無線通信により前記第 3 の情報を送信し、前記車載装置を搭載した車両の状態に基づいたタイミングで前記無線通信により前記更新要求を送信する送信手段と、

前記更新要求に応じて前記無線通信により送信される新たな第 2 の情報を受信する受信手段とを備え、

前記受信手段が受信した前記新たな第 2 の情報を前記第 2 の記憶手段に記憶する

ことを特徴とする車載装置。

(付記 6)

コンピュータに、

車両に搭載された車載装置から前記車両の位置を示す位置情報を受信する第 1 の受信ステップと、

複数の送信機にそれぞれ対応する複数の範囲のいずれかに前記車両の前記位置が含まれるか否かを、前記位置情報に基づいて判断する第 1 の判断ステップと、

前記車両の前記位置が前記複数の範囲のいずれかに含まれると判断した場合に、前記複数の送信機のうち、前記車両の前記位置を含むと判断された当該範囲に対応する送信機を送信先として選択し、前記送信先の前記送信機に対して、前記車載装置が認証用情報を生成するのに用いる情報である鍵情報を送信する送信ステップと、

を実行させるプログラム。

(付記 7)

前記車両の速度を示す速度を前記車載装置から受信する第 2 の受信ステップと、

前記速度情報に基づいて、前記車両が停止しているか否かを判断する第 2 の判断ステップ

をさらに前記コンピュータに実行させ、

前記車両が停止しているか判断された場合に、前記送信ステップにおいて前記送信先への前記鍵情報の送信を前記コンピュータに行わせる

ことを特徴とする付記 6 に記載のプログラム。

(付記 8)

前記鍵情報は、

前記車載装置が前記認証用情報を生成するのに前記鍵情報とともに利用する空間的情報が入力される入力領域を第 1 の個数の分割領域に分割する第 1 のパターンに対応する前記第 1 の個数のランダムな値、

前記入力領域を第 2 の個数の分割領域に分割する第 2 のパターン、または

前記入力領域を第 3 の個数の分割領域に分割する第 3 のパターンと前記第 3 のパターンに対応する前記第 3 の個数のランダムな値との組み合わせ

を示す

10

ことを特徴とする付記 6 または 7 に記載のプログラム。

(付記 9)

車両に搭載された車載装置から前記車両の位置を示す位置情報を受信する受信手段と、

複数の送信機にそれぞれ対応する複数の範囲のいずれかに前記車両の前記位置が含まれるか否かを、前記位置情報に基づいて判断する判断手段と、

前記車両の前記位置が前記複数の範囲のいずれかに含まれると前記判断手段が判断した場合に、前記複数の送信機のうち前記車両の前記位置を含むと判断された当該範囲に対応する送信機に対して、前記車載装置が認証用情報を生成するのに用いる情報である鍵情報を送信する送信手段と、

を備えることを特徴とする情報処理装置。

20

【符号の説明】

【0495】

100 車載装置

101 画面インタフェース部

102 上位機器インタフェース部

103 情報受信処理部

104 情報送信処理部

105 格納部

106 画面エリア判定部

107 画面乱数処理部

108 車両状態判定部

110 外部センサ

200 システム

201 a ~ 201 k 路側機

202 認証サーバ

203 交通管制サーバ

204 ネットワーク

301 a ~ 301 g 道路

302 a ~ 302 f 交差点

303 a ~ 303 k 信号機

304 駐車場

305 車両

401 鍵情報

402、404、406 画面と鍵情報の対応づけ

403、405、407 軌跡

500 フレーム

501 認証要求

502 認証通知

503 拒否通知

504 鍵情報更新要求

30

40

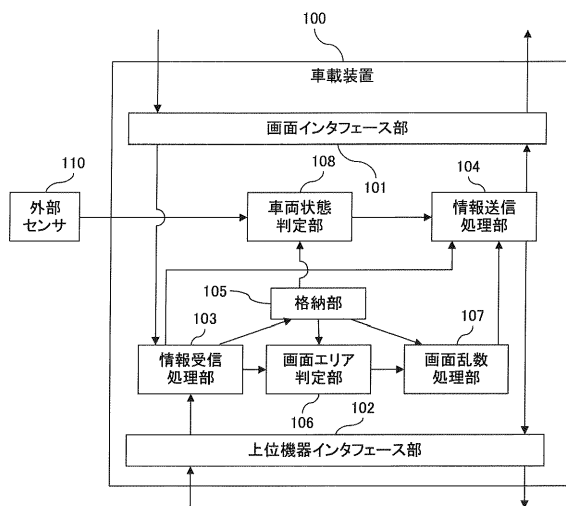
50

- 505 鍵情報更新通知
- 506 鍵情報受領通知
- 507、508 サービス中通信
- 509 認証要求兼更新要求
- 510 認証通知兼更新通知
- 511 位置通知
- 600 コンピュータ
- 601 CPU
- 602 ROM
- 603 RAM
- 604 通信インタフェース
- 605 入力装置
- 606 出力装置
- 607 記憶装置
- 608 駆動装置
- 609 バス
- 610 可搬型記憶媒体
- 611 プログラム提供者

10

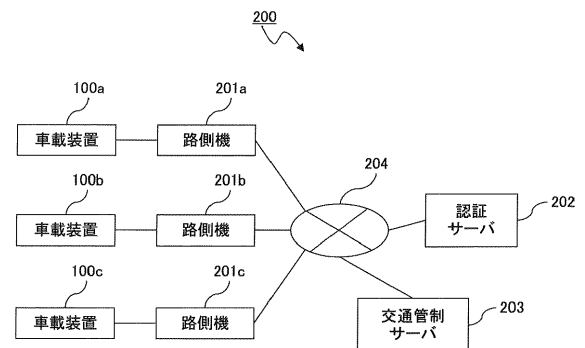
【図 1】

車載装置の構成図

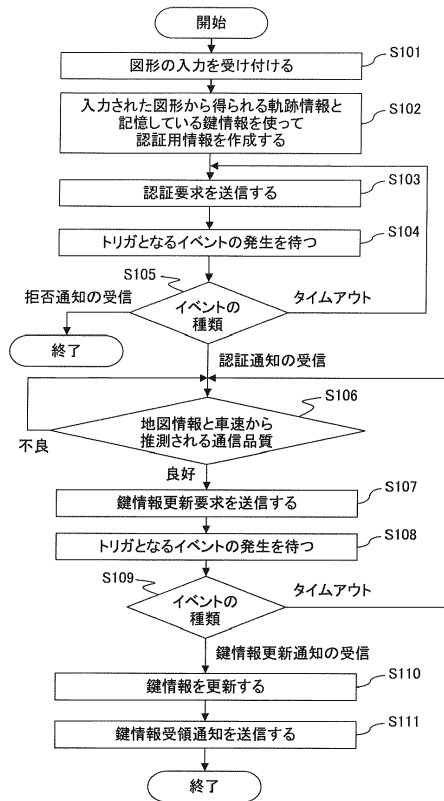


【図 2】

システム構成図



【図 4】

第1実施形態における
車載装置の動作のフローチャート

【図 6】

乱数とエリアの対応づけの例を示す図(その1)

乱数情報バージョン: R20091231103547
細分化エリア情報バージョン: S20091231103547

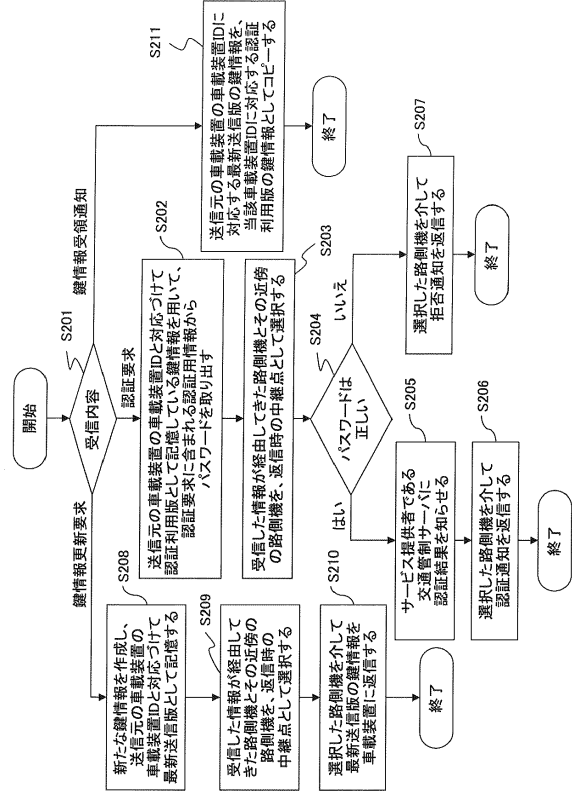
	1列目	2列目	3列目	4列目	5列目
1行目	2615	5499	7706	1598	7313
2行目	3673	9433	9782	2041	2134
3行目	5732	1882	4569	7734	2588
4行目	0044	5812	2102	4665	5793
5行目	7353	3814	8922	3223	0741
6行目	6748	0812	3174	0123	4346
7行目	6490	7261	6899	1132	4964
8行目	9158	4533	9857	7942	5702

401

	1列目	2列目	3列目	4列目	5列目
1行目	2615	5499	7706	1598	7313
2行目	3673	9433	9782	2041	2134
3行目	5732	1882	4569	7734	2588
4行目	0044	5812	2102	4665	5793
5行目	7353	3814	8922	3223	0741
6行目	6748	0812	3174	0123	4346
7行目	6490	7261	6899	1132	4964
8行目	9158	4533	9857	7942	5702

402

【図 5】

第1実施形態において、認証サーバが車載装置から
情報を受信したときの処理のフローチャート

【図 7】

乱数とエリアの対応づけを説明する図(その2)

	1列目	2列目	3列目	4列目	5列目
1行目	5989	6224	0160	2464	4626
2行目	6258	0771	6136	3889	3951
3行目	0833	9985	7806	9496	0337
4行目	8542	2828	2541	840	4073

404

	1列目	2列目	3列目	4列目	5列目
1行目	5989	6224	0160	2464	4626
2行目	6258	0771	6136	3889	3951
3行目	0833	9985	7806	9496	0337
4行目	8542	2828	2541	840	4073

405

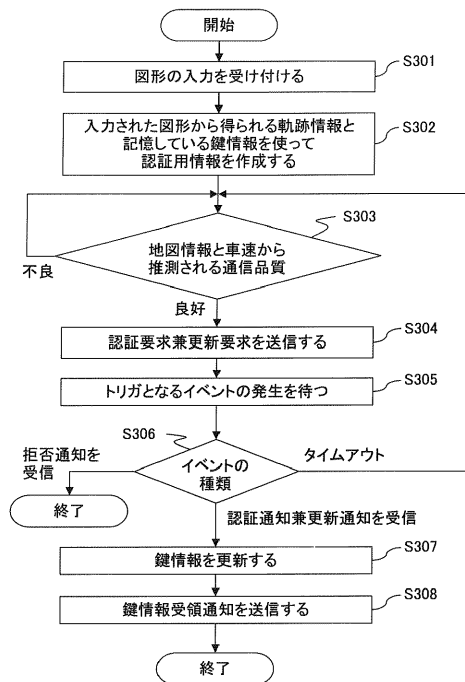
	1列目	2列目	3列目	4列目	5列目
1行目	5989	6224	0160	2464	4626
2行目	6258	0771	6136	3889	3951
3行目	0833	9985	7806	9496	0337
4行目	8542	2828	2541	840	4073

406

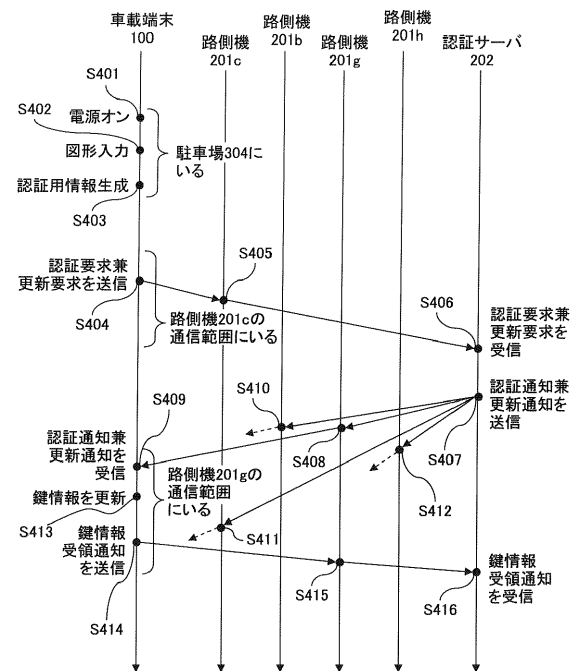
	1列目	2列目	3列目	4列目	5列目
1行目	5989	6224	0160	2464	4626
2行目	6258	0771	6136	3889	3951
3行目	0833	9985	7806	9496	0337
4行目	8542	2828	2541	840	4073

407

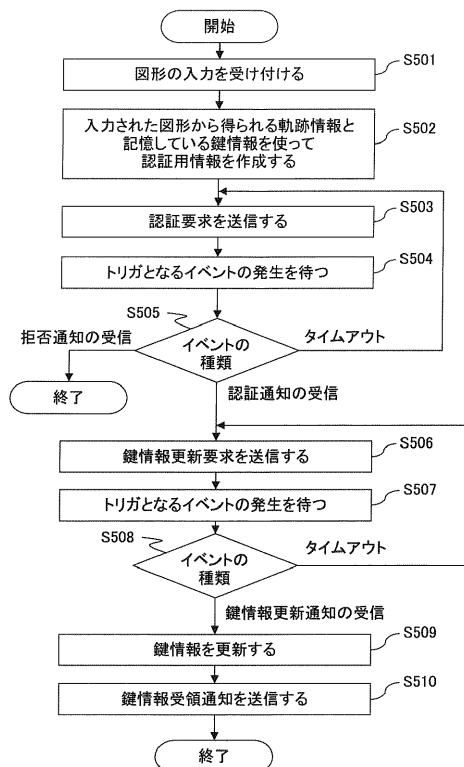
【図 9】

第2実施形態における
車載装置の動作のフローチャート

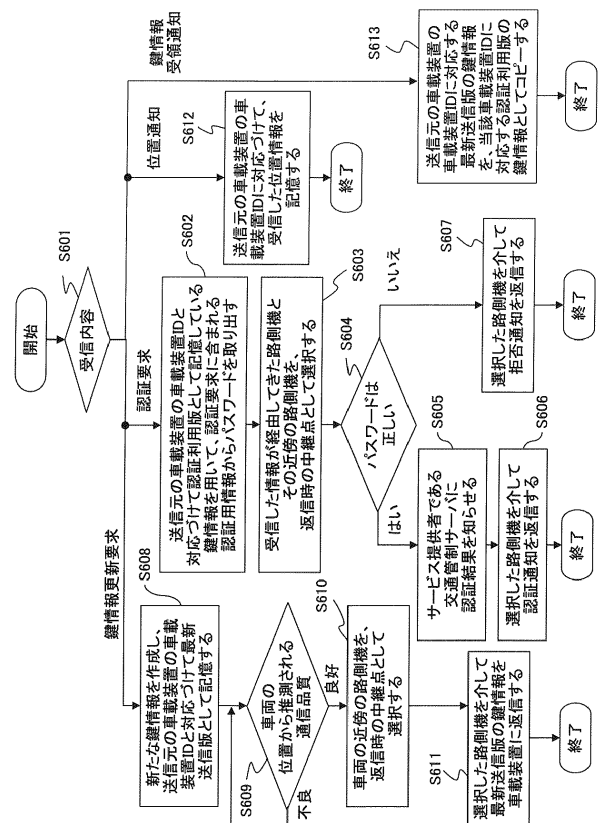
【図 10】

第2実施形態で認証に成功する場合の
タイミングチャートの例

【図 11】

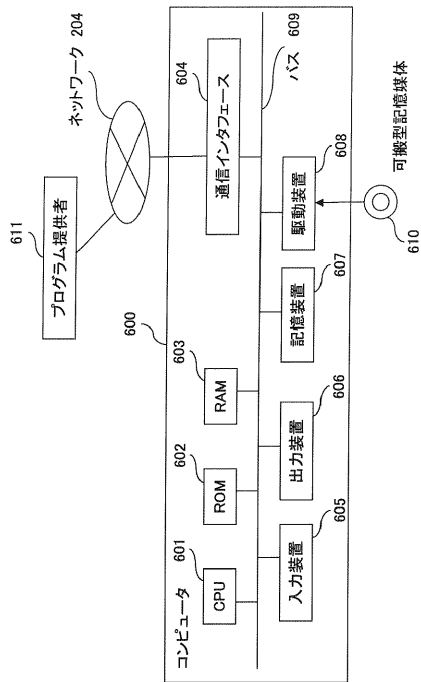
第3実施形態における
車載装置の動作のフローチャート

【図 12】

第3実施形態において、認証サーバが車載装置から
情報を受信したときの処理のフローチャート

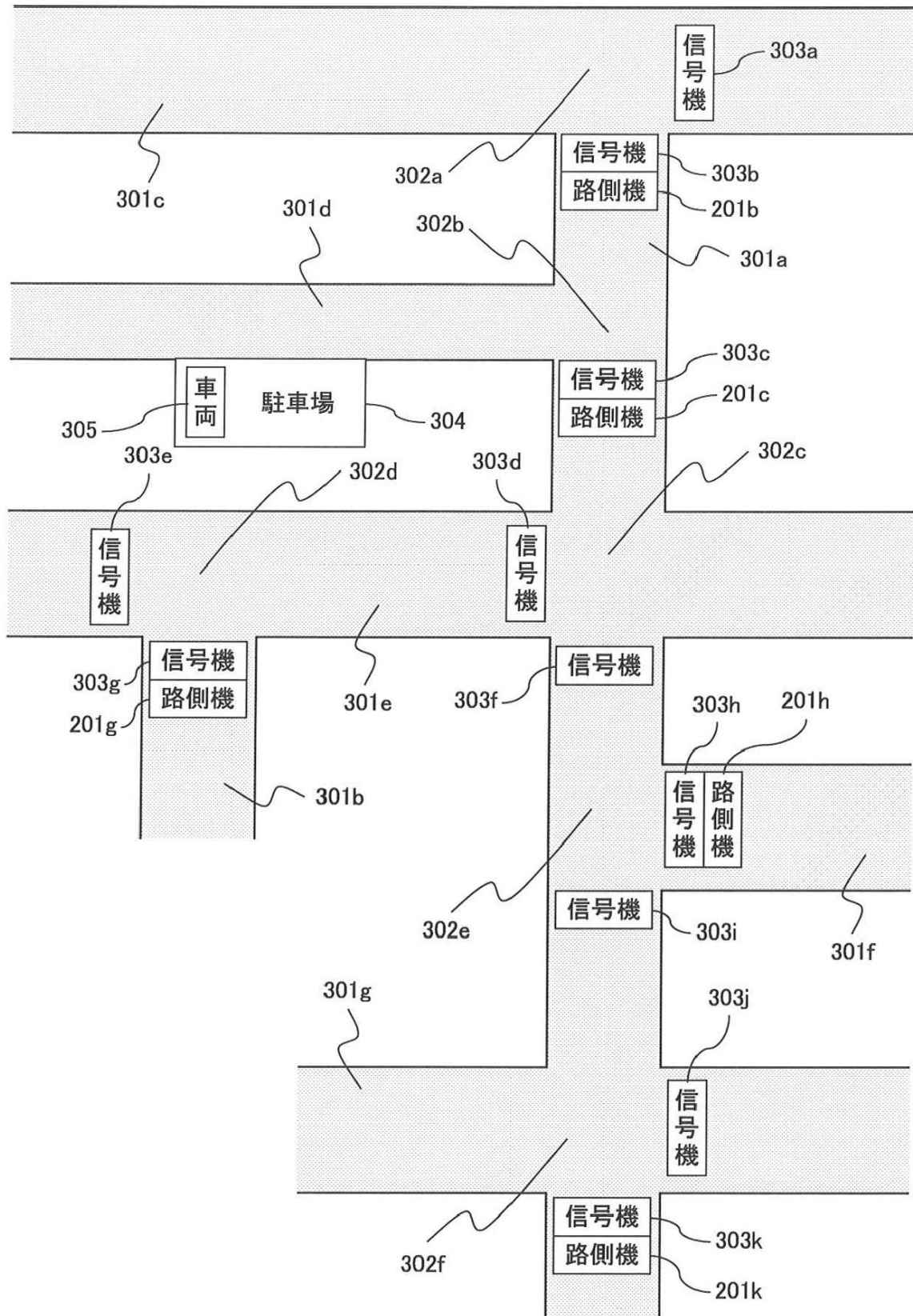
【図 1 3】

コンピュータの構成図



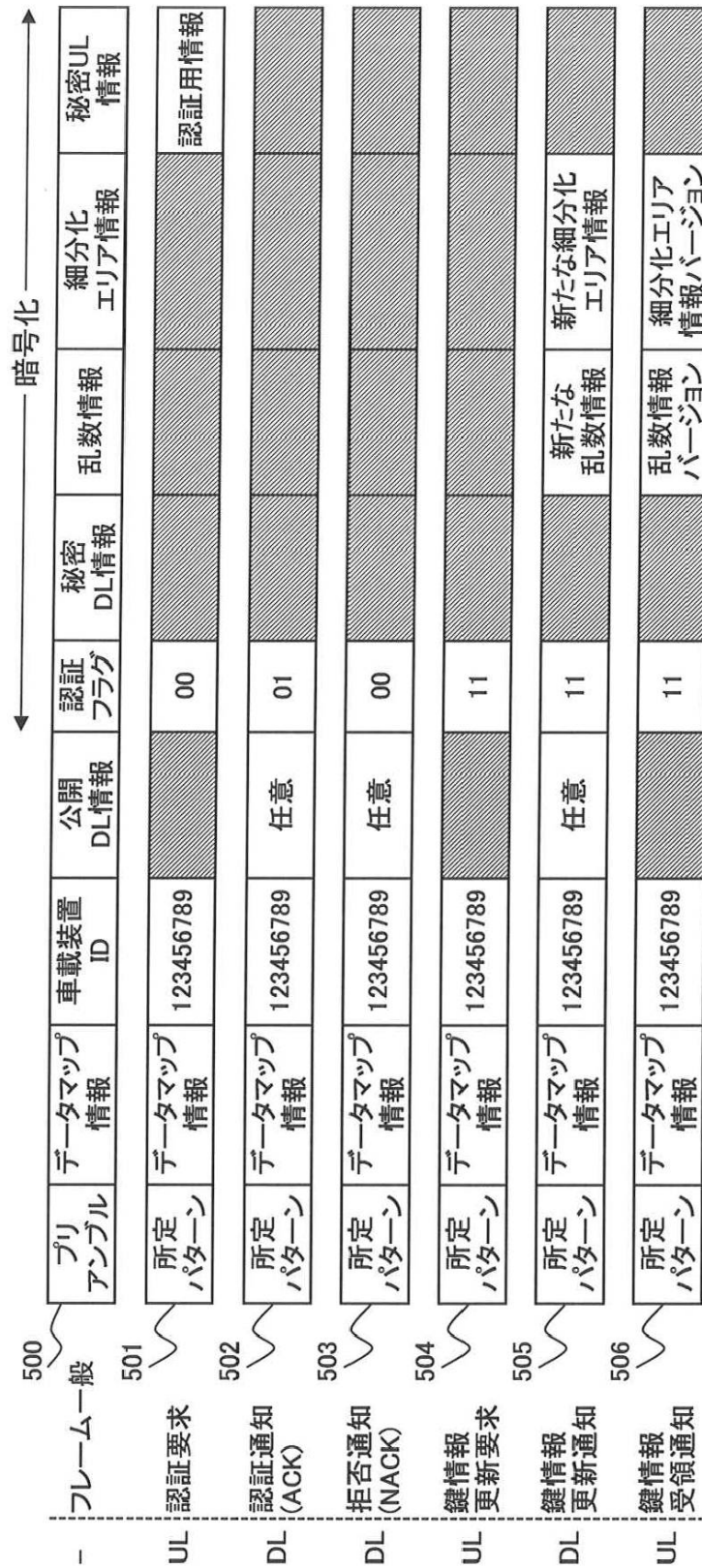
【図 3】

システムが適用される環境の例を示す図



【図 8 A】

フレームの例を説明する図(その1)



【図 8 B】

フレームの例を説明する図(その2)



フロントページの続き

Fターム(参考) 5B285 AA01 BA03 CA47 CA52 CB04 CB24 CB42 CB52 CB55 CB56
CB59 CB62 CB73 CB94 CB95 DA05 DA10