República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(21) BR 102018015354-4 A2

(22) Data do Depósito: 26/07/2018

(43) Data da Publicação Nacional: 04/02/2020

(54) Título: SISTEMA E MÉTODO DE COMUNICAÇÃO SEGURA PARA VEÍCULOS AUTOMOTORES

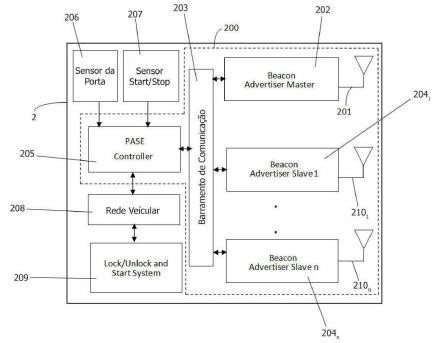
(51) Int. Cl.: H04W 4/80; G07C 9/00; B60R 25/24.

(52) CPC: H04W 4/80; G07C 9/00309; B60R 25/245.

(71) Depositante(es): UNIVERSIDADE FEDERAL DE PERNAMBUCO; FCA FIAT CHRYSLER AUTOMOVEIS BRASIL LTDA.

(72) Inventor(es): ABEL GUILHERMINO DA SILVA FILHO; RODRIGO CAMAROTTI FERREIRA DA ROCHA; VITOR ARRAIS DE SÁ; MARIA CIRENO RIBEIRO SILVEIRA; CAIO CESAR LIMA LACERDA FERREIRA; RAFAEL NUNES DE LIMA; HILSON GOMES VILAR DE ANDRADE; CARLOS ANDRÉ GUIMARÃES FERRAZ; MARCÍLIO ANDRÉ FÉLIX FEITOSA; RICARDO JOSÉ DO RÊGO BARROS; RODOLFO JOSÉ DE OLIVEIRA SOARES; LUIZ CARLOS QUINTINO DOS SANTOS; MAURICIO VIANNA DE REZENDE; GUILHERME MIGLIO DOXA.

(57) Resumo: SISTEMA E MÉTODO DE COMUNICAÇÃO SEGURA PARA VEÍCULOS AUTOMOTORES São descritos um sistema e um método de comunicação segura entre um veículo (2) e um dispositivo remoto, portado por um usuário, tal como um smartphone (3) ou um dispositivo vestível (4), os quais se comunicam a distância, através de um protocolo BLE. Através do dispositivo remoto, é possível ao usuário comandar ações, tais como a abertura de determinadas portas, ou habilitar a partida do veículo. Para tanto, o sistema (200) compreende um módulo de processamento PASE Controller (205), conectado aos sistemas e dispositivos veiculares (206, 207, 208, 209) além de conectado, através de um barramento de comunicação (203), a um módulo Beacon Advertiser Master (202) e respectiva antena (201), bem como a ao menos dois módulos Beacon Advertiser Slave (2041-n) dotados de respectivas antenas (2101-n). O dispositivo remoto/chave (3, 4) e módulo Beacon Advertiser Master (202) realizam um procedimento de autenticação primária entre estes, seguido de enlace e conexão via o código PIN da chave armazenado no Beacon Advertiser Master, e posteriormente a execução de um protocolo de autenticação mútua e, em seguida, Beacon Advertiser Master (202) habilita, em sequência, os módulos Beacon Advertiser Slave (2041-n) a respectivamente se autenticarem e realizarem o enlace com a chave (3, 4).



SISTEMA E MÉTODO DE COMUNICAÇÃO SEGURA PARA VEÍCULOS AUTOMOTORES

Campo da Invenção

[001] A presente invenção se refere a um sistema e a um método de comunicação segura que confere acesso e comando a veículos automotores, a partir da interação deste com um dispositivo de tipo *wearable* ou de comunicação, dentro de uma tecnologia BLE evoluída.

Antecedentes da Invenção

[002] Modernamente, a indústria automobilística vem presenciando um notável desenvolvimento de sistemas e dispositivos destinados a auxiliar os condutores na realização de certas tarefas, tais como, por exemplo, abertura e fechamento de portas, acionamento de vidros, ignição, e acionamento de alarmes, entre outras. Não obstante tais avanços, a possibilidade de atuação do condutor distante do veículo gera inúmeros problemas relacionados com a segurança dos mecanismos de comunicação veículo/condutor.

[003] Mais em particular, já são conhecidos na arte diversos dispositivos, sistemas e plataformas destinadas a promover uma interação do usuário com o seu veículo, de modo a permitir que algumas tarefas sejam realizadas de forma autônoma pelo veículo a partir da detecção de um sinal proveniente do usuário, ou de uma ação deste usuário. Dentre estas tecnologias conhecidas na arte, seguem abaixo alguns exemplos.

[004] O documento US 9045102 trata de sistema para abertura remota e acionamento remoto da ignição do veículo. A comunicação é realizada através de protocolo BLE, usando um conjunto de 3 antenas concentradas na parte interna frontal do veículo para minimizar fiação e avalia ser mais simples que demais sistemas conhecidos. No mesmo local, faz uso de antena LF para otimizar a determinação da intenção do condutor para a abertura do veículo.

[005] O documento US 2016/0347282 descreve um controle remoto de veículo. Utiliza do sistema de handoff, uma caixa preta dentro do veículo, para receber sinais transmitidos de um dispositivo remoto. O sistema de handoff pode prevenir o usuário do veículo de violar restrições de direção tais como viajar a uma velocidade acima da configurada ou viajar por

uma distância determinada.

[006] O documento US 2015/0048927 descreve um sistema para uso em after market. Este sistema pode travar ou destravar acesso a veículos, prédios e outros locais de forma passiva por proximidade ou por telecomando em aplicativo no smartphone.

[007] O documento US 2014/0240091 descreve um sistema onde a localização é determinada somente para dentro e fora do veículo. A localização é feita através da técnica de propagação eletromagnética (PLE – Effective Path Loss). Usa uma segunda antena, opcional, como antena de referência de forma a ter um melhor sinal para garantir resolução e determinar localização no interior ou exterior do veículo. A chave pode ser também um smartphone.

[008] O documento US 2015/0362997 demonstra um dispositivo wearable que reconhece gestos para realizar ações no veículo.

[009] O documento KR 1020160059793 descreve sistema para autenticar usuário e permitir controle do ambiente do veículo (cores, músicas, temperatura, iluminação) a partir da leitura de dados biométricos (reconhecimento de íris, batimentos cardíacos, estado emocional). Tais leituras seriam realizadas através de dispositivos wearable (smart watch, smart glass) e transmitidos via wireless para unidade de controle e autenticação do veículo.

[0010] O documento US 2016/0358389 foca em um sistema de acesso e ignição remota de veículo usando smartphone. Este utiliza três códigos distintos: de pareamento, de identificação e de autenticação armazenados no smartphone. A inserção dos códigos no smartphone pode ser realizada na montadora ou concessionária ou podem ser baixados via rede GSM, outro smartphone ou veículo habilitado. O código é armazenado em um chamado "secure memory element", recomendado pela descrição da invenção para que seja usado cartão SIM para tal. O processo de armazenagem dos códigos pode ser simultâneo ou em separado. Não utiliza criptografia adicional à do protocolo BLE. A memória segura é acessada via código de segurança.

[0011] O documento KR101680090000 descreve um dispositivo *wearable* do tipo "wristwatch" com controle de comandos do veículo por gestos e com propriedades de localização, usando técnica de fingerprinting. Para detecção de gestos utiliza de sensores

de movimento, seja magnetômetro, acelerômetro, giroscópio etc. Para a localização utiliza conjunto de quatro antenas. Realiza abertura e partida da ignição passivas, porém este não trata de questões de segurança da comunicação ou armazenamento de chaves.

[0012] O documento WO 2016/180724 ensina um sistema para acesso remoto a veículos que utiliza ondas sonoras para propagar mensagens de autenticação. Foca em técnicas para redução de consumo de energia como desligar módulos do sistema quando não utilizados ou logo após a realização de autenticação de usuário. Em relação à segurança comenta sobre "relay attacks", definindo uma região máxima de ativação para suprimir esse tipo de ataque. Não cita criptografia ou métodos de armazenamento de chaves nem como autenticação é realizada. Precisa de elemento para iniciar comunicação e, assim, diminuir consumo. Há necessidade de sincronizar relógios do "key fob" e do veículo para melhorar detecção de pisos e vales do sinal sonoro.

[0013] O documento US 2016/0183042 descreve um sistema para localização de usuários em ambiente "indoor", mas não ilustra um acesso passivo. Para tal, propõe o uso de dispositivos de comunicação ao longo do ambiente que enviam suas posições absolutas, a partir do uso de coordenadas ou outras variáveis como o piso do andar, para um receptor, o qual pode ser um celular.

[0014] O documento US 2016/0288770 descreve um sistema para entrada e partida veicular passiva. Foco maior em consumo de energia, principalmente com o automóvel desligado, em especial no tradeoff segurança versus "key-off current load" (KOL). Para tal, propõe inclusão de um novo módulo, denominado "remote sentinel" (RS), que monitora os movimentos próximos ao veículo e aciona os dispositivos, câmeras e radares, usados pelo sistema de prevenção a roubos reduzindo assim o tempo de funcionamento dos mesmos. Ou seja, ativa-os somente em caso de movimentos suspeitos próximos ao veículo. Cita mecanismos de entrada e partida passiva (PEPS) porque os mesmos compõem o mesmo subsistema do "theft-deterrent system" (TDS).

[0015] O documento WO 2016/184723 descreve sistema que tem como foco barrar "relay station attacks" (RSA) no acesso de emergência (chave dotada de transponder RFID para ignição). Para barrar tal ataque, usa elemento de autenticação e um sistema de autorização simples de ser integrado a sistemas existentes.

[0016] Por fim, o documento US 2016/0292941 descreve sistema de entrada e partida veicular passiva com foco em protocolo de comunicação entre veículo e key fob através de chaveamento de formas de modulação, tempos de cada modulação e seqüência durante troca de informações de autorização. Este utiliza inclusive chaveamento do sinal de requisição com pelo menos uma transição de modulação.

[0017] Tal como pode ser apreciado a partir das descrições supra, diversos são os mecanismos de controle de certas funcionalidades veiculares recentemente desenvolvidos para auxiliar os condutores no controle de seus veículos. Contudo, tais tecnologias afrontam a tricotomia entre o incremento no nível de proteção dos sistemas em desenvolvimento, a simplificação dos dispositivos necessários para a implementação dos sistemas veiculares, bem como a necessidade de redução no consumo de energia.

[0018] Desta forma, constitui um primeiro objetivo da presente invenção uma plataforma de comunicação veículo/usuário e de atuação de funcionalidades, a qual permita um alto grau de segurança entre as informações transmitidas e recebidas entre veículo e usuário. Constitui outro objetivo da presente invenção um sistema de comunicação seguro e baseado em uma infra-estrutura simplificada e de baixo consumo de energia.

Síntese da Invenção

[0019] Estes e outros objetivos são alcançados a partir de um sistema de comunicação segura para veículos automotores, a ser implementando entre um veículo e um dispositivo remoto/chave, via protocolo de comunicação BLE, dito dispositivo remoto podendo ser: um smartphone dotado de um sistema operacional Mobile OS o qual gerencia os módulos funcionais Security Module, BLE Manager e User Interface, além de ao menos uma antena de transmissão e recepção de sinais de RF, via protocolo de comunicação BLE; ou um dispositivo vestível dotado de um sistema operacional Embedded Firmware, o qual gerencia os módulos funcionais Security Module, BLE Manager e Input Buttons, além de ao menos uma antena de transmissão e recepção de sinais de RF, via protocolo de comunicação BLE, e sendo que o dito sistema compreende um módulo de processamento PASE Controller, conectado ao menos aos sistemas veiculares Lock/Unlock and Start System através da rede veicular e conectado diretamente ao menos os sensores de porta e ao sensor star/stop, e sendo que o dito PASE Controller é conectado, através de um

barramento de comunicação, a um módulo Beacon Advertiser Master e respectiva antena, bem como a ao menos dois módulos Beacon Advertiser Slave (204_{1-n}) dotados de respectivas antenas (210_{1-n}). Ademais, o módulo PASE Controller compreende: um módulo PASE Core interligado a uma interface de Input, a qual recebe os sinais dos ditos sensores do veículo, bem como a uma interface da rede veicular de conexão com a dita rede veicular; e um módulo de localização, o qual está conectado a uma interface de comunicação com o barramento de comunicação. O Beacon Advertiser Master compreende um módulo Link Logical Cypher diretamente conectado a um módulo Security Connection Starter e a um Authentication Module, dito módulo Link Logical Cypher é ainda conectado a uma interface de comunicação de modo a interligar o Beacon Advertiser Master ao barramento de comunicação, sendo que o módulo Security Connection Starter é interligado a uma interface de RF, de modo a transmitir e receber mensagens, via antena, entre o Beacon Advertiser Master e a chave. A chave e módulo Beacon Advertiser Master realizam um procedimento de autenticação primária entre estes, seguido de enlace e conexão via o código PIN da chave armazenado no Beacon Advertiser Master, e posteriormente a execução de um protocolo de autenticação mútua e, em seguida, o Beacon Advertiser Master habilita, em sequência, os módulos Beacon Advertiser Slave a respectivamente se autenticarem e realizarem o enlace com a chave. Assim, o sistema compreende a criptografia, tanto dos canais de comunicação sem-fio utilizados, como pela criptografia das informações trocadas entre os dispositivos remotos e o PASE Controller.

[0020] Mais em particular, o procedimento de autenticação mútua compreende o Authentication Module do Beacon Advertiser Master enviar para a chave uma mensagem de dados compreendendo um texto cifrado e receber da chave uma mensagem de dados compreendendo um texto cifrado, a chave sendo autenticada no Beacon Advertiser Master caso ao menos parte do texto cifrado da chave seja igual a correspondente parte do texto cifrado gerado pelo Beacon Advertiser Master. Em complementação, o procedimento de autenticação mútua compreende também a chave enviar para o Authentication Module do Beacon Advertiser Master uma mensagem de dados compreendendo um texto cifrado e receber do Beacon Advertiser Master uma mensagem de dados compreendendo um texto cifrado, o Beacon Advertiser Master sendo autenticado na chave caso ao menos parte do

texto cifrado do Beacon Advertiser Master seja igual a correspondente parte do texto cifrado gerado pela chave.

[0021] Ademais, os objetivos supra são ainda alcançados a partir de um método de comunicação segura para veículos automotores, o qual prevê a execução de um protocolo de autenticação mútua, dito protocolo compreendendo as etapas de: o dongle gera e envia um número aleatório RND1 para a chave; em resposta, a chave gera e envia um número aleatório RND2 para o dongle; o dongle realiza uma operação lógica XOR a partir dos números aleatórios RND1 e RND2 e uma chave K2, previamente armazenada neste; a chave realiza uma operação lógica XOR a partir dos números aleatórios RND1 e RND2, e uma chave K2, previamente armazenada nesta; o dongle aplica o resultado da operação lógica XOR no bloco AES_D de criptografia de 128 bits, dito bloco AES_D utilizando uma chave SK1 como chave de criptografia, e gerando um texto cifrado de 128 bits; a chave aplica o resultado da operação lógica XOR no bloco AES_{RK} de criptografia de 128 bits, dito bloco AES_{RK} utilizando uma chave SK1 como chave de criptografia, e gerando um texto cifrado de 128 bits; o dongle gera e envia, para a chave uma mensagem de dados CMD, compreendendo os 64 bits menos significativos do dito texto cifrado de 128 bits; a chave gera e envia, para o dongle, uma mensagem de dados CMD, compreendendo os 64 bits mais significativos do dito texto cifrado de 128 bits; o dongle compara os 64 bits menos significativos da mensagem CMD recebida e os compara com os 64 bits menos significativos do texto cifrado calculado pelo bloco AES_D, autenticando a chave no caso de igualdade entre ambos os 64 bits menos significativos; e a chave compara os 64 bits mais significativos da mensagem CMD recebida e os compara com os 64 bits menos significativos do texto cifrado calculado pelo bloco AES_{RK}, autenticando o dongle no caso de igualdade entre ambos os 64 bits mais significativos.

[0022] Em particular, as chaves de criptografia K2 e SK1 são previamente armazenadas no dongle e na chave, e os números aleatórios RND1 e RND2 são números aleatórios verdadeiros, preferencialmente gerados a partir da medição de uma grandeza física.

Descrição das figuras

[0023] A invenção poderá ser melhor compreendida através da seguinte descrição detalhada de uma sua forma preferencial e não limitativa de realização, a qual é feita em

consonância com as figuras em anexo, trazidas a título meramente ilustrativo e não limitativo, nas quais:

- a figura 1 é uma vista esquemática do ambiente interativo entre usuário e veículo, de acordo com a presente invenção;
- a figura 2 ilustra, na forma de um diagrama de blocos, os componentes da plataforma segura e energético-eficiente para acesso passivo e acionamento do veículo;
- a figura 3 mostra, na forma de um diagrama de blocos interconectado, as particularidades do módulo Beacon Advertiser Master;
- a figura 4 mostra, na forma de um diagrama de blocos interconectado, as particularidades dos módulos Beacon Advertiser Slave;
- a figura 5 ilustra, na forma de um diagrama de blocos, o módulo PASE Controller o qual centraliza as funcionalidades veiculares com os módulos Beacon;
- a figura 6 ilustra, na forma de um diagrama de blocos, a estruturação lógico funcional implementada em um smartphone;
- a figura 7 ilustra, na forma de um diagrama de blocos, a estruturação lógico funcional implementada em um dispositivo vestível; e
- a figura 8 é o fluxograma relativo ao protocolo de autenticação mútua de uma chave no Beacon Advertiser Master.

Descrição de uma Forma Preferencial de Realização da Invenção

[0024] De conformidade em particular com a figura 1 em anexo, com (1) é indicado o ambiente onde o veículo (2) a ser acessado encontra-se. A abertura de uma das portas, o acionamento da partida do veículo, ou a atuação de outra funcionalidade, se dá através da troca de informações, de forma passiva e utilizando um meio sem fio, entre o veículo e um aplicativo específico instalado em um smartphone (3), ou entre o veículo e um dispositivo vestível (4). A despeito da presente invenção ser descrita, a seguir, de forma particularizada e voltada as funcionalidades de acesso e partida passiva, deve ficar claro a qualquer técnico do setor que tais funcionalidades são meros exemplos ilustrativos de funções que podem ser executadas a distância, pelo usuário, entre tantas outras possíveis. Em outras palavras, o cerne da presente invenção está no sistema de comunicação e execução de funcionalidades entre veículo e usuário, a qual não é

particularizada ou definida pelo tipo de comando, ou sinal, transmitido entre as partes operantes do sistema.

[0025] Mais em particular, a presente invenção descreve uma plataforma lógico-funcional de comunicação entre o veículo (2) e um usuário (não ilustrado) que traz consigo um dispositivo de comunicação remota. Especificamente, o sistema é composto por dispositivo eletrônico embarcado no veículo e por uma chave que é carregada pelo usuário, tal como um dispositivo eletrônico vestível (4), também conhecido como *wearable* ou um smartphone (3). A invenção permite que a arquitetura do sistema seja a mesma para o dispositivo embarcado veicular independente da chave escolhida, seja wearable ou smartphone, sendo indiferente para o veículo a escolha do formato da chave. Os dispositivos wearable e smartphone somente têm a necessidade de apresentar capacidade de comunicação via BLE (Bluetooth Low Energy) e uma unidade de processamento central programável para gerenciar a comunicação e realizar criptografia das mensagens.

[0026] O sistema opera por proximidade usando nível de potência de sinal da comunicação BLE para determinar a posição da chave, através de troca de mensagens via BLE. Dentro do jargão utilizado no protocolo BLE, os chamados transponders BLE, que na forma preferencial de realização da invenção correspondem aos dongles, localizados no veículo fazem o papel de periféricos e a chave (3, 4) é o dispositivo central. Portanto, o veículo está em constante geração de beacons (modo de anunciação - *advertising*).

[0027] No tocante especificamente ao sistema veicular de comunicação da invenção, a figura 2 ilustra alguns componentes dos sistemas veiculares, conectados à plataforma, ou sistema (200) seguro e energético-eficiente para, por exemplo, acesso passivo e acionamento do veículo (2). O dito sistema (200) possui antenas (201, $210_{1\text{-}n}$) para transmissão e recepção de sinais sem fio, nas faixas de frequências reservadas, ou seja, nas bandas reservadas internacionalmente para o desenvolvimento industrial, científico e médico, dentro do qual se inclui o padrão Bluetooth Low Energy, ou BLE. Estas antenas (201, $210_{1\text{-}n}$) se conectam respectivamente ao módulo Beacon Advertiser Master (202) e os módulos Beacon Advertiser Slave ($204_{1\text{-}n}$), cujas características e funcionalidades serão descritas, a seguir, em relação as figuras 3 e 4, respectivamente. A interligação do conjunto de módulos de propagação e recepção de mensagens do tipo beacon com o

módulo controlador do sistema, ou PASE Controller (205) se dá através do barramento de comunicação (203). Por seu turno, o dito módulo PASE Controller (205) é conectado aos diversos sistemas veiculares tanto diretamente quanto através da rede veicular (208). Apenas a título ilustrativo, a figura 2 mostra o módulo PASE Controller (205) diretamente conectado aos sensores de porta (206) e ao sensor do sistema star/stop (207), enquanto que a conexão com os sistemas de partida e de destravamento de portas, dito Lock/Unlock and Start System (209) é realizada via rede veicular (208). Assim, e como fica claro, a conexão do módulo PASE Controller (205) segue as características originárias dos sistemas veiculares instalados e, portanto, sem a necessidade de reconfiguração dos mesmos sistemas. Por outro lado, o módulo PASE Controller (205) poderia estar igualmente conectado a outros sensores e sistemas veiculares para permitir a ativação e controle de outras funções não ilustrativamente descritas na presente descrição, tais como, por exemplo, acender as luzes do veículo, ligar o ar condicionado, além de outras possibilidades.

[0028] Conforme ilustra a figura 3, o dito módulo Beacon Advertiser Master (202) é destinado a implementar as funções de estabelecimento de uma conexão segura entre o veículo (2) e o smartphone (3) ou o dispositivo vestível (4) e gerencia o acionamento dos módulos Beacon Advertiser Slave (204_{1-n}), compatibilizando a gestão da energia consumida pelos mesmos, com a necessidade de informações de localização do dispositivo remoto. Para tanto, o mesmo subdivide-se em três módulos: Security Connection Starter (212), Link Logical Cypher (213) e Authentication Module (214). Com isso, é estabelecida uma conexão segura, com conteúdo criptografado, entre o dispositivo remoto (smartphone ou vestível) e o controlador, PASE Controller (205), do sistema. Em particular, o mecanismo de autenticação da invenção, será descrito mais adiante, em relação à figura 8.

[0029] De forma mais detalhada, o dito módulo Link Logical Cypher (213) é interna e diretamente conectado aos módulos Security Connection Starter (212) e Authentication Module (214). O módulo Link Logical Cypher (213) é ainda conectado a uma interface de comunicação (215) de modo a interligar o Beacon Advertiser Master (202) ao barramento de comunicação (203). Por fim, o módulo Security Connection Starter (212) é interligado a

uma interface de RF (216), de modo a transmitir e receber mensagens, via antena (201), entre este e a chave (3, 4).

[0030] A figura 4 detalha os componentes dos módulos Beacon Advertiser Slave (204). Com exceção da função de autenticação, esses módulos também provêm o estabelecimento de canais de comunicação seguros, distribuídos na periferia do veículo (2), para suportar a localização da chave (3, 4) utilizada para a abertura de portas e partida do veículo. Tal como no caso do Beacon Advertiser Master (202), cada módulo Beacon Advertiser Slave (204_{1-n}) possui respectivos módulos Security Connection Starter (222) e Link Logical Cypher (223), mas não o Authentication Module, já que a funcionalidade de autenticação é reservada ao módulo Beacon Master (202). De forma mais detalhada, o módulo Link Logical Cypher (223) é interna e diretamente conectado ao módulo Security Connection Starter (222) e a interface de comunicação (225), a qual conecta externamente o barramento de comunicação (203). Já o Security Connection Starter (222) é interligado a interface de RF (226) que, por sua vez, acopla a antena (210) de modo a receber e enviar mensagens da e para a chave (3, 4).

[0031] A comunicação entre os módulos beacon, como visto, e destes com o PASE Controller (205) é realizada através do barramento de comunicação (203) com protocolo de comunicação digital escolhido, podendo ser CAN, UART, SPI, ou outro.

[0032] No tocante especificamente ao módulo PASE Controller (205), a figura 5 detalha os seus componentes, cujas funcionalidades específicas são descritas a seguir. Especificamente, módulo PASE Controller (205) compreende um módulo PASE Core (251) interligado a uma interface de Input (254), a qual recebe os sinais dos sensores (206, 207) do veículo (2), bem como a uma interface da rede veicular (255), a qual conecta externamente a dita rede veicular (208). Ademais, o dito módulo PASE Core (251) é interna e diretamente conectado ao módulo de localização (252), o qual está conectado a uma interface de comunicação (253) para o barramento de comunicação (203).

[0033] A figura 6 ilustra os componentes do aplicativo específico (301), instalado em um smartphone (3), para acionamento remoto do sistema. Tal aplicativo (301) subdivide-se em três módulos: Security Module (302), responsável pela implementação das funções de criptografia e autenticação do sistema; BLE Manager (303), responsável pelo

gerenciamento da troca de informações baseadas na pilha de protocolos descritas no padrão Bluetooth Low Energy e User Interface (304), responsável pela implementação da interface de comunicação com o usuário final do sistema. Tal aplicação interage com os componentes de hardware do smartphone, tal como a antena (306) utilizada na transmissão e recepção de sinais de RF, através do sistema operacional do aparelho, ou Mobile OS (305).

[0034] A figura 7 ilustra os componentes (401) implementados no dispositivo vestível (4) para acionamento remoto do sistema. Tais componentes (401), possuem configuração similar ao aplicativo (301) implementado no smartphone (3), ou seja, subdivide-se em três módulos: Security Module (402), responsável pela implementação das funções de criptografia e autenticação do sistema; BLE Manager (403), responsável pelo gerenciamento da troca de informações baseadas na pilha de protocolos descritas no padrão Bluetooth Low Energy e Input Buttons (404), responsável pela implementação de uma interface mínima de comunicação com o usuário final do sistema. Tais componentes interagem com os módulos do sistema (200) embarcado utilizado (na modalidade SoC – System on Chip, por exemplo) através de um sistema operacional mínimo, ou Embedded Firmware (405), e se comunica externamente a partir de sua antena (406).

[0035] A seguir é fornecida uma descrição do funcionamento do sistema da presente invenção, de modo a permitir o seu entendimento completo, bem como definir de forma mais clara as suas vantagens. Para tanto, a descrição parte de um cenário no qual um usuário adquiriu o veículo (2), em uma concessionária, procedeu ao set up inicial do sistema (200), como o veículo estando estacionado em algum lugar, com o sistema ativado.

[0036] Com particular atenção ao set up inicial do sistema, o mesmo compreende o cadastro do smartphone (3) do usuário, bem como o download do aplicativo específico neste, de modo que o sistema passa a conter o registro do dito smartphone, bem como o smartphone passa a conter o registro do veículo ao qual este se vincula. Da mesma forma, a concessionária pode fornecer ao usuário um dispositivo vestível (4), o qual é igualmente cadastrado no sistema (200), e recebe o cadastro do sistema em sua memória. Deste modo, o sistema (200) tem registrado - *white list* - os códigos PIN de cada uma das

chaves (3, 4) previamente habilitadas para adentrar ao sistema, bem como cada uma das chaves (3, 4) está vinculada, via registro, ao veículo (2) específico. Obviamente que o sistema (200) da invenção permite que mais de um smartphone (3) e/ou mais de um dispositivo vestível (4) sejam devidamente cadastrados, desde que dito cadastro siga o procedimento específico de cadastro, o qual não faz parte da presente invenção, e assim não será descrito.

[0037] Assim, e ante o cenário supra estabelecido, o usuário se dirige ao veículo (2), por exemplo, estacionado em algum local público. Ainda, há de se destacar que, quando do estacionamento do veículo (2), o sistema (200) é ativado diretamente pelo usuário.

[0038] Ao ser ativado, o sistema entra em modo de detecção do usuário, com o objetivo de detectar a presença da chave (3, 4) dentro do seu raio de ação. Tipicamente, nos sistemas de comunicação via BLE, dito raio de ação gira em torno de 5-6 metros, não obstante ser possível definir, em projeto, um raio de ação diferenciado. Em particular, e sob instruções do PASE Controller (205), o módulo Beacon Advertiser Master (202) inicia a geração de beacons, transmitindo-os através da respectiva antena (201). Quando o usuário adentra no raio de ação definido pela antena (201) do Beacon Advertiser Master (202), a chave (3, 4) detecta o beacon e então gera um sinal em resposta que, sendo recebido pelo veículo (2), via antena (201), dá início ao processo de autenticação primária, ou seja o processo de autenticação do advertiser (mensagem de broadcast característica do protocolo BLE) da chave, realizado entre a chave (3, 4) e o Beacon Advertiser Master (202).

[0039] Concluída com sucesso esta fase de autenticação primária, a chave (3, 4) e módulo Beacon Advertiser Master (202) iniciam conexão e enlace usando o código PIN armazenado no Advertiser Master. Após ser realizado o enlace, inicia-se um novo processo de autenticação entre Advertiser Master e chave, chamado de autenticação mútua. O objetivo é que os dois elementos se autentiquem mutuamente, garantindo tanto que a chave está autorizada a destravar e partir o veículo (ou realizar qualquer outra funcionalidade programada) como também que o veículo é aquele ao qual a chave está associada. Como se verá mais adiante, estes protocolos de autenticação estão baseados na geração de números randômicos, chaves secretas armazenadas nos dispositivos e

protocolo de criptografia baseado no tamanho dessas chaves.

[0040] Assim, e completadas as fases de autenticação, primária e mútua, o Beacon Advertiser Master (202) comanda o primeiro módulo Beacon Advertiser Slave (204_1) a iniciar o processo de geração de beacon e de autenticação da mensagem advertiser, informando com qual chave ele deve se conectar. Completada esta fase de autenticação primária, o primeiro Beacon Advertiser Slave (204_1) realiza conexão e enlace utilizando o código PIN armazenado. Note-se que a etapa de autenticação mútua não acontece para os módulos Advertiser Slave (204_{1-n}).

[0041] Em seguida, com autenticação e conexão completadas pelo primeiro Advertiser Slave, o Advertiser Master (202) comanda o próximo módulo Advertiser Slave (204_2) a realizar o mesmo procedimento, até completarem-se as conexões da chave (3, 4) com todos os módulos Advertiser Slave (204_{1-n}). Destaque-se que todas essas conexões precisam ser efetivadas para mitigar o risco de ataques cibernéticos, através da troca de chaves criptografadas, cadastradas previamente em ambiente seguro.

[0042] Estando assim estabelecida uma conexão segura entre a chave (3, 4) e os módulos Advertiser Slave (204_{1-n}), tem início o processamento da localização da chave, ou seja, do usuário, processo este que é realizado pelo módulo PASE Controller (205) presente no dispositivo embarcado no veículo. O algoritmo de localização, via triangulação de sinal, e que é implementado pelo módulo de localização (252), somente é iniciado após a confirmação da autenticidade da chave (3, 4) detectada por todos os módulos Advertiser Slave (204_{1-n}), de modo que o módulo de localização (252) receba as informações de três níveis de potência de sinal ou mais, dependendo da quantidade de módulos Slave previstos no sistema. A partir deste algoritmo, o módulo de localização (252) gera e envia, para o módulo PASE Core (251), a posição relativa da chave/usuário por regiões definidas em relação ao veículo. Note-se que não é necessário obter a localização precisa da chave/usuário, mas somente a sua posição relativa, por exemplo, o usuário se encontra no interior do veículo, na região do bagageiro, ou em uma das laterais. As características e vantagens específicas deste mecanismo de localização relativa estão descritas, de forma detalhada, no pedido de patente dos mesmos inventores, de número BR 10 2018 015358 7, aqui incorporado como referência.

[0043] Em seguida, o módulo PASE core (251) compara uma solicitação de ação com a posição relativa do usuário, de modo a habilitar a funcionalidade demandada. Em outras palavras, o módulo PASE Controller (205) somente permite que seja dada a partida no veículo (2) - botão do start/stop (207) pressionado pelo usuário - caso o usuário esteja no interior do veículo. Em particular, pressionado o botão de partida (sensor do start/stop (207)), este comando é transmitido via interface de entrada (254) para o módulo PASE core (251), que o compara com a posição do usuário calculada e fornecida pelo módulo de localização (252). Caso a posição informada seja condizente com a ação demandada, o módulo PASE core (251) envia um sinal de partida do motor, via a interface da rede veicular (225) para a rede veicular (208). Deste ponto em diante, os próprios sistemas veiculares se incumbem das ações necessárias para que seja dada a partida no veículo (2), conforme procedimento interno.

[0044] De forma similar ao quanto supra descrito, o sistema da invenção permite que qualquer outro comando seja processado, qualquer que seja este comando: abertura de portas, acendimento de faróis, etc.

[0045] Por fim, a figura 8 representa um diagrama de fluxo relativo ao procedimento de autenticação mútua entre o Beacon Advertiser Master (202) e uma chave (3, 4), ou dispositivo periférico.

[0046] O protocolo, ou procedimento de autenticação mútua garante a autenticidade dos dois dispositivos, quais a chave (3, 4) (dispositivo central) e o dongle (dispositivo periférico), quando estiverem conectados, ou seja, possibilita a identificação do smartphone/dispositivo vestível como a chave do veículo e do dongle como pertencente ao veículo. Como sabido, dongle é um dispositivo conhecido na arte e define o conjunto formado por uma antena e um hardware apropriado de comunicação e processamento. No caso específico da presente invenção, um conjunto previamente definido pelo Advertiser Master (202) e pela antena (201) pode se materializar na forma de um dongle (202, 201). De forma similar, qualquer um dos módulos Advertiser Slave (204) e respectiva antena (210) pode igualmente se materializar na forma de um dongle (204, 210).

[0047] Como característica do sistema de transmissão BLE, o comprimento máximo de dados que podem ser transmitidos em cada pacote de conexão é de 18 bytes, ou seja,

144 bits. Este pacote de dados é dividido em duas partes: os dois bytes mais significativos definem quais dados são transmitidos (CMD) e os outros 16 bytes representam os dados em si. Tal codificação é usada em todos os pacotes que são trocados entre a chave (3, 4) e o dongle (202, 201), após a conexão primária ser estabelecida. A tabela 1 ilustra a composição de cada pacote de dados transmitido.

Tabela 1

CMD	DADOS
0x0000	Random 1 (RDN1)
0x0001	Random 2 (RND2)
0x0002	Texto cifrado 1 (CT1)
0x0003	Texto cifrado 2 (CT2)

[0048] O protocolo de autenticação mútua é iniciado quando o dongle (202, 201) gera e envia o número aleatório RND1 para a chave. Após receber esses dados, a chave (3, 4) gera e envia o número aleatório RND2 para o dongle. Os dois dispositivos tomam esses dois valores aleatórios (RND1 e RND2) e a chave K2, previamente armazenada na chave e no dongle, para realizar um uma operação lógica XOR com base nesses valores. O resultado da operação lógica XOR é aplicado a respectivos blocos AES_D e AES_{RK} de 128 bits utilizando a chave SK1 como chave de criptografia, chave SK1 que também é previamente armazenada na chave e no dongle. Os 64 bits menos significativos do resultado da última operação (texto cifrado) são enviados para a chave, e caso estes 64 bits sejam iguais ao resultado do cálculo da chave, o dongle será autêntico. Após isso, os 64 bits mais significativos são enviados para o dongle, e caso estes 64 bits forem iguais ao do cálculo do dongle, a chave é autêntica.

[0049] Se o protocolo for executado corretamente em todas as etapas, os dois dispositivos realizam uma autenticação mútua. Se em qualquer etapa houver um atraso no envio de uma informação o outro dispositivo executará um evento de desconexão.

[0050] O uso de tal protocolo nas comunicações entre smartphone (3) ou dispositivo vestível (4) e dongle (202, 201) garante segurança, prevenindo situações em que o protocolo de anunciação (advertising) seja adulterado, apesar de haver uma pequena possibilidade de acontecer e o nível de dificuldade ser elevado. Uma possibilidade é o atacante imitar um dongle válido ou um Smartphone autorizado. Há dois ataques possíveis:

• no primeiro caso, o atacante pode clonar o endereço MAC do Dongle, dessa forma o dispositivo clonado será considerado com um Dongle da lista branca, pronto para iniciar a conexão. Após a conclusão da conexão primária, caso o invasor possua o PIN correto, poderá criar o vínculo, porém, neste momento o protocolo de autenticação mútua acontecerá e o resultado não será compatível, desconectando desse modo o invasor.

• na situação em que o atacante imita a chave, através da clonagem de seu endereço MAC, o atacante conseguirá conectar-se ao dongle caso envie um pacote de advertising que contenha o KEY_ID correto e o contador seqüencial for maior que o armazenado no Dongle. Caso consiga gerar um pacote com esta informação e após a conexão enviar o PIN correto para solicitar o vínculo, conseguirá se conectar e executar o processo de vinculação. No entanto, após isso, o protocolo de autenticação mútua ocorrerá e o atacante será desconectado.

[0051] A tecnologia BLE utilizada para a comunicação entre smartphone/vestível e dongle suporta um recurso que reduz a capacidade de rastrear um dispositivo BLE ao longo de um período de tempo por meio da alteração do endereço do dispositivo Bluetooth com base na freqüência. O endereço em constante mudança é chamado de endereço privado e os dispositivos confiáveis podem resolvê-lo.

[0052] Para usar esse recurso, os dispositivos envolvidos na comunicação precisam estar previamente emparelhados. O endereço privado é gerado usando os dispositivos IRK trocados durante o procedimento de emparelhamento/conexão prévio. Os endereços privados são resolvidos e gerados pelo controlador sem envolver o host após o host fornecer as informações de identidade do dispositivo do controlador.

[0053] Além da vantagem inerente a segurança da conexão entre o sistema (200) e a chave (3, 4), tal como visto supra, o objeto da invenção ainda resulta energeticamente econômico. A otimização do consumo de energia é obtida usando somente o Advertiser Master (202) para gerar um beacon inicial, com os demais módulos Beacon Advertiser Slave ($204_{1\text{-}n}$) permanecendo em modo sleep. Ademais, como os módulos advertiser utilizam um sinal beacon na faixa de VHF (30 a 300 MHz), verifica-se um consumo de corrente de 3 mA, enquanto que, na solução proposta, baseada no protocolo BLE e cuja transmissão ocorre na faixa de UHF (300 MHz a 3 GHz), temos um consumo de corrente

de 1,8 mA. Essa medição de consumo de corrente segue o padrão ensinado no pedido de patente US 2016/0288770, onde é aferido o consumo de corrente com o veículo desligado (KOL - Key-off current load).

[0054] Como visto supra, a presente invenção permite uso de chaves de diversos formatos, do tipo *wearable* (4), podendo ser pingentes, pulseiras, anéis e etc., como também possibilita uso de smartphones (3), aumentando a gama de possibilidades de uso da tecnologia para aumentar número de funcionalidades do veículo acessíveis pelo aparato.

[0055] Já no quesito de segurança, a presente invenção inova ao prever a autenticação primaria, o enlace via PIN e posteriormente uma autenticação mútua entre o PASE Controller e o dispositivo remoto (chave). Além disto, e também como visto, tanto os canais de comunicação sem fio, quanto as mensagens trocadas entre o dispositivo remoto (3, 4) e o módulo Beacon Advertiser Master (202), ou qualquer um dos Beacon advertiser Slave ($204_{1\text{-}n}$), são criptografados, o que permite impedir eventuais ataques e interferências, mesmo os mais sofisticados.

[0056] Por fim, deve ser destacado que toda a segurança do processo dá-se desde a geração do parâmetro RND1 e RND2, tais parâmetros representam uma das entradas para o algoritmo de criptografia AES com as chaves secretas, para maximizar o potencial dos algoritmos de segurança, a fim de não serem decifrados, é necessário dispor de um gerador de números aleatórios verdadeiros em um nível de hardware, que é um dispositivo que gera números aleatórios a partir de um processo físico, em vez de um programa de computador. Tais dispositivos são freqüentemente baseados em fenômenos microscópicos que geram sinais de ruído estatisticamente aleatórios de baixo nível, como o ruído térmico.

Reivindicações

1. Sistema de comunicação segura para veículos automotores, do tipo a ser implementando entre um veículo (2) e um dispositivo remoto ou chave (3, 4) via protocolo de comunicação BLE, dito dispositivo remoto podendo ser:

- um smartphone (3) dotado de um sistema operacional Mobile OS (305) o qual gerencia os módulos funcionais Security Module (302), BLE Manager (303) e User Interface (304), além de ao menos uma antena (306) de transmissão e recepção de sinais de RF, via protocolo de comunicação BLE; ou

- um dispositivo vestível (4) dotado de um sistema operacional Embedded Firmware (405), o qual gerencia os módulos funcionais Security Module (402), BLE Manager (403) e Input Buttons (404), além de ao menos uma antena (406) de transmissão e recepção de sinais de RF, via protocolo de comunicação BLE,

e sendo que o dito sistema (200) compreende um módulo de processamento PASE Controller (205), conectado ao menos aos sistemas veiculares Lock/Unlock and Start System (209) através da rede veicular (208) e conectado diretamente ao menos os sensores de porta (206) e ao sensor star/stop (207), e sendo que o dito PASE Controller (205) é conectado, através de um barramento de comunicação (203), a um módulo Beacon Advertiser Master (202) e respectiva antena (201), bem como a ao menos dois módulos Beacon Advertiser Slave ($204_{1\text{-}n}$) dotados de respectivas antenas ($210_{1\text{-}n}$),

caracterizado pelo fato de que dito módulo PASE Controller (205) compreende:

- um módulo PASE Core (251) interligado a uma interface de Input (254), a qual recebe os sinais dos ditos sensores (206, 207) do veículo (2), bem como a uma interface da rede veicular (255) de conexão com a dita rede veicular (208); e

- um módulo de localização (252), o qual está conectado a uma interface de comunicação (253) com o barramento de comunicação (203)

e sendo que dito Beacon Advertiser Master (202) compreende um módulo Link Logical Cypher (213) diretamente conectado a um módulo Security Connection Starter (212) e a um Authentication Module (214), dito módulo Link Logical Cypher (213) é ainda conectado a uma interface de comunicação (215) de modo a interligar o Beacon Advertiser Master (202) ao barramento de comunicação (203), sendo que o módulo Security Connection

Starter (212) é interligado a uma interface de RF (216), de modo a transmitir e receber mensagens, via antena (201), entre o Beacon Advertiser Master (202) e a chave (3, 4),
e sendo que a chave (3, 4) e módulo Beacon Advertiser Master (202) realizam um procedimento de autenticação primária entre estes, seguido de enlace e conexão via o código PIN da chave armazenado no Beacon Advertiser Master, e posteriormente a execução de um protocolo de autenticação mútua,
e sendo que, em seguida, Beacon Advertiser Master (202) habilita, em sequência, os módulos Beacon Advertiser Slave (204_{1-n}) a respectivamente se autenticarem e realizarem o enlace com a chave (3, 4).

2. Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de compreender a criptografia, tanto dos canais de comunicação sem-fio utilizados, como pela criptografia das informações trocadas entre os dispositivos remotos (3, 4) e o PASE Controller (205).

3. Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de o procedimento de autenticação mútua compreende o Authentication Module (214) do Beacon Advertiser Master (202) enviar para a chave (3, 4) uma mensagem de dados (CMD) compreendendo um texto cifrado e receber da chave (3, 4) uma mensagem de dados (CMD) compreendendo um texto cifrado, a chave (3, 4) sendo autenticada no Beacon Advertiser Master (202) caso ao menos parte do texto cifrado da chave (3, 4) seja igual a correspondente parte do texto cifrado gerado pelo Beacon Advertiser Master (202).

4. Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de o procedimento de autenticação mútua compreende a chave (3, 4) enviar para o Authentication Module (214) do Beacon Advertiser Master (202) uma mensagem de dados (CMD) compreendendo um texto cifrado e receber do Beacon Advertiser Master (202) uma mensagem de dados (CMD) compreendendo um texto cifrado, o Beacon Advertiser Master (202) sendo autenticado na chave (3, 4) caso ao menos parte do texto cifrado do Beacon Advertiser Master (202) seja igual a correspondente parte do texto cifrado gerado pela chave (3, 4).

5. Método de comunicação segura para veículos automotores, **caracterizado** pelo fato de prever a execução de um protocolo de autenticação mútua, dito protocolo

compreendendo as etapas de:

- o dongle (202, 201) gera e envia um número aleatório RND1 para a chave;
- em resposta, a chave (3, 4) gera e envia um número aleatório RND2 para o dongle;
- o dongle (202, 201) realiza uma operação lógica XOR a partir dos números aleatórios (RND1 e RND2) e uma chave (K2), previamente armazenada neste;
- a chave (3, 4) realiza uma operação lógica XOR a partir dos números aleatórios (RND1 e RND2) e uma chave (K2), previamente armazenada nesta;
- o dongle (202, 201) aplica o resultado da operação lógica XOR no bloco AES_D de criptografia de 128 bits, dito bloco AES_D utilizando uma chave SK1 como chave de criptografia, e gerando um texto cifrado de 128 bits;
- a chave (3, 4) aplica o resultado da operação lógica XOR no bloco AES_{RK} de criptografia de 128 bits, dito bloco AES_{RK} utilizando uma chave SK1 como chave de criptografia, e gerando um texto cifrado de 128 bits;
- o dongle (202, 201) gera e envia, para a chave (3, 4), uma mensagem de dados CMD, compreendendo os 64 bits menos significativos do dito texto cifrado de 128 bits;
- a chave (3, 4) gera e envia, para o dongle (202, 201), uma mensagem de dados CMD, compreendendo os 64 bits mais significativos do dito texto cifrado de 128 bits;
- o dongle (202, 201) compara os 64 bits menos significativos da mensagem CMD recebida e os compara com os 64 bits menos significativos do texto cifrado calculado pelo bloco AES_D, autenticando a chave (3, 4) no caso de igualdade entre ambos os 64 bits menos significativos; e
- a chave (3, 4) compara os 64 bits mais significativos da mensagem CMD recebida e os compara com os 64 bits menos significativos do texto cifrado calculado pelo bloco AES_{RK}, autenticando o dongle (202, 201) no caso de igualdade entre ambos os 64 bits mais significativos.

6. Método, de acordo com a reivindicação 5, **caracterizado** pelo fato de que as chaves de criptografia (K2, SK1) são previamente armazenadas no dongle (202, 201) e na chave (3, 4).

7. Método, de acordo com a reivindicação 5, **caracterizado** pelo fato de que os números aleatórios RND1 e RND2 são números aleatórios verdadeiros.

8. Método, de acordo com a reivindicação 7, **caracterizado** pelo fato de que os números aleatórios RND1 e RND2 são gerados a partir da medição de uma grandeza física.

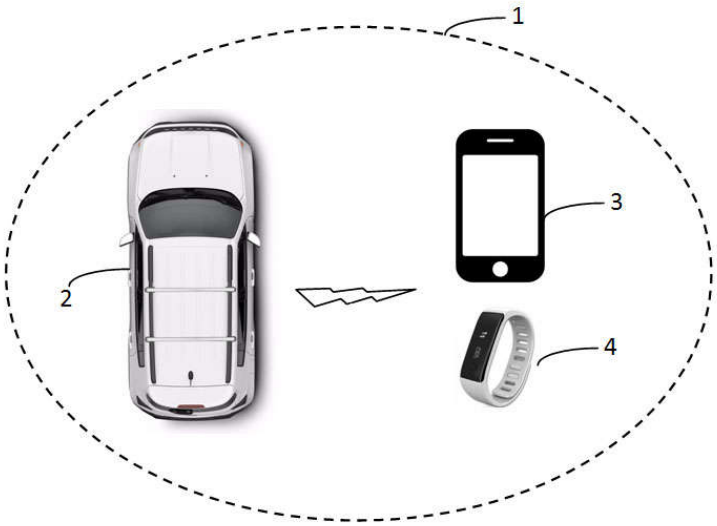


Figura 1

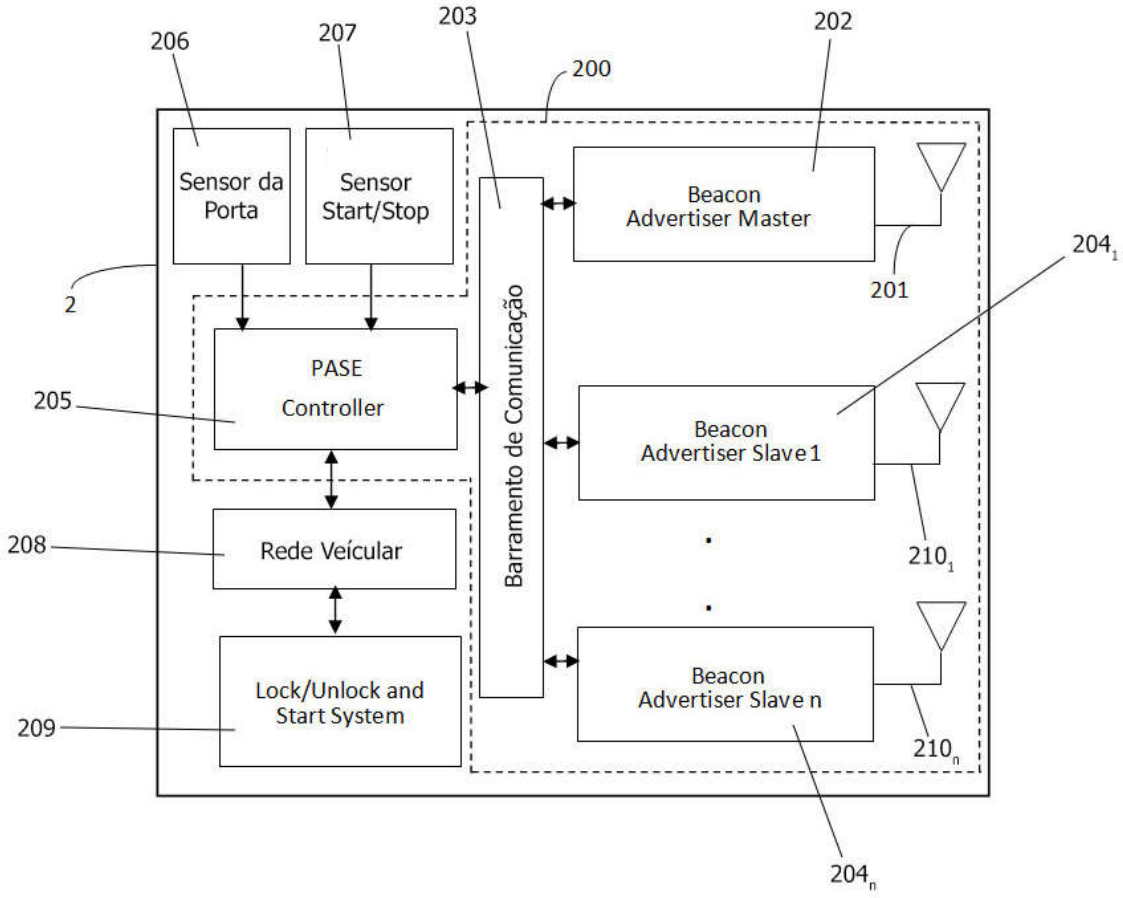


Figura 2

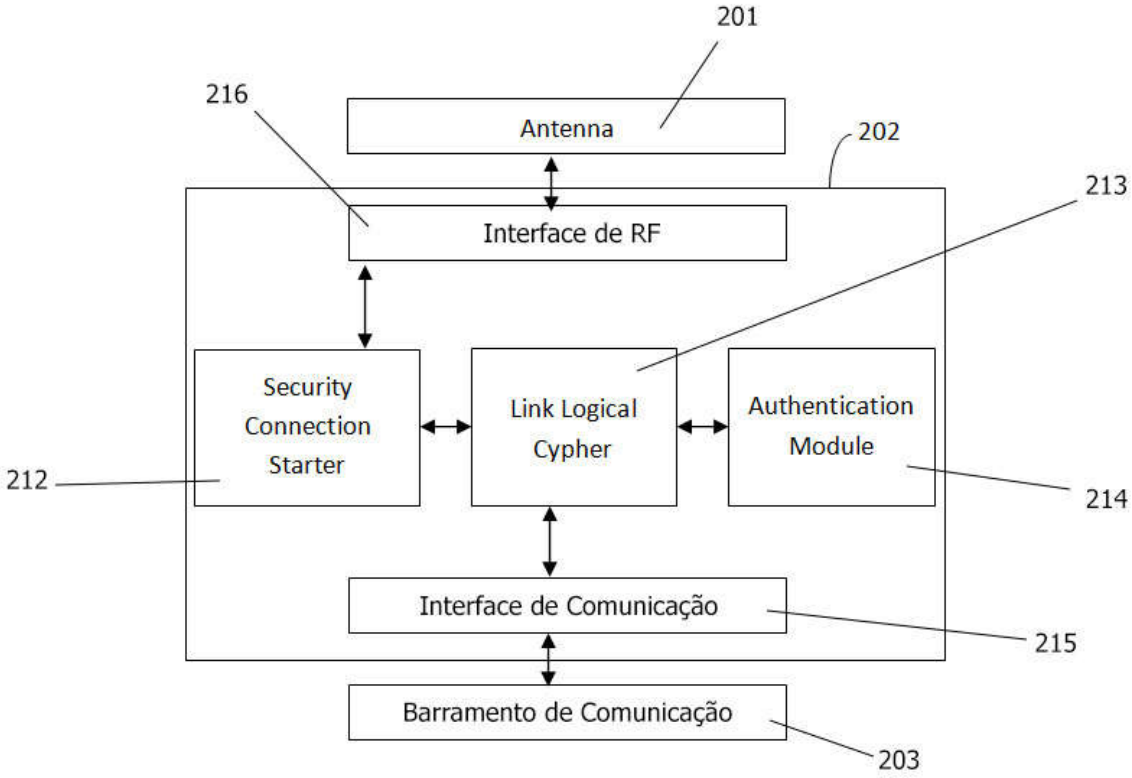


Figura 3

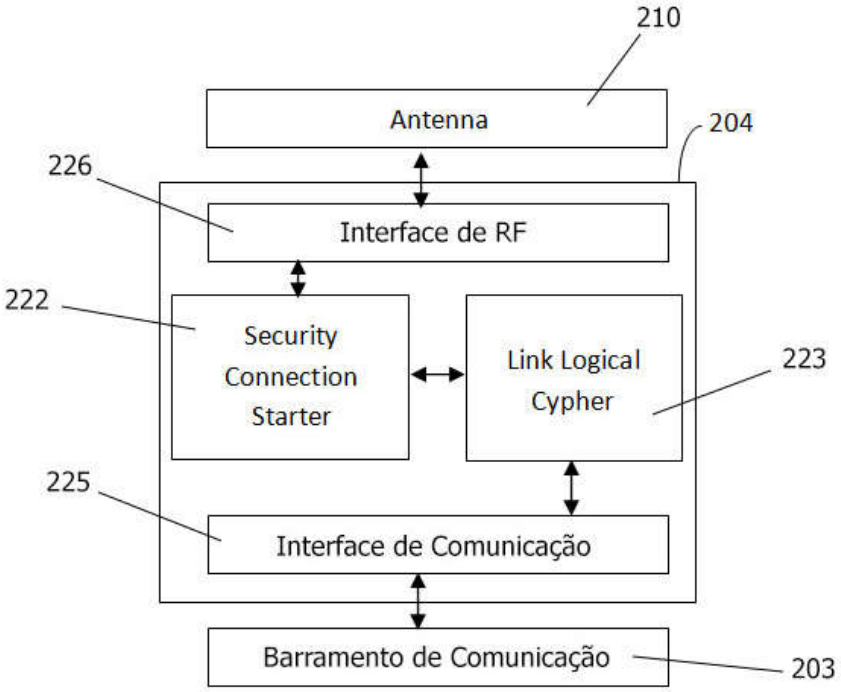


Figura 4

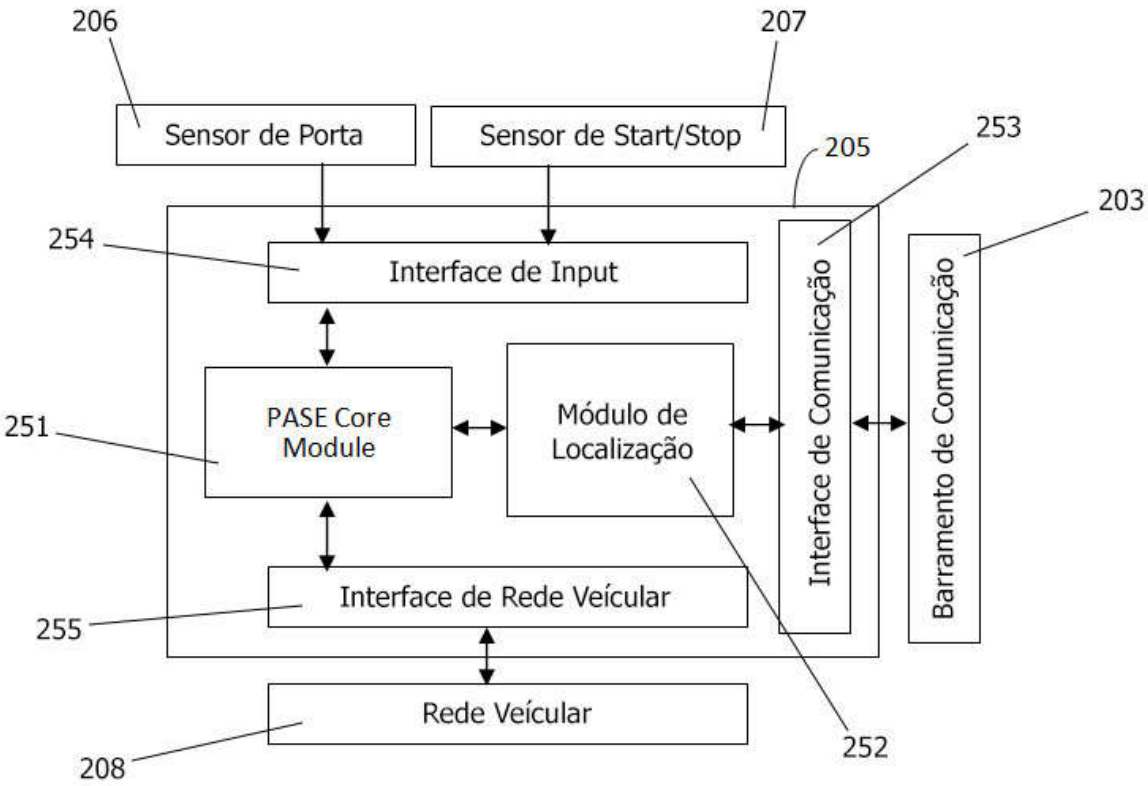


Figura 5

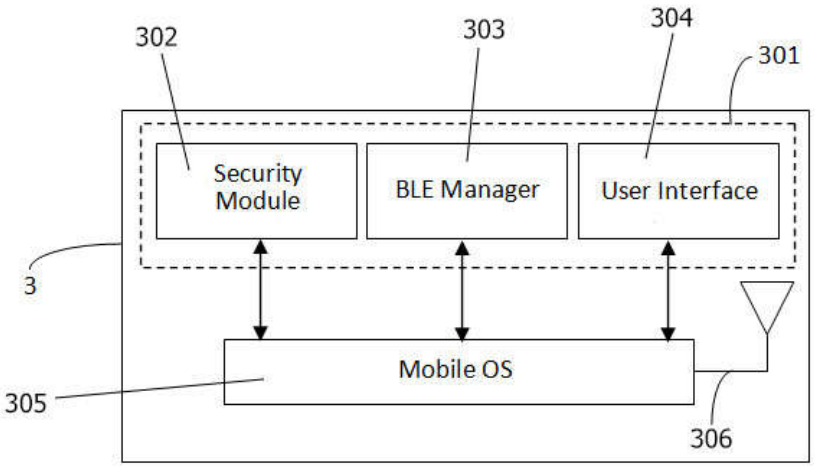


Figura 6

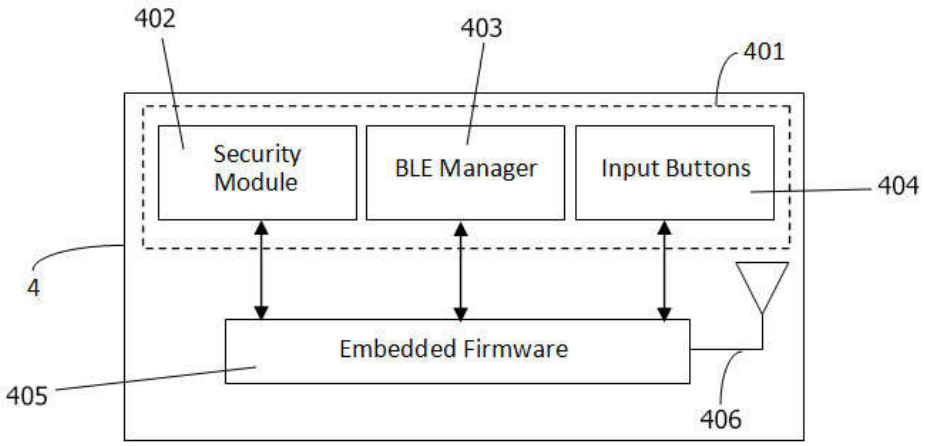


Figura 7

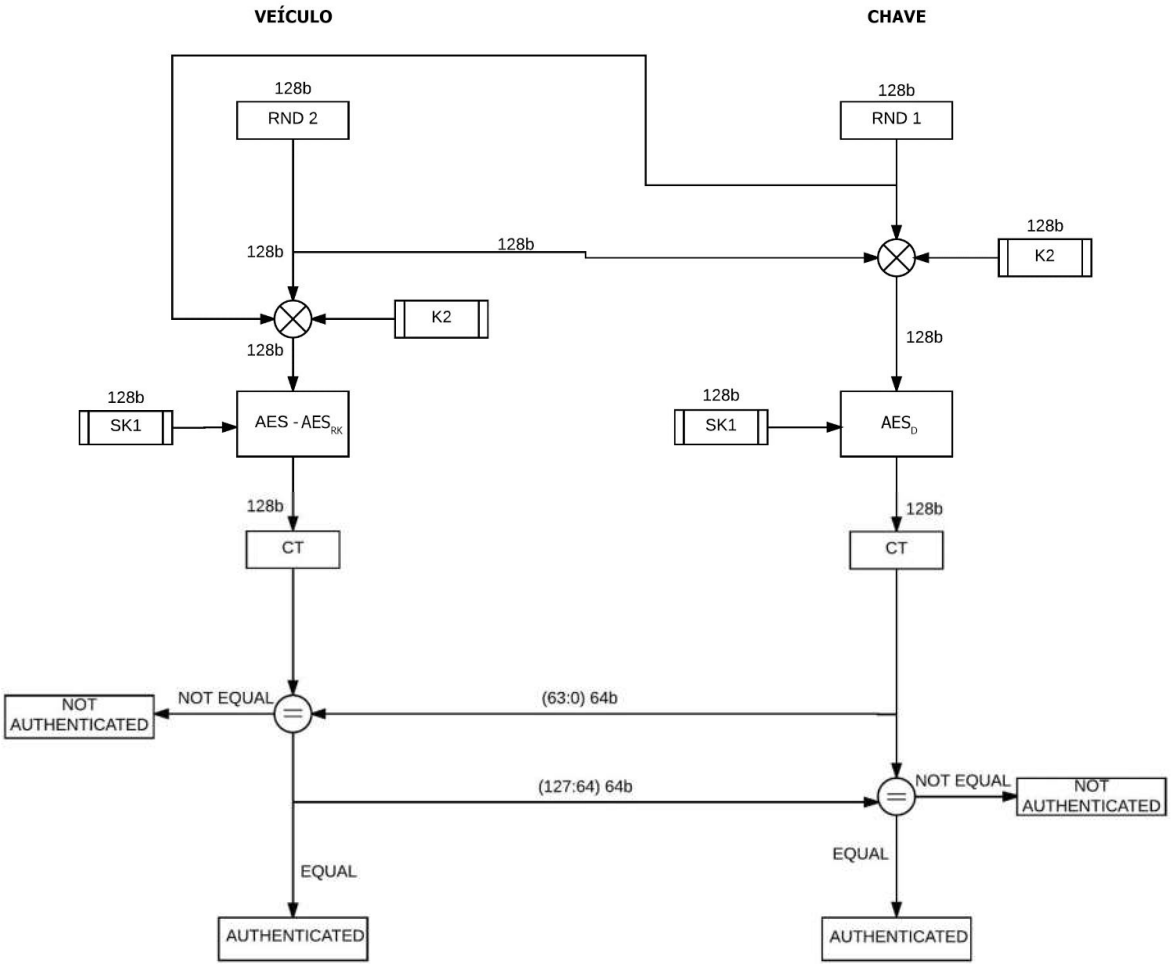


Figura 8

Resumo

SISTEMA E MÉTODO DE COMUNICAÇÃO SEGURA PARA VEÍCULOS AUTOMOTORES

São descritos um sistema e um método de comunicação segura entre um veículo (2) e um dispositivo remoto, portado por um usuário, tal como um smartphone (3) ou um dispositivo vestível (4), os quais se comunicam a distância, através de um protocolo BLE. Através do dispositivo remoto, é possível ao usuário comandar ações, tais como a abertura de determinadas portas, ou habilitar a partida do veículo. Para tanto, o sistema (200) compreende um módulo de processamento PASE Controller (205), conectado aos sistemas e dispositivos veiculares (206, 207, 208, 209) além de conectado, através de um barramento de comunicação (203), a um módulo Beacon Advertiser Master (202) e respectiva antena (201), bem como a ao menos dois módulos Beacon Advertiser Slave (2041-n) dotados de respectivas antenas (2101-n). O dispositivo remoto/chave (3, 4) e módulo Beacon Advertiser Master (202) realizam um procedimento de autenticação primária entre estes, seguido de enlace e conexão via o código PIN da chave armazenado no Beacon Advertiser Master, e posteriormente a execução de um protocolo de autenticação mútua e, em seguida, Beacon Advertiser Master (202) habilita, em sequência, os módulos Beacon Advertiser Slave (2041-n) a respectivamente se autenticarem e realizarem o enlace com a chave (3, 4).