(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 February 2020 (06.02.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/028502 A1

(51) International Patent Classification:
G07C 9/00 (2006.01)

(21) International Application Number:
PCT/US2019/044358

(22) International Filing Date:
31 July 2019 (31.07.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/713,527	01 August 2018 (01.08.2018)	US
62/786,837	31 December 2018 (31.12.2018)	US
62/812,642	01 March 2019 (01.03.2019)	US

(71) Applicant: **THE CHAMBERLAIN GROUP, INC.** [US/US]; 300 Windsor Drive, Oak Brook, Illinois 60523 (US).

(72) Inventors: **CATE, Casparus**; 728 West Jackson, Apartment 1133, Chicago, Illinois 60184 (US). **HOPKINS, Garth Wesley**; 585 South Road, Lisle, Illinois 60532 (US). **KHAMHARN, Oddy**; 212 South Westmore Meyers Road, Lombard, Illinois 60148 (US). **MILLER, Mark Edward**; 8446 Mending Wall Drive, Woodridge, Illinois 60517 (US). **SORICE, Cory**; 121 South Catherine Avenue, LaGrange, Illinois 60525 (US).

(74) Agent: **KRATZ, Rudy** et al.; Fitch, Even, Tabin & Flannery, LLP, 120 South LaSalle Street, Suite 2100, Chicago, Illinois 60603 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: 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, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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.

(54) Title: MOVABLE BARRIER OPERATOR AND TRANSMITTER PAIRING OVER A NETWORK

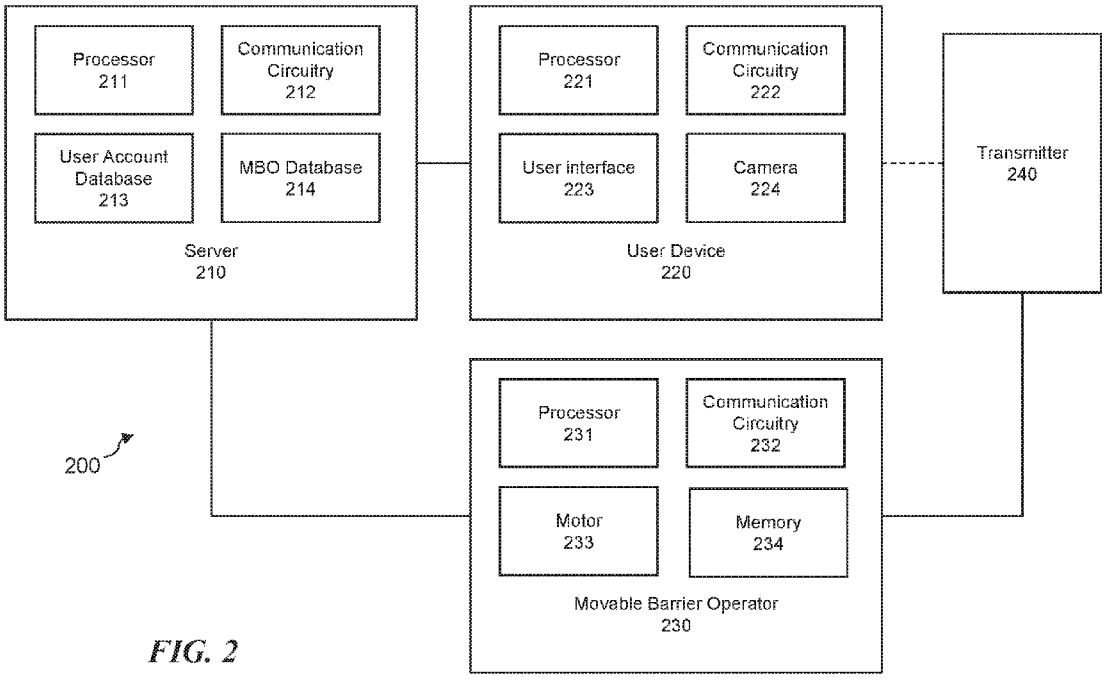


FIG. 2

(57) Abstract: In one aspect of the present disclosure, a system and method are provided for pairing a network-enabled movable barrier operator with a transmitter. The method may include receiving a pairing request, retrieving a hashed version of the transmitter fixed code, verifying access authorization, and forwarding the hashed version of the transmitter fixed code to a movable barrier operator to allow the movable barrier operator to determine whether a new transmitter is authorized to control the movable barrier operator.

WO 2020/028502 A1

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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).

Published:

— *with international search report (Art. 21(3))*

MOVABLE BARRIER OPERATOR AND TRANSMITTER PAIRING OVER A NETWORK

[0001] This application claims the benefit of U.S. Provisional Application Number 62/713,527, filed August 1, 2018, U.S. Provisional Application Number 62/786,837, filed December 31, 2018, and U.S. Provisional Application Number 62/812,642, filed March 1, 2019 all of which are incorporated herein by reference in their entireties.

TECHNICAL FIELD

[0002] The present disclosure relates generally to movable barrier operators, and more specifically to the pairing of transmitters and network-enabled moveable barrier operators.

BACKGROUND

[0003] Movable barriers are known, including, but not limited to, one-piece and sectional garage doors, pivoting and sliding gates, doors and cross-arms, rolling shutters, and the like. In general, a movable barrier operator system for controlling such a movable barrier includes a movable barrier operator coupled to the corresponding movable barrier and configured to cause the barrier to move (typically between closed and opened positions).

[0004] A movable barrier operator can typically be operated by a radio frequency (RF) transmitter that is provided/associated with or otherwise accompanies the movable barrier operator. Conventionally, to pair a movable barrier operator with a transmitter, a user presses a program/learn button on the movable barrier operator and then presses a button of the transmitter to cause the transmitter to transmit a code which may be constituted by a fixed portion (e.g. transmitter identification number) and a variable portion (e.g. rolling code that changes with each actuation of the transmitter's button). The movable barrier operator then learns the transmitter relative to the code (e.g. one or both of the fixed and variable portions) that was transmitted by the transmitter such that

subsequently received codes from the transmitter are recognized by the movable barrier operator to thereby cause performance of an action.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. 1 is a perspective view of a garage having a garage door opener mounted therein;

[0006] FIG. 2 is a block diagram of an example system for pairing a transmitter with a movable barrier operator;

[0007] FIG. 3 is a flow diagram of an example method performed at a user device for pairing a transmitter with a movable barrier operator;

[0008] FIG. 4 is a flow diagram of an example method performed at a server computer for pairing a transmitter with a movable barrier operator;

[0009] FIG. 5 is a flow diagram of an example method performed at a movable barrier operator for pairing a transmitter with the movable barrier operator;

[0010] FIG. 6 is a flow diagram of another example method for pairing a transmitter with a movable barrier operator;

[0011] FIG. 7 is a messaging diagram of another example method for pairing a transmitter with a movable barrier operator;

[0012] FIG. 8 is a schematic view of an example system for causing a movable barrier operator to learn one or more transmitters;

[0013] FIG. 9 is a perspective view an in-vehicle interface system including a human machine interface;

[0014] FIGS. 10A and 10B are portions of a flow diagram of an example method to associate a remote control with a movable barrier operator;

[0015] FIG. 11 is a schematic view of an interface system communicating with a remote server; and

[0016] FIG. 12 is a schematic view of an example movable barrier operator.

[0017] Corresponding reference characters indicate corresponding components throughout the several views of the drawings. Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions of some of the elements in the figures

may be exaggerated relative to other elements to help to improve understanding of various embodiments of the present invention. Also, common but well-understood elements that are useful or necessary in a commercially feasible embodiment are often not depicted to facilitate a less obstructed view of these various embodiments. It will be further appreciated that certain actions and/or operations may be described or depicted in a particular order of occurrence while those skilled in the art will understand that such specificity with respect to sequence is not actually required. It will also be understood that the terms and expressions used herein have the ordinary technical meaning as is accorded to such terms and expressions by persons skilled in the technical field as set forth above except where different specific meanings have otherwise been set forth herein.

SUMMARY

[0018] Methods and apparatuses for pairing a movable barrier operator and a transmitter are provided. In some embodiments, a movable barrier operator apparatus is provided that includes a memory and communication circuitry configured to receive an add transmitter request including a transmitter code from a remote computer via a network. The communication circuitry is configured to receive a radio frequency control signal from an unknown transmitter, the radio frequency control signal including a fixed code of the unknown transmitter. The apparatus further includes a processor configured to store, in the memory, the transmitter code of the add transmitter request received from the remote computer. The processor is further configured to determine whether to operate a movable barrier based at least in part upon whether the fixed code of the radio frequency control signal received from the unknown transmitter corresponds to the transmitter code received from the remote computer. Because the communication circuitry receives the transmitter code from the remote computer, the processor may place the transmitter code of an unknown transmitter on a transmitter whitelist stored in the memory of the movable barrier operator apparatus. The processor may decide to operate a movable barrier in response to receiving a control signal having a fixed code corresponding to the transmitter code stored in the whitelist without requiring a user to perform a conventional learning process with the transmitter and the movable barrier operator apparatus.

[0019] In some embodiments, a method for operating a movable barrier operator apparatus is provided. The method comprises receiving an add transmitter request including a transmitter code from a remote computer via communication circuitry of the movable barrier operator apparatus. The method includes storing, with a processor of the movable barrier operator apparatus, the transmitter code of the add transmitter request in a memory of the movable barrier operator apparatus. The method includes receiving, at the communication circuitry of the movable barrier operator apparatus, a radio frequency control signal from an unknown transmitter, the radio frequency control signal including a fixed code of the unknown transmitter. The method further includes determining, with the processor, whether to operate a movable barrier based at least in part upon whether the fixed code received from the unknown transmitter corresponds to the transmitter code received from the remote computer. The method thereby permits a movable barrier operator apparatus to respond to a control signal from a transmitter even if the transmitter is unknown to the movable barrier operator apparatus.

[0020] In some embodiments, a transmitter programmer apparatus is provided. The apparatus comprises communication circuitry configured to communicate with a remote computer via a network. The communication circuitry is configured to communicate with a transmitter, the transmitter operable to transmit a radio frequency control signal to a movable barrier operator apparatus. The transmitter programmer apparatus includes a processor configured to communicate a transmitter pairing request to the remote computer via the communication circuitry, receive a transmitter fixed code associated with a movable barrier operator from the remote computer in response to the transmitter pairing request, and program, via the communication circuitry, the transmitter to transmit a modified radio frequency control signal including the transmitter fixed code to actuate the movable barrier operator apparatus.

[0021] In some embodiments, a method for transmitter programming is provided. The method comprises, at a transmitter programmer apparatus, sending a transmitter pairing request to a remote computer, receiving a transmitter fixed code associated with a movable barrier operator from the remote computer in response to the transmitter pairing request, and programing a transmitter to transmit a modified radio frequency control signal including the transmitter fixed code to actuate the movable barrier.

[0022] In some embodiments, a server system for brokering movable barrier access is provided. The server system comprises communication circuitry configured to communicate with a plurality of user devices and a plurality of movable barrier operator apparatuses, and a processor operably coupled to the communication circuitry. The processor is configured to receive a transmitter pairing request from a user device requesting to access a movable barrier operator apparatus via a transmitter, verify the transmitter pairing request, and send an add transmitter request to the movable barrier operator apparatus, the add transmitter request including a transmitter code associated with the transmitter and configured to cause the movable barrier operator apparatus to store the transmitter code in a memory of the movable barrier operator apparatus.

[0023] In some embodiments, a method for brokering movable barrier access is provided. The method comprises, at server computer, receiving, via communication circuitry of the server computer, a transmitter pairing request from a user device requesting to access a movable barrier operator apparatus via a transmitter, verifying, with a processor of the server computer, the transmitter pairing request, and sending, via the communication circuitry, an add transmitter request to the movable barrier operator apparatus, the add transmitter request including a transmitter code associated with the transmitter and configured to cause the movable barrier operator apparatus to store the transmitter code in a memory of the movable barrier operator apparatus.

DETAILED DESCRIPTION

[0001] Prior to controlling a movable barrier operator with a transmitter, a user generally needs to pair the movable barrier operator with the transmitter. One prior approach for programming a garage door operator to respond to command signals from the remote control involves a user pressing a button on the garage door opener to cause the garage door opener to enter a learn mode. A user then manipulates the remote control to cause the remote control to send a control signal including an identification portion and a code portion. The code portion may include a rolling code. Because the garage door opener received the command signal when the garage door opener was in the learn mode, the garage door opener stores the identification portion and the code portion. After the garage door opener exits the learn mode, the garage door opener will respond to

command signals from the remote control because the identification portion and the code portion will be recognized by the garage door opener.

[0002] One problem with this approach is that garage door openers are often mounted to ceilings of garages. A user will typically have to get on a ladder or use an object such as, for example, a broom handle to press the learn mode button on the garage door opener. These interactions are inconvenient for a user.

[0003] This prior approach becomes even more inconvenient when a user is attempting to program a transmitter of a vehicle. In this situation, the user uses a ladder or a broom to press the learn button on the garage door opener. Then, the user may have to interact with buttons or a display of the vehicle to cause the transmitter to send one or more signals to the garage door opener. For some vehicles, the built-in transmitter rapidly transmits one signal after another with changing signal formats in an attempt to find one compatible with the garage door opener.

[0004] The garage door opener learns the first compatible signal sent by the universal transmitter of the vehicle; however, the transmitter does not know which of the signals it sent was learned. The user will then have to wait for the transmitter to cycle through the signals again slowly and wait for the signal that actuates the garage door opener. When the user observes the garage door begins to move, the user pushes a button of the transmitter or vehicle display within a window of time before the next signal is transmitted to confirm that the most recent signal sent is the signal the garage door opener has learned. If the user successfully presses the button within the time window, the transmitter will know that the most recently transmitted signal was the correct signal and will stop sending signals. If the user does not press the button within the time window, the transmitter will send the next signal and the user may have to repeat the process.

[0005] Causing a garage door opener to learn a transmitter according to this process presents many opportunities for a user to deviate from the process and be unable to program the transmitter to an opener. Further, the user may feel uncomfortable with the timing and user interactions required by the process.

[0006] Some prior systems attempt to address some of the inconvenience faced by users when attempting to cause a garage door opener to learn new a transmitter. For

example, one prior vehicle-based transmitter sold under the Homelink® brand name allows a vehicle to copy a signal transmitted by a hand-held transmitter that was previously learned by the garage door opener. The transmitter adds an automotive identifier to the copied signal to indicate the signal is from the vehicle-based transmitter rather than the hand-held transmitter.

[0007] The transmitter then transmits the copied signal with the automotive identifier to the garage door opener. If the garage door opener receives the copied signal and the automotive identifier together within a fixed period of time, the garage door opener learns the transmitter.

[0008] While a user does not have to climb a ladder or use a broom handle to put the movable barrier operator into a learn mode, inconvenience may still exist because a user may need to perform particular steps which may be complex, unclear or unforgiving such that programming/learning is not successful. For example, a user may be required to take an existing transmitter already paired to the garage door and transmit the signal to the vehicle. The user must know which transmitter button to press, where to point the transmitter, when to do so and for how long the button must be pressed. Additionally, if the garage door opener has not learned a transmitter or the learned transmitter is broken or lost, the user may be stuck setting up a transmitter by the inconvenient traditional approach described above.

[0024] Systems, methods, and apparatuses for pairing a movable barrier operator with a transmitter are described herein. One example method includes, at a movable barrier operator, receiving a hashed version of a fixed code associated with a transmitter from a server computer, receiving a state change request from a transmitter, and comparing a fixed code of the state change request with the hashed version of the fixed code to determine whether to respond to the state change request and/or store the fixed code in its learn table. The movable barrier operator may perform the comparing operation by performing a hash function on the fixed code of the state change request and determine whether there is a match with the hashed version of a fixed code received from the server computer. As used herein, a hashed version of a fixed code refers to the result of performing a hash function on a transmitter fixed code. Devices in the system may agree upon a hash function such that the same fixed code would result in the same hashed

version of the fixed code at each device. In some embodiments, a salt may be used with the hashing function and the devices (e.g., movable barrier operator and server computer) in the system may be similarly salted or performed relative to the same salt.

[0025] Referring now to the drawings and especially to FIG. 1, a movable barrier operator, such as a garage door opener system 10, is provided that includes a garage door opener 12 mounted within a garage 14. More specifically, the garage door opener system 10 includes a rail 18 and a trolley 20 movable along the rail 18 and having an arm 22 extending to a multiple paneled garage door 24 positioned for movement along a pair of tracks 26 and 28. The system 10 includes one or more transmitters, such as a hand-held or portable transmitter 30, adapted to communicate a status change request to the garage door opener 12 and cause the garage door opener 12 to move the garage door 24. In one embodiment, the state change request includes one or more radio frequency (RF) signals communicated between the transmitter 30 and an antenna 32 of the garage door opener 12. The transmitter 30 is generally a portable transmitter unit that travels in a vehicle and/or with a human user. The one or more transmitters may include an external control pad transmitter 34 positioned on the outside of the garage 14 having a plurality of buttons thereon that communicates via radio frequency transmission with the antenna 32 of the garage door opener 12. The one or more transmitters 30 may include, for example, a transmitter built into a dashboard or a rearview mirror of a vehicle.

[0026] An optical emitter 42 is connected via a power and signal line 44 to the garage door opener 12. An optical detector 46 is connected via a wire 48 to the garage door opener 12. The optical emitter 42 and the optical detector 46 comprise a safety sensor of a safety system for detecting an obstruction in the path of the garage door 24. In another embodiment, the optical emitter 42 and/or optical detector 46 communicate with the garage door opener 12 using wireless approaches.

[0027] The garage door opener 12 may further include communication circuitry 102 configured to connect to a network such as the Internet via a Wi-Fi router in the residence associated with the garage 14. In some embodiments, the communication circuitry 102 may broadcast a wireless signal similar to a Wi-Fi router to allow a user device (e.g. smartphone, laptop, PC) to connect to a controller 103 of the garage door opener 12 via the communication circuitry 102 to setup or configure the garage door

opener 12. For example, after a user device is wirelessly connected to the garage door opener 12, the user interface of the user device may be used to select a Wi-Fi network ID and input a network password to allow the garage door opener 12 to connect to the internet via the Wi-Fi router in the residence associated with the garage 14. In some embodiments, the garage door opener 12 may provide its specifications and status information to a server computer via the communication circuitry 102. In some embodiments, the garage door opener 12 may receive operation commands such as status change requests from a user device over a network via the server computer. In some embodiments, the communication circuitry 102 may further comprise a short-range wireless transceiver such as a Bluetooth transceiver for pairing with a user device during setup and receiving configurations (e.g. Wi-Fi settings) from the user device.

[0028] The garage door 24 may have a conductive member 125 attached thereto. The conductive member 125 may be a wire, rod or the like. The conductive member 125 is enclosed and held by a holder 126. The conductive member 125 is coupled to a sensor circuit 127. The sensor circuit 127 is configured to transmit an indication of an obstruction to the garage door opener 12 upon the garage door 24 contacting the obstruction. If an obstruction is detected, the garage door opener 12 can reverse the direction of the travel of the garage door 24. The conductive member 125 may be part of a safety system also including the optical emitter 42 and the optical detector 46.

[0029] The one or more transmitters may include a wall control panel 43 connected to the garage door opener 12 via a wire or line 43A. The wall control panel 43 includes a decoder, which decodes closures of a lock switch 80, a learn switch 82 and a command switch 84. The wall control panel 43 also includes an indicator such as a light emitting diode 86 connected by a resistor to the line 43A and to ground to indicate that the wall control panel 43 is energized by the garage door opener 12. Switch closures are decoded by the decoder, which sends signals along line 43A to the controller 103. The controller 103 is coupled to an electric of the garage door opener 12. In other embodiments, analog signals may be exchanged between wall control panel 43 and garage door opener 12.

[0030] The wall control panel 43 is placed in a position such that a human operator can observe the garage door 24. In this respect, the wall control panel 43 may be

in a fixed position. However, it may also be moveable as well. The wall control panel 43 may also use a wirelessly coupled connection to the garage door opener 12 instead of the line 43A.

[0031] The garage door opener system 10 may include one or more sensors to determine the status of the garage door 24. For example, the garage door opener system 10 may include a tilt sensor 135 mounted to the garage door 24 to detect whether the garage door 24 is vertical (closed) or horizontal (open). Alternatively or additionally, the one or more sensors may include a rotary encoder that detects rotation of a transmission component of the garage door opener 12 such that the controller 103 of the garage door opener 12 may keep track of the position of the garage door 24.

[0032] While a garage door is illustrated in FIG. 1, the systems and methods described herein may be implemented with other types of movable barriers such as rolling shutters, slide gates, swing gates, barrier arms, driveway gates, and the like. In some embodiments, one or more components illustrated in FIG. 1 may be omitted.

[0033] FIG. 2 is a block diagram of an example system 200 including a server computer 210, a movable barrier operator 230, a user device 220, and a transmitter 240. The transmitter 240 is configured for actuating the movable barrier operator 230 and may be, for example, a transmitter built into a vehicle or a transmitter clipped to a visor of a vehicle. The transmitter 240 is configured to send and, optionally, receive radio frequency signals. For example, the transmitter 240 may be configured to send a command signal including a fixed code and a variable (e.g. rolling) code. The server computer 210 generally comprises one or more processor-based devices that communicate with a plurality of user devices 220 and a plurality of movable barrier operators 230 to pair transmitters 240 with movable barrier operators 230. The server computer 210 comprises a processor 211, communication circuitry 212, a user account database 213, and a movable barrier operator (MBO) database 214. The processor 211 may comprise one or more of a central processing unit (CPU), a microprocessor, a microcontroller, an application specific integrated circuit (ASIC) and the like. The processor 211 is configured to execute computer-readable instructions stored on a non-transitory computer-readable memory to provide a process for pairing transmitters 240 with movable barrier operators 230. In some embodiments, the processor 211 is

configured to perform one or more operations described with reference to FIGS. 4-7 herein.

[0034] The communication circuitry 212 generally comprises circuitry configured to connect the processor 211 to a network and exchange messages with user devices 220 and movable barrier operators 230. In some embodiments, the server computer 210 may be further configured to use the communication circuitry 212 to exchange access information with servers operated by third-party service providers such as home security services, smart home systems, parking space reservation services, hospitality services, package/parcel delivery services, and the like. In some embodiments, the communication circuitry 212 may comprise one or more of a network adapter, a network port or interface, a network modem, a router, a network security device, and the like.

[0035] The user account database 213 comprises a non-transitory computer-readable memory storing user account information. Each user account record may comprise a user account identifier, log-in credential (e.g. password), associated movable barrier operator identifier(s), and/or associated transmitter(s). In some embodiments, the user account database may further store other user information such as email, phone number, physical address, associated internet protocol (IP) address, verified user devices, account preferences, linked third-party service (e.g. home security service, smart home system, parking space reservation service) accounts, and the like. In some embodiments, the user accounts database 213 may further store one or more transmitter identifiers including transmitter fixed code(s), hash(es) of the fixed code(s), and transmitter globally unique identifiers (TXGUIDs) associated with the user account. Hashing functions that may be utilized include MD5 and Secure Hashing Algorithms (e.g., SHA-1, SHA-2, SHA-256). As used herein, a transmitter code may refer to, for example, a transmitter fixed code and/or a hashed version of a transmitter fixed code. In some embodiments, user accounts database 213 may further comprise access conditions specifying the conditions (e.g. date, time) that the user or another user (e.g. visitor or guest) may be authorized to actuate a particular movable barrier operator. In some embodiments, the access conditions may be defined by a user account associated with the movable barrier operator and/or by a third-party access brokering service provider (e.g. parking space rental service, home-sharing service, etc.). In some embodiments, access conditions may

comprise a number of uses restriction (e.g. singe use, once to enter and once to exit, etc.) and an access time restriction (e.g. next three days, Fridays before 10 am, etc.).

[0036] The movable barrier operator (MBO) database 214 comprises a non-transitory computer-readable memory storing information associated with movable barrier operators 230 managed by the system 200. In some embodiments, the MBO database 214 may record network addresses and/or access credentials associated with a plurality of unique MBO identifiers. In some embodiments, the MBO database 214 may include an entry for each unique MBO identifier issued by a manufacturer/supplier. In some embodiments, the MBO database 214 may further track the operations and status of an MBO over time. In some embodiments, MBOs may be associated with a user account which can configure access authorizations to the MBO. In some embodiments, the MBO database 214 may store access condition information for one or more user accounts authorized to control the MBO. In some embodiments, access authorization may be conditioned upon location, date, time, etc. In some embodiments, the user account database 213 and the MBO database 214 may be combined as a single database or data structure.

[0037] The user device 220 generally comprises an electronic device configured to allow a user (e.g. via a client application executing on the electronic device) to communicate with the server computer 210 to pair a movable barrier operator 230 and a transmitter 240 via the server computer 210. The user device 220 is a computing device and may include or be a smartphone, a laptop computer, a tablet computer, a personal computer (PC), an internet of things (IoT) device, and as some examples. Other examples of the user device 220 include in-vehicle computing devices such as an infotainment system. The user device 220 includes a processor 221, communication circuitry 222, a user interface 223, and a camera 224.

[0038] The processor 221 may comprise one or more of a central processing unit (CPU), a microprocessor, a microcontroller, an application specific integrated circuit (ASIC) and the like. The processor 221 may be configured to execute computer-readable instructions stored on a memory to provide a graphical user interface (e.g. relative to a client application executed by the processor 221) on a display of the user interface 223 and permit a user to pair a transmitter 240 with a movable barrier operator 230 via the

server computer 210. In some embodiments, the graphical user interface may comprise a mobile application, a desktop application, a web-based user interface, a website, an augmented reality image, a holographic image, sound-based interactions or combinations thereof. In some embodiments, the processor 211 of the user device 220 is configured to perform one or more operations described with reference to FIGS. 4-7 herein.

[0039] The communication circuitry 222 is configured to connect the user device 220 with the server computer 210 over a network to exchange information. In some embodiments, the communication circuitry 222 may be further configured to communicate with the transmitter 240. For example, the user device 220 may receive the transmitter fixed code or a hashed version of the fixed code from the transmitter via Bluetooth, Bluetooth low energy (BLE), Near Field Communication (NFC) transmission, etc. In another example, the user device 220 may be configured to program into the transmitter 240 one or more fixed codes and/or deprogram the one or more fixed codes from the transmitter 240 via the communication circuitry 222. In some embodiments, the communication circuitry 222 may be further configured to communicate with the movable barrier operator 230. For example, a movable barrier operator 230 may broadcast a beacon signal which the user device 220 may use to identify the movable barrier operator 230 and request access to the movable barrier operator 230 at the server computer 210. The beacon signal may include, for example, a uniform resource locator (URL) that the user device may use to access a server. The communication circuitry 222 may comprise one or more of a network adapter, a network port, a cellular network (3G, 4G, 4G-LTE, 5G) interface, a Wi-Fi transceiver, a Bluetooth transceiver, a mobile data transceiver, and the like.

[0040] The user interface 223 of the user device 220 comprises one or more user input/output devices. In some embodiments, the user interface 223 comprises one or more of a display screen, a touch screen, a microphone, a speaker, one or more buttons, a keyboard, a mouse, an augmented reality display, a holographic display, and the like. The user interface 223 is generally configured to allow a user to interact with the information provided by the user device 220, such as a graphical user interface for pairing transmitters 240 and movable barrier operators 230. In some embodiments, the user interface 223 on the user device 220 may comprise an optical sensor, such as a camera

224, configured to capture images and/or videos. In some embodiments, the camera 224 may be used to scan visible, machine-readable indicium or indicia (e.g., Quick Response (QR) code, UPC barcode, etc.) and/or human-readable text associated with the transmitter 240. For example, a user may use the camera 224 to capture a barcode on the transmitter 240 and/or transmitter packaging and the processor 221 uses data decoded from the barcode to obtain a TXGUID, a hashed version of a transmitter fixed code, and/or a transmitter fixed code associated with the transmitter 240. As another example, the machine-readable indicium includes an invisible code such as an RFID signal and the communication circuitry 222 includes an RFID transceiver configured to obtain the machine-readable indicium from the transmitter 240.

[0041] The movable barrier operator 230 comprises an apparatus configured to actuate a movable barrier. The movable barrier operator 230 includes a processor 231 or logic circuitry, communication circuitry 232, a motor 233, and a memory 234. In some embodiments, the movable barrier operator 230 may include one or more other components such as those described with reference to FIG. 1 herein. In some embodiments, the movable barrier operator 230 may refer to a combination of a conventional movable barrier operator with a retrofit bridge that provides network capability to the movable barrier operator. An example of a retrofit bridge is the MyQ® Smart garage hub from The Chamberlain Group, Inc. While a motor 233 is shown as part of the movable barrier operator 230, in some embodiments, the movable barrier operator 230 may refer to a retrofit bridge without a motor. For example, a smart garage hub not directedly connected to a motor may store transmitter codes received from the server 210 and include an RF receiver. When the smart garage hub receives an RF command signal including a fixed code that is recognized by the hub but not the head unit, the hub may send a second RF signal using another fixed code previously learned by the head unit to actuate the movable barrier via the motor of the head unit.

[0042] The processor 231 comprises one or more of a central processing unit (CPU), a microprocessor, a microcontroller, an application specific integrated circuit (ASIC), logic circuitry and the like. The processor 231 is configured to execute computer-readable instructions stored on a non-transitory computer-readable memory 234 to control a movable barrier operator based on commands received from one or more

transmitter such as a portable transmitter, a wall-mounted transmitter, an exterior keypad transmitter, a server, a user device, etc. In some embodiments, the processor 231 updates and accesses a learn table stored in the memory 234 of the movable barrier operator 230. The learn table includes codes of wireless transmitters authorized to actuate the movable barrier operator 230. In some embodiments, the learn table stores one or more fixed codes associated with one or more transmitters 240. In some embodiments, the learn table may further store one or more rolling codes associated with the one or more transmitters 240. The learn table may be updated through a learning/programming mode of the movable barrier operator 230. The processor 231 is further configured to communicate with the server computer 210 to receive hashes or fixed codes associated with transmitters 240 not yet stored in the learn table from the server computer 210. The memory 234 of the movable barrier operator 230 may store a table of hashes of authorized, but not yet learned, transmitters 240. When the processor 231 receives a signal from a transmitter 240 transmitting a fixed code not in the learn table, the processor 231 may hash the fixed code to obtain a hashed fixed code and compare the hashed fixed code with the stored hashes to determine whether the transmitter 240 is authorized to actuate the movable barrier operator 230. While "learn table" and "hash table" are generally used herein to describe a record of transmitter codes recognized and accepted by the movable barrier operator 230 for the operation of a movable barrier, transmitter codes may be stored in the memory 234 of movable barrier operator 230 in any data format and structure. In some embodiments, the processor 231 of the movable barrier operator 230 is configured to perform one or more operations described with reference to FIGS. 4-7 herein.

[0043] The communication circuitry 232 is configured to connect the processor 231 of the movable barrier operator 230 with the server computer 210 over a network that may be at least one of wide area and short range. In some embodiments, the communication circuitry 232 may further be configured to communicate with the user device 220. For example, the movable barrier operator 230 may broadcast a beacon signal which the user device 220 may use to identify the movable barrier operator 230 to request access. The communication circuitry 232 may comprise one or more of a network adapter, a network port or interface, a Wi-Fi transceiver, a Bluetooth transceiver, and the like. The communication circuitry 232 also includes a radio frequency (RF) receiver or

transceiver for receiving radio frequency (RF) control signals from known and unknown transmitters. An unknown transmitter generally refers to, for example, a transmitter that has not been paired with (or had been unlearned e.g., previously paired with, but subsequently deleted, deprogrammed or otherwise forgotten) the movable barrier operator locally through the movable barrier operator's learn mode or to a transmitter that has been added to the memory of the movable barrier operator through an add transmitter request from a brokering server but has not yet been used to actuate the movable barrier operator. In some embodiments, the communication circuitry 232 may be integrated into the head unit (e.g. opener 12 of FIG. 1) of a garage door opener or the control box of other types of movable barrier operators. In some embodiments, the communication circuitry 232 may be a separate unit that communicates with the processor 231 of the movable barrier operator 230 via a wired or wireless (e.g. RF, Bluetooth) connection. For example, the communication circuitry 232 may comprise a retrofit bridge connected to the gate operator. The motor 233 is configured to cause a state change of the movable barrier in response to control from the processor 231.

[0044] The transmitter 240 is a wireless device configured to send a state change communication (e.g. request or command) to the movable barrier operator. In some embodiments, the transmitter 240 comprises a handheld remote control. In some embodiments, the transmitter 240 comprises a vehicle-based remote control such as a HomeLink® transmitter. In some embodiments, the state change request includes a fixed code. In some embodiments, the state change request further includes a rolling code. The transmitter 240 may comprise a control circuit, a power source (e.g. battery or wired alternating current or direct current power source), a user interface that may include one or more buttons or switches, and a radio frequency transmitter or transceiver. In some embodiments, the transmitter 240 may be associated with a unique identifier, such as a TXGUID, and/or a machine-readable code (e.g., UPC barcode, QR code, etc.) that can be decoded and used by the user device 220 and/or the server computer 210 to generate and/or retrieve a hashed version of the transmitter fixed code. The unique identifier and/or the machine-readable code may be printed on the transmitter 240 and/or the transmitter's packaging.

[0045] In some embodiments, the transmitter 240 comprises a radio frequency transmitter configured to transmit a single fixed code. For example, the transmitter 240 may comprise a conventional remote control with two or more buttons each configured to cause transmission of a single fixed code. The fixed code(s) may be stored in a memory of the control circuit of the transmitter 240. In some embodiments, the transmitter 240 may not include a network communication circuit, may not communicate with the server computer 210 directly, and/or may be configured to send, but not receive, signals from the movable barrier operator 230. In some embodiments, the transmitter 240 may comprise a conventional one-way (i.e. transmit only) garage door remote.

[0046] In some embodiments, the transmitter 240 may be programmable by the user device 220 such that the fixed code that the transmitter 240 transmits may be provided or altered based on communications with server 210 via the user device 220. For example, the user device 220 may be configured to program the fixed code of the transmitter 240 using a fixed code received from the server computer 210 to allow the transmitter 240 to control a selected movable barrier operator. In some embodiments, the transmitter 240 may further be configured to be deprogrammed by the user device 220 to remove one or more fixed codes stored on its memory. A programmable transmitter 240 may comprise a two-way transceiver such as a Bluetooth transceiver, a near-field communication (NFC) transmitter, infrared (IR) and the like for communicating directly with the user device 220. In some embodiments, a transmitter 240 may comprise programmable and nonprogrammable buttons. In some embodiments, the transmitter 240 may include two or more buttons for sending an RF signal. The user device 220 may be used to individually program each of the two or more buttons to assign different buttons to actuate different movable barrier operators.

[0047] In some embodiments, the transmitter 240 may be integrated with the user device 220 and the connection between the user device 220 and the transmitter 240 may be a wired connector. For example, the user device 220 may comprise an RF transmitter configured to send command signals to movable barrier operators 230.

[0048] While one user device 220, one movable barrier operator 230, and one transmitter 240 are shown in FIG. 2, the server computer 210 (or middleware constituted

by one or more servers) may communicate with a plurality of user devices 220 and movable barrier operators 230 to pair transmitters 240 and movable barrier operators 230.

[0049] Next referring to FIG. 3 an example method 300 for pairing a transmitter with a movable barrier operator according to some embodiments is shown. In some embodiments, one or more of the operations in FIG. 3 may be performed by a user device communicating with a server. In some embodiments, one or more of the operations in FIG. 3 may be performed by the user device 220 described with reference to FIG. 2.

[0050] A system implementing the method 300 may entail a user establishing or otherwise signing up for a user account and/or logging into an existing user account managed by a server of the system. In some embodiments, the server may provide a graphical user interface on the user device to perform one or more operations in FIG. 3. For example, the server computer may include a web server that responds to requests for resources by communicating via html/xml. For example, the server computer may respond to requests include HTML CSS Javascript and and/or offer a RESTful web API that responds with JSON data. The server computer may send asynchronous push notifications that may contain machine readable metadata, in JSON format. These machine-readable pushes may contain pairing or brokering information if the channel is securely encrypted like the web and RESTful APIs.

[0051] In some embodiments, the graphical user interface may comprise a website and/or be instantiated relative to execution of a client application or a mobile application. In some embodiments, the user interface may comprise an application program interface (API) used by one or more applications. For example, a parking space rental mobile application may contain computer executable instructions to perform operations of the method 300.

[0052] In operation 311, the system implementing the method 300 identifies the transmitter 301. In some embodiments, the user device may communicate with the transmitter 301 via a wireless signal (e.g. Bluetooth Low Energy) to obtain one or more of a transmitter unique identifier (e.g., TXGUID), a transmitter fixed code, and a hashed version of the transmitter fixed code. In some embodiments, the user device may receive the transmitter's unique identifier through the user entering the transmitter's unique identifier using a user input (e.g. touch screen) of the user device in response to

prompting the user. In some embodiments, the user device comprises an optical scanner or imaging device such as a camera 302 for capturing a machine-readable code (e.g., QR code, UPC barcode, etc.) or an image of the transmitter unique identifier and/or fixed code. For example, the transmitter 301 may include a QR code that provides the unique transmitter identifier, a fixed code, and/or a hashed version of the fixed code when scanned by the user device's camera and decoded. Alternatively or in addition, the operation 311 involves the user device or server providing a fixed code to the transmitter and the transmitter learning the fixed code. In some embodiments, if the transmitter includes two or more buttons each configured to cause transmission of a control signal, process 311 may further include selecting a specific button on the transmitter. For example, the user interface may prompt the user to indicate which button is being programmed during setup.

[0053] In operation 312, the system identifies the movable barrier operator to pair with the transmitter. In some embodiments, the user may enter a code or an identifier associated with a specific movable barrier operator. For example, a vacation home owner may provide a code or a digital file associated with the garage door opener of the property to a renter's user account such that the renter's transmitter may be paired with the garage door opener via the server prior to the renter's arrival. In some embodiments, the movable barrier operator may be selected from a list of movable barrier operators previously associated with the user account. For example, when a user purchases a new transmitter, the user may obtain the transmitter unique identifier using the optical scanner 302 of the user device and select the user's garage door opener using the user interface of the user device. In some embodiments, the movable barrier operator may comprise a wireless broadcast beacon 303 that transmits a code or identifier of the movable barrier operator. For example, when a renter arrives at a vacation home, the renter's user device may scan for a wireless beacon transmission to obtain an identifier associated with the garage door opener of the vacation home. In some embodiments, the movable barrier operator identifier may be provided by a third-party service or application 304. For example, a vacation home or parking space rental website or application may automatically add the movable barrier operator identifier to the user account of the renter and/or communicate the movable barrier operator identifier to the transmitter pairing

application running on the renter's user device. In some embodiments, the server may receive the movable barrier operator identifier directly from the third party access brokering service provider and match the movable barrier operator identifier to the user's pairing request based on one or more of a user account, a transaction ID, a transmitter ID, a session ID, and the like.

[0054] In operation 313, the user device communicates or generates a pairing request. In some embodiments, the transmitter pairing request comprises at least one of a movable barrier operator identifier, a movable barrier access passcode, a user credential, and a transmitter identifier. In some embodiments, the pairing request includes the transmitter identifier, and the server is configured to retrieve a hash version of the transmitter's fixed code from a transmitter database of the server using the transmitter unique identifier. The transmitter database may be populated by a transmitter manufacturer that programmed the transmitters. In some embodiments, the transmitter may be previously associated with the user account and the pairing request may include a selection of a previously stored transmitter. In some embodiments, the pairing request includes the transmitter's hashed version of a fixed code, and the server is configured to forward the hashed version of the transmitter fixed code to the selected operator. In some embodiments, if the user device receives the transmitter's fixed code in operation 311, the user device may be configured to perform a hash function on the fixed code prior to sending it to the server such that the fixed code itself is not transmitted over the network. In some embodiments, the operator identifier may be included in the pairing request. In some embodiments, the operator identifier may be supplied by a third-party service. In some embodiments, the pairing request may be generated by the third-party service. For example, a user may provide user account information to the third-party access brokering service, and the brokering service provider may supply the operator identifier directly to the server and/or receive a hashed version of the transmitter fixed code to forward to the selected operator.

[0055] In some embodiments, after operation 313, the user device may receive a confirmation from the server after the pairing request is authorized. The confirmation may then be displayed to the user via the user interface of the user device. In some embodiments, the authorization may be conditioned upon time and date, and the access

restrictions may also be displayed along with the confirmation. The user interface may prompt the user to enter a handle or name for the transmitter or a select button on the transmitter. The user may then use the transmitter to operate the selected movable barrier operator according to the granted access condition without further involvement of the user device and the server.

[0056] For a programmable transmitter, the user device may receive a transmitter fixed code from the remote computer in response to the transmitter pairing request and communicate with the transmitter to program the transmitter to transmit a modified control signal including the transmitter fixed code to actuate a movable barrier operator apparatus. In some embodiments, the user device may further receive an access condition associated with the transmitter fixed code and deprogram the transmitter fixed code from the transmitter based on the access condition. For example, if the access condition specifies that access is limited to a set period time, the user device may deprogram the fixed code from the transmitter after time period passes. In some embodiments, operation 311 may be omitted for a programmable transmitter. For example, the user device may communicate a transmitter pairing request to the remote computer via the communication circuitry without identifying a transmitter and select one or more transmitters to program at a later time.

[0057] Next referring to FIG. 4, an example method 400 for brokering movable barrier access according to some embodiments is shown. In some embodiments, one or more of the operations in FIG. 4 may be performed by a server communicating with a user device and a movable barrier operator. In some embodiments, one or more of the operations in FIG. 4 may be performed by the server computer 210 described with reference to FIG. 2.

[0058] In operation 411, the server receives a pairing request from the user device 401. In some embodiments, the pairing request may comprise a transmitter identifier, the transmitter fixed code, and/or a hashed version of the transmitter fixed code. In some embodiments, the pairing request further comprises one or more of an operator identifier and a user account credential. The pairing request may be received over a network such as the Internet. In some embodiments, the server may be configured to validate the pairing request by comparing the transmitter ID and a hashed version of a fixed code (or

fixed code) in the pairing request with a hashed version of the fixed code (or fixed code) associated with the transmitter ID in a transmitter database populated by the transmitter manufacturer. In some embodiments, the server may validate that the transmitter identified in the pairing request by verifying that the transmitter had previously been associated with the requesting user account.

[0059] In operation 412, the server retrieves a transmitter code associated with the transmitter. In some embodiments, if a transmitter unique identifier is provided, the server may retrieve the fixed code or the hashed version of the fixed code from a transmitter database 402 using the transmitter identifier. In some embodiments, if a transmitter includes a plurality of buttons, the pairing request may further identify a specific button and the transmitter code may be retrieved based on the selected button. In some embodiments, each button on a transmitter device may be considered a transmitter or to be configured to control a distinct transmitter, and may be associated with a unique transmitter ID. In some embodiments, the transmitter database 402 is populated by one or more transmitter manufacturers and stores fixed codes and/or hashed version of a fixed codes associated with each unique transmitter identifier produced by the manufacturer. In some embodiments, the server may associate a user account with one or more transmitters, and the transmitter database 402 may store hashed version of the fixed codes of the one or more transmitters as previously provided by the user. For example, the user may provide the fixed code of a transmitter (e.g. operation 311 discussed above) and the server hashes the fixed code and stores the hashed version of a fixed code in the transmitter database 402. In some embodiments, the fixed code and/or the hashed version of a fixed code may be provided by the user device as part of or along with the pairing request received in operation 411. In some embodiments, the user device may directly communicate the fixed code of the transmitter to the server.

[0060] In operation 413, the server verifies access authorization for the pairing request. In some embodiments, the server may verify that the requesting user is authorized to access the selected movable barrier operator. In some embodiments, the verification may be based on at least one of a movable barrier operator access passcode, a user account associated the transmitter pairing request, and a user device location. In some embodiments, the verification may be performed by querying a movable barrier

operator database and/or a user account associated with the operator. For example, the owner of the movable barrier operator may have a list of preauthorized user accounts, and the server may compare the requesting user account against the list of preauthorized user accounts. In another example, a message may be sent to the owner of the operator to request access. In some embodiments, the verification may be performed based on the information provided in the access request. For example, a movable barrier operator may have an access passcode associated with the movable barrier operator in addition to an operator identifier. Access may be granted if the pairing request includes the correct access passcode. In some embodiments, the owner may provide the requesting user a digital file (e.g. authentication cookie) that may be read by the server as proof of access authorization. In some embodiments, access authorization may further include access conditions set by the owner of the movable barrier operator and/or a third-party service. For example, certain user accounts/transmitters may be permitted to operate the movable barrier operator during a select time period (e.g. daytime, rental period) or only a predetermined number of times (e.g. one-time use, one entry and one exit, etc.).

[0061] In operation 414, if the access authorization is verified in operation 413, the server forwards the transmitter code to the movable barrier operator 403. The movable barrier operator 403 may then use the transmitter code to verify state change requests received from the transmitter. If access authorization fails, the server may return an access-denied message to the requesting user device.

[0062] In some embodiments, after operation 414, the server may further communicate with the movable barrier operator apparatus to enforce the access condition based on access condition associated with the transmitter pairing request. For example, if access is granted for a set period of time, at the expiration of the time period, the server may send a remove transmitter request to the movable barrier operator apparatus that is configured to cause the movable barrier operator apparatus to remove the transmitter code from the memory.

[0063] In some embodiments, for a programmable transmitter, operation 412 may comprise generating a new fixed code or retrieving a fixed code associated with a movable barrier operator identified in the pairing request. In such embodiments, after operation 413, the fixed code may be communicated in operation 414 to the user device

401 to program the transmitter to transmit a control signal including the fixed code. In some embodiments, operation 414 may be omitted if the movable barrier operator had previously learned the fixed code selected in step 412. In some embodiments, the fixed code may be communicated to both the user device and the movable barrier operator to broker access.

[0064] Next referring to FIG. 5, an example method 500 for pairing a transmitter with a movable barrier operator according to some embodiments is shown. In some embodiments, one or more of the operations in FIG. 5 may be performed by a movable barrier operator communicating with a server. In some embodiments, one or more of the operations in FIG. 5 may be performed by the movable barrier operator 230 described with reference to FIG. 2.

[0065] In operation 511, the movable barrier operator receives a hashed version of a transmitter fixed code from a server 501 and stores the hashed version of the fixed code in a hash table 503. The hash table 503 generally comprises a computer-readable memory storage. In some embodiments, the hash table 503 may be implemented on the same physical device as the learn table 504. In some embodiments, the hashed versions of fixed codes in the hash table 503 may be automatically deleted if not used for a set period of time. In some embodiments, one or more hashed versions of fixed codes in the hash table 503 may have associated access conditions (e.g. date/time).

[0066] In operation 512, the movable barrier operator receives a state change request from a transmitter 502. The state change request may comprise an RF signal comprising a fixed code and/or a rolling code. In operation 513, the operator determines whether the fixed code and/or rolling code transmitted by the transmitter 502 is in the learn table 504. The learn table 504 generally stores the fixed and/or rolling code of a transmitter already paired with the movable barrier operator. If the fixed code and/or the rolling code matches a known transmitter, in operation 515, the operator actuates the movable barrier to cause a state change of the movable barrier.

[0067] If the fixed code is not associated with a known transmitter in the learn table 504, at operation 514, the movable barrier operator calculates a hash of the received fixed code and determines whether the calculated hash of the received fixed code matches a hashed version of a fixed code in the hash table 503. If the hashed version the

fixed code received from the transmitter does not match any record in the hash table 503, the process terminates in operation 520 and the operator does not respond to the state change request.

[0068] If the hashed version of the received fixed code matches an entry in the hash table 503 at operation 514, the process 500 proceeds to operations 515 and/or 516. In some embodiments, the operator may also determine whether the access conditions (e.g. time of day, number of entries/exits) associated with the matching hashed version of a fixed code has been met before proceeding to operation 515 and/or operation 516. In some embodiments, the entries in the hash table 503 may be added or deleted by the server to enforce access conditions. In some embodiments, after finding a match in the hash table 503 the movable barrier operator updates the learn table in operation 516 by adding the received fixed code to the learn table to allow the transmitter to control the movable barrier operator in the future. In some embodiments, the movable barrier operator also synchronizes with the rolling code of the transmitter in operation 516 and stores the rolling code information in the learn table 504. In some embodiments, the associated hashed version of a fixed code may be removed from the hash table 503 after operation 516. In some embodiments, in operation 515, the same transmitter transmission used to update the learn table 504 may also cause the barrier to be actuated. In some embodiments, a second transmission is used to actuate the barrier.

[0069] In some embodiments, the movable barrier operator may actuate the barrier in operation 515 without updating the learn table, omitting operation 516. For example, the operator may instead be configured to query the hash table 503 each time a state change is requested by the transmitter. This approach may be taken for transmitters with access restrictions such that the records in the hash table 503 are dynamically added and removed to control access for transmitters with temporary access whereas the learn table 504 stores fixed codes of transmitters with permanent access. In some embodiments, the fixed codes of transmitters with conditional access may be stored in the hash table 503 or in a separate computer readable storage area. In some embodiments, records (fixed code and/or hashed version of a fixed code) in the learn table 504 and/or the hash table 503 may be modified based on access conditions by the operator and/or the server to enforce access authorization conditions. For example, a transmitter's hashed

version of a fixed code may be removed from the hash table 503 and/or the transmitter's fixed code may be removed from the learn table 504 when the authorized access period (e.g. rental period) expires. In another example, a hashed version of a fixed code with one-time use restriction may be removed from the hash table 503 after the hashed version of a fixed code is matched with a hashed version of a fixed code associated with a transmitter transmission.

[0070] In some embodiments, the transmitter fixed code may be used in one or more operations of FIG. 5 instead of the hashed version of the fixed code. For example, a transmitter fixed code may be received in operation 511. The movable barrier operator may add the received fixed code associated with a previously unknown transmitter to the learn table 504 without going through the conventional learn mode. In such embodiments, the hash table 503 and operation 514 may be omitted. If the fixed code is not found in the learn table in operation 513, the process will directly terminate at operation 520. In some embodiments, even when fixed codes are received in procedure 511, the movable barrier operator may still separately store fixed codes with permanent access permission (e.g. added through learn mode) and fixed codes with conditional access permission (e.g. added through an access brokering server with attached access condition). For example, the head unit may store a set of fixed codes learned through the learn mode while a retrofit bridge (e.g. smart garage hub) may store transmitter codes received from the server.

[0071] Now referring to FIG. 6, an example method 600 for pairing a transmitter with a movable barrier operator according to some embodiments is shown. In some embodiments, the operations in FIG. 6 may be performed using a user device, a transmitter, a server, and/or a movable barrier operator. In some embodiments, one or more operations in FIG. 6 may be performed by one or more of the user device 220, the transmitter 240, the server computer 210, and the movable barrier operator 230 described with reference to FIG. 2 herein.

[0072] In operation 601, the user device identifies the transmitter. In some embodiments, operation 601 may comprise operation 311 as shown in FIG. 3 and described previously. The user device then sends the transmitter unique identifier, transmitter fixed code, and/or hashed version of the fixed code to the server. In some

embodiments, in operation 602, the user device further identifies the operator to pair with the transmitter. In some embodiments, operation 602 may comprise operation 312 as shown in FIG. 3 and described previously. The user device then sends the operator identifier to the server.

[0073] In operation 611, the server retrieves the hashed version of a transmitter fixed code from the user device and/or a transmitter database. In some embodiments, operation 611 may comprise operation 412 as shown in FIG. 4 and described previously. The server then forwards the hashed version of the fixed code to the movable barrier operator identified by the user device. In operation 621, the movable barrier operator stores the hashed version of the transmitter fixed code.

[0074] In operation 631, the transmitter transmits a state change request. In some embodiments, operation 631 may comprise a radio frequency transmission from a handheld or in-vehicle transmitter. In operation 622, the movable barrier operator receives the transmitted state change request, performs a hash function on the fixed code of the state change request from the transmitter with the stored hashed version(s) of fixed code(s) received from the server. In some embodiments, operation 622 may comprise operation 514 as shown in FIG. 5 and described previously. In operation 624, the movable barrier operator changes the barrier state if the fixed code of the transmitter matches a hashed version of a fixed code received from the server. In some embodiments, the operator may further update a learn table as described in operation 516 as shown in FIG. 5 and described previously.

[0075] Now referring to FIG. 7, an example process for pairing a transmitter with a movable barrier operator according to some embodiments is shown. In some embodiments, the operations in FIG. 7 may be performed using a transmitter programmer, a transmitter, a server, a pairing application running on a user device, and/or a movable barrier operator (such as a garage door opener (GDO) as shown in FIG. 7). In some embodiments, one or more operations in FIG. 7 may be performed by one or more of the user device 220, the transmitter 240, the server computer 210, and the movable barrier operator 230 described with reference to FIG. 2 herein.

[0076] During manufacturing, a transmitter programmer 701 of a manufacturer seeds a transmitter with a fixed code, a rolling code, and a transmitter globally unique

identifier (TXGUID). The programmer 701 calculates and stores the hashed version of a fixed code and the TXGUID at a server 703.

[0077] Next as shown, a pairing application 704 starts the setup process and allows a user to select a garage door opener (GDO) 705. The device running the application 704 has stored or retrieves a movable barrier operator ID for the selected GDO 705. The application 704 queries the transmitter 702 for the TXGUID and receives the TXGUID in return. The application 704 then sends the TXGUID and the movable barrier operator device ID to the server 703 in a pairing request. In response to receiving the request, the server 703 looks up or calculates the hashed version of the fixed code associated with the TXGUID. The server 703 then communicates or generates a pairing request comprising the hashed version of the fixed code and an "enter learn mode" command to the selected GDO 705. In response, the GDO 705 may send a confirmation for learn mode to the server 703, which is forwarded to the application 704. The application 704 can then instruct the transmitter 702 (or alternatively prompt a user to actuate the transmitter 702) to send a transmission. The transmission from the transmitter 702 may comprise a fixed code and a rolling code. Upon receiving the transmission from the transmitter 702, the GDO 705 computes the hash of the transmitter fixed code and compares the hashed version of the received fixed code to the hashed version of the fixed code received from the server 703. If a match is confirmed, the GDO 705 adds a learn table entry for the transmitter 702. A "transmitter added" message, including the transmitter identifier, is then sent to the server 703. When the GDO 705 and the transmitter 702 are successfully paired, the server 703 sends the application 704 a message which then allows the application 704 to give a name to the transmitter to be stored at the server.

[0078] During operation of the movable barrier operator, the transmitter 702 sends a state change request including fixed code and a rolling code to the GDO 705, to actuate the movable barrier such as via a radio frequency signal. As shown in FIG. 7, once the setup process is completed, the transmitter is configured to control the movable barrier operator without further involvement of the application 704 and the server 703.

[0079] The operations in FIGS. 3-7 are provided as example processes according to some embodiments. In some embodiments, one or more operations in FIGS. 3-7 may

be omitted, combined, or modified without departing from the spirit of the present disclosure. For example, the transmitter identifier and/or the hashed version of a fixed code may be obtained by the server through one or more ways described herein. The operator identifier may also be supplied from various sources including the user device, a movable barrier operator owner, and/or a third-party service. In some embodiments, enforcement of access conditions may be performed by the server, the movable barrier operator, and/or a third-party service communicating with the movable barrier operator. In some embodiments, the systems and methods described herein allow a network-enabled movable barrier operator to be operated by a new transmitter through the use of a hashed version of the transmitter fixed code to avoid transmitting the transmitter fixed code over the network. In some embodiments, the operator includes a learn table and a more temporary hash table (or two learn tables) that separately store codes associated with transmitters with permanent access and conditional access. In some embodiments, the hash table and the learn table may be collectively referred to as a dynamic learn table. In some embodiments, the learn table may be dynamically managed by the movable barrier operator and/or the server to enforce access conditions for a plurality of transmitters. In some embodiments, the user device may be used to program a transmitter to transmit a fixed code supplied by the server. For example, the server may generate a fixed code, send the fixed code to the user device which provides the fixed code to the transmitter, and/or send the fixed code or hashed version of the fixed code to the movable barrier operator such that the movable barrier operator can recognize the transmitter as an authorized transmitter.

[0080] While FIGS. 3-7 generally describes using hashed versions of transmitter fixed codes in the communications between user devices, the server, and movable barrier operators, in some embodiments, one or more operations described herein may be performed with unhashed transmitter fixed codes. For example, a pairing request may contain a transmitter fixed code that is sent to the movable barrier operator without being hashed. The movable barrier operator may then compare the received signal with the stored fixed code to determine whether the transmitter is authorized for access without performing a hash function on the received signal's fixed code.

[0081] In some embodiments, the systems and methods described herein use server/middleware connectivity to broker communications and access between a transmitter and a movable barrier operator that have not previously exchanged an RF radio packet. The server may have a trusted relationship with both the transmitter and operator. This server brokers an exchange where a token is given to the transmitter or operator to be used for long-term pairing or one-time access. This token can also be given a time to live or persist until it is revoked. In some embodiments, a movable barrier operator may be enhanced with this function. In some embodiments, one or more functions described herein may be added through a retrofit bridge such as a MyQ® smart garage hub from The Chamberlain Group, Inc.

[0082] In some embodiments, with the methods and systems described herein, a new transmitter may be added to a customer account to operate a movable barrier operator without having to pair the transmitter and the movable barrier operator locally after unboxing. Pairing and management of transmitters may be coordinated through an application and a server over a network. In some embodiments, a customer may pair a specific button or buttons of a transmitter, such as buttons of a HomeLink® transmitter, with network-connected operators remotely and be able to control a movable barrier with the convenience of pressing a physical button without operating their user device such as a mobile phone. The methods and systems described herein permit the buttons of a transmitter to each be paired with a different movable barrier. For example, the operation 311 may include determining an identifier of a button of the transmitter the user wants to program to operate a particular movable barrier operator. In one embodiment, the user may pair the first two buttons of a transmitter with two garage door openers of the user's home. After reserving a parking space using a parking space reservation application or website via the user device, the user may pair the third button of the transmitter with a movable barrier operator of a parking structure that contains the parking space. The user can then drive up to the parking structure and press the third button to cause the movable barrier operator of the parking structure to move the associated barrier. The user does not need to locally pair the transmitter and the movable barrier operator because a server of the parking space reservation service has already instructed a server associated with the

movable barrier operator to pair the transmitter and the movable barrier operator upon the user reserving the parking space.

[0083] In some embodiments, the features described herein may comprise a modification to the movable barrier operator and/or may be added through a retrofit bridge. In some embodiments, the system allows identifying information for a transmitter to be inserted into a learn table when the transmitter is present. In some embodiments, the system allows the operator to accept a one-time command from a transmitter. In some embodiments, the system allows an un-provisioned HomeLink® button to be trained remotely to operate a movable barrier operator. In some embodiments, the operator may be configured to receive a fixed code generated by a server and then send an encrypted fixed /roll over a low-band radio channel to a user device and/or a transmitter. In some embodiments, the operator may send data representative of a fixed/roll code received over a low band radio channel to a server such as via the Internet for verification. In some embodiments, the operator may comprise a beacon transmitting a signal receivable by new users seeking to request access to the movable barrier operator.

[0084] In some embodiments, the transmitter may include a code to facilitate setup. In some embodiments, the transmitter may comprise a Bluetooth Low Energy (BLE) transceiver to facilitate setup from a user device such as a smartphone or tablet. In some embodiments, the BLE may also be used for firmware updates and/or dynamic fixed codes. In some embodiments, the BLE may be used to maintain constant communication with a mobile application on the smartphone even if an application for operating or adjusting the transmitter is only running in the background.

[0085] This disclosure provides a system and method to set up a remote control 812 for a controllable device 825, such as a movable barrier operator, light, or other electronic device. With reference to FIG. 8, a system 801 is provided including one or more remote controls 812, one or more controllable devices 825, and a remote server 835. The remote server 835 may include one or more computers that provide functionality for an account platform 1020 (see FIG. 10A), one or more of the remote controls 812, one or more controllable devices 825, and one or more interface systems 915 (see FIG. 11). The one or more controllable device 825 may include, for example, a movable barrier operator 830, a lightbulb, a lock, and/or a security system. The one or

more remote controls 812 may include, for example, a keypad near a garage door, a portable electronic device, and/or a transmitter 810 of a vehicle 850. The transmitter 810 may include, for example, a transmitter built into the vehicle 850, a transmitter sold with the movable barrier operator 830 that may be clipped onto a visor of the vehicle 850, or an aftermarket universal transmitter that may be mounted in the vehicle 850. The universal transmitter may be programmable to operate movable barrier operators from different manufacturers. Regarding FIG. 11, the user interacts with the transmitter 810 via the interface system 915. The interface system 915 may take the form of, for example, a component of the vehicle 850 or a component of a user's device such as a desktop computer, a smartphone, or a tablet computer. The interface system 915 is operatively connected 1127 to the transmitter 810. The connection 1127 may be, for example, a permanent wired connection or a temporary connection such as via a short-range wireless communication protocol.

[0086] The transmitter 810 controls operation of the movable barrier operator 830 by sending a communication 840 to the movable barrier operator 830. The communication 840 may be communicated wirelessly via radio frequency (RF) signals in the 300 MHz to 900 MHz range. The communication 840 may include a fixed portion and a variable or changing (e.g., rolling code) portion. The fixed portion may include information identifying the transmitter 810 such as a unique transmitter identification (ID) and an input ID. If an input ID is used, the input ID may identify which button on the transmitter 810 causes the transmitter to send the particular communication 840. The transmitter IDs are fixed codes that are unique to each transmitter device 810. The variable portion of the communication 840 includes an encrypted code that changes, e.g., rolls, with each actuation of the input of the transmitter 810. As another example, the communication 840 may include a message communicated via cellular, Wi-Fi, WiMax, LoRa WAN, Bluetooth, Bluetooth Low Energy (BLE), Near Field Communication (NFC) or other approaches. The communication 840 may be direct, such as a radio frequency signal transmitted between the transmitter 810 and the controllable device 825. The communication may be indirect, such as a message communicated via one or more networks 834 to the remote server 835 and the remote server 835 sending an associated message to the controllable device 825.

[0087] In one embodiment, the system 801 permits a user to set up the transmitter 810 to operate the movable barrier operator 830 without having to cause the movable barrier operator 830 to enter a learning mode. This simplifies setup because the user does not have to manually cause the movable barrier operator 830 to enter the learn mode, nor does the transmitter 810 have to be operated to perform a trial-and-error approach to determine the correct signal characteristic(s) that will cause operation of the movable barrier operator 830. Rather, the remote server 835 communicates remote control information for the transmitter 810 to the movable barrier operator 830 and/or the transmitter 810. The remote control information may include, for example, a fixed component of the communication 840 such as a transmitter ID and a button ID and a variable component of the communication 840. As a few examples, the variable portion of the communication 840 may include an initial roll of a rolling code or may include data indicative of the rolling code so that the movable barrier operator 830 and/or the remote control 812 will be able to determine the current roll of the rolling code based on the data.

[0088] In one approach, the remote server 835 pushes the remote control information to the movable barrier operator 830. The remote server 835 causes the movable barrier operator 830 to learn the transmitter 810 and respond to signals 840 from the transmitter 810 by, for example, directing the movable barrier operator 830 to put the transmitter on a whitelist of learned transmitters. In another embodiment, the remote server 835 pushes the remote control information to the transmitter 810 and the transmitter 810 configures itself to use the remote control information to transmit communications 840 to the movable barrier operator 830. In another approach, the transmitter 810 and/or the movable barrier operator 830 will pull the remote control information from the remote server 835. The transmitter 810 and/or the movable barrier operator 830 may poll the remote server 835 according to a random or set time period or in response to an event, such as a user instructing the transmitter 810 to poll the remote server 835, to determine when there is remote control information to be pulled from the remote server 835.

[0089] Regarding FIG. 8, the system 801 may include a vehicle database 832 operated by a vehicle manufacturer or a supplier in communication with the remote

server 835. The vehicle manufacturer database 832 may store a vehicle identification number (VIN) for the vehicle 850 and a transmitter ID for the transmitter 810. The vehicle manufacturer database 832 may also store information related to the changing code of the signal transmitted by the transmitter 810, such as a seed value. In one embodiment, the remote server 835 will query the vehicle database 832 upon the remote server 835 receiving a request for the movable barrier operator 830 to learn the transmitter 810. The vehicle database 832 sends the remote control information (e.g., a transmitter ID and changing code) for the transmitter 810 to the remote server 835, which communicates the remote control information for the transmitter 810 to the movable barrier operator 830. The movable barrier operator 830 then puts the remote control information for the transmitter 810 on the whitelist stored in the memory of the movable barrier operator 830. In this manner, the movable barrier operator 830 will respond to a communication 840 sent from the transmitter 810 because the communication 840 will include the remote control information on the whitelist.

[0090] Regarding FIG. 8, the transmitter 810 may communicate with the movable barrier operator 830 by sending and/or receiving communications 840. The communications 840 may be transmitted wirelessly such as via radio frequency (RF) signals in the 300 MHz to 900 MHz range. Regarding FIGS. 9 and 10A, the transmitter 810 may be operatively connected to an interface system 915 of the vehicle 850. The interface system 915 includes a human machine interface 945 that may include, for example, a display, a microphone, a speaker, or a combination thereof. The human machine interface 945 may include a vehicle infotainment system in a center stack of the vehicle 850 or an electronic dashboard as some examples. The human machine interface 945 may include one or more physical or virtual buttons that may be selected or actuated to program the transmitter 810 and operate the transmitter 810 when desired by a user. The display may include an icon of the account platform 1020 that causes the interface system 915 to operate the transmitter 810 and control the movable barrier operator 830. The transmitter 810 may be connected to a vehicle bus to receive power and communicate with components of the vehicle 850. In yet another embodiment, the human machine interface 945 includes physical buttons that are disposed on a driver-side visor, a rear-view mirror, or a dashboard of the vehicle 850. In another embodiment, the interface

system 915 is a component of a user device such as the smartphone 837. The interface system 915 connects to the transmitter 810 by a communication device 1180 of the interface system 915 using a short-range wireless communication protocol such as Bluetooth.

[0091] The system 801 utilizes an account platform 1020 to configure and manage the remote controls 812 that are authorized to operate the movable barrier operator 830. The remote server 835 stores for a given user account, user account information including an ID of the movable barrier operator 830, information identifying the authorized remote controls including transmitter ID and button ID, and the user's login information for the user account. The user may utilize a computing device, such as a desktop computer, laptop computer, tablet computer, or smartphone 837 to provide the account information to the remote server 835. The computing device may connect to the remote server 835 via one or more networks including the internet.

[0092] In one embodiment, the user has an account configured for the account platform 1020 with which movable barrier operator 830 has been associated. The user may associate the transmitter 810 with the movable barrier operator830 so that the transmitter 810 may operate the movable barrier operator 830. More specifically, upon the user entering the vehicle 850, such as when the user is purchasing the vehicle or renting the vehicle, the user may log into the user's account by selecting an icon for the account platform 1020 on a display of the human-machine interface 945 and entering the correct user name and password into the human-machine interface 945. In examples where the interface system 915 is a component of the vehicle 850, the vehicle 850 includes the communication device 1180 for connecting to the remote server 835 via one or more networks, such as a wireless wide area network and the internet. The one or more networks may include networks utilizing 4G LTE, 5G, LoRaWAN, WiMax approaches. The communication device 1180 of the vehicle 850 establishes a wireless connection for communications 840 that transmit and receive data from the remote server 835.

[0093] Upon the user successfully logging into the user's account, the remote server 835 communicates data indicative of the movable barrier operator 830 associated with the user's account. The human-machine interface 945 may display a graphical user interface that allows the user to select an input of the transmitter 810, which may be for

example a physical button of the transmitter 810 or a digital button of the human-machine interface 945, to associate with the movable barrier operator 830. The user interacts with the human-machine interface 945, such as by pressing a portion of the display of the human-machine interface 945, to indicate which input of the transmitter 810 should be operable to cause the transmitter 810 to send the communication 840 to the movable barrier operator 830 and cause operation of the movable barrier operator 830. In another example, the human-machine interface 945 is configured to communicate with the user using audio, such as allowing the user to verbally select an input of the transmitter 810 to associate with a remote device 825.

[0094] Once the user associates the input of the transmitter 810 with the movable barrier operator 830, the remote server 835 communicates the remote control information for the transmitter 810 to the movable barrier operator830 so that the movable barrier operator830 will operate in response to receiving the communication 840 from the transmitter 810. The movable barrier operator830 adds the remote control information to the whitelist of the movable barrier operator 830 and may thereby learn the transmitter 810 before the user drives the vehicle 850 away from the car dealership or car rental lot.

[0095] The remote server 835 facilitates operation of the account platform 1020 (see FIGS. 10A and 10B) of the user account. The account platform 1020 may include middleware and one or more user-facing applications that operate to connect the user to the details of her user account including the user's remote controls and controllable devices 825. For example, the account platform 1020 may include the myQ® application offered by Chamberlain® and running or installed in a user's smartphone 837 or the human-machine interface 945. As another example, the account platform 1020 may include a website accessible by an internet browser. The remote server 835 maintains a list of the controllable devices 825 associated with the user's account as well as the remote controls 812 that are authorized to operate the controllable devices 825. The remote server 835 may provide data representative of the list to the interface system 915. The human-machine interface 945 displays the account platform 1020, which in an embodiment includes icons graphically representing the controllable devices 825 and the remote controls 812, to the user and permits the user to readily select which user input on a given remote control 812 the user would like to cause one or more of the controllable

devices 825 to learn. The input of the remote control 812 may be a physical button, an icon displayed on a screen, or a spoken secret word as some examples.

[0096] With reference to FIGS. 10A and 10B, a method 1041 is provided as an example of how a transmitter of a vehicle may be learned by a movable barrier operator in accordance with the disclosures herein. Although the method 1041 discloses learning of a vehicle transmitter by a movable barrier operator, the method 1041 may be similarly utilized to cause other controllable devices 825 to learn one or more remote controls. For example, the controllable devices 825 may include a light, a security system, a lock, or a combination thereof.

[0097] In one embodiment, the controllable device 825 is configured to delete the remote control information for the transmitter 810 from the whitelist of the controllable device 825 after the transmitter 810 has operated the controllable device 825 using the communication 840. For example, a user may purchase a one-time use of a parking spot of a parking lot/garage using a parking application running on the user's smartphone 837. A parking server 839 (see FIG. 8) associated with the parking application communicates with the remote server 835 and causes the remote server 835 to send the remote control information of the transmitter 810 to a controllable device 825 (e.g. such as a gate operator) of a parking garage that contains the parking spot. The remote server 835 may also communicate a number of entries permitted by the vehicle 850, such as one entry or ten entries, for example. Alternatively or additionally, the remote server 835 may communicate a parking time window/duration after which the user may incur additional charges or fees if the vehicle has not timely exited the parking garage. The gate operator adds the remote control information for the transmitter 810 to the whitelist of the gate operator. When the user pulls up to the gate operator and causes the transmitter 810 to transmit the communication 840, the gate operator recognizes the communication 840 and opens the gate. After the vehicle 850 has pulled into the parking garage, the gate operator erases the transmitter 810 from the whitelist if the number of entries indicated by the remote server 835 is one. If the number of entries is one, the remote control information may include the transmitter ID but not the variable component of the communication 840. This is because the gate operator need only identify the transmitter 810 for the single use and is not concerned with a subsequent roll of the variable

component. If the number of entries is greater than one, the gate operator may locally monitor of the number of entries and delete the remote control information for the transmitter 810 upon the number of entries being reached. Alternatively, the remote server 835 and/or the gate operator may monitor the number of entries and the gate operator sends a communication to the gate operator after each time the transmitter 810 has operated the gate operator. In the parking garage or other access-limited applications, the user may program a particular input of the transmitter 810 to be the default input for movable barrier operators the user gains access to using the parking application.

[0098] In another embodiment, the transmitter 810 is programmed with information from the controllable device 825, rather than the controllable device 825 being sent remote control information for the transmitter 810. For example, in the parking garage context, once the user associates the input of the transmitter 810 with the controllable device 825, the remote server 835 or the controllable device 825 sends a communication to the transmitter device 810. The communication contains remote control information that the transmitter 810 uses to actuate the selected controllable device 825, such as a transmitter ID and/or a code. The transmitter 810 configures itself to send the communication 840 with the transmitter ID and a changing code. The controllable device 825 may learn the changing code if the communication 840 contains the transmitter ID that the controllable device 825 is expecting.

[0099] For applications where the controllable device 825 includes a movable barrier operator 830 such as a garage door opener or a gate operator, the ability of the gate operator to temporarily learn remote controls 812 provides intelligent access control for a number of different types of applications. For example, the movable barrier operator 830 may learn a transmitter 810 of a driver of a delivery service for a single use so that the delivery driver may gain access to a garage or a gated community to deliver a package. As another example, the movable barrier operator 830 may learn a transmitter 810 of emergency personnel so that the emergency personnel may readily open a gate of a gated community to gain access to a home in the community. The transmitter 810 of emergency personnel may be a small transmitter built into or part of the equipment or clothing of emergency personnel. For example, the transmitter 810 of the emergency personnel could be attached near or on their radio communication devices or bodycam.

The small transmitter may share power with the communication devices or bodycam, or the small transmitter may have its own battery. As another example, the controllable device 825 may include an access control device for residential communities. One example of such a device is the Connected Access Portal, High Capacity (CAPXL) sold by LiftMaster®. The access control device may learn remote controls according to the foregoing discussion and open a lock or a gate associated with the access control device upon receiving a communication 840 from a learned remote control 812.

[00100] Regarding FIG. 11, the interface system 915 is configured to allow the user to select which transmitter input should be associated with one or more controllable devices 825. The interface system 915 includes a processor 1175 in communication with a memory 1170 and a communication device 1180. The communication device 1180 may communicate using wired or wireless approaches, including short-range and long-range wireless communication protocols. The processor 1175 may operate the account platform 1020 and receive information regarding a user's account via the communication device 1180, such as information regarding the remote controls 812 and controllable devices 825 associated with the user's account.

[00101] As noted previously, the interface system 915 may be a component of the vehicle 850, may be a component of a portable electronic device such as smartphone 837, or may be another device. The account platform 1020 may receive account login information via the human-machine interface 945. The login information includes at least one user credential such as, for example, a username and password, biometric information, etc. Once the remote server 835 verifies the at least one user credential, the remote server 835 provides information to the interface system 915 regarding the controllable devices 825 associated with the user's account that are available to learn the transmitter 810. The interface system 915 also displays the transmitter 810 inputs that are available to be programmed and associated with one or more of the controllable devices 825 associated with the user's account. The platform 1020 allows a user to associate a button of a transmitter 810 with a controllable device 825. The platform 1020 can do this in a variety of ways. In one example, the platform 1020 causes the interface system 915 to display the transmitter 810 inputs and the controllable devices 825 associated with the user's account on a screen. The user then selects, using the human-machine interface 945,

one of the controllable devices 825 and selects one of the inputs of the transmitter 810. The interface system 915 then prompts or asks the user to press a digital "Accept" button or to otherwise confirm that the user would like to associate the selected controllable device 825 with the selected input of the transmitter 810. Once the user confirms the association, the processor 1175 of the interface system 915 causes the communication device 1180 to communicate a message to the remote server 835 requesting the selected controllable device 825 learn the remote control information for the selected input of the transmitter 810. In another example, the human-machine interface 945 displays the available inputs of transmitter 810 inputs on one screen. The user then selects the input of the transmitter 810 to be programmed. Next, the human-machine interface 945 displays a screen that displays the controllable devices 825 available to associate with the previously selected input of the transmitter 810. The user selects the desired controllable device 825 and the processor 1175 causes the communication device 1180 to communicate a message to the remote server 835 requesting the selected controllable device 825 learn the remote control information for the selected input of the transmitter 810.

[00102] The user credential for accessing the user's account may take a variety of forms. In one embodiment, the user credential is a username and a password for the account. In another embodiment, the user credential is provided by the user's smartphone 837. For example, the user's smartphone 837 may include a digital token that is passed to the interface system 915 of the vehicle 850. The communication of the user credential from the smartphone 837 to the interface system 915 may be done automatically upon pairing the smartphone 837 and the interface system 915 or the user may be prompted to authorize the communication. In another embodiment, the user credential may be a device ID of the smartphone 837 which the interface system 915 of the vehicle 850 and/or the remote server 835 recognizes to be an authorized device associated with the user's account.

[00103] In another embodiment, the user may be signed into the account platform 1020 on the user's smartphone 837, such as a myQ® account on the myQ® application or service. Upon the smartphone 837 connecting to the communication device 1180 of the interface system 915 of the vehicle 850, the smartphone 837 communicates the user

credentials to the communication device 1180. In one embodiment, the user credential may be communicated to the interface system 915 via near field communication (NFC). In another embodiment, the user credential may include biometric information of the user read by the interface system 915, such as a fingerprint as one example.

[00104] Having the user credential associated with a user's portable electronic device, such as the smartphone 837, allows for a number of additional features. For example, the user may be able to operate their controllable devices 825 using a new or unprogrammed transmitter of a new vehicle upon the user entering the vehicle and the user's smartphone 837 pairing with vehicle. In one example, when the user enters a new vehicle that includes an interface system 915, the user's smartphone 837 connects to the interface system 915 and automatically configures the interface system 915 for use with one or more controllable devices 825 known by or otherwise associated with the user's account on platform 1020. The interface system 915 of the new vehicle receives information from the remote server 835 regarding the controllable devices 825, remote controls 812, and inputs of the remote controls 812 that are associated with the user's account. The interface system 915 configures itself so that the inputs of the human machine interface 945 will cause operation of the associated controllable devices 825 according to the settings of the user's account. For example, if the user's account specifies that a first button of a mirror-mounted transmitter 810 in the user's primary vehicle causes operation of the user's garage door opener, the interface system 915 of a rental car will automatically communicate remote control information for the transmitter 810 of the rental car with the remote server 835 so that the transmitter 810 of the rental car will transmit a signal that causes operation of the user's garage door opener when the user presses a first button of a mirror-mounted transmitter 810 of the rental car. When the user and her smartphone 837 exits the rental car, the interface system 915 automatically signs the user out of her account on the account platform 1020. As another example, a user may have the interface system 915 of the user's vehicle 850 programmed to access a parking garage at work with the pressing of a particular button of the transmitter 810 of the vehicle 850. If the user takes her spouse's vehicle to work, the user's smartphone 837 will automatically sign into their account of the account platform 1020 provided by the interface system 915 of the spouse's vehicle. The interface system 915 may automatically

communicate with the remote server 835 so that the user's pressing of a similar button in the spouse's vehicle will operate the parking garage at work.

[00105] As one example, a user has programmed buttons on the user's primary vehicle 850 through the user's myQ® account and has a myQ® application on the user's smartphone 837. The vehicle 850 includes an interface system 915 and a transmitter 810 built into the vehicle. The human machine interface 945 includes an infotainment system running a myQ® application. The user sets up the user's myQ® account so that: a) pressing a first virtual button displayed on a display of the infotainment system of the rental car causes the transmitter 810 of the vehicle 850 to transmit a signal that operates a garage door opener; and b) pressing a second virtual button displayed on the display causes the transmitter 810 to transmit a signal that operates a light in the user's home. The user may, at some point, enter a secondary vehicle, such as a rental car, having an interface system 915 and a transmitter 810. When the user activates, drives or otherwise uses the secondary vehicle 850, the user's smartphone 837 automatically communicates with a myQ® application of the interface system 915 and signs into the user's myQ® account. The interface system 915 then configures the virtual buttons on the infotainment system to match the virtual buttons in the user's primary vehicle 850 according the user's myQ account settings. When the user presses the second virtual button, the transmitter 810 of the secondary vehicle 850 transmits a signal that causes operation of the light in the user's home. The interface system 915 in the secondary vehicle 850 thereby provides similar functionality as the interface system 915 in the primary vehicle 850 upon the interface system 915 receiving the user credentials for the myQ account, the interface system 915 communicating the remote control information for the transmitter 810 of the secondary vehicle to the remote server 835, and the remote server 835 requesting the controllable devices 825 associated with the myQ® account learn the remote control information for the transmitter 810 of the secondary vehicle. Instead of using the smartphone 837, the user may sign into their myQ® account manually using the human-machine interface 945 of the secondary vehicle. Alternatively, users can have their preferred transmitter 810 input associations with controllable devices 825 stored in a vehicle key fob that communicates with the interface system 915 of a vehicle to cause the

interface system 915 to automatically configure itself according to the user's settings in the myQ® account once the user and her key fob enter the vehicle.

[00106] The inputs of the remote controls 812 and the controllable devices 825 can be associated using the interface system 915 in a number of approaches. In one approach, after the user selects an input of a remote control 812 to associate with a controllable device 825, the interface system 915 sends to the remote server 835 the transmitter ID of the remote control 812, the input ID of the selected input, and, optionally, a current changing code (e.g., rolling code) of the remote control 812. The remote server 835 stores this remote control information and sends the remote control information to the controllable device 825. When the user is in proximity to the controllable device 825 and operates the remote control 812, the remote control 812 transmits a signal including the transmitter ID, the input ID, and a changing code. If the transmitter ID and input ID sent from the remote control 812 matches the expected transmitter ID and input ID received at the controllable device 825 from the remote server 835, the controllable device 825 actuates and stores the transmitter ID, input ID, and (optionally) the changing code in a memory of the controllable device 825. The controllable device 825 may also compare the changing code from the remote server and the changing code received from the remote control 812 to confirm the remote control 812 is authorized to operate the controllable device 825. The controllable device 825 reports actuation to the remote server 835, such as for reconciliation of use and fee-charging in a parking garage context. In another embodiment, to ensure the controllable device 825 utilizes the correct changing code algorithm, the controllable device 825 predicts an expected changing code and waits for the remote control 812 to send another signal containing a second changing code. The controllable device 825 will actuate and learn the remote control 812 if the second changing code matches the expected changing code.

[00107] In another embodiment, the user's smartphone 837 contains the interface system 915 displaying the account platform 1020 and the user selects an input of a remote control 812 to associate with a controllable device 825 using the account platform 1020 on the smartphone 837. The smartphone 837 communicates the user selection to the remote server 835. The remote server 835 retrieves remote control information for the selected remote control 812 from a memory of the remote server 835. The remote control

information includes a transmitter ID and optionally an input ID and/or a changing code of the selected remote control 812. The remote server 835 communicates the remote control information to the controllable device 825, which stores the remote control information in a memory of the controllable device 825. When the remote control 812 is operated to send a local radio frequency signal to the controllable device 825, the controllable device 825 receives the local radio frequency signal. The controllable device 825 validates the remote control 812 by comparing the transmitter ID, input ID, and changing code of the local radio frequency signal to the remote control information received from the remote server 835. The controllable device 825 learns the remote control 812 upon the transmitter ID, input ID, and changing code of the local radio frequency signal corresponding to the transmitter ID, input ID, and changing code of the remote control information the controllable device 825 received from the remote server 835.

[00108] In another example, the user associates an input of a remote control 812 with a controllable device 825 using the account platform 1020 such as with the smartphone 837, a tablet computer, or a desktop computer. The remote server 835 sends a message to the controllable device 825 indicating the user wants to associate the remote control 812 with the controllable device 825. The controllable device 825 sends a response message to the remote server 835 containing remote control information for use by the remote control 812 such as one or more of a transmitter ID, button ID, and a changing code. The remote server 835 sends the remote control information to the remote control 812, and the remote control 812 configures itself according to the remote control information. The remote control 812 may use the changing code from the controllable device 825 as a starting point and may change the changing code (e.g., index a rolling code) with each transmission by the remote control 812. The controllable device 825 predicts the changing code using known techniques.

[00109] In yet another example, upon the user associating a remote control 812 with a controllable device 825 via the account platform 1020, the remote server 835 generates remote control information including one or more of a transmitter ID, input ID, and a changing code and communicates this generated remote control information to the controllable device 825 and the remote control 812. Upon the user actuating the remote

control 812, the remote control 812 transmits a local radio frequency signal to the controllable device 825 including the one or more of the transmitter ID, input ID, and changing code received from the remote server 835. The controllable device 825, having received the remote control information from the remote server 835, expects to receive the remote control information from the remote control 812. Upon the device 825 receiving the remote control information locally from the remote control 812, the controllable device 825 whitelists the remote control 812 and may actuate.

[00110] In still another example, the vehicle 850 must be in proximity to the controllable device 825 for setup. Upon the user selecting which transmitter 810 button of the vehicle 850 to associate with which controllable device 825 via the account platform 1020, the remote server 835 sends a signal to the controllable device 825 putting the controllable device 825 in learn mode. The server then sends a signal over the network to the vehicle 850 causing the transmitter 810 to transmit different radio frequency communications 840 to the controllable device 825. Once the controllable device 825 receives a compatible communication 840, the controllable device 825 learns the transmitter 810. The controllable device 825 then sends a communication to the transmitter 810, either directly via a radio frequency signal or indirectly via the network 834 and the remote server 835, indicating the communication 840 the controllable device 825 has learned.

[00111] The one or more controllable devices 825 can be any type of device that can be actuated or controlled remotely. Example controllable devices 825 include movable barrier operators, garage door operators, gates, doors, lights, etc. Regarding FIG. 12, the controllable device 825 may include the movable barrier operator 830 discussed above with respect to FIG. 8. The movable barrier operator 830 shown comprises a motor 1285, communication circuitry 1290, and a controller 1295 comprising a memory 1260 and a processor 1210. The one or more controllable devices 825 are capable of communicating over one or more networks 834 with the remote server 835 and/or the remote controls 812. For example, the one or more controllable devices 825 may be capable of wirelessly connecting to a wireless access point, such as a Wi-Fi router, and communicating with the remote server 835 via the internet.

[00112] It is intended that the phrase "at least one of" as used herein be interpreted in the disjunctive sense. For example, the phrase "at least one of A and B" is intended to encompass only A, only B, or both A and B. Those skilled in the art will recognize that a wide variety of modifications, alterations, and combinations can be made with respect to the above-described embodiments without departing from the scope of the invention and that such modifications, alterations, and combinations are to be viewed as being within the ambit of the inventive concept.

CLAIMS

1. A movable barrier operator apparatus comprising:

a memory;

communication circuitry configured to receive an add transmitter request from a remote computer via a network, the add transmitter request including a transmitter code;

the communication circuitry configured to receive a radio frequency control signal from an unknown transmitter, the radio frequency control signal including a fixed code of the unknown transmitter; and

a processor operably coupled to the memory and the communication circuitry, the processor configured to:

store, in the memory, the transmitter code of the add transmitter request received from the remote computer; and

determine whether to operate a movable barrier based at least in part upon whether the fixed code of the radio frequency control signal received from the unknown transmitter corresponds to the transmitter code received from the remote computer.

2. The apparatus of claim 1, wherein the communication circuitry is further configured to receive a remove transmitter request, from the remote computer, identifying the transmitter code; and

wherein the processor is further configured to delete the transmitter code from the memory in response to the remove transmitter request.

3. The apparatus of claim 1, wherein the transmitter code comprises a hashed version of a transmitter fixed code and the processor is further configured to perform a hash function on the fixed code of the radio frequency control signal received from the unknown transmitter to determine whether the fixed code of the radio frequency control signal corresponds to the transmitter code.

4. The apparatus of claim 1, wherein the add transmitter request further comprise an access condition associated with the transmitter code, and the processor is further

configured to determine whether to operate the movable barrier in response to receiving the radio frequency control signal from the unknown transmitter based at least in part upon the access condition.

5. The apparatus of claim 4, wherein the access condition comprises at least one of:

a number of uses restriction; and

an access time restriction.

6. The apparatus of claim 1, wherein the processor is configured to cause the communication circuitry to transmit a radio frequency signal including the transmitter code to a trainable transmitter to permit the trainable transmitter to learn the transmitter code.

7. The apparatus of claim 1 wherein the communication circuitry includes a network adapter configured to receive the add transmitter request from the remote computer, and a radio frequency receiver configured to receive the radio frequency control signal.

8. A method for operating a movable barrier operator apparatus, the method comprising:

receiving an add transmitter request from a remote computer via communication circuitry of the movable barrier operator apparatus, the add transmitter request including a transmitter code;

storing, with a processor of the movable barrier operator apparatus, the transmitter code of the add transmitter request in a memory of the movable barrier operator apparatus;

receiving, at the communication circuitry of the movable barrier operator apparatus, a radio frequency control signal from an unknown transmitter, the radio frequency control signal including a fixed code of the unknown transmitter; and

determining, with the processor, whether to operate a movable barrier based at least in part upon whether the fixed code received from the unknown transmitter corresponds to the transmitter code received from the remote computer.

9. The method of claim 8, further comprising:

receiving, via the communication circuitry of the movable barrier operator apparatus, a remove transmitter request from the remote computer identifying the transmitter code; and

deleting the transmitter code from the memory in response to the remove transmitter request.

10. The method of claim 8, wherein the transmitter code comprises a hashed version of a transmitter fixed code and the processor is configured to perform a hash function on the fixed code of the radio frequency control signal received from the unknown transmitter to determine whether the fixed code corresponds to the stored transmitter code in the memory.

11. The method of claim 8, wherein the add transmitter request includes an access condition associated with the transmitter code,

wherein determining whether to operate the movable barrier in response to receiving the radio frequency control signal is based at least in part on the access condition.

12. The method of claim 11, wherein the access condition comprises at least one of:

a number of uses restriction; and

an access time restriction.

13. The method of claim 8, further comprising causing the communication circuitry of the movable barrier operator apparatus to transmit a radio frequency signal

including the transmitter code to a trainable transmitter to permit the trainable transmitter to learn the transmitter code.

14. A transmitter programmer apparatus comprising:

communication circuitry configured to communicate with a remote computer via a network;

the communication circuitry configured to communicate with a transmitter, the transmitter operable to transmit a radio frequency control signal to a movable barrier operator apparatus; and

a processor operably coupled to the communication circuitry, the processor configured to:

communicate a transmitter pairing request to the remote computer via the communication circuitry;

receive a transmitter fixed code associated with a movable barrier operator from the remote computer in response to the transmitter pairing request; and

program, via the communication circuitry, the transmitter to transmit a modified radio frequency control signal including the transmitter fixed code to actuate the movable barrier operator apparatus.

15. The apparatus of claim 14 wherein the transmitter pairing request comprises at least one of:

a movable barrier operator identifier;

a movable barrier access passcode;

a user credential; and

a transmitter identifier.

16. The apparatus of claim 14 wherein the transmitter pairing request comprises a movable barrier operator identifier received from a broadcast beacon or an access brokering service.

17. The apparatus of claim 14, wherein the transmitter comprises two or more buttons and the processor is further configured to:

receive a selection of a button of the transmitter via a user interface and program the selected button of the transmitter to transmit the transmitter fixed code.

18. The apparatus of claim 14, wherein the processor is further configured to:

receive an access condition associated with the transmitter fixed code; and

deprogram the transmitter fixed code from the transmitter based on the access condition.

19. The apparatus of claim 14, wherein the communication circuitry comprises at least one of:

a wired connector; and

a Bluetooth transceiver.

20. A method for transmitter programming comprising:

at a transmitter programmer apparatus:

sending a transmitter pairing request to a remote computer;

receiving a transmitter fixed code associated with a movable barrier operator from the remote computer in response to the transmitter pairing request; and

programing a transmitter to transmit a modified radio frequency control signal including the transmitter fixed code to actuate the movable barrier.

21. The method of claim 20, wherein the transmitter pairing request comprises at least one of:

a movable barrier operator identifier;

a movable barrier access passcode;

a user credential; and

a transmitter identifier.

22. The method of claim 20, wherein the transmitter pairing request comprises a movable barrier operator identifier received from a broadcast beacon or an access brokering service.

23. The method of claim 20, further comprising:

receiving a selection of a button from two or more buttons of the transmitter via a user interface; and

programming the selected button of the transmitter to transmit the transmitter fixed code.

24. The method of claim 20, further comprising:

receiving an access condition associated with the transmitter fixed code; and

deprogramming the transmitter fixed code from the transmitter based on the access condition.

25. The method of claim 20, wherein programming the transmitter includes programming the transmitter using at least one of a wired connector and a Bluetooth transceiver.

26. A server system for brokering movable barrier access comprising:

communication circuitry configured to communicate with a plurality of user devices and a plurality of movable barrier operator apparatuses; and

a processor operably coupled to the communication circuitry and configured to:

receive a transmitter pairing request from a user device requesting to access a movable barrier operator apparatus via a transmitter;

verify the transmitter pairing request; and

send an add transmitter request to the movable barrier operator apparatus, the add transmitter request including a transmitter code associated with the transmitter and configured to cause the movable barrier operator apparatus to store the transmitter code in a memory of the movable barrier operator apparatus.

27. The system of claim 26, wherein the transmitter code comprises at least one of a transmitter fixed code and a hashed version of a transmitter fixed code.

28. The system of claim 26, wherein the transmitter pairing request comprises a transmitter identifier and the processor is further configured to retrieve a fixed code or a hashed version of a fixed code associated with the transmitter identifier from a transmitter database.

29. The system of claim 26, wherein verifying the transmitter pairing request comprises comparing the transmitter pairing request with an access condition associated with the movable barrier operator apparatus in a movable barrier operator apparatus database.

30. The system of claim 26, wherein verifying the transmitter pairing request includes verifying at least one of:

a movable barrier operator access passcode;

a user account associated the transmitter pairing request; and

a user device location.

31. The system of claim 26, wherein the processor is further configured to:

determine an access condition associated with the transmitter pairing request; and

communicate with the movable barrier operator apparatus to enforce the access condition.

32. The system of claim 26, wherein the processor is further configured to send a remove transmitter request to the movable barrier operator apparatus, the remove transmitter request configured to cause the movable barrier operator apparatus to remove the transmitter code from the memory.

33. A method for brokering movable barrier access comprising:

at server computer:

receiving, via communication circuitry of the server computer, a transmitter pairing request from a user device requesting to access a movable barrier operator apparatus via a transmitter;

verifying, with a processor of the server computer, the transmitter pairing request; and

sending, via the communication circuitry, an add transmitter request to the movable barrier operator apparatus, the add transmitter request including a transmitter code associated with the transmitter and configured to cause the movable barrier operator apparatus to store the transmitter code in a memory of the movable barrier operator apparatus.

34. The method of claim 33, wherein the transmitter code comprises at least one of a transmitter fixed code and a hashed version of a transmitter fixed code.

35. The method of claim 33, wherein the transmitter pairing request comprises a transmitter identifier and the processor is further configured to retrieve a fixed code or a hashed version of the fixed code associated with the transmitter identifier from a transmitter database.

36. The method of claim 33, wherein verifying the transmitter pairing request comprises comparing the transmitter pairing request with an access condition associated with the movable barrier operator in a movable barrier operator database.

37. The method of claim 33, wherein verifying the transmitter pairing request comprises verifying at least one of:

a movable barrier operator access passcode;

a user account associated the transmitter pairing request; and

a user device location.

38. The method of claim 33, further comprising:

determining an access condition associated with the transmitter pairing request; and

communicating with the movable barrier operator apparatus to enforce the access condition.

39. The method of claim 33, further comprising:

sending a remove transmitter request to the movable barrier operator apparatus, the remove transmitter request causing the movable barrier operator to remove the transmitter code from the memory.

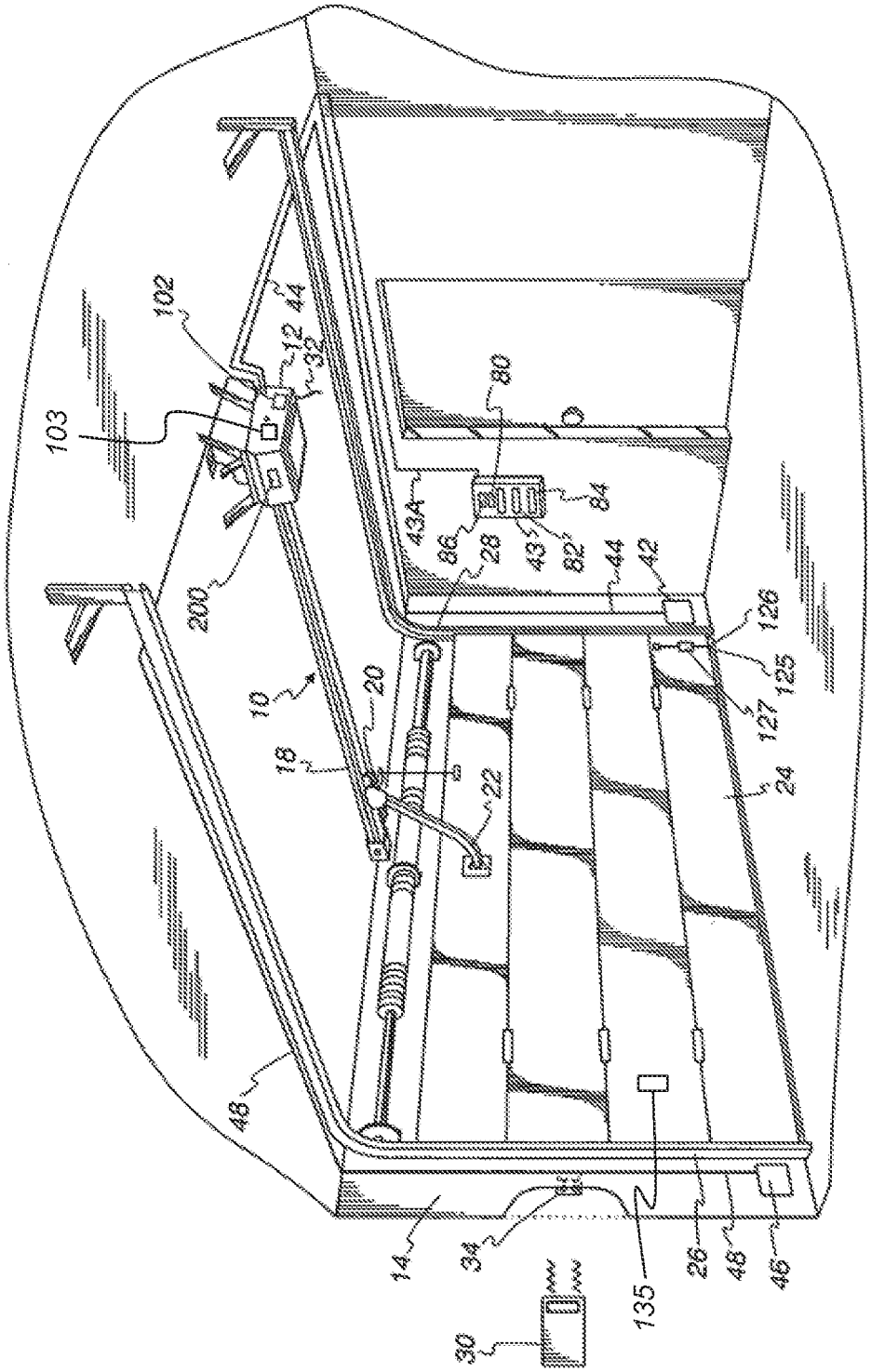

102
44
12
32
103
80
84
43A
86
28
43
82
44
42
200
126
125
127
10
20
18
22
24
48
14
34
135
26
48
46
30

FIG. 1

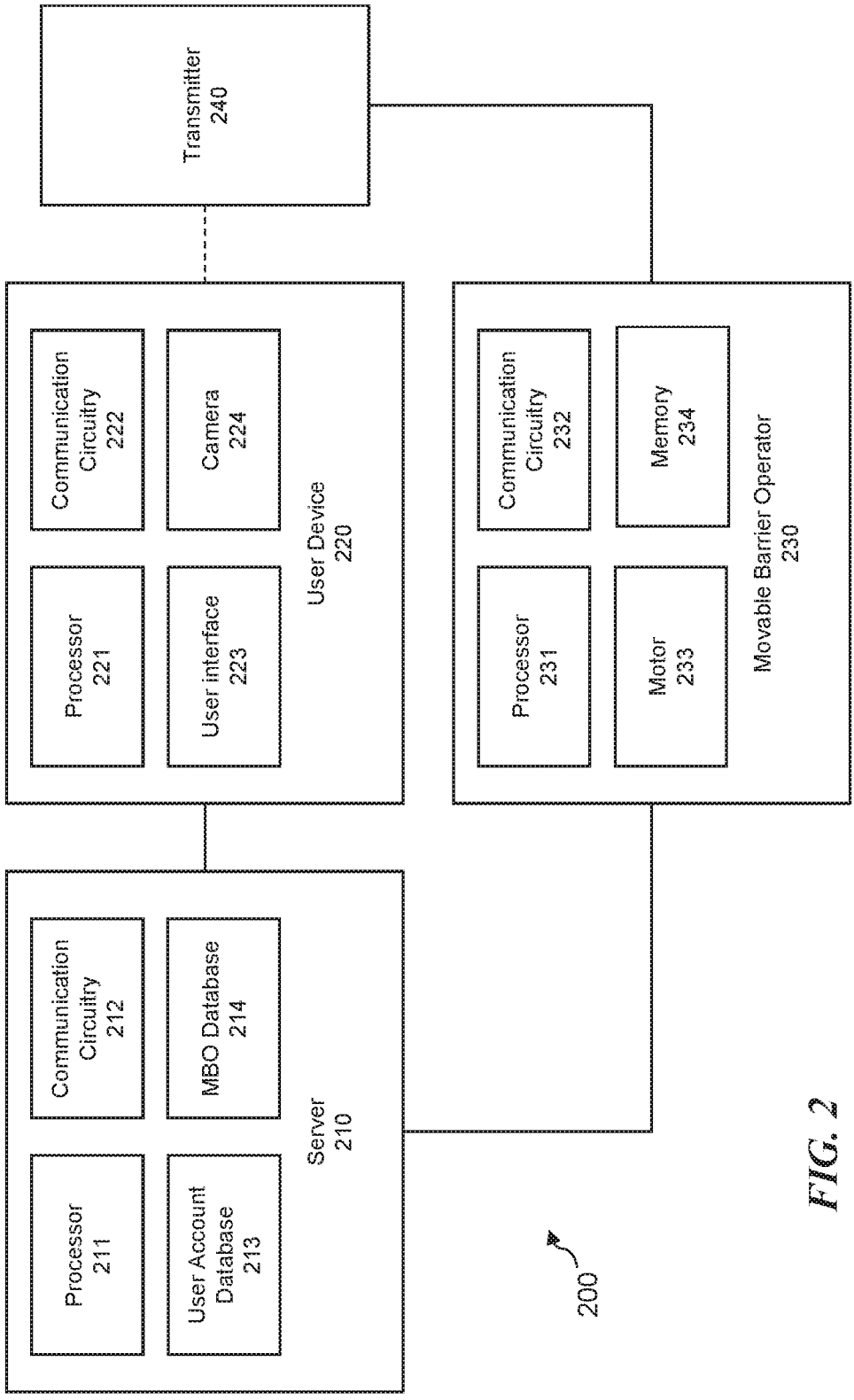

Transmitter
240
Communication Circuitry
222
Camera
224
Processor
221
User interface
223
User Device
220
Communication Circuitry
232
Memory
234
Processor
231
Motor
233
Movable Barrier Operator
230
Communication Circuitry
212
MBO Database
214
Processor
211
User Account Database
213
Server
210
200

FIG. 2

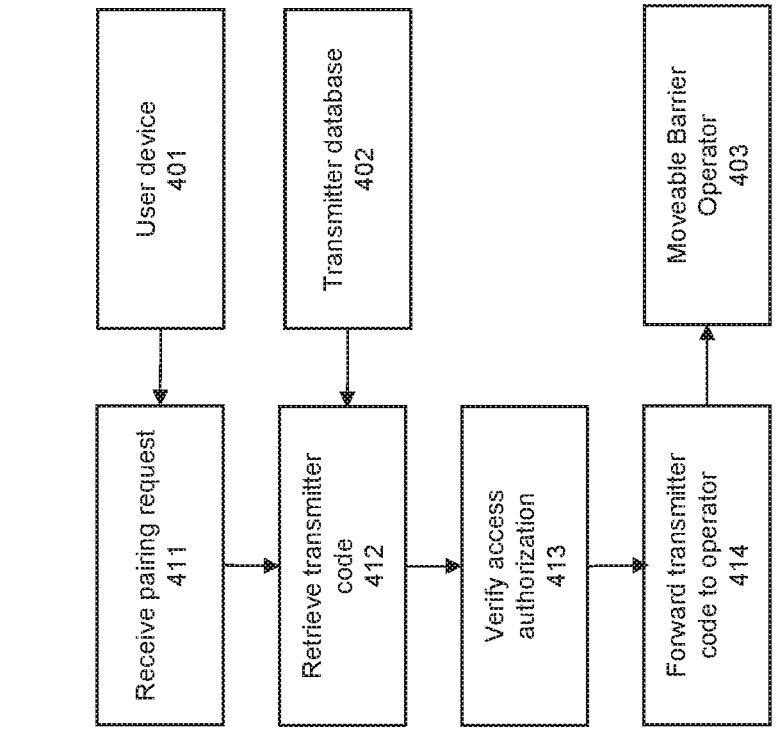

User device
401
Transmitter database
402
Moveable Barrier Operator
403
Receive pairing request
411
Retrieve transmitter code
412
Verify access authorization
413
Forward transmitter code to operator
414
400

FIG. 4

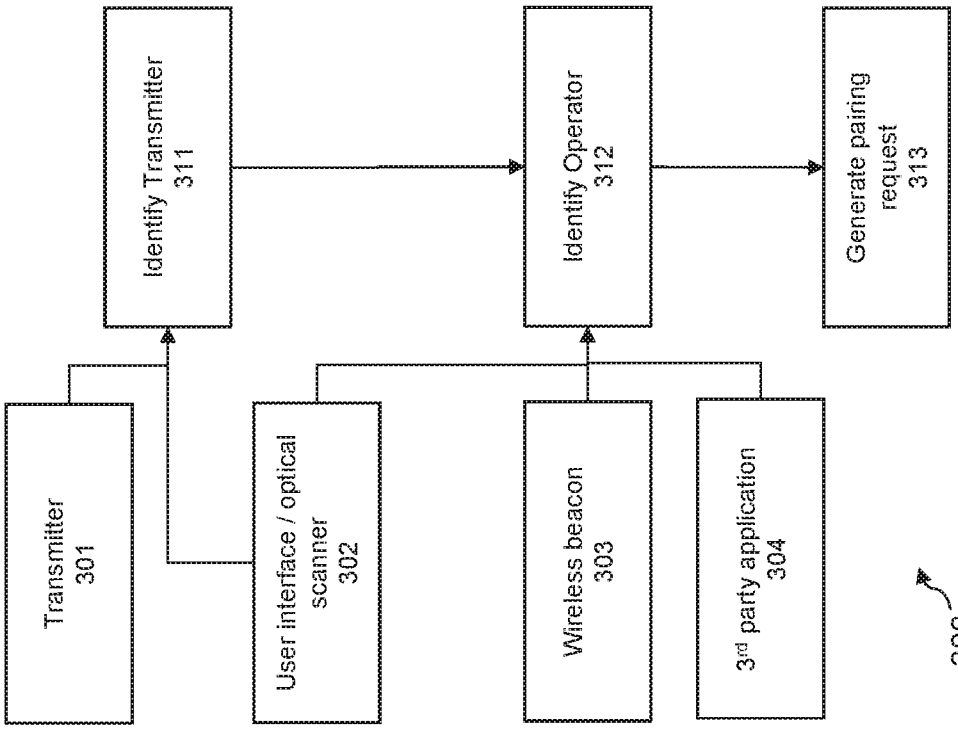

Identify Transmitter
311
Identify Operator
312
Generate pairing request
313
Transmitter
301
User interface / optical scanner
302
Wireless beacon
303
3rd party application
304
300

FIG. 3

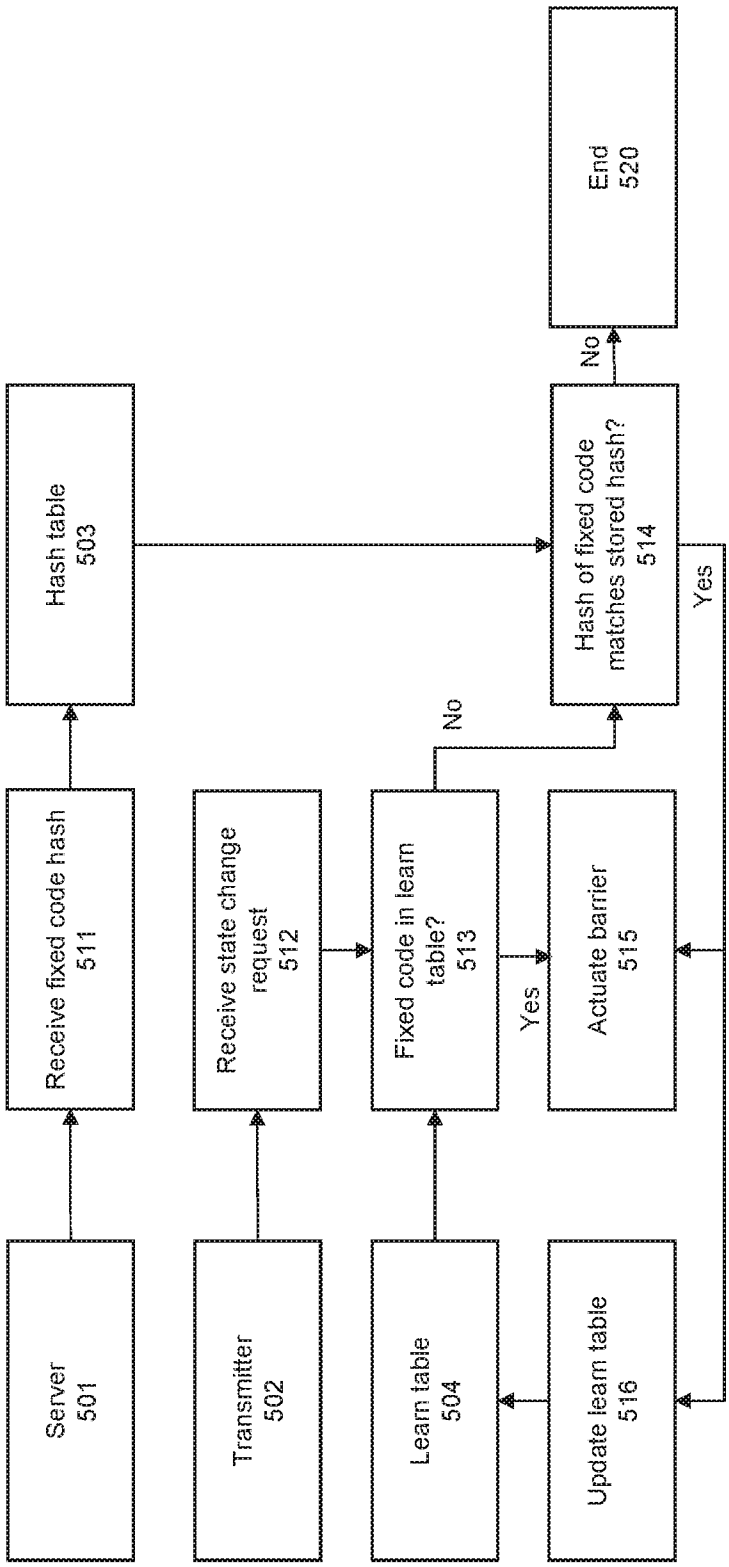

Server
501
Transmitter
502
Learn table
504
Update learn table
516
Receive fixed code hash
511
Receive state change request
512
Fixed code in learn table?
513
Yes
No
Actuate barrier
515
Hash table
503
Hash of fixed code matches stored hash?
514
Yes
No
End
520
500

FIG. 5

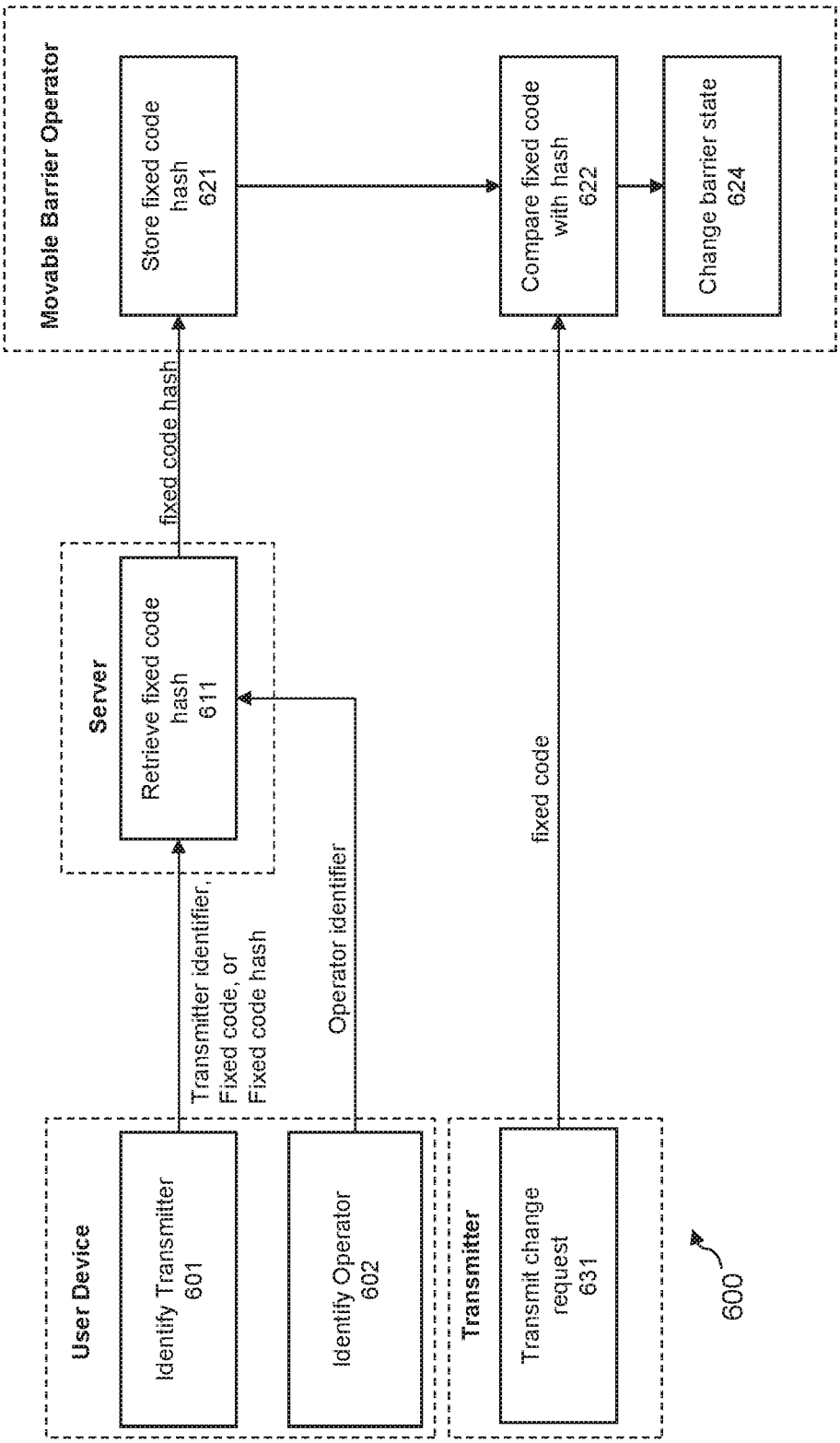

Movable Barrier Operator
Store fixed code hash 621
Compare fixed code with hash 622
Change barrier state 624
fixed code hash
Server
Retrieve fixed code hash 611
Transmitter identifier, Fixed code, or Fixed code hash
Operator identifier
fixed code
User Device
Identify Transmitter 601
Identify Operator 602
Transmitter
Transmit change request 631
600

FIG. 6

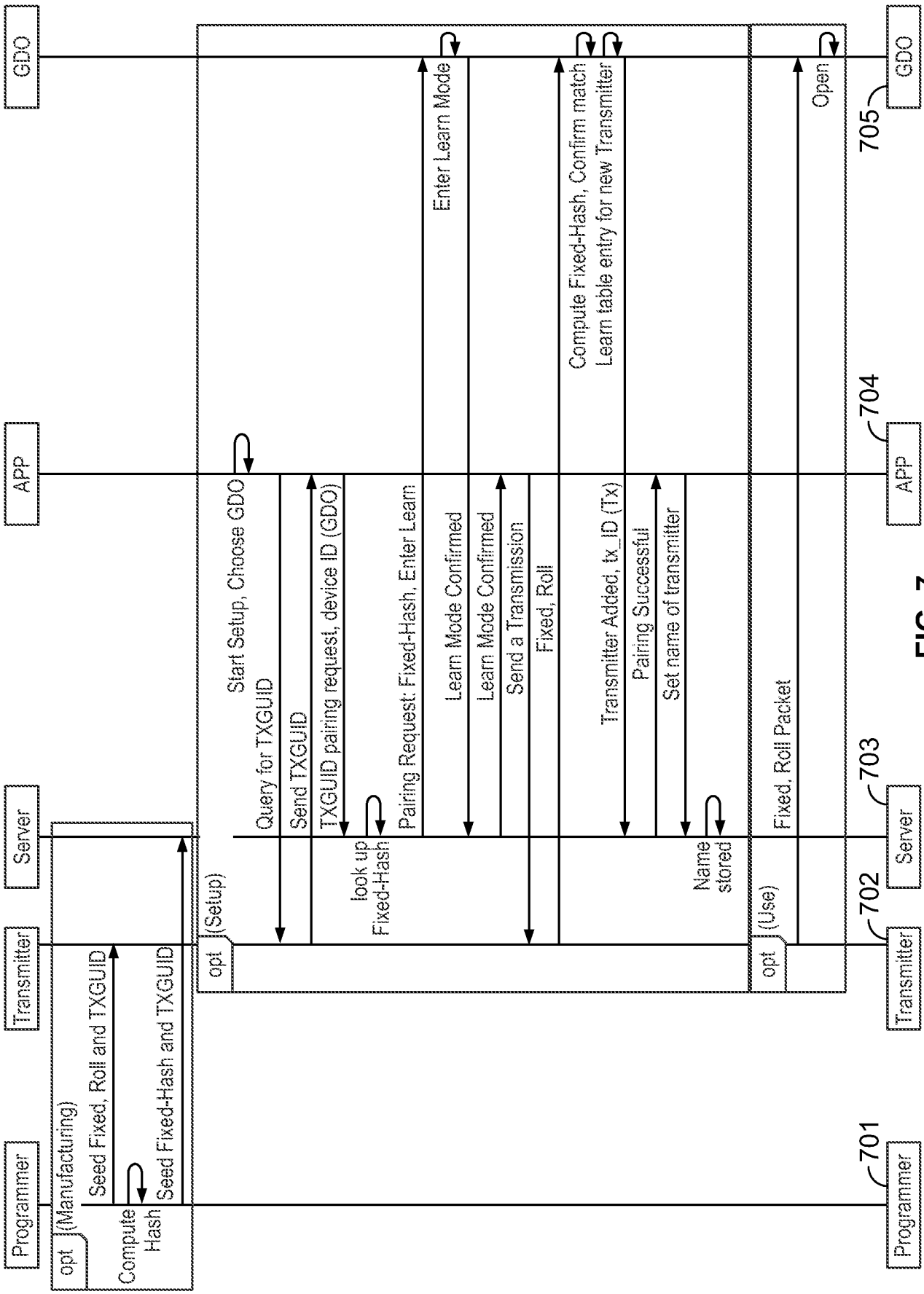

Programmer
Transmitter
Server
APP
GDO
701
702
703
704
705
opt (Manufacturing)
Seed Fixed, Roll and TXGUID
Compute Hash
Seed Fixed-Hash and TXGUID
opt (Setup)
Start Setup, Choose GDO
Query for TXGUID
Send TXGUID
TXGUID pairing request, device ID (GDO)
look up Fixed-Hash
Pairing Request: Fixed-Hash, Enter Learn
Enter Learn Mode
Learn Mode Confirmed
Learn Mode Confirmed
Send a Transmission
Fixed, Roll
Compute Fixed-Hash, Confirm match
Learn table entry for new Transmitter
Transmitter Added, tx_ID (Tx)
Pairing Successful
Set name of transmitter
Name stored
opt (Use)
Fixed, Roll Packet
Open

FIG. 7

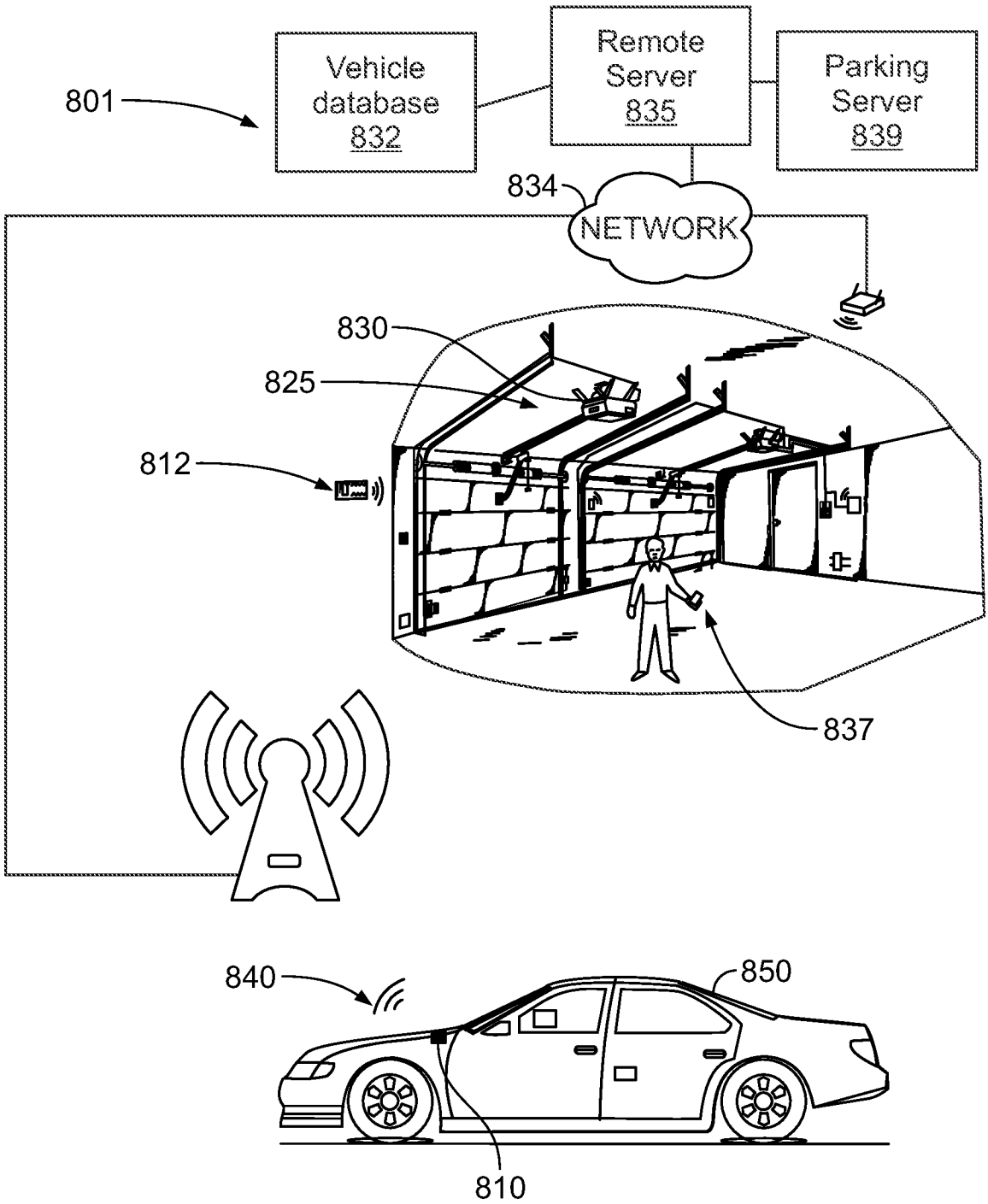

801
Vehicle database 832
Remote Server 835
Parking Server 839
834
NETWORK
830
825
812
837
840
850
810

FIG. 8

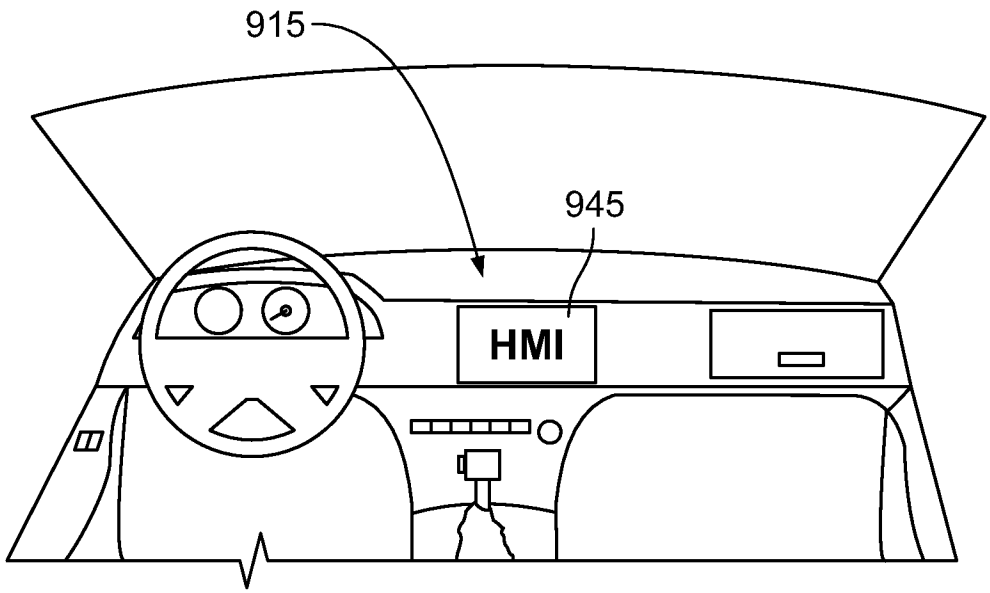


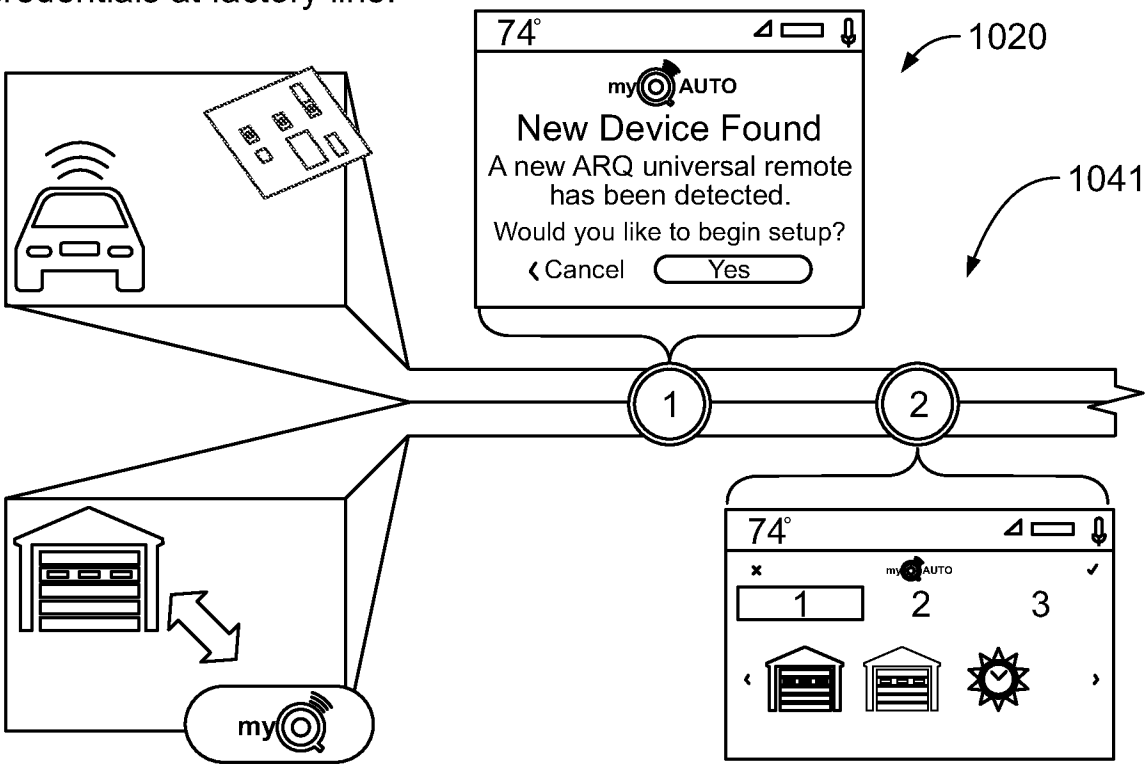
FIG. 9

MyQ Auto Smart Learning

Auto Discovery - Vehicle
MyQ auto discovers ARQ credentials at factory line.

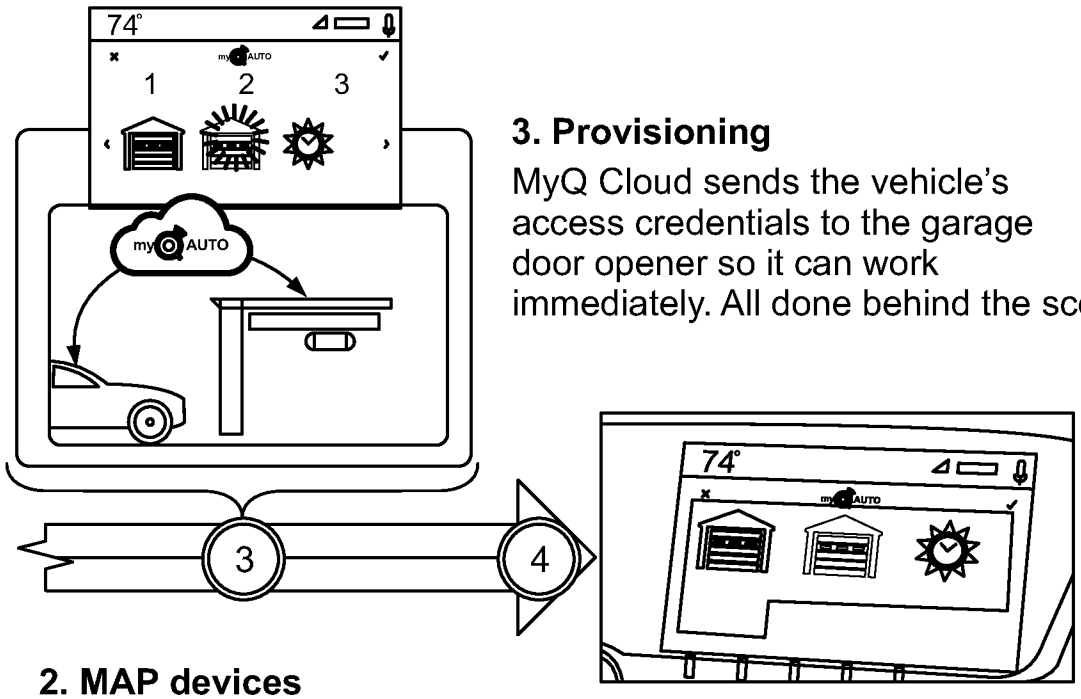
1. Log-in Establish Link
Existing MyQ users log in to the app with their MyQ user name and password.

The vehicle detects an “unprogrammed” ARQ device and begins setup.



Auto Discovery - Home
MyQ Cloud knows all available access and control devices

FIG. 10A



3. Provisioning

MyQ Cloud sends the vehicle's access credentials to the garage door opener so it can work immediately. All done behind the scenes.

2. MAP devices

MyQ Cloud provides list of available devices.

The user maps buttons to the device or scene populated from the MyQ cloud account.

4. Works Instantly

Seamlessly works. No manual programming like homelink.

Happy customers, utilized systems, higher quality ratings.

FIG. 10B

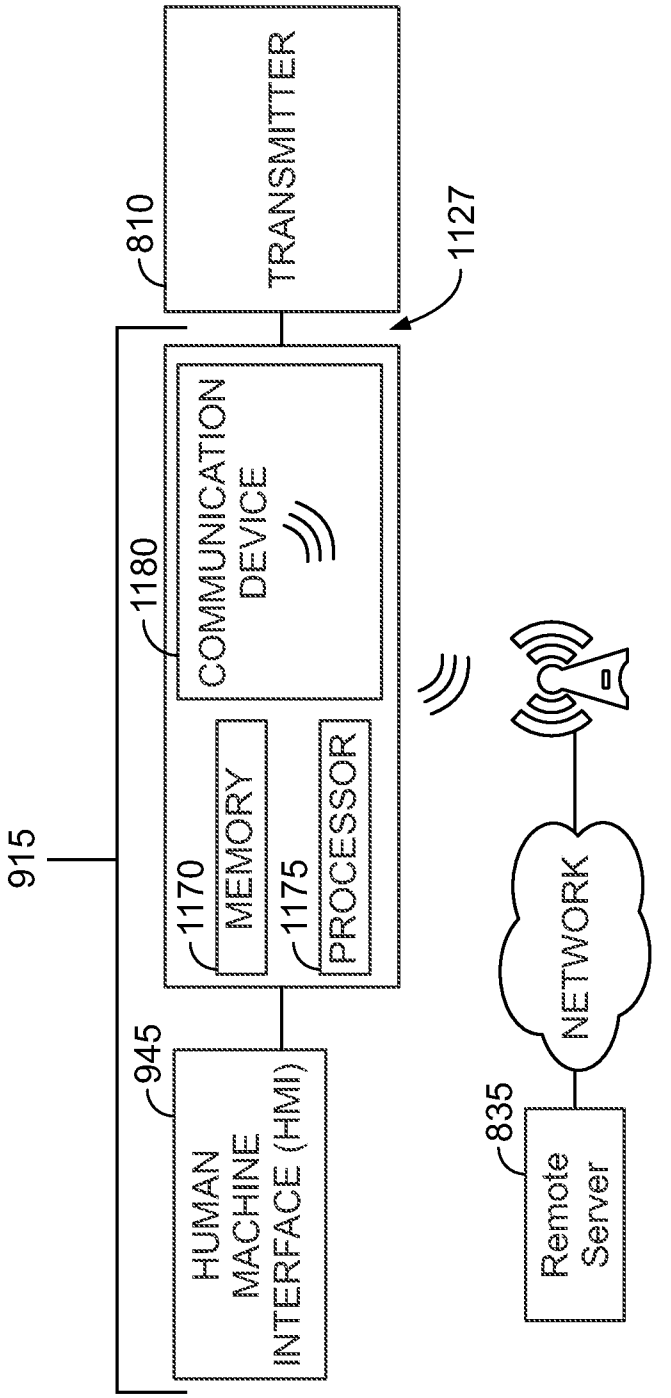

TRANSMITTER
810
1127
COMMUNICATION DEVICE
1180
MEMORY
1170
PROCESSOR
1175
915
945
HUMAN MACHINE INTERFACE (HMI)
NETWORK
835
Remote Server

FIG. 11

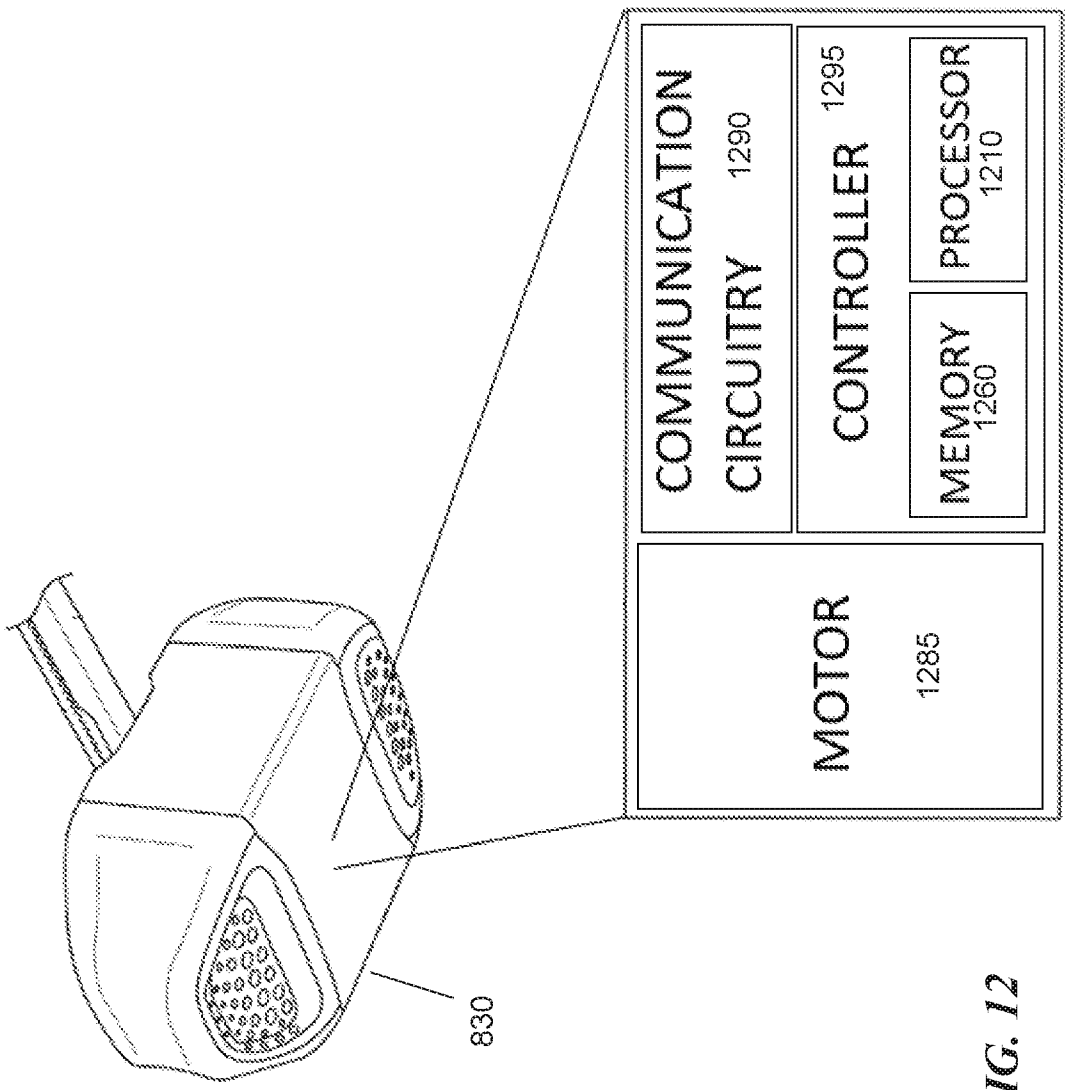

COMMUNICATION CIRCUITRY 1290
CONTROLLER 1295
MEMORY 1260
PROCESSOR 1210
MOTOR 1285
830

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/044358

A. CLASSIFICATION OF SUBJECT MATTER
IPC (20190101) G07C 9/00
CPC (20130101) G07C 9/00309, G07C 9/00182, G07C 9/00817
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)
IPC (20190101) G07C 9/00
CPC (20130101) G07C 9/00309, G07C 9/00182, G07C 9/00817

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Databases consulted: Esp@cenet, Google Patents, Orbit
Search terms used: movable barrier , gate , garage door openers, learn mode , record , regist, similar, same , match, transmitter , reciever , remote.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6778064 B1 Alps Electric Co Ltd. 17 Aug 2004 (2004/08/17) entire document	1,3,6-10,13-16, 19-22,25-28,33-35
Y	entire document	2,4,5,11,12,17,18, 23,24,29-32,36-39
Y	US 6140938 A Flick Kenneth E. 01 Oct 2000 (2000/10/01) entire document	2,9,32,39
Y	US 5872513 A Chamberlain Group Inc. 16 Feb 1999 (1999/02/16) entire document	4,5,11,12,17,18,23, 24,29-31,35-38
A	US 6037858 A Alps Electric Co Ltd. 14 Mar 2000 (2000/03/14) entire document	1-39

[X] Further documents are listed in the continuation of Box C.

[X] 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
"D" document cited by the applicant in the international application
"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	Date of mailing of the international search report
14 Nov 2019	17 Nov 2019

Name and mailing address of the ISA:	Authorized officer
Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Email address: pctoffice@justice.gov.il	ZAHDEH Jihad Telephone No. 972-73-3927237

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/044358

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 20060035951 A IREVO INC. 27 Apr 2006 (2006/04/27) entire document	1-39
A	US 2014125499 A1 Chamberlain Group Inc 08 May 2014 (2014/05/08) entire document	1-39
A	KR 20050005150 A LG ELECTRONICS INC 13 Jan 2005 (2005/01/13) entire document	1-39

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2019/044358

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 6778064 B1	17 Aug 2004	US 6778064 B1	17 Aug 2004
		DE 60033254 D1	22 Mar 2007
		DE 60033254 T2	22 Nov 2007
		EP 1092825 A2	18 Apr 2001
		EP 1092825 A3	19 Nov 2003
		EP 1092825 B1	07 Feb 2007
		JP 2001115696 A	24 Apr 2001
US 6140938 A	01 Oct 2000	US 6140938 A	31 Oct 2000
		AU 5447196 A	30 Oct 1996
		AU 701285 B2	21 Jan 1999
		AU 5447396 A	29 Oct 1997
		BR 9604820 A	30 Nov 1999
		CA 2218101 A1	17 Oct 1996
		CA 2218101 C	26 Mar 2002
		DE 69609408 D1	24 Aug 2000
		DE 69609408 T2	15 Feb 2001
		EA 199700312 A1	30 Apr 1998
		EA 000298 B1	29 Apr 1999
		EP 0817734 A1	14 Jan 1998
		EP 0817734 B1	19 Jul 2000
		JP H11503388 A	26 Mar 1999
		JP 3290440 B2	10 Jun 2002
		KR 19980703875 A	05 Dec 1998
		KR 100429293 B1	06 Oct 2004
		MX 9707908 A	31 Jul 1998
		US 5654688 A	05 Aug 1997
		US 5729191 A	17 Mar 1998
		US 5818329 A	06 Oct 1998
		US 5982277 A	09 Nov 1999

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2019/044358

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 5986571 A	16 Nov 1999
		US 6037859 A	14 Mar 2000
		US 6130606 A	10 Oct 2000
		US 6140939 A	31 Oct 2000
		US 6144315 A	07 Nov 2000
		US 6184780 B1	06 Feb 2001
		US 6188326 B1	13 Feb 2001
		US 6320514 B1	20 Nov 2001
		US 6366198 B1	02 Apr 2002
		US 6480095 B1	12 Nov 2002
		US 6480117 B1	12 Nov 2002
		US 2002075133 A1	20 Jun 2002
		US 7737820 B2	15 Jun 2010
		WO 9632307 A1	17 Oct 1996
		WO 9737813 A1	16 Oct 1997
US 5872513 A	16 Feb 1999	US 5872513 A	16 Feb 1999
		AU 1905697 A	30 Oct 1997
		AU 714420 B2	06 Jan 2000
		BR 9701929 A	10 Nov 1998
		DE 29707454 U1	04 Sep 1997
		FR 2748143 A1	31 Oct 1997
		GB 9708159 D0	11 Jun 1997
		GB 2312539 A	29 Oct 1997
		GB 2312539 B	03 May 2000
		GB 2312539 A8	21 Jun 2000
US 6037858 A	14 Mar 2000	US 6037858 A	14 Mar 2000
		JP H1096353 A	14 Apr 1998
		JP 3748635 B2	22 Feb 2006
KR 20060035951 A	27 Apr 2006	KR 20060035951 A	27 Apr 2006

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2019/044358

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		KR 100649571 B1	28 Nov 2006
US 2014125499 A1	08 May 2014	US 2014125499 A1	08 May 2014
		US 9122254 B2	01 Sep 2015
		AU 2013254889 A1	22 May 2014
		AU 2013254889 B2	17 Aug 2017
		AU 2017261560 A1	07 Dec 2017
		AU 2017261560 B2	02 May 2019
		AU 2019210566 A1	22 Aug 2019
		CA 2831589 A1	08 May 2014
		NZ 617360 A	26 Jun 2015
		NZ 706180 A	25 Sep 2015
		NZ 711160 A	25 Nov 2016
		NZ 717251 A	31 Mar 2017
		US 2014129606 A1	08 May 2014
		US 9141099 B2	22 Sep 2015
		US 2016010382 A1	14 Jan 2016
		US 9376851 B2	28 Jun 2016
		US 2016194912 A1	07 Jul 2016
		US 9644416 B2	09 May 2017
		US 2017241189 A1	24 Aug 2017
		US 9896877 B2	20 Feb 2018
		US 2018148971 A1	31 May 2018
		US 10138671 B2	27 Nov 2018
		US 2019085615 A1	21 Mar 2019
KR 20050005150 A	13 Jan 2005	KR 20050005150 A	13 Jan 2005