

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)公開番号

特開2022-59777

(P2022-59777A)

(43)公開日 令和4年4月14日(2022.4.14)

(51)国際特許分類		F I		テーマコード(参考)	
G 0 6 F	21/44 (2013.01)	G 0 6 F	21/44	3 5 0	2 E 2 5 0
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/00	6 7 5 A	5 K 0 6 7
H 0 4 W	12/06 (2021.01)	H 0 4 W	12/06		
H 0 4 W	64/00 (2009.01)	H 0 4 W	64/00		
E 0 5 B	49/00 (2006.01)	E 0 5 B	49/00	J	
		審査請求	未請求	請求項の数	14 O L (全18頁) 最終頁に続く

(21)出願番号	特願2020-167583(P2020-167583)	(71)出願人	000003551 株式会社東海理化電機製作所 愛知県丹羽郡大口町豊田三丁目2 6 0 番地
(22)出願日	令和2年10月2日(2020.10.2)	(74)代理人	100140958 弁理士 伊藤 学
		(74)代理人	100137888 弁理士 大山 夏子
		(72)発明者	大橋 洋介 愛知県丹羽郡大口町豊田三丁目2 6 0 番地 株式会社東海理化電機製作所内
		(72)発明者	長谷川 洋祐 愛知県丹羽郡大口町豊田三丁目2 6 0 番地 株式会社東海理化電機製作所内
		F ターム(参考)	2E250 AA21 BB08 DD06 FF25 最終頁に続く

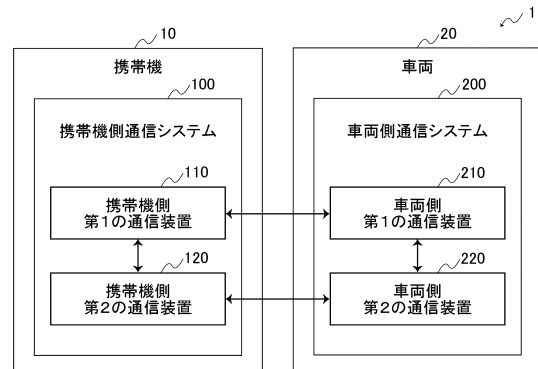
(54)【発明の名称】 通信システム、通信方法、及びプログラム

(57)【要約】

【課題】セキュリティをさらに向上させることが可能な仕組みを提供する。

【解決手段】第1の通信装置と、第2の通信装置と、を備える通信システムであって、第1の通信装置は、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第1の認証処理を実行し、第2の通信装置は、通信システムと他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、他の通信システムとの間で送受信することを含む第2の認証処理を実行し、第2の通信装置は、第1の認証処理が実行される際に、第2の認証処理において測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報を更新し、且つ、鍵関連情報が更新された場合に変更される数であるカウンタ値を変更し、鍵関連情報及びカウンタ値を使用して第2の認証処理を実行する、通信システム。

【選択図】図1



【特許請求の範囲】**【請求項 1】**

第 1 の通信装置と、
第 2 の通信装置と、
を備える通信システムであって、
前記第 1 の通信装置は、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第 1 の認証処理を実行し、
前記第 2 の通信装置は、前記通信システムと前記他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、前記他の通信システムとの間で送受信することを含む第 2 の認証処理を実行し、
前記第 2 の通信装置は、
前記第 1 の認証処理が実行される際に、前記第 2 の認証処理において前記測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報を更新し、且つ、前記鍵関連情報が更新された場合に変更される数であるカウンタ値を変更し、
前記鍵関連情報及び前記カウンタ値を使用して前記第 2 の認証処理を実行する、
通信システム。

10

【請求項 2】

前記第 2 の通信装置は、前記第 2 の認証処理において使用される前記カウンタ値が前回の前記第 2 の認証処理において使用された前記カウンタ値と同一である場合、前記測距用信号を送受信しない、
請求項 1 に記載の通信システム。

20

【請求項 3】

前記第 2 の通信装置は、前記第 2 の認証処理において使用される前記カウンタ値が回の前記第 2 の認証処理において使用された前記カウンタ値と異なる場合、前記測距用信号を送受信する、
請求項 1 又は 2 に記載の通信システム。

【請求項 4】

前記第 2 の認証処理において使用される前記カウンタ値が、前回の前記第 2 の認証処理において使用された前記カウンタ値と同一である場合、前記第 2 の認証処理における認証失敗が判定される、
請求項 1 ~ 3 のいずれか一項に記載の通信システム。

30

【請求項 5】

前記第 2 の通信装置は、前記測距用信号を送受信することにより、前記通信システムと前記他の通信システムとの間の距離を測定し、
測定された前記距離に基づいて、前記第 2 の認証処理における認証成否が判定される、
請求項 1 ~ 4 のいずれか一項に記載の通信システム。

【請求項 6】

前記第 2 の認証処理において使用される前記カウンタ値が、前回の前記第 2 の認証処理において使用された前記カウンタ値と異なり、且つ、測定された前記距離が規定の条件を満たす場合に、前記第 2 の認証処理における認証成功が判定される、
請求項 5 に記載の通信システム。

40

【請求項 7】

前記第 1 の通信装置は、前記第 1 の認証処理を実行する際に、前記鍵関連情報の更新及び前記カウンタ値の変更を指示する信号である指示信号を前記第 2 の通信装置に送信し、
前記第 2 の通信装置は、前記指示信号を受信した場合に、前記鍵関連情報を更新し、前記カウンタ値を変更する、
請求項 1 ~ 6 のいずれか一項に記載の通信システム。

【請求項 8】

前記第 1 の通信装置は、
前記第 1 の認証処理において前記鍵関連情報の更新に関する情報を送受信し、

50

前記第 1 の認証処理において送受信した前記鍵関連情報の更新に関する情報を前記指示信号に含めて前記第 2 の通信装置に送信し、
前記第 2 の通信装置は、前記指示信号に含まれる前記鍵関連情報の更新に関する情報に基づいて前記鍵関連情報を更新し、前記カウンタ値を変更する、
請求項 7 に記載の通信システム。

【請求項 9】

前記第 1 の認証処理における無線通信に異常が発生した場合、
前記第 1 の通信装置は、前記第 1 の認証処理を再度実行し、
前記第 2 の通信装置は、鍵関連情報の更新、及びカウンタ値の変更を行った上で、前記第 2 の認証処理を実行する、
請求項 1 ~ 8 のいずれか一項に記載の通信システム。

10

【請求項 10】

前記第 2 の通信装置は、前記鍵関連情報に基づいて前記鍵を生成し、前記他の通信システムに送信する前記測距用信号を前記鍵により暗号化する、
請求項 1 ~ 9 のいずれか一項に記載の通信システム。

【請求項 11】

前記第 2 の通信装置は、前記鍵関連情報に基づいて前記鍵を生成し、前記他の通信システムから受信した前記測距用信号を前記鍵により復号する、
請求項 1 ~ 10 のいずれか一項に記載の通信システム。

【請求項 12】

前記通信システム又は前記他の通信システムの一方は、車両に搭載され、
前記通信システム又は前記他の通信システムの他の一方は、車両のユーザに携帯される装置に搭載される、
請求項 1 ~ 11 のいずれか一項に記載の通信システム。

20

【請求項 13】

第 1 の通信装置と、
第 2 の通信装置と、
を備える通信システムにより実行される通信方法であって、
前記第 1 の通信装置により、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第 1 の認証処理を実行させることと、
前記第 2 の通信装置により、前記通信システムと前記他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、前記他の通信システムとの間で送受信することを含む第 2 の認証処理を実行させることと、
前記第 1 の認証処理が実行される際に、前記第 2 の通信装置により、前記第 2 の認証処理において前記測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報を更新し、且つ、前記鍵関連情報が更新された場合に変更される数であるカウンタ値を変更させ、前記鍵関連情報及び前記カウンタ値を使用して前記第 2 の認証処理を実行させることと、
を含む通信方法。

30

【請求項 14】

第 1 の通信装置と、
第 2 の通信装置と、
を備える通信システムを制御するコンピュータに、
前記第 1 の通信装置により、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第 1 の認証処理を実行させることと、
前記第 2 の通信装置により、前記通信システムと前記他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、前記他の通信システムとの間で送受信することを含む第 2 の認証処理を実行させることと、
前記第 1 の認証処理が実行される際に、前記第 2 の通信装置により、前記第 2 の認証処理において前記測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報

40

50

を更新し、且つ、前記鍵関連情報が更新された場合に更新される数であるカウンタ値を変更させ、前記鍵関連情報及び前記カウンタ値を使用して前記第2の認証処理を実行させることと、
を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、通信システム、通信方法、及びプログラムに関する。

【背景技術】

【0002】

近年、スマートエントリーシステムを搭載した車両が広く普及している。スマートエントリーシステムとは、ユーザが携帯する携帯機と車両との間で無線通信を介した認証を行い、認証が成功した場合にドア錠のアンロック等を行うシステムである。スマートエントリーシステムに関する技術として、例えば、下記特許文献1では、車両と携帯機とが同一のシードから生成された共通鍵に基づいて認証を行う技術が開示されている。

【先行技術文献】

【特許文献】

【0003】

【特許文献1】特開2013-234520号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかし、特許文献1等が開示された技術は、開発されてから未だ日が浅く、スマートエントリーシステムのセキュリティには向上の余地が残されている。

【0005】

そこで、本発明は、上記問題に鑑みてなされたものであり、本発明の目的とするところは、セキュリティをさらに向上させることが可能な仕組みを提供することにある。

【課題を解決するための手段】

【0006】

上記課題を解決するために、本発明のある観点によれば、第1の通信装置と、第2の通信装置と、を備える通信システムであって、前記第1の通信装置は、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第1の認証処理を実行し、前記第2の通信装置は、前記通信システムと前記他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、前記他の通信システムとの間で送受信することを含む第2の認証処理を実行し、前記第2の通信装置は、前記第1の認証処理が実行される際に、前記第2の認証処理において前記測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報を更新し、且つ、前記鍵関連情報が更新された場合に更新される数であるカウンタ値を変更し、前記鍵関連情報及び前記カウンタ値を使用して前記第2の認証処理を実行する、通信システムが提供される。

【0007】

また、上記課題を解決するために、本発明の別の観点によれば、第1の通信装置と、第2の通信装置と、を備える通信システムにより実行される通信方法であって、前記第1の通信装置により、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第1の認証処理を実行させることと、前記第2の通信装置により、前記通信システムと前記他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、前記他の通信システムとの間で送受信することを含む第2の認証処理を実行させることと、前記第1の認証処理が実行される際に、前記第2の通信装置により、前記第2の認証処理において前記測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報を更新し、且つ、前記鍵関連情報が更新された場合に更新される数であるカウンタ値を変更させ、前記鍵関連情報及び前記カウンタ値を使用して前記第2

10

20

30

40

50

の認証処理を実行させることと、を含む通信方法が提供される。

【0008】

また、上記課題を解決するために、本発明の別の観点によれば、第1の通信装置と、第2の通信装置と、を備える通信システムを制御するコンピュータに、前記第1の通信装置により、認証を行うための信号である認証用信号を、他の通信システムとの間で送受信することを含む第1の認証処理を実行させることと、前記第2の通信装置により、前記通信システムと前記他の通信システムとの間の距離を測定するために送受信される信号である測距用信号を、前記他の通信システムとの間で送受信することを含む第2の認証処理を実行させることと、前記第1の認証処理が実行される際に、前記第2の通信装置により、前記第2の認証処理において前記測距用信号の暗号化及び復号に用いられる鍵に関する情報である鍵関連情報を更新し、且つ、前記鍵関連情報が更新された場合に変更される数であるカウンタ値を変更させ、前記鍵関連情報及び前記カウンタ値を使用して前記第2の認証処理を実行させることと、を実行させるためのプログラムが提供される。

10

【発明の効果】

【0009】

以上説明したように本発明によれば、セキュリティをさらに向上させることが可能な仕組みが提供される。

【図面の簡単な説明】

【0010】

【図1】本実施形態に係るシステムの構成の一例を示すブロック図である。

20

【図2】本実施形態に係るシステムにより実行される測距処理の流れの一例を示すシーケンス図である。

【図3】本実施形態に係るシステムにより実行される2段階認証処理の流れの一例を示すシーケンス図である。

【発明を実施するための形態】

【0011】

以下に添付図面を参照しながら、本発明の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【0012】

30

<< 1. 構成例 >>

図1は、本実施形態に係るシステム1の構成の一例を示すブロック図である。図1に示すように、システム1は、携帯機10及び車両20を含む。

【0013】

携帯機10は、車両20のユーザにより携帯される任意の装置として構成される。任意の装置には、電子キー、スマートフォン、及びウェアラブル端末等が含まれる。携帯機10には、携帯機側通信システム100が搭載される。車両20は、ユーザにより利用される対象の一例である。車両20には、車両側通信システム200が搭載される。携帯機側通信システム100及び車両側通信システム200は、本実施形態における通信システム及び他の通信システムの一例である。

40

【0014】

携帯機側通信システム100及び車両側通信システム200の一方は、認証者として機能し、他方は被認証者として機能する。認証者とは、被認証者を認証する装置である。被認証者とは、認証される装置である。本実施形態では、携帯機側通信システム100が被認証者であるものとする。また、車両側通信システム200が認証者であるものとする。

【0015】

システム1においては、ユーザ（例えば、車両20のドライバー）が携帯機10を携帯して車両20に近づくと、携帯機側通信システム100と車両側通信システム200との間で認証のための無線通信が行われる。そして、認証が成功すると、車両20のドア錠がアンロックされたりエンジンの始動が許可されたりして、車両20がユーザにより利用可能

50

な状態になる。このようなシステムは、スマートエントリーシステムとも称される。以下、各構成要素について順に説明する。

【0016】

(1) 携帯機側通信システム100

図1に示すように、携帯機側通信システム100は、携帯機側第1の通信装置110及び携帯機側第2の通信装置120を備える。

【0017】

携帯機側第1の通信装置110は、車両側通信システム200との間で無線通信を行う装置である。具体的には、携帯機側第1の通信装置110は、車両側第1の通信装置210との間で無線通信を行う。即ち、携帯機側第1の通信装置110は、車両側第1の通信装置210へ無線信号を送信する。また、携帯機側第1の通信装置110は、車両側第1の通信装置210から無線信号を受信する。携帯機側第1の通信装置110は、記憶装置及び制御装置を含み、各種情報の記憶及び各種情報処理を行う。例えば、携帯機側第1の通信装置110は、車両側通信システム200との間で行った無線通信に基づく各種処理を実行する。

10

【0018】

携帯機側第2の通信装置120は、車両側通信システム200との間で無線通信を行う装置である。具体的には、携帯機側第2の通信装置120は、車両側第2の通信装置220との間で無線通信を行う。即ち、携帯機側第2の通信装置120は、車両側第2の通信装置220へ無線信号を送信する。また、携帯機側第2の通信装置120は、車両側第2の通信装置220から無線信号を受信する。携帯機側第2の通信装置120は、記憶装置及び制御装置を含み、各種情報の記憶及び各種情報処理を行う。例えば、携帯機側第2の通信装置120は、車両側通信システム200との間で行った無線通信に基づく各種処理を実行する。

20

【0019】

携帯機側第1の通信装置110と携帯機側第2の通信装置120とは有線又は無線により接続される。そのため、携帯機側第1の通信装置110と携帯機側第2の通信装置120とは情報を送受信することができる。

【0020】

(2) 車両側通信システム200

図2に示すように、車両側通信システム200は、車両側第1の通信装置210及び車両側第2の通信装置220を備える。

30

【0021】

車両側第1の通信装置210は、携帯機側通信システム100との間で無線通信を行う装置である。具体的には、車両側第1の通信装置210は、携帯機側第1の通信装置110との間で無線通信を行う。即ち、車両側第1の通信装置210は、携帯機側第1の通信装置110へ無線信号を送信する。また、車両側第1の通信装置210は、携帯機側第1の通信装置110から無線信号を受信する。車両側第1の通信装置210は、記憶装置及び制御装置を含み、各種情報の記憶及び各種情報処理を行う。例えば、車両側第1の通信装置210は、携帯機側通信システム100との間で行った無線通信に基づく各種処理を実行する。

40

【0022】

車両側第2の通信装置220は、携帯機側通信システム100との間で無線通信を行う装置である。具体的には、車両側第2の通信装置220は、携帯機側第2の通信装置120との間で無線通信を行う。即ち、車両側第2の通信装置220は、携帯機側第2の通信装置120へ無線信号を送信する。また、車両側第2の通信装置220は、携帯機側第2の通信装置120から無線信号を受信する。車両側第2の通信装置220は、記憶装置及び制御装置を含み、各種情報の記憶及び各種情報処理を行う。例えば、車両側第2の通信装置220は、携帯機側通信システム100との間で行った無線通信に基づく各種処理を実行する。

50

【 0 0 2 3 】

車両側第 1 の通信装置 2 1 0 と車両側第 2 の通信装置 2 2 0 とは有線又は無線により接続される。そのため、車両側第 1 の通信装置 2 1 0 と車両側第 2 の通信装置 2 2 0 とは情報を送受信することができる。一例として、車両側第 1 の通信装置 2 1 0 と車両側第 2 の通信装置 2 2 0 とは、CAN (Controller Area Network) 又は LIN (Local Interconnect Network) 等の車載ネットワークにより接続される。車両側第 1 の通信装置 2 1 0 及び車両側第 2 の通信装置 2 2 0 の各々は、ECU (Electronic Control Unit) として構成されてもよい。

【 0 0 2 4 】

(3) 無線通信規格に関する補足

携帯機側第 1 の通信装置 1 1 0 と携帯機側第 2 の通信装置 1 2 0 との間で行われる無線通信は、第 1 の無線通信規格に準拠して行われる。他方、携帯機側第 2 の通信装置 1 2 0 と車両側第 2 の通信装置 2 2 0 との間で行われる無線通信は、第 2 の無線通信規格に準拠して行われる。

【 0 0 2 5 】

第 1 の無線通信規格では、超短波 (UHF : Ultra-High Frequency) 及び長波 (LF : Low Frequency) 帯の信号が使用されてもよい。典型的なスマートエントリーシステムにおいては、携帯機 1 0 側から車両 2 0 側への送信に UHF 帯の信号が使用され、車両 2 0 側から携帯機 1 0 側への送信に LF 帯の信号が使用される。以下では、携帯機側第 1 の通信装置 1 1 0 及び車両側第 1 の通信装置 2 1 0 は、UHF 帯の信号及び LF 帯の信号での通信を行うものとして説明する。即ち、以下では、携帯機側第 1 の通信装置 1 1 0 から車両側第 1 の通信装置 2 1 0 への送信に UHF 帯の信号が使用され、車両側第 1 の通信装置 2 1 0 から携帯機側第 1 の通信装置 1 1 0 への送信に LF 帯の信号を使用するものとする。

【 0 0 2 6 】

第 2 の無線通信規格では、UWB (Ultra-Wide Band) を用いた信号が使用されてもよい。UWB によるインパルス方式の信号は、測位及び測距を高精度に行うことができるという特性を有する。すなわち、ナノ秒オーダー以下の非常に短いパルス幅の電波を使用することで電波の伝搬時間を高精度に測定することができ、伝搬時間に基づく測位及び測距を高精度に行うことができる。以下では、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 は、UWB を用いた信号を送受信するものとする。

【 0 0 2 7 】

< < 2 . 技術的特徴 > >

(1) 測距処理

携帯機側通信システム 1 0 0 及び車両側通信システム 2 0 0 は、測距処理を行う。測距処理とは、携帯機側通信システム 1 0 0 と車両側通信システム 2 0 0 との間の距離を測定する処理である。測距処理において測定された距離を、以下では測距値とも称する。

【 0 0 2 8 】

測距処理においては、測距処理のための信号が送受信され得る。

【 0 0 2 9 】

測距処理のために送受信される信号の一例は、測距用信号である。測距用信号は、装置間の距離を測定するために送受信される信号である。測距用信号は、計測の対象となる信号でもある。例えば、測距用信号の送受信にかかる時間 (即ち、伝搬時間) が計測される。典型的には、測距用信号は、データを格納するペイロード部分を有さないフレームフォーマットで構成される。もちろん、測距用信号は、データを格納するペイロード部分を有するフレームフォーマットで構成されてもよい。

【 0 0 3 0 】

測距処理においては、装置間で複数の測距用信号が送受信され得る。複数の測距用信号のうち、一方の装置から他方の装置へ送信される測距用信号を第 1 の測距用信号とも称する。そして、第 1 の測距用信号を受信した装置から、第 1 の測距用信号を送信した装置へ送

10

20

30

40

50

信される測距用信号を、第2の測距用信号とも称する。

【0031】

測距処理のために送受信される信号の他の一例は、データ信号である。データ信号は、データを格納して搬送する信号である。データ信号は、データを格納するペイロード部分を有するフレームフォーマットで構成される。

【0032】

測距処理において信号を送受信することを、以下では測距通信とも称する。本実施形態では、携帯機側第2の通信装置120と車両側第2の通信装置220とが測距通信を行うものとする。測距処理においては、携帯機側通信システム100と車両側通信システム200との間の距離として、測距用信号を送受信した携帯機側第2の通信装置120と車両側第2の通信装置220との間の距離が、測定される。

10

【0033】

測距処理の一例を、図2を参照しながら説明する。

【0034】

図2は、本実施形態に係るシステム1により実行される測距処理の流れの一例を示すシーケンス図である。図2に示すように、本シーケンスでは、携帯機側通信システム100と車両側通信システム200とが関与する。

【0035】

図2に示すように、まず、携帯機側通信システム100の携帯機側第2の通信装置120は、第1の測距用信号を送信する(ステップS12)。例えば、第1の測距用信号は、UWBを用いた信号として送信されてもよい。

20

【0036】

次いで、車両側通信システム200の車両側第2の通信装置220は、携帯機側第2の通信装置120から第1の測距用信号を受信すると、第1の測距用信号の応答として第2の測距用信号を送信する(ステップS14)。例えば、第2の測距用信号は、UWBを用いた信号として送信されてもよい。

【0037】

このとき、車両側第2の通信装置220は、車両側第2の通信装置220における第1の測距用信号の受信時刻から第2の測距用信号の送信時刻までの時間 T_2 を計測しておく。他方、携帯機側第2の通信装置120は、車両側第2の通信装置220から第2の測距用信号を受信すると、携帯機側第2の通信装置120における第1の測距用信号の送信時刻から第2の測距用信号の受信時刻までの時間 T_1 を計測しておく。

30

【0038】

次に、携帯機側第2の通信装置120は、時間 T_1 を示す情報を含むデータ信号を送信する(ステップS16)。例えば、データ信号は、UWBを用いた信号として送信されてもよい。

【0039】

そして、車両側第2の通信装置220は、データ信号を受信すると、計測した T_2 、及びデータ信号に含まれる情報により示される時間 T_1 に基づいて、携帯機側第2の通信装置120と車両側第2の通信装置220との間の距離を示す測距値を計算する(ステップS18)。詳しくは、車両側第2の通信装置220は、 $T_1 - T_2$ の結果を2で割ることで片道の信号の伝搬時間を計算する。そして、車両側第2の通信装置220は、かかる伝搬時間に信号の速度を掛けることで、携帯機側第2の通信装置120と車両側第2の通信装置220との間の距離を示す測距値を計算する。

40

【0040】

ここで、測距通信では、UWBを用いた信号が送受信されることが望ましい。少なくとも測距用信号は、UWBを用いた信号として送受信されることが望ましい。かかる構成によれば、UWBに関して上記説明したように、測距を高精度に行うことが可能となる。

【0041】

(2) 2段階認証

50

本実施形態に係る携帯機側通信システム 100 及び車両側通信システム 200 は、複数の認証処理を行う。認証処理とは、認証者が被認証者を認証する処理である。複数の認証処理の全てが成功裏に完了した場合に認証が成功し、少なくとも一部の認証処理において異常が発生した場合に認証が失敗する。

【0042】

- 第 1 の認証処理

1 段階目の認証処理（以下、第 1 の認証処理とも称する）は、例えば要求応答認証を含む。認証応答要求とは、認証を行うための信号である認証用信号を、認証者と被認証者との間で送受信することを含む認証処理である。具体的には、認証者は、認証用信号としての認証要求を生成して、被認証者に送信する。被認証者は、受信した認証要求に基づいて、認証用信号としての認証応答を生成し、生成した認証応答を認証者に送信する。そして、認証者は、受信した認証応答に基づき被認証者の認証を行う。

10

【0043】

認証要求は、認証の実行を要求する信号である。認証応答は、認証要求に対する応答である。認証応答は、認証要求及び被認証者の情報（例えば、ID 及びパスワード等）に基づいて生成される。典型的には、認証要求は乱数であり認証のたびに変化するので、要求応答認証はいわゆるリプレイアタックに耐性を有する。また、認証応答は被認証者の情報（例えば、ID 及びパスワード等）に基づいて生成され、即ち ID 及びパスワードそのものは送受信されないため、盗聴に起因するリスクが低減される。

【0044】

- 第 2 の認証処理

2 段階目の認証処理（以下、第 2 の認証処理とも称する）は、認証者と被認証者との相対的な位置関係に基づいて、携帯機側通信システム 100 を認証する処理である。

20

【0045】

一例として、第 2 の認証処理は、認証者と被認証者との間の距離に基づく認証を行う処理である。距離に基づく認証は、測距用信号を送受信することにより測距値を測定する測距処理、及び測定された測距値に基づき認証成否を判定する処理を含む。第 2 の認証処理においては、車両側通信システム 200 は、測距値が規定の条件を満たすか否かにより、携帯機側通信システム 100 の認証を行う。規定の条件の一例は、測距値が規定の閾値以下であることである。

30

【0046】

ここで、測距処理では、携帯機側通信システム 100 と車両側通信システム 200 との間で送受信した無線信号の伝搬時間に基づいて測距値が測定される。従って、携帯機側通信システム 100 と車両側通信システム 200 との間に中継器を持ち込んで無線信号を中継する、いわゆるリレーアタックによる被害を防止することができる。無線信号を中継した分、伝搬時間が長くなり、測距値が規定の条件を満たさなくなるためである。

【0047】

- 補足

一例として、第 1 の認証処理では、第 1 の無線通信規格に準拠して信号が送受信される。これにより、認証要求及び認証応答といったデータの送受信を含む第 1 の認証処理を、より利得が高い第 1 の無線通信規格を用いて効率よく行うことができる。

40

【0048】

一例として、第 2 の認証処理では、第 2 の無線通信規格に準拠して信号が送受信される。これにより、距離に基づく認証を含む第 2 の認証処理を、より測距に適した第 2 の無線通信規格を用いて高精度に行うことができる。

【0049】

これらの認証処理に先行して、起動を指示するウェイクアップ信号、及びウェイクアップ信号に対する応答の送受信が行われてもよい。ウェイクアップ信号により、受信側をスリープ状態から復帰させることができる。ウェイクアップ信号に対する応答としては、起動することを示す肯定応答（ACK : Acknowledgement）信号、及び起動しないことを

50

示す否定応答 (N A C K : Negative Acknowledgement) 信号が挙げられる。ウェイクアップ信号に対して A C K が返信された場合、認証処理がトリガされる。

【 0 0 5 0 】

第 1 の認証処理及び第 2 の認証処理は、段階的に行われてもよく、その順番は任意である。また、第 1 の認証処理及び第 2 の認証処理は、一部又は全部が並行して行われてもよい。以下では、第 1 の認証処理の後に第 2 の認証処理が実行されるものとする。

【 0 0 5 1 】

(3) 第 2 の認証処理におけるシード及びカウンタの使用

携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の各々は、鍵関連情報を用いて第 2 の認証処理を実行する。鍵関連情報とは、測距用信号の暗号化及び復号に用いられる鍵に関する情報である。鍵関連情報の一例は、ストリーム暗号における鍵ストリーム (疑似乱数系列) を生成するための鍵の初期値 (即ち、疑似乱数生成器に入力されるシード) である。シードの一例は、乱数である。その場合、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の各々は、シードに基づいて生成した暗号化鍵又は復号鍵を使用して、測距用信号の暗号化又は復号を行う。暗号化鍵及び復号鍵は、同一のシードに基づいて生成される場合、同一 (即ち、共通鍵) となる。鍵関連情報の他の一例は、測距用信号の暗号化及び復号に用いられる鍵そのものである。本実施形態では、鍵関連情報はシードであり、同一のシードに基づいて生成された共通鍵が暗号化及び復号に使用されるものとする。

10

【 0 0 5 2 】

具体的には、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の各々は、シードを用いて第 2 の認証処理を実行することとして、シードに基づいて共通鍵を生成し、生成した共通鍵により無線信号の暗号化及び復号を行う。詳しくは、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の一方は、他方に送信する測距用信号を、シードに基づいて生成した共通鍵により暗号化する。図 2 に示した例に関して言えば、一例として、携帯機側第 2 の通信装置 1 2 0 は、シードを用いて生成した共通鍵により第 1 の測距用信号を暗号化する。他の一例として、車両側第 2 の通信装置 2 2 0 は、シードを用いて生成した共通鍵により第 2 の測距用信号を暗号化する。また、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の一方は、他方から受信した測距用信号を、シードに基づいて生成した共通鍵により復号する。図 2 に示した例に関して言えば、一例として、車両側第 2 の通信装置 2 2 0 は、シードを用いて生成した共通鍵により第 1 の測距用信号を復号する。他の一例として、携帯機側第 2 の通信装置 1 2 0 は、シードを用いて生成した共通鍵により第 2 の測距用信号を復号する。

20

30

【 0 0 5 3 】

暗号化のために使用されたシードと復号のために使用されたシードとが同一である場合、復号は成功する。他方、暗号化のために使用されたシードと復号のために使用されたシードとが異なる場合、復号は失敗し、第 2 の認証処理における認証失敗が判定される。そのため、第 2 の認証処理においてシードを使用することで、第 2 の認証処理のセキュリティを向上させることが可能である。

【 0 0 5 4 】

セキュリティをさらに向上させるために、シードは適宜更新されることが好ましい。これにより、例えば更新前のシードが盗聴された場合であっても、車両側通信システム 2 0 0 は、更新後のシードを第 2 の認証処理において使用することで、盗聴者による更新前のシードを使用した測距用信号に対し認証失敗を判定することができる。更新前のシードと更新後のシードとは、典型的には異なる。ただし、更新前のシードと更新後のシードとが同一になる場合もある。

40

【 0 0 5 5 】

シードの更新に関し、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の各々は、鍵関連情報に加え、カウンタ値を用いて第 2 の認証処理を実行する。カウンタ値とは、シードが更新された場合に変更される数である。一例として、カウンタ値は、シ

50

ドが更新される度に所定数が加算される。所定数の一例は、1である。かかる構成によれば、携帯機側第2の通信装置120及び車両側第2の通信装置220の各々は、更新前後のシードが同一であっても、カウンタ値が変更されていることをもって、シードの更新が行われたことを把握することができる。

【0056】

詳しくは、第2の認証処理において使用される前記カウンタ値が、前回の第2の認証処理において使用されたカウンタ値と同一である場合、第2の認証処理における認証失敗が判定される。他方、第2の認証処理において使用されるカウンタ値が、前回の第2の認証処理において使用されたカウンタ値と異なり、且つ、測定された測距値が規定の条件を満たす場合に、第2の認証処理における認証成功が判定される。かかる構成によれば、前回の第2の認証処理の後にシードの更新が行われている場合に限定して認証成功が判定されるので、セキュリティを向上させることが可能である。

10

【0057】

携帯機側第2の通信装置120及び車両側第2の通信装置220の各々は、第2の認証処理において使用されるカウンタ値が前回の第2の認証処理において使用されたカウンタ値と同一である場合、測距用信号を送受信しなくてもよい。他方、携帯機側第2の通信装置120及び車両側第2の通信装置220の各々は、第2の認証処理において使用されるカウンタ値が前回の第2の認証処理において使用されたカウンタ値と異なる同一である場合、測距用信号を送受信してもよい。かかる構成によれば、カウンタ値が変更済みである場合、即ち第2の認証処理において測距値によっては認証成功が判定され得る場合に限定して、測距用信号を送受信することができる。他方、カウンタ値が未変更である場合、即ち第2の認証処理において測距値によらず認証失敗が判定される場合には、測距用信号の送受信を省略して認証失敗を判定することができる。従って、携帯機側通信システム100及び車両側通信システム200の各々の消費電力を抑制することが可能である。

20

【0058】

携帯機側第2の通信装置120及び車両側第2の通信装置220の各々は、第2の認証処理を実行する前に、シードを更新し、共有する。具体的には、携帯機側第2の通信装置120及び車両側第2の通信装置220の各々は、第1の認証処理が実行される際に、シードを更新し、且つカウンタ値を変更する。詳しくは、携帯機側第1の通信装置110は、第1の認証処理を実行する際に、シードの更新及びカウンタ値の変更を指示する信号である指示信号を携帯機側第2の通信装置120に送信する。そして、携帯機側第2の通信装置120は、指示信号を受信した場合に、シードを更新し、カウンタ値を変更する。同様に、車両側第1の通信装置210は、第1の認証処理を実行する際に、シードの更新及びカウンタ値の変更を指示する信号である指示信号を車両側第2の通信装置220に送信する。そして、車両側第2の通信装置220は、指示信号を受信した場合に、シードを更新し、カウンタ値を変更する。かかる構成によれば、第2の認証処理よりも前にシードの更新及びカウンタ値の変更を行うことが可能となる。従って、第2の認証処理において、最新のシードを用いて暗号化及び復号を行うことが可能となる。

30

【0059】

携帯機側第1の通信装置110及び車両側第1の通信装置210の各々は、第1の認証処理において、シードの更新に関する情報を送受信する。一例として、車両側第1の通信装置210は、認証要求にシードの更新に関する情報を含めて送信してもよい。他の一例として、携帯機側第1の通信装置110は、認証応答にシードの更新に関する情報を含めて送信してもよい。シードの更新に関する情報の一例は、更新後のシードそのものである。シードの更新に関する情報の他の一例は、更新後のシードの元となる情報である。

40

【0060】

携帯機側第1の通信装置110は、第1の認証処理において、シードの更新に関する情報を送受信すると、当該シードの更新に関する情報を指示信号に含めて携帯機側第2の通信装置120に送信する。そして、携帯機側第2の通信装置120は、受信した指示信号に含まれるシードの更新に関する情報に基づいてシードを更新し、カウンタ値を変更する。

50

【 0 0 6 1 】

同様に、車両側第 1 の通信装置 2 1 0 は、1 の認証処理において、シードの更新に関する情報を送受信すると、当該シードの更新に関する情報を指示信号に含めて車両側第 2 の通信装置 2 2 0 に送信する。そして、車両側第 2 の通信装置 2 2 0 は、受信した指示信号に含まれるシードの更新に関する情報に基づいてシードを更新し、カウンタ値を変更する。

【 0 0 6 2 】

かかる構成によれば、第 1 の認証処理において、同一のシードを携帯機側通信システム 1 0 0 と車両側通信システム 2 0 0 との間で共有することができる。従って、第 2 の認証処理において、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の各々は、同一のシードから生成された共通鍵を使用して測距用信号の暗号化及び復号を行うことが可能となる。

10

【 0 0 6 3 】

ここで、第 1 の認証処理において無線通信に異常が発生する場合がある。第 1 の認証処理において無線通信に発生する異常の一例は、ノイズが発生して認証要求又は認証応答の受信に失敗することである。第 1 の認証処理において無線通信に異常が発生した場合、携帯機側通信システム 1 0 0 及び車両側通信システム 2 0 0 の各々は、2 段階認証のリトライを行う。具体的には、第 1 の認証処理における無線通信に異常が発生した場合、携帯機側第 1 の通信装置 1 1 0 及び車両側第 1 の通信装置 2 1 0 の各々は、第 1 の認証処理を再度実行する。携帯機側第 1 の通信装置 1 1 0 及び車両側第 1 の通信装置 2 1 0 の各々は、かかるリトライ時の第 1 の認証処理において、シードの更新に関する情報を送受信する。そして、携帯機側第 2 の通信装置 1 2 0 及び車両側第 2 の通信装置 2 2 0 の各々は、鍵関連情報の更新、及びカウンタ値の変更を行った上で、第 2 の認証処理を実行する。よって、リトライ時の第 2 の認証処理においては、リトライ前から更新された最新のシード、及びリトライ前から変更されたカウンタ値に基づいて、認証成否が判定されることとなる。従って、リトライ時のセキュリティを向上させることが可能である。

20

【 0 0 6 4 】

なお、シードの更新、及びカウンタ値の更新は、第 1 の認証処理が実行される度に行われてもよい。他に、シードの更新、及びカウンタ値の更新は、所定の条件が満たされた場合に限定して行われてもよい。所定の条件の一例は、上述した第 1 の認証処理において無線通信に異常が発生したことである。

30

【 0 0 6 5 】

(4) 処理の流れ

以下、図 3 を参照しながら、本実施形態に係る 2 段階認証処理の流れの一例を説明する。図 3 は、本実施形態に係るシステム 1 により実行される 2 段階認証処理の流れの一例を示すシーケンス図である。図 3 に示すように、本シーケンスには携帯機側通信システム 1 0 0 及び車両側通信システム 2 0 0 が関与する。

【 0 0 6 6 】

まず、車両側第 1 の通信装置 2 1 0 は、シードの更新に関する情報として、シードそのものを含む認証要求を送信する (ステップ S 1 0 2) 。

【 0 0 6 7 】

次いで、車両側第 1 の通信装置 2 1 0 は、シードの更新に関する情報としてのシードを含む指示信号を車両側第 2 の通信装置 2 2 0 に送信する (ステップ S 1 0 4) 。

40

【 0 0 6 8 】

車両側第 2 の通信装置 2 2 0 は、指示信号を受信すると、受信した指示信号に含まれるシードを最新のシードとして記憶することによりシードを更新し、カウンタ値を変更する (ステップ S 1 0 6)

【 0 0 6 9 】

他方、携帯機側第 1 の通信装置 1 1 0 は、車両側第 1 の通信装置 2 1 0 から認証要求を受信すると、受信した認証要求に基づいて認証応答を生成する。そして、生成した認証応答を送信する (ステップ S 1 0 8) 。

50

【 0 0 7 0 】

次いで、携帯機側第 1 の通信装置 1 1 0 は、車両側第 1 の通信装置 2 1 0 から受信した任用要求に含まれるシードを含む指示信号を、携帯機側第 2 の通信装置 1 2 0 に送信する（ステップ S 1 1 0）。

【 0 0 7 1 】

携帯機側第 2 の通信装置 1 2 0 は、指示信号を受信すると、受信した指示信号に含まれるシードを最新のシードとして記憶することによりシードを更新し、カウンタ値を変更する（ステップ S 1 1 2）

【 0 0 7 2 】

他方、車両側第 1 の通信装置 2 1 0 は、携帯機側第 1 の通信装置 1 1 0 から認証応答を受信すると、受信した認証応答に基づいて携帯機側通信システム 1 0 0 の認証を行う（ステップ S 1 1 4）。

【 0 0 7 3 】

次いで、携帯機側第 2 の通信装置 1 2 0 は、ステップ S 1 1 2 において記憶した最新のシードに基づいて共通鍵を生成する。そして、携帯機側第 2 の通信装置 1 2 0 は、生成した共通鍵により第 1 の測距用信号を暗号化して、暗号化した第 1 の測距用信号を送信する（ステップ S 1 1 6）

【 0 0 7 4 】

車両側第 2 の通信装置 2 2 0 は、ステップ S 1 0 6 において記憶した最新のシードに基づいて共通鍵を生成する。次いで、携帯機側第 2 の通信装置 1 2 0 は、第 1 の測距用信号を受信すると、生成した共通鍵により、受信した第 1 の測距用信号を復号する。ここでは、第 1 の測距用信号の復号に成功したものとする。そして、携帯機側第 2 の通信装置 1 2 0 は、生成した共通鍵により第 2 の測距用信号を暗号化して、暗号化した第 2 の測距用信号を送信する（ステップ S 1 1 8）。

【 0 0 7 5 】

ここで、車両側第 2 の通信装置 2 2 0 は、車両側第 2 の通信装置 2 2 0 における第 1 の測距用信号の受信時刻から第 2 の測距用信号の送信時刻までの時間 T_2 を計測しておく。他方、携帯機側第 2 の通信装置 1 2 0 は、車両側第 2 の通信装置 2 2 0 から第 2 の測距用信号を受信すると、携帯機側第 2 の通信装置 1 2 0 における第 1 の測距用信号の送信時刻から第 2 の測距用信号の受信時刻までの時間 T_1 を計測しておく。

【 0 0 7 6 】

携帯機側第 2 の通信装置 1 2 0 は、第 2 の測距用信号を受信すると、ステップ S 1 1 6 において生成した共通鍵により、受信した第 2 の測距用信号を復号する。ここでは、第 2 の測距用信号の復号に成功したものとする。すると、携帯機側第 2 の通信装置 1 2 0 は、時間 T_1 を示す情報を含むデータ信号を送信する（ステップ S 1 2 0）。当該データ信号は、ステップ S 1 1 6 において生成した共通鍵により暗号化されて送信されてもよい。

【 0 0 7 7 】

車両側第 2 の通信装置 2 2 0 は、データ信号を受信すると、計測した時間 T_2 、及びデータ信号に含まれる情報により示される時間 T_1 に基づいて、携帯機側第 2 の通信装置 1 2 0 と車両側第 2 の通信装置 2 2 0 との間の距離を示す測距値を計算する（ステップ S 1 2 2）。詳しくは、車両側第 2 の通信装置 2 2 0 は、 $T_1 - T_2$ の結果を 2 で割ることで片道の信号の伝搬時間を計算する。そして、車両側第 2 の通信装置 2 2 0 は、かかる伝搬時間に信号の速度を掛けることで、携帯機側第 2 の通信装置 1 2 0 と車両側第 2 の通信装置 2 2 0 との間の距離を示す測距値を計算する。

【 0 0 7 8 】

そして、車両側第 2 の通信装置 2 2 0 は、計算した測距値が規定の条件を満たすか否かに基づいて、携帯機側通信システム 1 0 0 の認証を行う（ステップ S 1 2 4）。

【 0 0 7 9 】

以上、本実施形態に係る 2 段階認証処理の流れの一例を説明した。以下、上記説明した 2 段階認証処理の流れの一例に関する補足を行う。

10

20

30

40

50

【0080】

図3では、上記ステップS102及びステップS104において、車両側第1の通信装置210が認証要求を送信後に指示信号を送信する例を示したが、本発明はかかる例に限定されない。一例として、車両側第1の通信装置210は、認証要求を送信中に指示信号を送信してもよい。他の一例として、車両側第1の通信装置210は、認証応答を受信した場合に指示信号を送信してもよい。

【0081】

また、図3では、上記ステップS108及びステップS110において、携帯機側第1の通信装置110が認証応答を送信後に指示信号を送信する例を示したが、本発明はかかる例に限定されない。一例として、携帯機側第1の通信装置110は、認証応答を送信中に指示信号を送信してもよい。他の一例として、携帯機側第1の通信装置110は、認証要求を受信してから認証応答を送信するまでの間に、指示信号を送信してもよい。

10

【0082】

ステップS116～ステップS124に係る処理は、ステップS114における認証成否によらず、実行されてもよい。

【0083】

図3では、ステップS124において、車両側第2の通信装置220が携帯機側通信システム100の認証を行う例を示したが、本発明はかかる例に限定されない。例えば、車両側第2の通信装置220は、ステップS122において計算した測距値を、車両側第1の通信装置210に送信してもよい。そして、車両側第1の通信装置210は、受信した測距値に基づいて、携帯機側通信システム100の認証を行ってもよい。

20

【0084】

ステップS102において送信された認証要求、又はステップS108において送信された認証応答の受信が失敗した場合、図3に示した処理が再度実行される。その際、ステップS106及びステップS112において、シードの更新及びカウンタ値の変更が行われる。従って、リトライ時（即ち、今回実行時）のカウンタ値は、リトライ前（即ち、前回実行時）のカウンタ値と異なるものとなる。よって、リトライ時のシードとリトライ前のシードとが、シードの更新を経た上で一致した場合であっても、リトライ時のカウンタ値とリトライ前のカウンタ値との相違に基づいて、ステップS124における認証が最新のシードに基づく認証であることが保証される。

30

【0085】

比較例として、カウンタ値を用いずに、シードのみを使用して第2の認証処理を行う例が考えられる。比較例では、カウンタ値を参照できないので、リトライ時の第2の認証処理において使用するシードが、最新のシードであるか否かを区別することが困難である。よって、比較例では、リトライ時にも古いシードに基づいて第2の認証処理を行ってしまうおそれがあった。この点、本実施形態では、リトライ時にも最新のシードに基づいて第2の認証処理を行うことができるので、比較例と比較してセキュリティを向上させることが可能である。

【0086】

<<3. 補足>>

以上、添付図面を参照しながら本発明の好適な実施形態について詳細に説明したが、本発明はかかる例に限定されない。本発明の属する技術の分野における通常の知識を有する者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本発明の技術的範囲に属するものと了解される。

40

【0087】

例えば、上記実施形態では、携帯機側通信システム100における第1の測距用信号の送信時刻から第2の測距用信号の受信時刻までの時間 T1を示す情報がデータ信号に含まれるものと説明したが、本発明はかかる例に限定されない。データ信号は、第1の測距用信号の送信時刻及び第2の測距用信号の受信時刻に関する情報を含んでいればよい。以下

50

、データ信号に含まれる情報の他の一例を説明する。

【0088】

データ信号に含まれる情報の他の一例は、携帯機側通信システム100における第1の測距用信号の送信時刻及び第2の測距用信号の受信時刻を示す情報である。つまり、携帯機側通信システム100は、 T_1 を計算せずに、 T_1 の始期と終期のタイムスタンプを送信してもよい。

【0089】

データ信号に含まれる情報の他の一例は、第1の測距用信号の送信時刻から第2の測距用信号の受信時刻までの時間に基づき計算された測距値である。つまり、携帯機側通信システム100は、測距値を計算し、計算した測距値をデータ信号に含めて送信してもよい。例えば T_2 が固定値である場合、携帯機側通信システム100は、 T_1 を計測することで、測距値を計算することができる。

10

【0090】

例えば、上記実施形態では、携帯機側通信システム100が第1の測距用信号を送信する例を説明したが、本発明はかかる例に限定されない。例えば、車両側通信システム200が第1の測距用信号を送信してもよい。その場合、携帯機側通信システム100は、第1の測距用信号を受信すると、その応答として第2の測距用信号を送信する。そして、携帯機側通信システム100は、第1の測距用信号の受信時刻から第2の測距用信号の受信時刻までの時間 T_2 を示す情報を含むデータ信号を送信する。他方、車両側通信システム200は、第1の測距用信号の送信時刻から第2の測距用信号の受信時刻までの時間 T_1 と、データ信号に含まれる時間 T_2 とに基づいて、測距値を計算する。また、 T_2 は固定値であってもよく、その場合、車両側通信システム200は、 T_1 を計測することで、計測した T_1 及び固定値である T_2 に基づいて測距値を計算することができる。そのため、 T_2 を示す情報を含むデータ信号の送受信は省略されてもよい。

20

【0091】

例えば、上記実施形態では、伝搬時間に基づいて測距値を計算する例を説明したが、本発明はかかる例に限定されない。例えば、電波強度に基づいて測距値が計算されてもよい。

【0092】

例えば、上記実施形態では、第1の無線通信規格においてUHF帯及びLF帯の信号が使用され、第2の無線通信規格においてUWBを用いた信号が使用される例を説明したが、本発明はかかる例に限定されない。一例として、第1の無線通信規格又は第2の無線通信規格として、Bluetooth(登録商標)、Wi-Fi(登録商標)、NFC(Near Field Communication)、又は赤外線を使用する無線通信規格等が、用いられてもよい。

30

【0093】

例えば、上記実施形態では、携帯機側通信システム100が被認証者であり、車両側通信システム200が認証者である例を説明したが、本発明はかかる例に限定されない。携帯機側通信システム100が認証者であり、車両側通信システム200が被認証者であってもよい。

【0094】

例えば、上記実施形態では、車両側通信システム200が車両に搭載される例を説明したが、本発明はかかる例に限定されない。車両側通信システム200は、車両以外の航空機、又は船舶等の任意の移動体に搭載されてもよい。ここで、移動体とは、移動する装置である。

40

【0095】

例えば、上記実施形態では、本発明がスマートエントリーシステムに適用される例を説明したが、本発明はかかる例に限定されない。本発明は、無線通信を行う任意のシステムに適用可能である。例えば、携帯機、車両、スマートフォン、ドローン、家、及び家電製品等のうち任意の2つの装置を含むペアに、本発明は適用可能である。なお、ペアは、2つの同じ種類の装置を含んでいてもよいし、2つの異なる種類の装置を含んでいてもよい。

50

【 0 0 9 6 】

なお、本明細書において説明した各装置による一連の処理は、ソフトウェア、ハードウェア、及びソフトウェアとハードウェアとの組合せのいずれを用いて実現されてもよい。ソフトウェアを構成するプログラムは、例えば、各装置の内部又は外部に設けられる記録媒体（非一時的な媒体：non-transitory media）に予め格納される。そして、各プログラムは、例えば、本明細書において説明した各装置を制御するコンピュータによる実行時にRAMに読み込まれ、CPUなどのプロセッサにより実行される。上記記録媒体は、例えば、磁気ディスク、光ディスク、光磁気ディスク、フラッシュメモリ等である。また、上記のコンピュータプログラムは、記録媒体を用いずに、例えばネットワークを介して配信されてもよい。

10

【 0 0 9 7 】

また、本明細書においてシーケンス図を用いて説明した処理は、必ずしも図示された順序で実行されなくてもよい。いくつかの処理ステップは、並列的に実行されてもよい。また、追加的な処理ステップが採用されてもよく、一部の処理ステップが省略されてもよい。

【 符号の説明 】

【 0 0 9 8 】

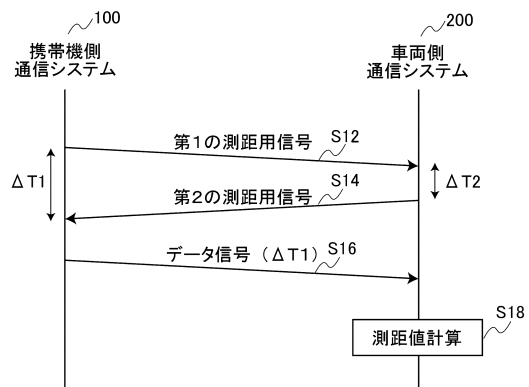
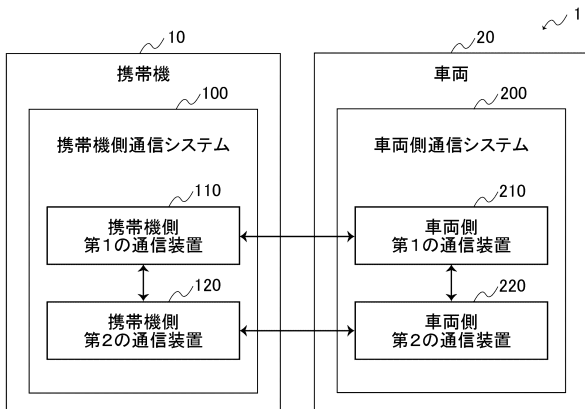
1：システム、 10：携帯機、 20：車両、 100：携帯機側通信システム、 110：携帯機側第1の通信装置、 120：携帯機側第2の通信装置、 200：車両側通信システム、 210：車両側第1の通信装置、 220：車両側第2の通信装置

【 図面 】

20

【 図 1 】

【 図 2 】

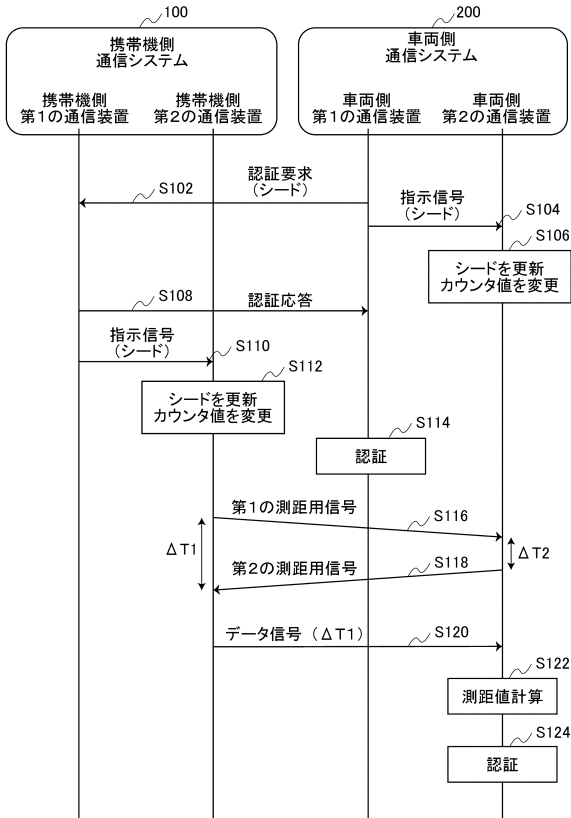


30

40

50

【図 3】



10

20

30

40

50

フロントページの続き

(51)国際特許分類

B 6 0 R 25/24 (2013.01)

F I

B 6 0 R 25/24

テーマコード (参考)

Fターム (参考)

FF27 FF36 HH01 JJ03 JJ05

5K067 AA30 BB03 EE02 EE25 HH36 JJ51