

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年1月9日(09.01.2020)



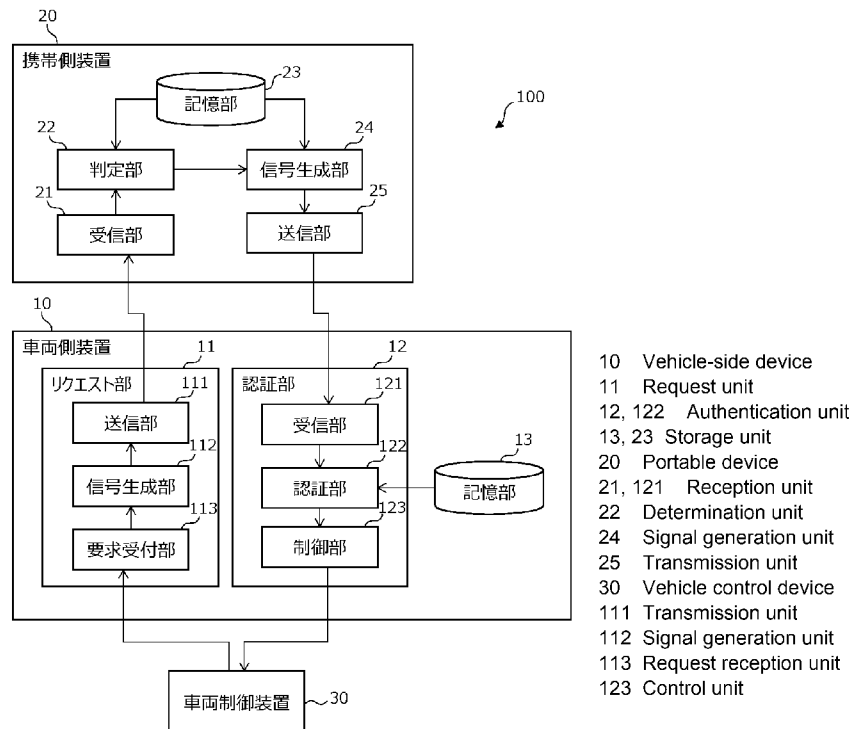
(10) 国際公開番号

WO 2020/008698 A1

- (51) 国際特許分類:
E05B 49/00 (2006.01) *G08C 17/00* (2006.01)
B60R 25/24 (2013.01) *H04B 1/3827* (2015.01)
- (21) 国際出願番号: PCT/JP2019/016283
- (22) 国際出願日: 2019年4月16日(16.04.2019)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2018-129259 2018年7月6日(06.07.2018) JP
- (71) 出願人: 株式会社デンソー (DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町1丁目1番地 Aichi (JP).
- (72) 発明者: 馬場 厚志 (BABA Atsushi); 〒4488661 愛知県刈谷市昭和町1丁目1番地 株式会社デンソー内 Aichi (JP).
- (74) 代理人: 加藤 真司, 外 (KATO Shinji et al.); 〒1500021 東京都渋谷区恵比寿西1-5-8 D I S 恵比寿ビル6階 K S I パートナーズ法律特許事務所 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) Title: VEHICLE AUTHENTICATION SYSTEM, VEHICLE-SIDE DEVICE, PORTABLE DEVICE, VEHICLE AUTHENTICATION METHOD, AND VEHICLE AUTHENTICATION PROGRAM

(54) 発明の名称: 車両用認証システム、車両側装置、携帯側装置、車両用認証方法、及び車両用認証プログラム



(57) Abstract: A vehicle authentication system (100) in which a vehicle-side device (10) and a portable device (20) are associated by authentication information, wherein the vehicle-side device (10) comprises: a transmission unit (111) that wirelessly transmits a request signal including a request (r) in a low-frequency band, and including noise (n) having a

MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告（条約第21条(3)）

prescribed intensity distribution in a high-frequency band; and a control unit (123) that performs a prescribed control in a vehicle (C) when an answer signal including authentication information is received by a reception unit (121), and the portable device (20) comprises: a determination unit (22) that determines whether the wireless signal received by a reception unit (21) is the request signal including a request in a low-frequency band, and including noise having a prescribed intensity distribution in a high-frequency band; and a transmission unit (25) that wirelessly transmits the answer signal including the authentication information when the wireless signal received by the reception unit (21) is determined by the determination unit (22) to be the request signal including a request in a low-frequency band, and including noise having a prescribed intensity distribution in a high-frequency band.

(57) 要約：車両側装置（10）と携帯側装置（20）とが認証情報によって関連付けられた車両用認証システム（100）であって、車両側装置（10）は、低周波数帯域に要求（r）を含み、高周波数帯域に所定の強度分布を有するノイズ（n）を含むリクエスト信号を無線送信する送信部（111）と、受信部（121）にて認証情報を含むアンサー信号を受信した場合に、車両（C）に所定の制御を行う制御部（123）とを備え、携帯側装置（20）は、受信部（21）にて受信した無線信号が、低周波数帯域に要求を含み、高周波数帯域に所定の強度分布のノイズを含むリクエスト信号であるか否かを判定する判定部（22）と、判定部（22）にて、受信部（21）にて受信した無線信号が、低周波数帯域に要求を含み、高周波数帯域に所定の強度分布のノイズを含むリクエスト信号であると判定した場合に、認証情報を含むアンサー信号を無線送信する送信部（25）とを備えている。

明 細 書

発明の名称：

車両用認証システム、車両側装置、携帯側装置、車両用認証方法、及び車両用認証プログラム

関連出願への相互参照

[0001] 本出願は、2018年7月6日に提出された日本出願番号2018-129259号に基づくものであって、その優先権の利益を主張するものであり、その特許出願のすべての内容が、参照により本明細書に組み入れられる。

技術分野

[0002] 本開示は、車両認証に用いる車両用認証装置、車両用認証方法および車両用認証プログラムに関するものである。

背景技術

[0003] 車両をキーレスで制御する技術としては、車両利用者が携帯機のボタンを操作することで、携帯機から車両に信号が送信されて、車両がドアロックの開錠を行う技術が知られている。

[0004] 近年では、いわゆるスマートキーシステムが採用され、利用者の更なる利便性向上が図られている。スマートキーシステムでは、利用者が携帯機を持っていれば、利用者が携帯機を操作しなくとも、携帯機と車両との自動通信によりドアの開錠、エンジンの始動等の車両制御を行うことができる。スマートキーシステムでは、車両からリクエスト信号が送信され、利用者が携帯する携帯機（即ち、スマートキー）でリクエスト信号を受信する。スマートキーを携帯する利用者が車両のごく近傍におり、携帯機がリクエスト信号受信可能であれば、携帯機は認証情報を含むアンサー信号を送信する。車両側ではアンサー信号を受信して、そこに含まれる認証情報を検証して認証を行い、認証に成功すれば車両制御を行う。

[0005] しかし、このようなスマートキーシステムは、いわゆるリレーアタックと称される不正攻撃技術により、正規の利用者の意図に反して悪用され、車両

利用者に不利益を引き起こす場合がある。

[0006] リレーアタックでは、攻撃者は、一例として車両近傍と使用者の近傍にそれぞれ増幅中継器を配置し、正規のリクエスト信号を増幅させて携帯機まで遠隔中継する。不正な中継器を経由してはいるものの、リクエスト信号自体は正規であるため、携帯機はアンサー信号を発信する。このため車両のセキュリティは不正に解除されてしまい、利用者のあずかり知らぬところで車上狙いや車両盗難被害を許してしまう。

[0007] このような問題に対応するため、リクエスト信号の強度を変化させるように車両側送信部を制御し、この強度変化パターンを携帯機に検出させることで、不正なリクエスト信号を検出し、リレーアタックを防止する方法が提案されている（特許文献１）。

先行技術文献

特許文献

[0008] 特許文献１：特開２０１０－１８５１８６号公報

発明の概要

[0009] 本発明者の詳細な検討の結果、特許文献１に記載のシステムでは、以下の課題が発見された。すなわち、車両側では本来の開錠用のリクエスト信号とは別の信号として、リレーアタック防止のための強度測定用信号を送信する必要があった。

[0010] そこで、本開示は、リクエスト信号とは別のリレーアタック防止用の信号を送信しなくてもリレーアタックを検知できる車両用認証システムを提供することを目的とする。

[0011] 上記目的を達成するために、本開示の第１の態様は、車両に搭載された車両側装置と、可搬性を有する携帯側装置とからなり、前記車両側装置と前記携帯側装置とが認証情報によって関連付けられた車両用認証システムであって、前記車両側装置は、第１の周波数帯域に要求を含み、前記第１の周波数帯域よりも高周波側の第２の周波数帯域に所定の強度分布を有するノイズを含むリクエスト信号を無線送信する車両側送信部と、無線信号を受信する車

両側受信部と、前記車両側受信部にて前記認証情報を含むアンサー信号を受信した場合に、前記車両に所定の制御を行う制御部とを備え、前記携帯側装置は、無線信号を受信する携帯側受信部と、前記携帯側受信部にて受信した前記無線信号が、前記第1の周波数帯域に前記要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布の前記ノイズを含む前記リクエスト信号であるか否かを判定する判定部と、前記判定部にて、前記携帯側受信部にて受信した前記無線信号が、前記第1の周波数帯域に前記要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布の前記ノイズを含む前記リクエスト信号であると判定した場合に、前記認証情報を含むアンサー信号を無線送信する携帯側送信部とを備えた構成を有している。

[0012] この構成によれば、車両側装置は第1の周波数帯域の要求と高周波側の第2の周波数帯域の所定の強度分布のノイズとを含むリクエスト信号を無線送信する。リレーアタックが行われる場合には、中継器の周波数特性によって、リクエスト信号のノイズの強度は一部帯域（特に高周波側）において減衰し、あるいは、ノイズの一部帯域（特に高周波側）または全部がカットされて、もとの強度分布が変更される。このため、リクエスト信号が第2周波数帯域に所定の強度分布を有する場合に、携帯側装置がアンサー信号を送信することで、リレーアタックがない場合にアンサー信号を送信することができる。このように、リクエスト信号自体に所定の強度分布のノイズを含めることで、リクエスト信号とは別のリレーアタック防止用の信号を送信することなくリレーアタックを検知できる。

[0013] また、本開示の他の態様は、車両に搭載され、認証情報によって携帯側装置と関連付けられて車両用認証システムを構成する車両側装置であって、この車両側装置は、第1の周波数帯域に要求を含み、前記第1の周波数帯域よりも高周波側の第2の周波数帯域に所定の強度分布を有するノイズを含むリクエスト信号を無線送信する送信部と、無線信号を受信する受信部と、前記リクエスト信号に対応して前記受信部にて前記認証情報を含むアンサー信号を受信した場合に、前記車両に所定の制御を行う制御部とを備えた構成を有

している。

[0014] また、本開示のさらに他の態様は、認証情報によって車両側装置に関連付けられて車両用認証システムを構成する携帯側装置であって、この携帯側装置は、無線信号を受信する受信部と、前記受信部にて受信した前記無線信号が、第1の周波数帯域に要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布を有するノイズを含むリクエスト信号であるか否かを判定する判定部と、前記判定部にて、前記受信部にて受信した前記無線信号が、第1の周波数帯域に要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布を有するノイズを含む前記リクエスト信号であると判定した場合に、前記認証情報を含むアンサー信号を無線送信する構成を有している。

[0015] また、本開示の他の態様は、車両に搭載された車両側装置と、可搬性を有する携帯側装置とからなり、前記車両側装置と前記携帯側装置とが認証情報によって関連付けられた車両用認証システムにおける車両認証方法であって、この車両認証方法は、前記車両側装置が、第1の周波数帯域に要求を含み、前記第1の周波数帯域よりも高周波側の第2の周波数帯域に所定の強度分布を有するノイズを含むリクエスト信号を送信するステップと、前記携帯側装置が、無線信号を受信するステップと、前記携帯側装置が、前記無線信号として、前記第1の周波数帯域に前記要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布の前記ノイズを含む前記リクエスト信号を受信した場合に、前記認証情報を含むアンサー信号を無線送信するステップと、前記車両側装置が、無線信号を受信するステップと、前記車両側装置が、前記無線信号として前記認証情報を含むアンサー信号を受信した場合に、前記車両に所定の制御を行うステップとを含む構成を有している。

[0016] 本開示の他の態様は、車両用認証プログラムであって、この車両用認証プログラムは、車両に搭載されて、認証情報によって携帯側装置と関連付けられて車両用認証システムを構成する車両側装置に、第1の周波数帯域に前記要求を含み、前記第1の周波数帯域よりも高周波側の第2の周波数帯域に前記所定の強度分布の前記ノイズを含むリクエスト信号を無線送信する送信ス

テップと、無線信号を受信する受信ステップと、前記リクエスト信号に対応して前記認証情報を含むアンサー信号を受信した場合に、車両に所定の制御を行う制御ステップとを実行させる構成を有している。

[0017] 本開示の他の態様は、車両用認証プログラムであって、この車両用認証プログラムは、可搬性を有し、認証情報によって車両側装置に関連付けられて車両用認証システムを構成する携帯側装置に、無線信号を受信する受信ステップと、前記受信ステップにて受信した前記無線信号が、第1の周波数帯域に要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布を有するノイズを含むリクエスト信号であるか否かを判定する判定ステップと、前記判定部にて、前記受信部にて受信した前記無線信号が、第1の周波数帯域に要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布を有するノイズを含む前記リクエスト信号であると判定した場合に、前記認証情報を含むアンサー信号を無線送信する送信ステップとを実行させる構成を有している。

図面の簡単な説明

[0018] 本開示についての上記目的およびその他の目的、特徴や利点は、添付の図面を参照しながら下記の詳細な記述により、より明確になる。その図面は、
[図1]図1は、車両用認証システムの通常の使用態様とリレーアタックとを説明する図であり、
[図2]図2は、本開示の実施の形態の車両用認証システムの構成を示すブロック図であり、
[図3]図3は、本開示の実施の形態のリクエスト信号の周波数ごとの強度を示すグラフであり、
[図4]図4は、本開示の実施の形態の判定部における処理を説明する図であり、
[図5]図5は、リレーアタックを受けたリクエスト信号の周波数ごとの強度分布を示すグラフであり、
[図6]図6は、本開示の実施の形態の判定部におけるリレーアタックが行われ

た場合の処理を説明する図であり、

[図7]図7は、本開示の実施の形態の車両用認証システムにおいて実行される車両用認証方法のフロー図である。

発明を実施するための形態

[0019] 以下に説明する実施の形態は、本開示を実施する場合の一例を示すものであって、本開示を以下に説明する具体的構成に限定するものではない。本開示の実施にあたっては、実施の形態に応じた具体的構成が適宜採用されてよい。

[0020] 図1は、車両用認証システムの通常の使用態様とリレーアタックとを説明する図である。図1において、上段は、車両用認証システム100の通常の使用態様を示している。車両用認証システム1は、車両側装置10と携帯側装置20とからなる。車両側装置10は、車両に搭載され、携帯側装置20は、可搬性を有するスマートキーSに内蔵される。

[0021] 車両側装置10と携帯側装置20とは、認証情報によって互いに関連付けられている。したがって、携帯側装置20は、認証情報によって関連付けられた特定の車両側装置10に対して有効に用いられる。1つの携帯側装置20が認証情報によって関連付けられる車両側装置10は複数存在していてもよい。ただし、その数は、同一の認証情報に関連付けられた車両側装置10が街中で偶然に接近する確率が極めて少なくなる程度に少ないものとする。また、1つの車両側装置10に対応する携帯側装置20が複数用意されていてもよい。

[0022] 図1の上段に示すように、通常の使用態様では、車両Cに備えられた車両側装置10からリクエスト信号が無線送信され、これを車両側装置10の近傍にいるユーザUが携帯する携帯側装置20で受信する。リクエスト信号の受信可能範囲に携帯側装置20が存在する場合には、携帯側装置20はリクエスト信号を受信する。携帯側装置20は、リクエスト信号に含まれる要求に従って、認証情報を含むアンサー信号を無線送信する。車両側装置10は、携帯側装置20からのアンサー信号に含まれる認証情報を用いて認証を行

う。車両側装置 10 は、認証が成功すると、車両制御装置 30 を制御して、ドアロックを開錠する、エンジンを始動する等の所定の車両制御を行う。

[0023] ここで、車両側装置 10 から送信されるリクエスト信号としては、意図しない認証の実行を防止するために、通信範囲が比較的狭い LF (kHz 帯) 信号が用いられる。これによって、携帯側装置 20 を所持したユーザが車両から十分に離れている場合には認証を行わないようにすることが可能となる。一方、携帯側装置 20 から送信されるアンサー信号としては、通信範囲が比較的広い RF (MHz 帯) 信号が用いられる。

[0024] 図 1 の下段は、リレーアタックを受けている状況を示している。リレーアタックを受けると、携帯側装置 20 を所持しているユーザ U が車両 C から十分に離れているにもかかわらず、悪意のある第三者（以下、「攻撃者」という。）A によって、車両側装置 10 において認証が行われ、車両 C のドアロックの開錠、エンジン始動等の車両制御が行われてしまう。上述のように、リクエスト信号の受信可能範囲は比較的狭い。したがって、通常は、携帯側装置 20 が車両側装置 10 から十分に離れると、携帯側装置 20 はリクエスト信号を受信できなくなり、携帯側装置 20 からアンサー信号が送信されることもない。

[0025] 攻撃者 A は、車両側装置 10 と、車両側装置 10 から十分に離れた携帯側装置 20 との間に、1 つ又は複数の中継器 40 を用意することで、リクエスト信号を携帯側装置 20 まで伝達する。そうすると、携帯側装置 20 は、車両側装置 10 から十分に離れているにもかかわらず、リクエスト信号を受信でき、受信したリクエスト信号に対応してアンサー信号を送信してしまう。このアンサー信号が車両側装置 10 に届くと、車両側装置 10 は認証を行い、対応する種々の車両制御を許してしまう。

[0026] 本実施の形態の車両用認証システムは、上記のようなリレーアタックを防止するための構成を有する。以下、本実施形態を説明する。

[0027] 図 2 は、本開示の実施の形態の車両用認証システムの構成を示すブロック図である。車両用認証システム 100 は、車両側装置 10 と、携帯側装置 2

0と、車両制御装置30を備えている。車両側装置10及び車両制御装置30は、車両に搭載される。車両側装置10は、特定の携帯側装置20と認証情報によって関連付けられている。このように認証情報によって互いに関連付けられた車両側装置10と携帯側装置20とで、車両制御装置30を制御するための車両用認証システム100が構成される。

[0028] 車両側装置10は、リクエスト部11と、認証部12と、記憶部13とを備えている。リクエスト部11は、携帯側装置20に対してリクエスト信号を無線送信する。認証部12は、リクエスト信号に対応して携帯側装置20から送信されてきたアンサー信号に基づいて、車両制御装置30を制御する。

[0029] なお、1台の車両に複数のリクエスト部11が設けられていてもよい。すなわち、リクエスト信号が車内にのみ届くように設置されたリクエスト部11、リクエスト信号が車外における車両近傍にのみ届くように設置されたリクエスト部11等の複数のリクエスト部11が車両に設けられていてよい。また、図2では、リクエスト部11と認証部12とが一体となって車両側装置10を構成しているが、これらが別体となってもよい。

[0030] リクエスト部11は、送信部111と、信号生成部112と、要求受付部113とを備えている。要求受付部113は、車両制御装置30から要求を受け付ける。例えば、ユーザがエンジンスターボタンを押下すると、車両制御装置30は、エンジンスターの要求をリクエスト部11に出力する。あるいは、ユーザがドアノブに触れると、車両制御装置30は、ドアロックの開錠又は施錠の要求をリクエスト部11に出力する。要求受付部113が要求を受け付けると、信号生成部112は、リクエスト信号を生成する。

[0031] 図3は、本開示の実施の形態のリクエスト信号の周波数ごとの強度を示すグラフである。図3に示すように、リクエスト信号は、要求rとノイズnとを含む。リクエスト信号において、要求rの周波数帯域とノイズnの周波数帯域とは分離している。また、ノイズnの周波数帯域は、要求rの周波数帯域よりも高い。すなわち、リクエスト信号は、低周波数側に要求rを含み、

かつ、高周波側にノイズ n を含む。また、ノイズ n は広い周波数帯域（即ち、広帯域）に亘っている。さらに、本実施の形態では、ノイズ n は、当該広帯域に亘って強度が一定であり、即ち、ホワイトノイズである。

[0032] 送信部 111 は、信号生成部 112 にて生成されたリクエスト信号を無線送信する。

[0033] 認証部 12 は、受信部 121 と、認証部 122 と、制御部 123 とを備えている。受信部 121 は、無線信号を受信する。後述するように、携帯側装置 20 は、リクエスト信号に応じて認証情報を含むアンサー信号を無線送信するので、受信部 121 は、このアンサー信号を受信する。認証部 122 は、受信部 121 で受信した無線信号の認証を行う。認証部 122 は、無線信号に含まれる認証情報を用いて認証を行う。記憶部 13 には、車両側装置 10 と携帯側装置 20 とを関連付ける認証情報が記憶されている。認証部 122 は、記憶部 13 に記憶された認証情報と、受信部 121 にて受信した無線信号に含まれる認証情報とを照合することにより認証を行う。

[0034] 制御部 123 は、認証部 122 における認証が成功した場合、即ち、記憶部 13 に記憶された認証情報と、受信部 121 にて受信した無線信号に含まれる認証情報とが一致した場合には、車両制御装置 30 に、要求を許可する指令を出力することで車両を制御する。車両制御装置 30 は、この指令に従ってドアロックの開錠又は施錠、エンジン始動等の車両制御を行う。

[0035] 携帯側装置 20 は、受信部 21 と、判定部 22 と、記憶部 23 と、信号生成部 24 と、送信部 25 とを備えている。受信部 21 は、車両側装置 10 から無線送信されてきたリクエスト信号を受信する。判定部 22 は、受信部 21 にて受信したリクエスト信号がリレーアタックで用いられる中継器を経たものであるか否かを判定する。具体的には、判定部 22 は、受信部 21 にて受信したリクエスト信号が、低周波数側に要求を含み、かつ、高周波数側に所定の強度分布を有するノイズを含むか否かを判定する。

[0036] 図 4 は、本開示の実施の形態の判定部における処理を説明する図である。判定部 22 は、ローパスフィルタ 221 と、減算器 222 とを備えている。

受信部 2 1 にて受信したリクエスト信号は、低周波数側に要求 r を含み、高周波数側の広帯域にノイズ n を含む。ローパスフィルタ 2 2 1 は、このリクエスト信号について高周波成分をカットする。これによって、要求 r の部分のみが取り出される。判定部 2 2 は、この要求 r を解析して要求 r の内容を把握する。

[0037] 減算器 2 2 2 は、受信したリクエスト信号からローパスフィルタ 2 2 1 の出力を減算することで、ノイズ成分のみを取り出す。判定部 2 2 は、このノイズ成分の強度分布が、正規のリクエスト信号のノイズの強度分布と一致するか否かを判定する。記憶部 2 3 には、正規のリクエスト信号のノイズの強度分布が記憶されており、判定部 2 2 は、記憶部 2 3 を参照することで、正規のリクエスト信号のノイズの強度分布と減算器 2 2 2 で得られたノイズの強度分布とを比較する。

[0038] 判定部 2 2 において、受信部 2 1 にて受信したリクエスト信号がリレーアタックで用いられる中継器を経たものでないと判定された場合に、信号生成部 2 4 は、アンサー信号を生成する。このアンサー信号には、車両側装置 1 0 と共通にもつ認証情報が含まれる。送信部 2 5 は、信号生成部 2 4 で生成されたアンサー信号を無線送信する。

[0039] 次に、リレーアタックが行われた場合の携帯側装置 2 0 における動作を説明する。図 5 は、リレーアタックを受けたリクエスト信号の周波数ごとの強度分布を示すグラフである。上述のように、リレーアタックでは 1 台又は複数台の中継器が用いられる。この中継器はリクエスト信号を増幅する増幅器としての機能を有する。中継器を経たリクエスト信号は、この増幅器の周波数特性によって、高周波帯域がカットされる。すなわち、図 5 に示すように、リクエスト信号には、高周波側に、所定の周波数帯域に亘って信号強度が一定であるホワイトノイズが印加されているので、中継器において、図 5 において破線で示すこのホワイトノイズの全部又は高周波側の一部がカットされる。よって、リレーアタックを受けたリクエスト信号のノイズ n は、強度分布が変形したノイズ n_m となる。

[0040] 図6は、本開示の実施の形態の判定部におけるリレーアタックが行われた場合の処理を説明する図である。受信部21は、中継器を経てノイズの強度分布が変形したリクエスト信号を受信する。ローパスフィルタ221は、このようなリクエスト信号の高周波成分をカットして要求 r を取り出す。減算器222は、受信したリクエスト信号から、ローパスフィルタ221にて取り出された要求 r を減算することで、ノイズ n_m を取り出す。

[0041] そして、判定部22は、このノイズ n_m の周波数ごとの強度部分が記憶部23に記憶された強度分布と一致するか否かを判定する。リレーアタックを受けて強度分布が変形したノイズ n_m の強度分布と記憶部23に記憶されている正規のリクエスト信号におけるノイズの強度分布とは一致しないので、判定部22は、リレーアタックを受けたものと判定する。

[0042] この場合には、信号生成部24は、アンサー信号を生成せず、よって、送信部25もアンサー信号を送信しない。したがって、車両側装置10では、リクエスト信号を送信したにもかかわらず、携帯側装置20からアンサー信号を受けることはなく、リレーアタックを有効に防止できる。

[0043] なお、携帯側装置20がブザー等の警報手段を備え、判定部22にてリレーアタックを受けたと判定した場合に、警報を発するようにしてよい。また、上記の例では、信号生成部24は、判定部22にて、リレーアタックを受けたものと判定された場合に、アンサー信号を生成せず、送信部25もアンサー信号を送信しない構成であったが、これ代えて、信号生成部24は、リレーアタックを受けたと判定した場合に、車両制御を許可しない旨のアンサー信号を生成して、送信部25から送信してよい。さらに、車両にも警報手段を設けて、車両制御を許可しない旨のアンサー信号を受けたときに警報手段によって警報を発してもよい。

[0044] また、上記の実施の形態において、車両側装置10のリクエスト部11及び認証部12の構成は、コンピュータが非遷移的実体的記録媒体に格納された本開示の実施の形態の車両用認証プログラムを実行することで実現されてもよい。また、携帯側装置20の受信部21、判定部22、信号処理部24

、送信部 25 の構成も、コンピュータが非遷移的実体的記録媒体に格納された本開示の実施の形態の車両用認証プログラムを実行することで実現されてよい。

[0045] 図 7 は、本開示の実施の形態の車両用認証システムにおいて実行される車両用認証方法のフロー図である。車両用認証方法のフローは、車両側装置 10 と携帯側装置 20 とによって実行される。まず、ステップ S 711 で、車両側装置 10 の要求受付部 113 が、車両制御装置 30 から要求を受け付ける。ステップ S 712 で、信号生成部 112 は、要求受付部 113 にて要求を受けたことに応答してリクエスト信号を生成する。

[0046] ステップ S 713 で、送信部 111 は、リクエスト信号を無線送信し、ステップ S 721 で、携帯側装置 20 の受信部 21 にてこれを受信する。ステップ S 722 で、判定部 22 は、受信部 21 にて受信したリクエスト信号がリレーアタックを受けたものであるか否を判定する。ステップ S 722 が要件を満たす場合、すなわち判定部 22 が、リレーアタックを受けたものと判定した場合には、アンサー信号の生成及び送信を行わずに処理を終了する。なお、これに代えて、ステップ S 722 が要件を満たす場合、すなわちリレーアタックを受けたものと判定した場合に、認証を許可しない旨のアンサー信号を生成して送信してもよいことは上述した通りである。

[0047] ステップ S 722 が要件を満たさない場合、すなわち判定部 22 が、受信したリクエスト信号がリレーアタックを受けていないものであると判定した場合には、ステップ S 723 で、信号生成部 24 は、認証情報を含むアンサー信号を生成し、ステップ S 724 で、送信部 25 は、生成されたアンサー信号を無線送信する。

[0048] 車両側装置 10 では、ステップ S 714 で、認証部 12 の受信部 121 にてアンサー信号を受信する。ステップ S 715 で、認証部 122 は、アンサー信号に含まれる認証情報を記憶部 13 に記憶された認証情報と照合することで認証を行い、ステップ S 715 が要件を満たす場合、すなわち認証に成功すると、ステップ S 716 で、制御部 123 は、車両制御装置 30 に対し

て要求を許可する指令を出力することにより車両を制御する。一方、ステップS 7 1 5 が要件を満たさない場合、すなわち認証部 1 2 2 における認証に失敗した場合には、車両制御を行わずに処理を終了する。

[0049] 以上のように、本実施の形態の車両用認証システムによれば、リクエスト信号の高周波側に広帯域のノイズを印加するので、リクエスト信号がリレーアタックを受けて高周波成分がカットされた場合に、携帯側装置においてそのことを判定できる。よって、リクエスト信号とは別にリレーアタック防止用の信号を生成して送信しなくても、リレーアタックを検知して不正な認証を防止することができる。

[0050] なお、上記の実施の形態では、リクエスト信号に印加するノイズを所定の帯域に亘って強度が同じであるホワイトノイズとしたが、これに代えて、所定の帯域に亘って一定ではない所定の強度分布を有するノイズとしてもよい。この場合にも、携帯側装置 2 0 において、当該強度分布を記憶し、受信したリクエスト信号のノイズの周波数帯の強度分布が、この記憶された強度分布と異なるときに、リレーアタックを受けたと判定することができる。

[0051] 攻撃者の立場からは、本実施の形態の車両用認証システム 1 0 0 による防御策を回避するには、全帯域にわたって、あるいは少なくともノイズが印加されている帯域にわたって、信号を適切に増幅しなければならないが、これは簡単なことではない。よって、本実施の形態の車両用認証システム 1 0 0 は、リレーアタックを行う攻撃者に対して有効な防御策となる。

[0052] また、ノイズを印加する周波数帯域ないし強度分布は、車両ごとに異なってもよい。このようにすることで、上記の実施の形態の車両用認証システム 1 0 0 に対応したリレーアタックを行おうとしても、攻撃者は、当該車両が、どの帯域にノイズが印加されたリクエスト信号を送信するかを事前に知ることはないため、設定されている帯域を試行錯誤的に発見する必要があり、より強固な防御策となる。

[0053] 以上、本開示の実施の形態について説明したが、本開示の応用対象は上記の実施例に限られない。リレーアタックに対して耐性を持つ車両用認証技術

は、車両の駐車自動化や、将来的な実現が視野に入っている自動運転のトリガーとすることも可能である。

[0054] 更に、当該技術は、いわゆるカーセキュリティとしての車両側装置と携帯側装置との関係のみに限定して応用されるものではない。リレーアタックは近・中距離無線通信装置全般において起こりうる問題である。本開示は、例えば家庭用無線機器の情報漏洩対策や、ドローンに代表される小型無人航空機との不正通信によるプライバシー侵害対策や、貨物盗難防止などにも応用できる。

請求の範囲

[請求項1] 車両に搭載された車両側装置（１０）と、可搬性を有する携帯側装置（２０）とからなり、前記車両側装置と前記携帯側装置とが認証情報によって関連付けられた車両用認証システム（１００）であって、前記車両側装置は、

第１の周波数帯域に要求（ｒ）を含み、前記第１の周波数帯域よりも高周波側の第２の周波数帯域に所定の強度分布を有するノイズ（ｎ）を含むリクエスト信号を無線送信する車両側送信部（１１１）と、無線信号を受信する車両側受信部（１２１）と、

前記車両側受信部にて前記認証情報を含むアンサー信号を受信した場合に、前記車両に所定の制御を行う制御部（１２３）と、

を備え、

前記携帯側装置は、

無線信号を受信する携帯側受信部（２１）と、

前記携帯側受信部にて受信した前記無線信号が、前記第１の周波数帯域に前記要求を含み、かつ、前記第２の周波数帯域に前記所定の強度分布の前記ノイズを含む前記リクエスト信号であるか否かを判定する判定部（２２）と、

前記判定部にて、前記携帯側受信部にて受信した前記無線信号が、前記第１の周波数帯域に前記要求を含み、かつ、前記第２の周波数帯域に前記所定の強度分布の前記ノイズを含む前記リクエスト信号であると判定した場合に、前記認証情報を含むアンサー信号を無線送信する携帯側送信部（２５）と、

を備えた、車両用認証システム。

[請求項2] 前記判定部が、前記携帯側受信部にて受信した前記無線信号が、前記第２の周波数帯域に前記所定の強度分布を有するノイズを含まないと判定した場合には、前記携帯側送信部は、前記認証情報を含むアンサー信号を無線送信しない、請求項１に記載の車両用認証システム。

[請求項3] 前記ノイズは、前記第2の周波数帯域に亘って一定の強度分布を有するホワイトノイズである、請求項1又は2に記載の車両用認証システム。

[請求項4] 前記第2の周波数帯域は、車両毎に可変である、請求項1～3のいずれかに記載の車両用認証システム。

[請求項5] 車両に搭載され、認証情報によって携帯側装置と関連付けられて車両用認証システム（100）を構成する車両側装置（10）であって、

第1の周波数帯域に要求（r）を含み、前記第1の周波数帯域よりも高周波側の第2の周波数帯域に所定の強度分布を有するノイズ（n）を含むリクエスト信号を無線送信する送信部（111）と、

無線信号を受信する受信部（121）と、

前記リクエスト信号に対応して前記受信部にて前記認証情報を含むアンサー信号を受信した場合に、前記車両に所定の制御を行う制御部（123）と、

を備えた車両側装置。

[請求項6] 認証情報によって車両側装置に関連付けられて車両用認証システム（100）を構成する携帯側装置であって、

無線信号を受信する受信部（21）と、

前記受信部にて受信した前記無線信号が、第1の周波数帯域に要求（r）を含み、かつ、第2の周波数帯域に所定の強度分布を有するノイズ（n）を含むリクエスト信号であるか否かを判定する判定部（22）と、

前記判定部にて、前記受信部にて受信した前記無線信号が、第1の周波数帯域に要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布を有するノイズを含む前記リクエスト信号であると判定した場合に、前記認証情報を含むアンサー信号を無線送信する、携帯側装置。

[請求項7] 車両に搭載された車両側装置（１０）と、可搬性を有する携帯側装置（２０）とからなり、前記車両側装置と前記携帯側装置とが認証情報によって関連付けられた車両用認証システム（１００）における車両認証方法であって、

前記車両側装置が、第１の周波数帯域に要求（ｒ）を含み、前記第１の周波数帯域よりも高周波側の第２の周波数帯域に所定の強度分布を有するノイズ（ｎ）を含むリクエスト信号を送信するステップと、

前記携帯側装置が、無線信号を受信するステップと、

前記携帯側装置が、前記無線信号として、前記第１の周波数帯域に前記要求を含み、かつ、前記第２の周波数帯域に前記所定の強度分布の前記ノイズを含む前記リクエスト信号を受信した場合に、前記認証情報を含むアンサー信号を無線送信するステップと、

前記車両側装置が、無線信号を受信するステップと、

前記車両側装置が、前記無線信号として前記認証情報を含むアンサー信号を受信した場合に、前記車両に所定の制御を行うステップと、
を含む車両用認証方法。

[請求項8] 車両に搭載されて、認証情報によって携帯側装置（２０）と関連付けられて車両用認証システム（１００）を構成する車両側装置（１０）に、

第１の周波数帯域に要求（ｒ）を含み、前記第１の周波数帯域よりも高周波側の第２の周波数帯域に所定の強度分布のノイズ（ｎ）を含むリクエスト信号を無線送信する送信ステップと、

無線信号を受信する受信ステップと、

前記リクエスト信号に対応して前記認証情報を含むアンサー信号を受信した場合に、車両に所定の制御を行う制御ステップと、

を実行させる車両用認証プログラム。

[請求項9] 可搬性を有し、認証情報によって車両側装置（１０）に関連付けられて車両用認証システム（１００）を構成する携帯側装置（２０）に

、

無線信号を受信する受信ステップと、

前記受信ステップにて受信した前記無線信号が、第1の周波数帯域に要求（ r ）を含み、かつ、

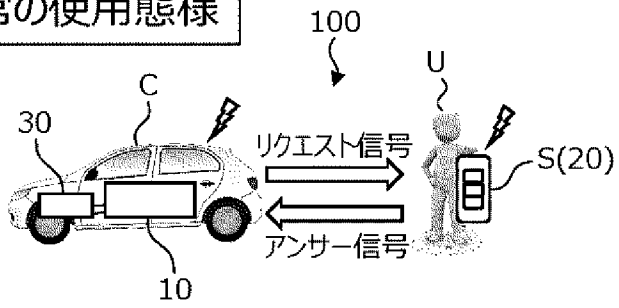
第2の周波数帯域に所定の強度分布を有するノイズ（ n ）を含むリクエスト信号であるか否かを判定する判定ステップと、

前記判定ステップにて、前記受信ステップにて受信した前記無線信号が、前記第1の周波数帯域に要求を含み、かつ、前記第2の周波数帯域に前記所定の強度分布を有するノイズを含む前記リクエスト信号であると判定した場合に、前記認証情報を含むアンサー信号を無線送信する送信ステップと、

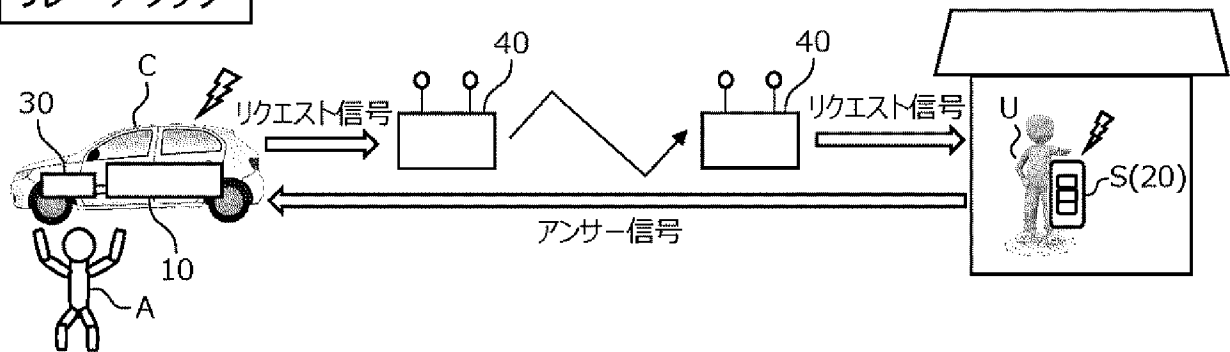
を実行させる車両用認証プログラム。

[図1]

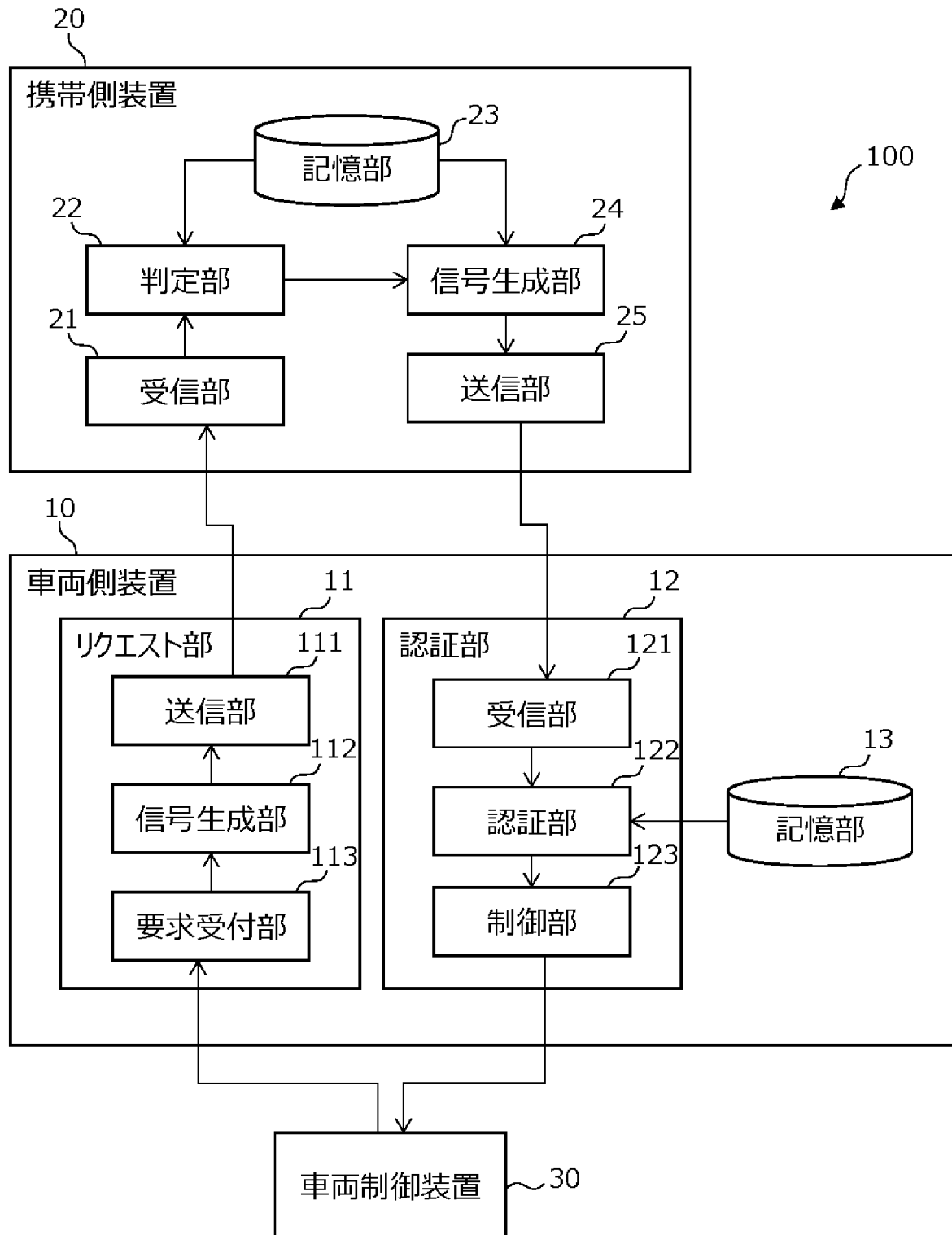
通常の使用態様

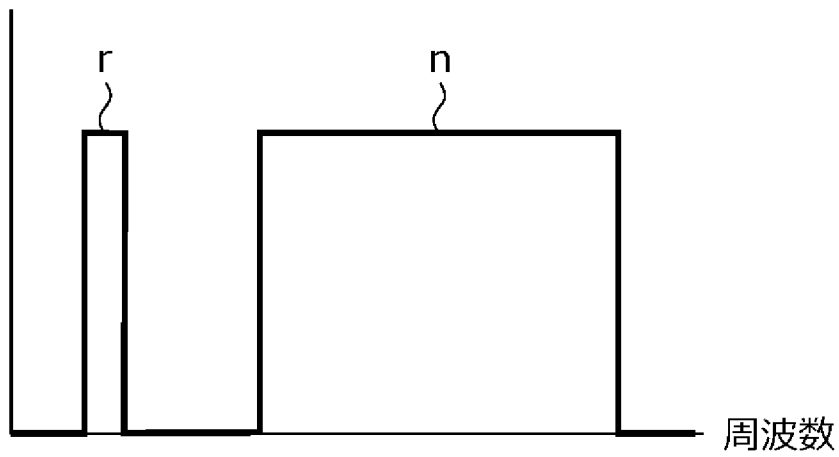


リレーアタック

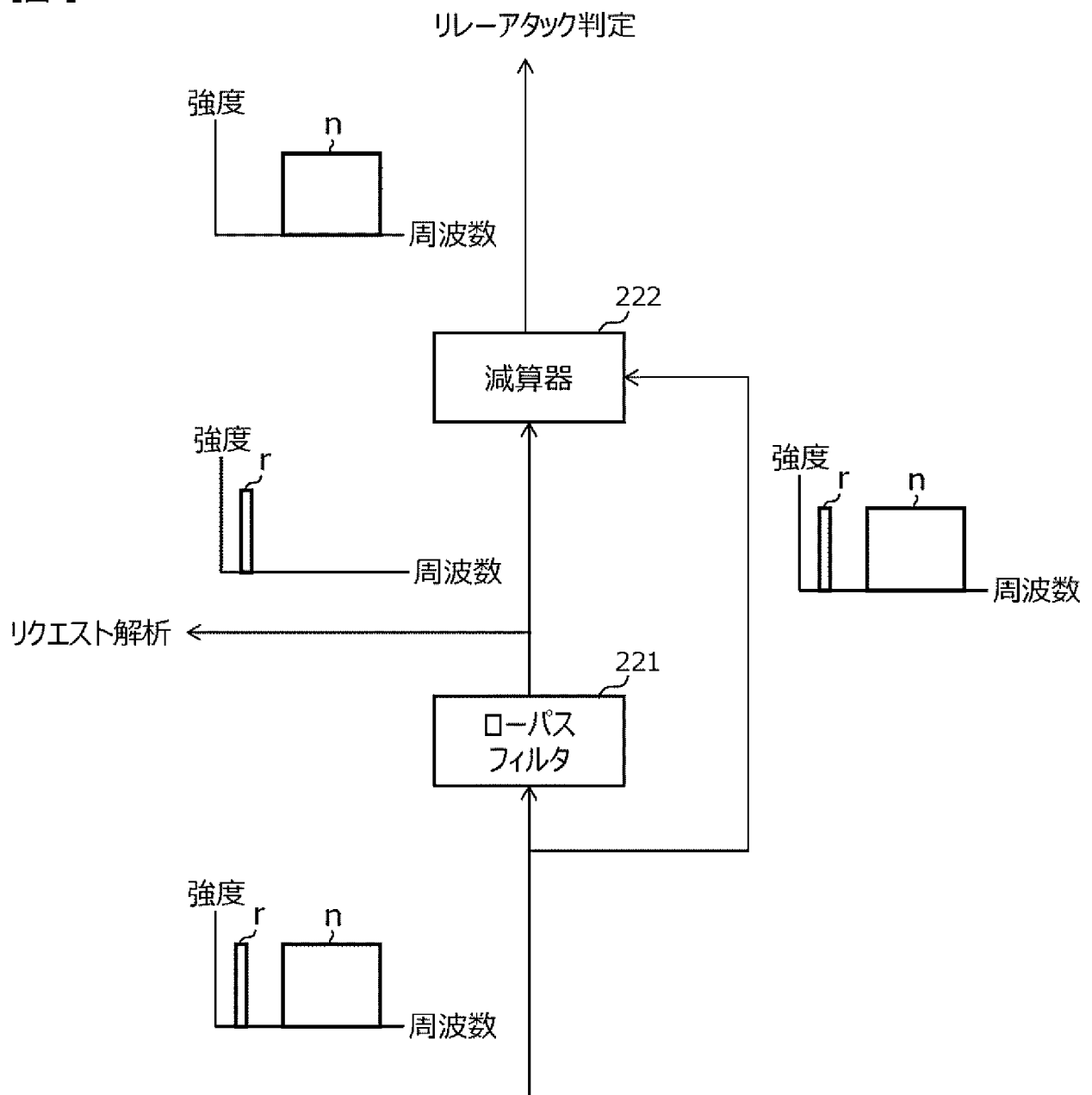


[図2]



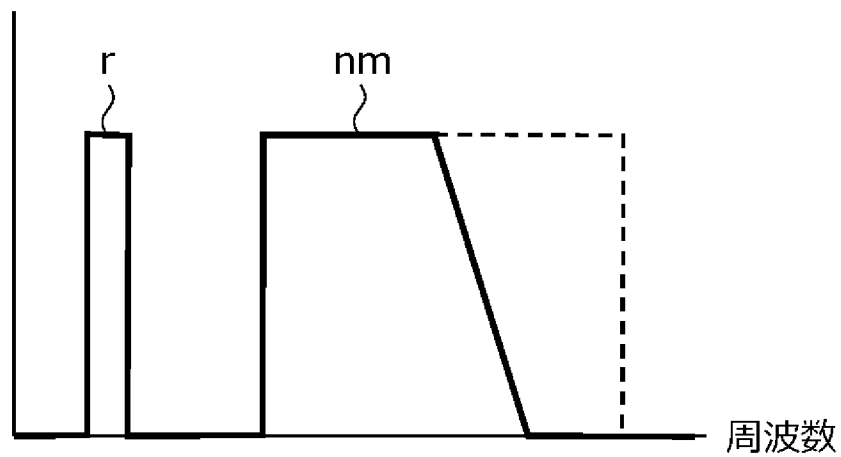
[図3]
強度

[図4]

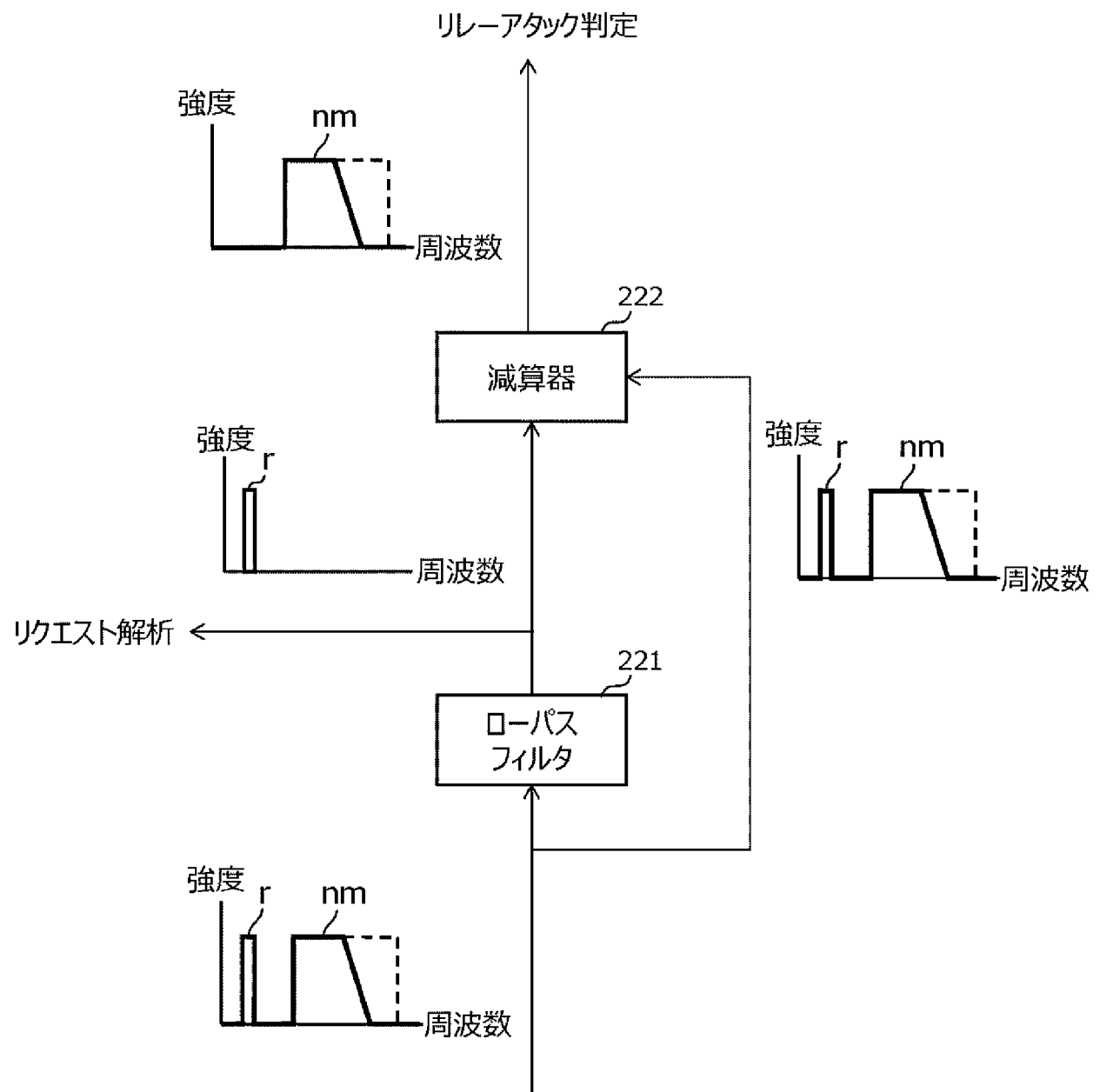


[図5]

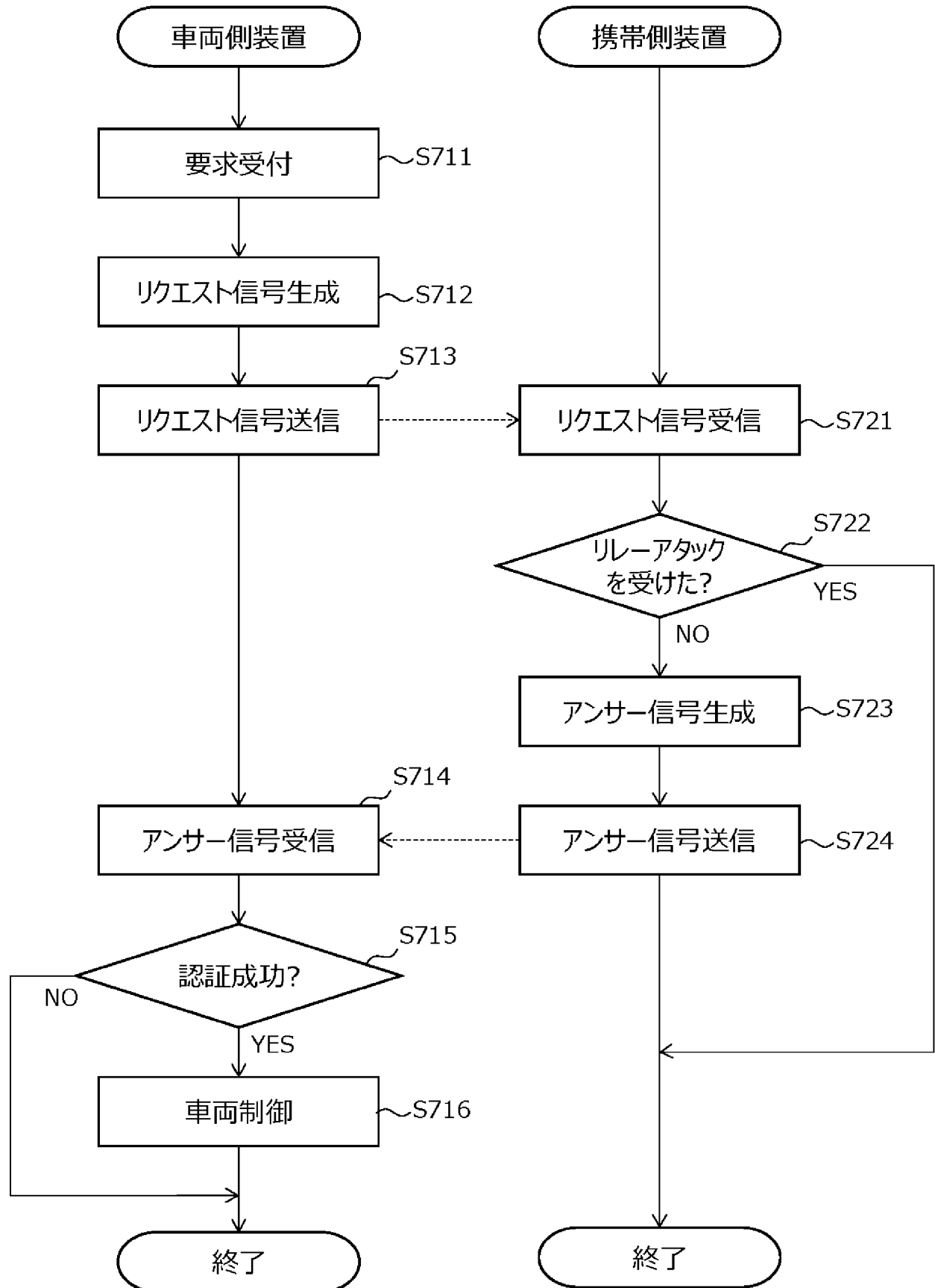
強度



[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/016283

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. E05B49/00 (2006.01) i, B60R25/24 (2013.01) i, G08C17/00 (2006.01) i, H04B1/3827 (2015.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. E05B49/00-49/04, 77/00-85/28, B60R25/24, G08C17/00, H04B1/3827

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2019

Registered utility model specifications of Japan 1996-2019

Published registered utility model applications of Japan 1994-2019

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-62651 A (DENSO CORP.) 29 March 2012, abstract, fig. 4 (Family: none)	1-9
A	JP 2012-52361 A (DENSO CORP.) 15 March 2012, abstract (Family: none)	1-9
A	JP 2008-240315 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 09 October 2008, abstract (Family: none)	1-9
A	JP 2010-185186 A (ALPS ELECTRIC CO., LTD.) 26 August 2010, abstract, paragraphs [0039]-[0041] (Family: none)	1-9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
29.05.2019

Date of mailing of the international search report
11.06.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/016283

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016/0200291 A1 (DAE DONG CO., LTD.) 14 July 2016, paragraph [0013] & WO 2015/026001 A1 & EP 3037306 A1 & KR 10-1469783 B1 & KR 10-1483153 B1 & KR 10-1483154 B1 & KR 10-1483155 B1 & CN 105473392 A	1-9

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. E05B49/00(2006.01)i, B60R25/24(2013.01)i, G08C17/00(2006.01)i, H04B1/3827(2015.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl. E05B49/00-49/04, 77/00-85/28, B60R25/24, G08C17/00, H04B1/3827

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2012-62651 A（株式会社デンソー）2012.03.29, 【要約】, 図4 （ファミリーなし）	1-9
A	JP 2012-52361 A（株式会社デンソー）2012.03.15, 【要約】 （ファミリーなし）	1-9
A	JP 2008-240315 A（松下電器産業株式会社）2008.10.09, 【要約】 （ファミリーなし）	1-9

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

29.05.2019

国際調査報告の発送日

11.06.2019

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

砂川 充

2R

9231

電話番号 03-3581-1101 内線 3285

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2010-185186 A (アルプス電気株式会社) 2010.08.26, 【要約】 【0039】 - 【0041】 (ファミリーなし)	1-9
A	US 2016/0200291 A1 (DAE DONG CO., LTD.) 2016.07.14, [0013] & WO 2015/026001 A1 & EP 3037306 A1 & KR 10-1469783 B1 & KR 10-1483153 B1 & KR 10-1483154 B1 & KR 10-1483155 B1 & CN 105473392 A	1-9