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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 December 2016 (08.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/196481 A1

(51) International Patent Classification:
G08C 17/02 (2006.01) *E05F 15/70* (2015.01)
E05B 49/02 (2006.01)

(21) International Application Number:
PCT/US2016/035045

(22) International Filing Date:
31 May 2016 (31.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/169,069 1 June 2015 (01.06.2015) US
15/162,782 24 May 2016 (24.05.2016) US

(71) Applicant: **SCHLAGE LOCK COMPANY LLC** [US/US]; 2720 Tobey Drive, Indianapolis, IN 46219 (US).

(72) Inventors: **TELLJOHANN, Brian, A.**; 20309 New Jersey Street, Indianapolis, IN 46280 (US). **KIELKOWSKI, Ron, M.**; 403 Chris Lane, Noblesville, IN 46062 (US). **NARDELLI, Frank, A.**; 7918 Dillon Place, Indianapolis, IN 46236 (US). **STEINER, Russell**; 9534 W. Airport Road, St. Helen, MI 48656 (US).

(74) Agents: **SCHEPERS, Brad A.** et al.; Taft Stettinius & Hollister LLP, One Indiana Square, Suite 3500, Indianapolis, IN 46204 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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.

(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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: ANTENNA DIVERSITY IMPLEMENTATION FOR WIRELESS LOCKS

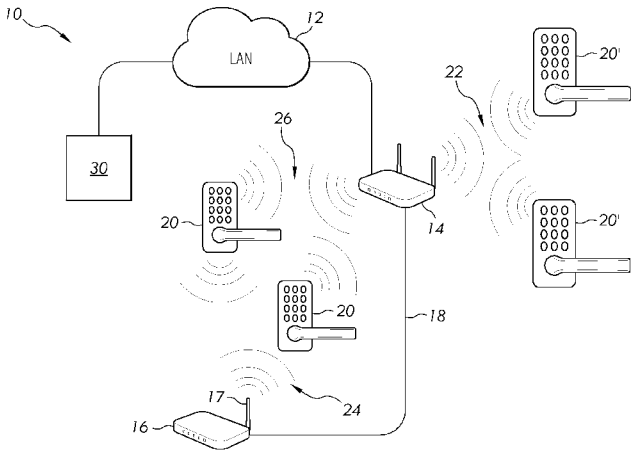

FIG. 1

(57) Abstract: An electronic lock system including an access control device configured to provide system instructions, an interface module electrically coupled to the access control device and configured to transmit RF signals in response to system instructions received from the access control device, and a plurality of wireless electronic door locks each configured to wirelessly communicate with the interface module. Each of the wireless electronic door locks includes a controller and a wireless receiver operatively connected to the controller, the wireless receiver including a first antenna defined as a circuit board trace and a second antenna, spaced from the first antenna and defined as a circuit board trace. Each of the first antenna and the second antenna include one of a monopole antenna and a fractal antenna. The controller is configured to switch between the first antenna and the second antenna to receive a wireless signal having a greater signal strength.

WO 2016/196481 A1

ANTENNA DIVERSITY IMPLEMENTATION FOR WIRELESS LOCKS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Provisional Application No. 62/169,069 filed on June 1, 2015 entitled "Antenna Diversity Implementation for Wireless Locks", the disclosure of which is herein incorporated by reference in its entirety.

FIELD OF THE INVENTION

[0002] The present disclosure relates to a security device, and more particularly to a door lock for securing a door.

BACKGROUND

[0003] Existing electronic lock systems are used to control access to various areas within a facility. Some systems employ wireless locks that communicate with an interface device, also known as a panel interface module, sufficiently proximate to the electronic locks to enable radio communication. The interface device is configured to monitor and control the state of a predetermined number of electronic locks, such that multiple interfaced devices can be required in a facility of a large size, since one interface device can be insufficient to monitor and control all of the electronic locks in the facility. Consequently, a number of interface devices are hardwired to a central controller, also known as an access control panel, and are connected to the computer system of the facility. In some facilities, more than one access control panel can be required. The computer system provides updates to the electronic locks through this radio communication network. However, the hardwired connection of the interfaces devices with the access control device can be expensive in large facilities, and creates concerns that the hardwiring is redundant with the existing wiring of the various area networks of the facility.

[0004] Some existing systems, when used inside a building or other structure, are susceptible to multi-path interference from door and hall passages, individuals, and architectural construction which limit the effective range of communication between the interface device and the electronic lock, each of which includes a receiver and a transceiver. Because of the multi-path interference, wireless locks sometimes have intermittent reception in indoor environments that makes the

working range unpredictable. When the interface device and the electronic lock are in clear sight of each other, the electronic communication between the two can pass directly from one antenna to the other.

[0005] When there is no clear line-of-sight between the interface device and the electronic lock, the wireless electronic signal can reach the receiver of the electronic lock over multiple paths. The electronic signals traveling along multiple paths will be out of phase with other received signals and cause the multi-path distortion. In a typical office or industrial setting, multi-path distortion can be caused by the location of locks relative to interface device, and can even change dynamically as individuals move about the facility and doors are opened and closed. A receiver at the electronic lock attempts to decode the original signal from the distorted signal. If the distortion is too high, the receiver can fail to decode the transmitted signal and a communication error results. Because of this, the interface device must be relocated, usually closer to the electronic lock. In some cases, the number of interface devices must be increased to accommodate the facility, even though the interface device is not being fully utilized. What is needed, therefore, is an electronic door lock system which reduces signal distortion resulting from the configuration of the facility and the location of the electronic locks.

SUMMARY

[0006] In one embodiment, there is provided a system, components, devices, and methods for improving wireless communication in an electronic lock system, including communication between interface modules and electronic locks. Other embodiments include apparatuses, systems, devices, hardware, methods, and combinations improving communication to and from wireless locks by utilizing antenna diversity.

[0007] In one embodiment, there is provided a method of wireless electronic communication between an electronic door lock and an interface module. The method includes receiving a first wireless signal at a first antenna of the electronic door lock and receiving a second wireless signal at a second antenna of the electronic door lock. The method further includes determining the signal strength of each of the first signal and second signal and selecting one of the first antenna and the second antenna to receive one of the first signal and the second signal based on the determined signal strength.

[0008] In another embodiment, there is provided an electronic lock system including an electronic door lock having a controller, a wireless receiver operatively connected to the controller, and a first and second antenna each operatively connected to the receiver. An interface module includes a wireless transmitter wherein the wireless transmitter is configured to transmit wireless signals configured to modify an operating condition of the door lock. The controller is configured to execute stored program instructions to: (i) determine a first signal strength of a first RF signal received by the first antenna; (ii) determine a second signal strength of a second RF signal received by the second antenna; (iii) compare the first signal strength to the second signal strength to determine which is greater; and (iv) determine the content of the greater of the first signal and the second signal based on the compared first signal strength and the second signal strength.

[0009] In still another embodiment, there is provided an electronic lock system including an access control device configured to provide system instructions, an interface module electrically coupled to the access control device and configured to transmit RF signals in response to system instructions received from the access control device, and a plurality of wireless electronic door locks each configured to wirelessly communicate with the interface module. Each of the wireless electronic door locks includes a housing having disposed therein a controller and a wireless receiver operatively connected to the controller, the wireless receiver including a first antenna and a second antenna spaced from the first antenna.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The description herein makes reference to the accompanying figures wherein like reference numerals refer to like parts throughout the several views, and wherein:

[0011] FIG. 1 is a schematic view of an example wireless lock system; and

[0012] FIG. 2 is a block diagram of another example wireless lock system.

[0013] FIG. 3 is a block diagram of a lock device.

[0014] FIG. 4 is a block diagram of a lock device operatively coupled to an external device.

[0015] FIG. 5 is a diagram of a lock device coupled to a door.

[0016] FIG. 6 is a schematic diagram of one embodiment of a transceiver.

[0017] FIG. 7 is a schematic diagram of one embodiment of a transceiver.

[0018] FIG. 8 is a schematic diagram of the reception of a first signal and a second signal by a first antenna and a second antenna.

[0019] FIG. 9 is a block diagram of a process to select one of multiple antennas to pass a signal to a selector.

DESCRIPTION

[0020] For the purposes of promoting an understanding of the principles of the invention, reference will now be made to the embodiments illustrated in the drawings and specific language will be used to describe the same. It will nevertheless be understood that no limitation of the scope of the invention is thereby intended, any alterations and further modifications in the illustrated embodiments, and any further applications of the principles of the invention as illustrated therein as would normally occur to one skilled in the art to which the invention relates are contemplated herein.

[0021] FIG. 1 illustrates a plurality of access devices 20, in the form of wireless door locks, e.g. for use on an entrance door of a building, room or other part of a structure, that is configured to receive RF signals as part of an RF network 24. The door locks 20 are also configured to send and receive signals to computer network 12 via a WI-FI connection 26. It should be understood that many other devices, in different embodiments, send and receive RF signals as part of the RF network 24 and WI-FI connection 26 and the illustrated door lock is simply an example of one of these devices. The received RF signals received by the door lock are configured to change or modify the operating conditions or operating states of the door lock.

[0022] In the RF network 24, each door lock 20 acts as a communication node that receives a radio signal as a wakeup signal from an access control device 30 through its assigned bridge device 16, also described as a panel interface module. The access control device 30 is configured to provide system instructions and to receive signals from both the interface module 16. The door locks 20 communicate to send and receive information packets via the RF network or via a WI-FI connection 26 with computer network 12 to other devices in the system 10, such as the access control device 30. If a wakeup signal is not addressed to the door lock 20 in RF network 24, the door lock 20 ignores the wakeup signal. If the particular wakeup signal is addressed to the door lock 20 that interrogates it, the door lock 20 is awakened from a sleep mode and operates in a wake or run mode to communicate with access control device 30. In this arrangement, a battery operating life of each door lock 20, if a battery is included, is maintained

since only door locks 20 that are designated to receive information from access control device 30 are awakened in real time for information downloads and uploads. The interrogation of the wakeup signal by door lock 20 occurs in conjunction with radio frequency communications, increasing battery life since the bridge device 16 transmits RF signals and the RF receiver of the access device 20 can operate at a lower power level when compared to standard wireless networks.

[0023] FIG. 2 illustrates a schematic view of another configuration of an electronic lock system 100. The system 100 includes an electronic lock device 102, such as the lock device 20. The lock device 102 includes a lock mechanism including, for instance, a bolt, a latch, or the like to secure a door. The lock device 102 includes at least one wireless transceiver, including a receiver and a transmitter, (e.g., WIFI, Bluetooth, RF etc.) to enable the lock device 102 to communicate with a gateway or router 104 which communicates with a server 106. The gateway or router, in one embodiment corresponds to the panel interface module 16. The lock device 102 and the server 106 communicate various information with each other such as access requests, user databases, and audits.

[0024] The lock device 102 includes a processor 108 that implements software controlled antenna diversity. The antenna diversity process is designed to minimize the additional length of the preamble and processor overhead so that there is a minimal effect on additional power consumption, thereby maintaining battery life. The lock device 102 includes two or more antennas 110 to receive a signal from the gateway or router 104. The diversity antennas of the lock device 102 are placed in different locations/orientations on a printed circuit board (PCB) and/or otherwise within or at the lock device 102 with firmware being used to sense which antenna has better reception signal strength and to automatically switch to one of the two or more antennas which receives the best signal.

[0025] The circuitry in the wireless transceiver of the lock device 102, in different embodiments, is configured to provide appropriate signal conditioning to transmit and receive desired information (data). The circuitry includes one or more of filters, amplifiers, limiters, modulators, demodulators, CODECs, digital signal processing, and/or different circuitry or functional components as would occur to those skilled in the art to perform the desired communications.

[0026] In one embodiment, the lock device 102 is a wireless electronic door lock, which is further shown in a block diagram form in FIG. 3. The lock device 102 includes a logic and memory module 140, a suitable power source 142, such as A/C power and/or battery power, a keyless entry system 144, a keyed entry mechanism 146, a locking mechanism 148, a multi-frequency transceiver 150 (receiver and transmitter), and a user interface 152.

[0027] The keyless entry system 144 includes a keypad 144a for entering an access code and other data. In other embodiments, other data entry systems may be used in place of the keypad, such as biometric entry, smart cards, infrared readers, etc. The keyless entry system 144, in different embodiments, includes a card reader for electronically reading an access code from a card carried by the user. The keyless entry system 144 communicates with the logic and memory module 140 that stores access codes, other user identification information, other data and carrying out the functions of the lock device 102. The logic and memory module 140, in different embodiments, stores individual user codes, where each user having access to the door is issued a unique user code that is stored and compared to input codes at the door to allow access decisions to be made at the door without transmissions over computer network 100.

[0028] In one embodiment, logic and memory module includes a processor that drives communications with RF network 24 and establishes WI-FI connection 26 through appropriate hardware on access device 20 and interface device 16. The logic and memory module 140 may further include an internal memory for storing credential data and audit data, and a real-time clock for determining times associated with access events. In addition, logic and memory module 140 is operable in a low power mode to preserve battery life. In one specific embodiment, logic and memory module 140 includes an advance reduced instruction set computer machine.

[0029] Software routines resident in the included memory are executed in response to the signals received and signals transmitted. The executed software routines include one or more specific applications, components, programs, objects, modules or sequence of instructions typically referred to as "program code". The program code includes one or more instructions located in memory and other storage devices which execute the operation of the lock device 102.

[0030] The keyed entry mechanism 146, in some embodiments, manually operates the locking mechanism 148, for example in case of power loss or other malfunction. The locking mechanism 148 of the lock device 102 includes locking features such as a sliding deadbolt, or

other suitable locking mechanism coupled to a door handle or knob and/or to a key mechanism. In the illustrated construction, the locking mechanism 148 is power-driven, for example by a solenoid or an electric motor, to facilitate remote operation. The lock device 102 may also include a user interface 152 having visual components, such as a display, an LED light and/or an LCD screen, and/or audio components, such as a speaker or other sound-generating device.

[0031] Where the lock device 102 is part of a networked system 10, such as that described herein, functions that can be performed remotely through access control device 30 include, but are not limited to, confirming the status of a lock, such as whether the door lock is locked or unlocked, notifying the network of an attempted access, including whether the lock was accessed, when it was accessed and by whom, whether there were attempts at unauthorized access, and other audit information. In some constructions, the lock device 102 can also receive and execute a signal to unlock the lock, add or delete user codes for locks having such codes, and, if the door lock is paired with a suitable camera (not shown), transmit images of the person seeking entry. The lock device 102 can also be used to send a command to disarm an electronic alarm or security system, or to initiate a duress command from the keypad 144a, where the duress command may be utilized by the network to transmit a message to access control device 30 or other linked device, such as a computer terminal or mobile device, an electronic alarm or security system, or a networked computer server.

[0032] The keypad 144a can also be used to program and configure the operation of the lock device 102, such as adding access codes, deleting access codes, enabling audible operation, and setting relocking time delays. Additionally, the lock device 102 includes multi-frequency transceiver 150, or interface, that can include an RF module 150a including an antenna or programmable card for the reception and transmission of sub 1-GHz RF signals, a WI-FI module 150b configured to establish WI-FI connection 26 to and send and receive WI-FI signals to computer network 12, and all necessary electronic components required for the reception and generation of RF signals and WI-FI connection/disconnection with logic-memory module 140. The WI-FI interface with access control device 30 provides the same operation, programming, and configuration functionality as that afforded by the keypad 144a, in addition to a wide range of features including but not limited to audit information such as lock status reporting, lock operation reporting, lock battery status, and the like.

[0033] The logic and memory module 140, in different embodiments, is a programmable type, a dedicated, hardwired state machine, or any combination of these. The logic and memory module can include multiple processors, Arithmetic-Logic Units (ALUs), Central Processing Units (CPUs), Digital Signal Processors (DSPs), or the like. The logic and memory module may be dedicated to performance of the operations described herein or may be utilized in one or more additional applications. In the depicted form, logic and memory module is of a programmable variety that executes algorithms and processes data in accordance with operating logic as defined by programming instructions (such as software or firmware) stored in memory. In other embodiments, the memory is separate from the logic and is part of the logic or is coupled to the logic.

[0034] The memory is of one or more types, such as a solid-state variety, electromagnetic variety, optical variety, or a combination of these forms. Furthermore, the memory can be volatile, nonvolatile, or a combination of these types, and some or all can be of a portable variety, such as a disk, tape, memory stick, cartridge, or the like. In addition, memory can store data that is manipulated by the operating logic of the logic and memory 108, such as data representative of signals received from and/or sent to input/output device interface devices 16.

[0035] FIG. 4 illustrates another example of a lock device 200 including a processing device 202, which corresponds to the logic and memory module 140, and an input/output device 204, which corresponds to the transceiver 150. A memory 206 and operating logic 208 are also included in the processing device 202. Furthermore, the lock device 200 communicates with one or more external devices 210.

[0036] The input/output device 204 allows the lock device 200 to communicate with one or more external devices 210. For example, the input/output device 204 may be a transceiver, network adapter, network card, interface, or a port (e.g., a USB port, serial port, parallel port, an analog port, a digital port, VGA, DVI, HDMI, FireWire, CAT 5, or any other type of port or interface). The input/output device 204 may include hardware, software, and/or firmware. It is contemplated that the input/output device 204 will include more than one of these adapters, cards, or ports.

[0037] The external device 210 may be any type of device that allows data to be inputted or outputted from the lock device 200. For example, the external device 210 may be a switch, a router, a firewall, a server, a database, a mobile device, a networking device, a controller, a

computer, a processing system, a printer, a display, an alarm, an illuminated indicator such as a status indicator, a keyboard, a mouse, or a touch screen display. Furthermore, it is contemplated that the external device 210 may be integrated into the lock device 200. It is further contemplated that there may be more than one external device in communication with the lock device 200.

[0038] Processing device 202 can be a programmable type, a dedicated, hardwired state machine, or any combination of these. Alternatively or additionally, operating logic 208 for processing device 202 is at least partially defined by hardwired logic or other hardware. Processing device 202 may include one or more components of any type suitable to process the signals received from input/output device 204 or elsewhere, and to provide desired output signals. Such components may include digital circuitry, analog circuitry, or a combination of both. Memory 206 may be of one or more types, such as a solid-state variety, electromagnetic variety, optical variety, or a combination of these forms.

[0039] The various aspects of the processes in the present application may be implemented in operating logic 208 as operations by software, hardware, artificial intelligence, fuzzy logic, or any combination thereof, or at least partially performed by a user or operator. In certain embodiments, operations represent software elements as a computer program encoded on a computer readable medium, wherein the processor of the lock device 102 performs the described operations when executing the computer program.

[0040] FIG. 5 illustrates one embodiment of the lock device 102 coupled to a door 160. The lock device 160 supports a handle 162 which when moved with respect to the door 160 operates a latch 164, as is understood by those skilled in the art. The lock device 160 includes a housing 166, a portion of which is removed to show a transceiver 170 which includes a first antenna 172 and a second antenna 174. See also FIGS. 6 and 7 for antennas 172 and 174.

[0041] By incorporating at least a first and second antenna into the transceiver 170, multi-path interference from door and hall passages, personnel, and architectural construction, which limits the effective range of communication between transceivers, is overcome. By providing multiple antennas at the transceiver 170, a more robust antenna system is provided which improves the wireless communication range and which also maintains or exceeds existing performance while reducing the package size of the antenna system.

[0042] The RF signals being transmitted by the interface module16, if there is no clear line-of-sight between the transmitter and receiver, may reach the receiver of the transceiver 170 from multiple paths. RF signals reaching the receiver via multiple paths will be out of phase with each other and cause the multi-path distortion. The disclosed door lock system overcomes the problems inherent in multi-path distortion caused by the location of locks relative to interface modules, which distortion can change dynamically as individuals move within a structure and when doors are opened and closed.

[0043] The present disclosure utilizes antenna diversity, or the use of multiple antennas, generally in close proximity to each other, and in some embodiment within a housing of the door lock, to receive a signal having sufficient definition to be demodulated. A software algorithm is configured to minimize the amount of information needed from the preamble to determine which antenna has the better reception. Since less information from the preamble is needed, the processor overhead is reduced so that there is a minimal effect on additional power consumption, thereby maintaining battery life. The multiple antennas are placed in different locations and/or orientations with firmware configured to sense which antenna has a better reception signal strength and to automatically switch to the antenna having the best signal.

[0044] In systems that have a single antenna at a door lock system, the installer often tries to locate the interface module at the margins of acceptable reception and transmission. In so doing, a lock on the RF signal at the margins can often be received more strongly, but such reception can disrupt the reception of another lock or even multiple locks in the system. Since, in one embodiment, the system can support sixteen (16) locks per interface module, multiple antennas at a single door lock reduces the difficulty in locating the interface modules, so that all the locks have reliable communication.

[0045] When the installer is checking for communication link reliability with a wireless portable reader (WPR), the installer expects that if the WPR shows reliable communication at a certain place, then the lock will also have the same reliable communication in the general vicinity. This is not always the case, however, because holding the WPR in the general area where a lock is to be installed does not always guarantee that the lock will not be placed at a null location. Antenna diversity reduces the likelihood of this placement, by providing a lock with two or more uncorrelated antennas for reception. This decreases the amount of service calls needed by the customer.

[0046] Battery life is also improved when utilizing antenna diversity because the existence of a robust communication link reduces the number attempts to communicate, and fewer retransmissions result, which conserves power.

[0047] In addition, a system having door locks, each of which utilizes two or more antennas, which are selected based on signal quality and/or strength, effectively provides a multiple position antenna system for each wireless electronic door lock. Consequently, even though the door lock is not subject to multipath interference such as is experienced by mobile phones on the move, the disclosed door lock adapts to a building structure that provides a significant dynamic multipath environment, even though the door lock is relatively stationary.

[0048] As seen in FIG. 6, the transceiver 170 includes a circuit board 176 adapted to support circuitry or function components 178 coupled to the first antenna 172 and the second antenna 176. Each of the first antenna 172 and 174 are monopole antennas which are coupled to the circuitry 178 through a selector 180. The first and second antennas 172 and 174 are not limited to monopole antennas. In other embodiments, one or both of the antennas are of another type including microstrip and planar inverted-F antennas. The selector 180 electrically connects one or the other of the first antenna 172 and the second antenna 174 to the circuitry 178. In this configuration, each of the antennas 172 and 174 acts separately from the other antenna as a standalone antenna. Depending on the output of the selector 180, only one of the antennas 172 and 174 is electrically coupled to the circuit 178 at a time.

[0049] Each of the antennas 172 and 174 are mirror images of the other such that while the structure of each is the same, the orientation is mirrored. In one embodiment, each of the antennas 172 and 174 are configured as a circuit board trace which are formed by etching. Other embodiments include the deposition of conductive material on the circuit board or the placement of a physical wire either fixed to the surface of the circuit board or placed in a channel formed in the circuit board.

[0050] Each of the first antenna 172 and the second antenna 174 includes a generally straight first portion 182 extending along the circuit board at a generally ninety (90) degree angle with respect to each other. At an end 185 of each of the first portions 182, a second portion 184 extends at about a ninety (90) degree angle with respect to the first portion 182. Each of the second portions 184 includes terminating ends 186. Each of the second portions 184 are separated from one another by an expanse of the circuit board not supporting any traces,

conductors, or components. In this embodiment, each of the antennas are oriented on the same plane and spaced a physical distance apart. In other embodiments, each of the antennas differs in mounting orientation, or polarization, relative to the circuitry 178.

[0051] FIG. 7 illustrates another embodiment of the transceiver 170 including the first antenna 172, the second antenna 174, circuit 178, and selector 180. In this embodiment, the first antenna 172 and the second antenna 174 are each a fractal antenna, so named after the geometric pattern and which are used to "fold the antenna" on itself. Other shapes of monopole antennas are also possible. The fractal antenna is a reduced size version of a quarter wavelength antenna. In this embodiment, each of the antennas are oriented on the same plane and spaced a physical distance apart. In one embodiment, the antennas 172 and 174 are fractal Koch antennas.

[0052] In other embodiments, the first and second antennas 172 and 174 are placed at the same location but are at different orientations or different polarizations with respect to each other.

[0053] FIG. 8 illustrates a schematic diagram of the reception of a first signal 190 and a second signal 192 respectively by each of the first antenna 172 and the second antenna 174. Each of the first signal 190 and the second signal 192 includes data having a defined structure which includes an n bit preamble, a sync word, and data. The illustration is representational of each of the signals 190 and 192 and in other embodiments, the signals are analog or digital signals having different arrangements of frequency, modulation, phase, preambles, sync, and data packets are possible. Each of the antennas 172 and 174 receives signals which travel along multiple paths within the building structure and which, depending on the path taken, can be out of phase with each of other received signals resulting in a signal suffering from the multi-path distortion. To determine which of the signals received by each of the antennas is readable, the selector 180 includes a first signal strength detector 194 and second signal strength detector 196. The determined signal strength is identified as a received signal strength indication (RSSI). The signal strength detectors determine the signal strength as a function of the preamble of the received signals. In one embodiment, the strength of the preamble is determined by the number of received bits which is compared to known preamble bits sequences. In another embodiment, the strength is determined by a signal strength value measured in decibel-milliwatts (dBm).

[0054] The measured strength values are compared at a comparator 198 which determines which of the received signals is greater in strength. The comparator 198 generates and provides an indicator identifying the preferred signal to a switch 200, which selects the antenna receiving

the preferred signal. The signal having the best signal quality and/or strength is then further processed to determine the content of the sync word and the data.

[0055] The processor 108 is configured to process the received signals based on a set of instructions located in firmware or in memory. As illustrated in FIG. 9, the transceiver 150 recognizes a wakeup signal at block 220 and begins to search for signals being transmitted by the interface 16. At block 222, the receiver searches for a preamble of a signal being received at only one of the antennas, for instance antenna 172. Once a preamble is found on the received signal, the receiver determines at block 224 whether the preamble is invalid or whether the preamble is not recognizable with a predetermined amount of time. If the outcome is yes, the receiver switches to the other antenna, for instance antenna 174 at block 226. Once switched, a preamble for the signal received is searched for at block 222. If the preamble is valid for the signal appearing at either one of the antennas, then the signal strength of the signal having the recognized preamble is determined at block 228. In this example, is it assumed that the signal having the recognizable preamble is received at the first antenna 172. The value of the signal strength is then stored in the memory of the memory and logic module 142.

[0056] After determining the signal strength, the receiver switches to the other antenna, the second antenna 174 in this example, at block 230. Once switched, the signal strength of the signal received by the second antenna is determined at block 232. In this embodiment, the first and second signals include the same content (i.e. the same preamble, the same sync word, and the same data) but vary in signal strength. The signal strength of the second signal is then stored in the memory and logic module 142.

[0057] Once the signal strengths have been determined, the first signal strength is compared to the second signal strength at block 234 to determine if the first signal strength is stronger. If the first signal strength is stronger, the selector 180 selects the first antenna at block 236. The received signal is re-verified to include a valid preamble at block 238. If, however, the first signal strength was not stronger than the second signal strength, the selector selects to the second antenna at block 240. Once the second signal is received, the second signal is re-verified to determine if the preamble is valid at block 238. If the preamble is verified for either of the first signal and the second signal, the remainder of the packet is received at block 242. During this process, dynamic switching between antennas occurs to determine which signal is more

acceptable. If, however, one or both of the preambles is not verified, the process for determining the content of a received signal returns to block 222.

[0058] Because the door moves between open and closed positions and all points in between, the use of multiple antennas improves the working range of the electronic door lock should the interface module 16 transmit instructions while the door is located at any one of the possible locations. Incorporating multiple antennas in a wireless electronic door lock provides a working range significantly more consistent and repeatable, which results in better and more reliable communication with the door lock.

[0059] It is contemplated that the various aspects, features, computing devices, processes, and operations from the various embodiments may be used in any of the other embodiments unless expressly stated to the contrary.

[0060] While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is to be considered as illustrative and not restrictive in character, it being understood that only certain exemplary embodiments have been shown and described and that all changes and modifications that come within the spirit of the inventions are desired to be protected.

[0061] In reading the claims, it is intended that when words such as “a,” “an,” “at least one,” or “at least one portion” are used there is no intention to limit the claim to only one item unless specifically stated to the contrary in the claim. When the language “at least a portion” and/or “a portion” is used the item can include a portion and/or the entire item unless specifically stated to the contrary.

WHAT IS CLAIMED IS:

1. A method of wireless electronic communication between an electronic door lock and an interface module, the method comprising:

receiving a first wireless signal at a first antenna of the electronic door lock;

receiving a second wireless signal at a second antenna of the electronic door lock;

determining the signal strength of each of the first signal and second signal; and

selecting one of the first antenna and the second antenna to receive one of the first signal and the second signal based on the determined signal strength.

2. The method of claim 1 further comprising:

selecting the first antenna to receive the first signal if the first signal strength is greater than the second signal strength.

3. The method of claim 2 further comprising:

determining if a preamble of the first signal is valid; and

receiving a remainder of the first signal if the preamble is valid.

4. The method of claim 1 wherein the receiving a second wireless signal at a second antenna of includes receiving a second wireless signal at a second antenna spatially separated from the first antenna.

5. The method of claim 1 wherein the receiving a first wireless signal includes receiving a first wireless signal at a first fractal antenna and the receiving a second wireless signal includes receiving a second wireless signal at a second fractal antenna.

6. The method of claim 1 further comprising:

selecting the second antenna to receive the second signal if the second signal strength is greater than the first signal strength.

7. The method of claim 6 further comprising:

determining if a preamble of the second signal is valid; and

receiving a remainder of the second signal if the preamble is valid.

8. The method of claim 1 further comprising:

receiving a preamble of one of the first signal and the second signal from one of the first antenna and the second antenna; and

determining if the preamble of the received preamble is invalid; and

receiving a preamble of the other of the first signal and the second signal if the received preamble is invalid.

9. The method of claim 8 wherein the receiving a first wireless signal includes receiving a first wireless signal at a first antenna if the preamble is valid.

10. The method of claim 9 wherein the receiving a first wireless signal includes receiving a first wireless signal at a first antenna if a timeout has not occurred.

11. An electronic lock system comprising:

an electronic door lock including a controller, a wireless receiver operatively connected to the controller, and a first and second antenna each operatively connected to the receiver; and

an interface module including a wireless transmitter, the wireless transmitter configured to transmit wireless signals configured to modify an operating condition of the door lock, wherein the controller is configured to execute stored program instructions to:

determine a first signal strength of a first RF signal received by the first antenna;

determine a second signal strength of a second RF signal received by the second antenna;

compare the first signal strength to the second signal strength to determine which is greater; and

determine the content of the greater of the first signal and the second signal based on the compared first signal strength and the second signal strength.

12. The electronic lock system of claim 11 wherein each of the first signal and the second signal are organized as a packet of data including an n-bit preamble and a data sequence.

13. The electronic lock system of claim 12 wherein the controller is further configured to execute stored program instructions to:

determine if the preamble the first signal at the first antenna is valid; and

determine the first signal strength of the first signal if the determined preamble of the first signal is valid.

14. The electronic lock system of claim 13 wherein the controller is further configured to execute stored program instructions to:

determine whether the preamble of the second signal at the second antenna is valid; and

determine the second signal strength of the second signal if the determined preamble of the second signal is valid.

15. The electronic lock system of claim 14 further comprising switching from one of the first antenna and the second antenna to the other of the first antenna and the second antenna to receive the one of the first signal and the second signal having the greatest signal strength.

16. The electronic lock system of claim 15 further comprising verifying that the preamble of the greater of the first signal and the second signal is valid.

17. The electronic lock system of claim 15 further comprising determining the content of the data sequence if the preamble of the greater of the first signal and the second signal is valid.

18. An electronic lock system comprising:

an access control device configured to provide system instructions;

an interface module electrically coupled to the access control device and configured to transmit RF signals in response to system instructions received from the access control device;

and

a plurality of wireless electronic door locks each configured to wirelessly communicate with the interface module, wherein each of the wireless electronic door locks includes a housing having disposed therein a controller and a wireless receiver operatively connected to the controller, the wireless receiver including a first antenna and a second antenna spaced from the first antenna.

19. The electronic lock system of claim 18 wherein the each of the first antenna and the second antenna comprise one of a monopole antenna and a fractal antenna.

20. The electronic lock system of claim 19 wherein the first antenna and the second antenna are oriented at an angle of about ninety degrees with respect to each other.

21. The electronic lock system of claim 20 wherein the first antenna and the second antenna are defined as a circuit board trace.

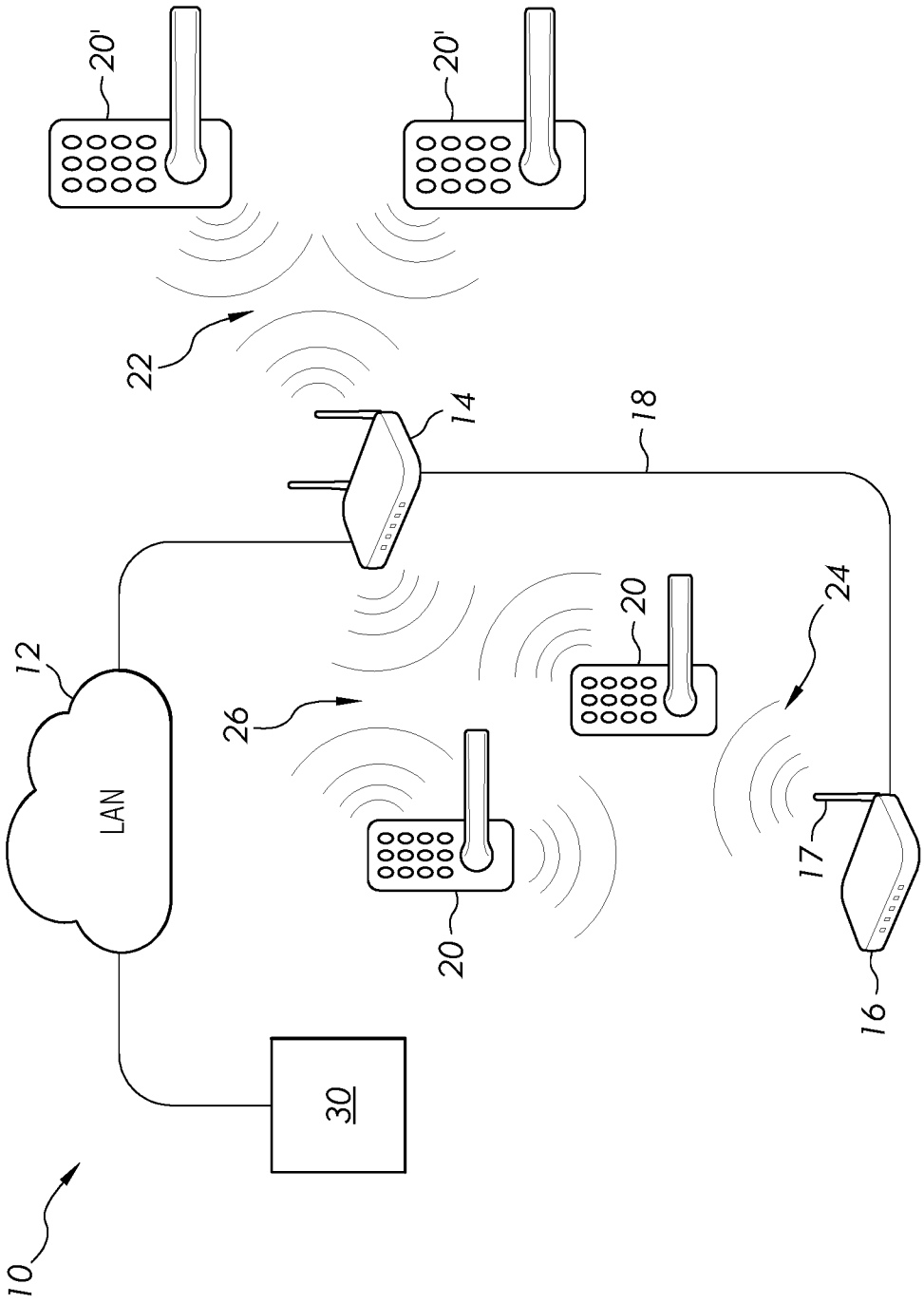

FIG. 1

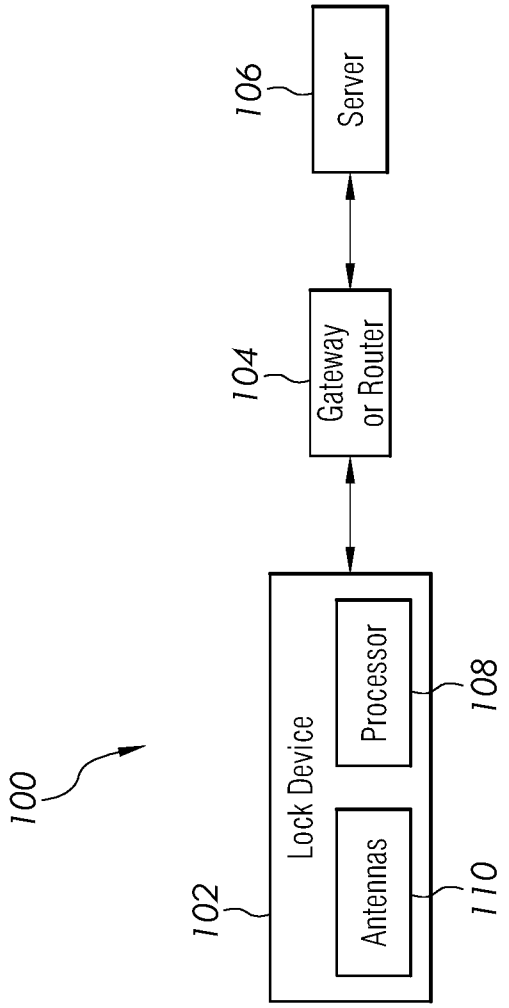
100
102
Lock Device
Antennas
110
Processor
108
104
Gateway or Router
106
Server

FIG. 2

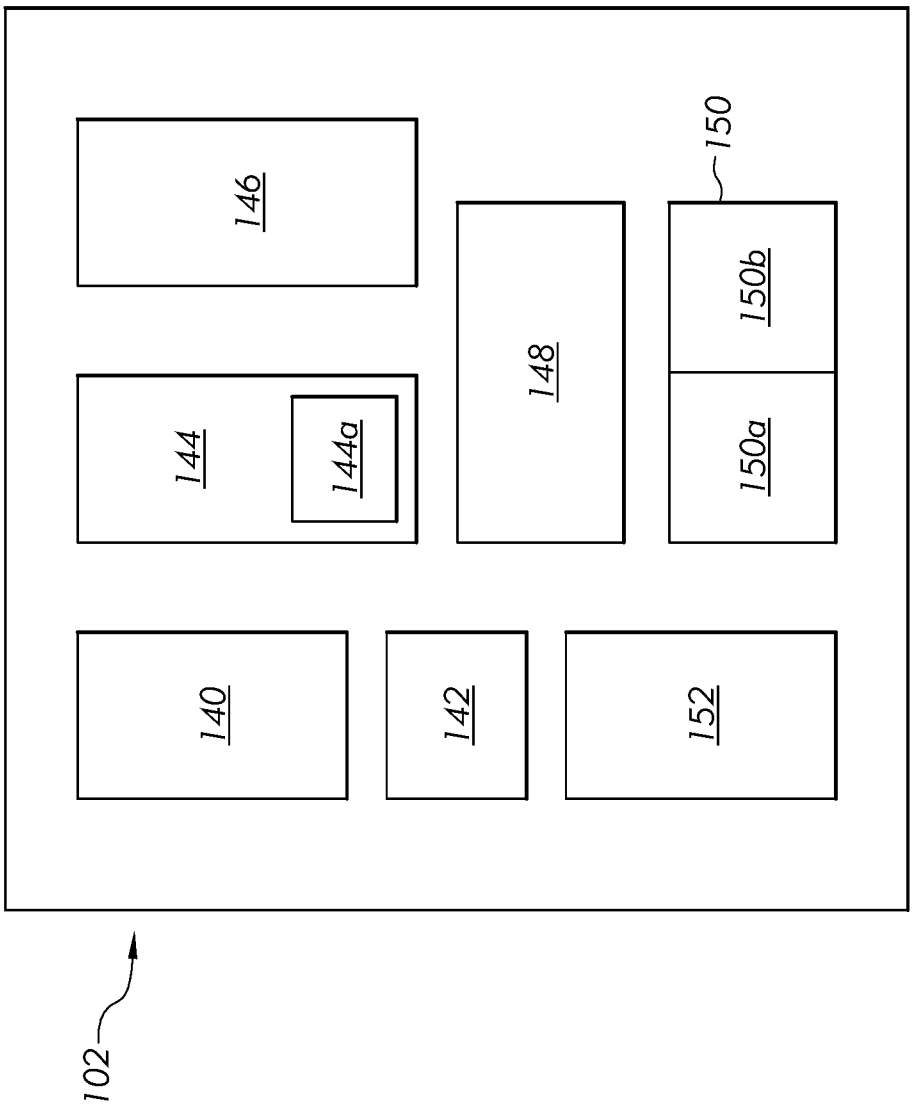

FIG. 3

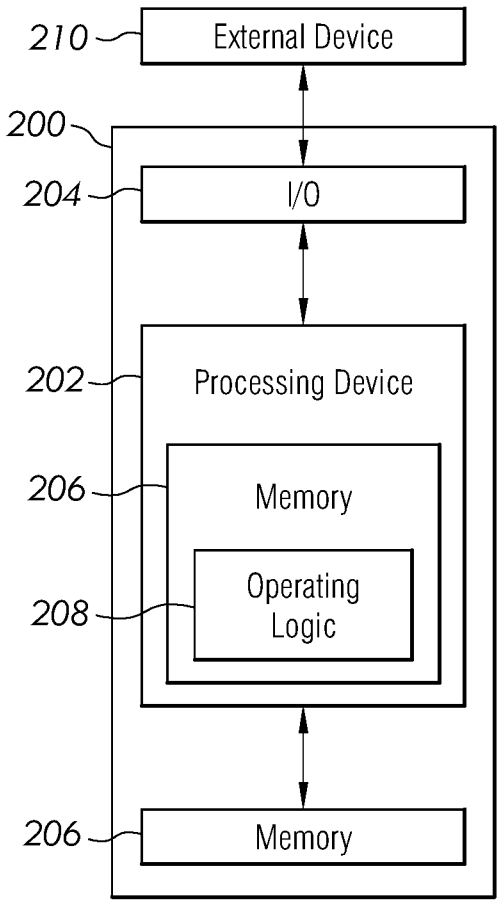
210
External Device
200
204
I/O
202
Processing Device
206
Memory
208
Operating Logic
206
Memory

FIG. 4

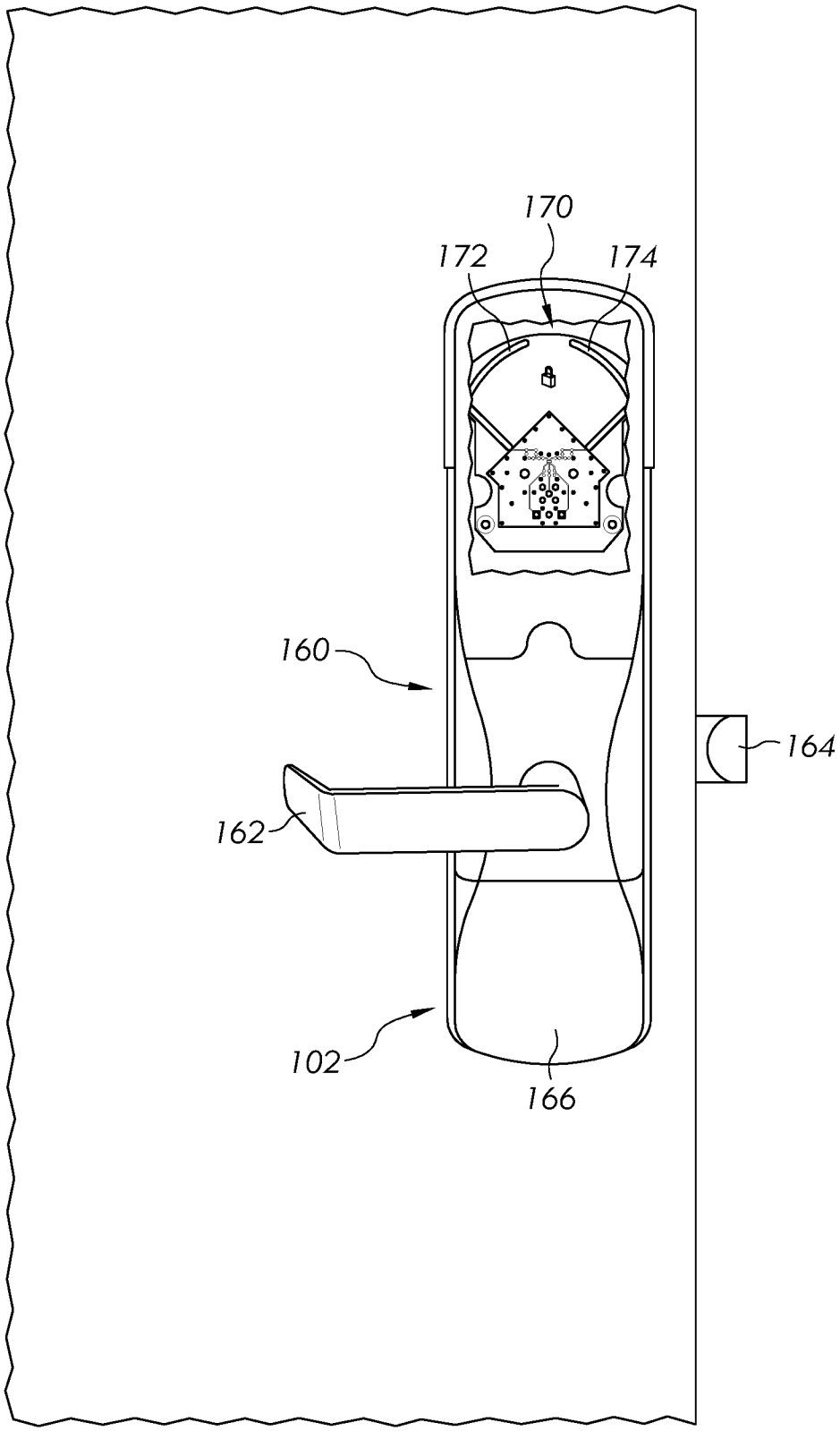

FIG. 5

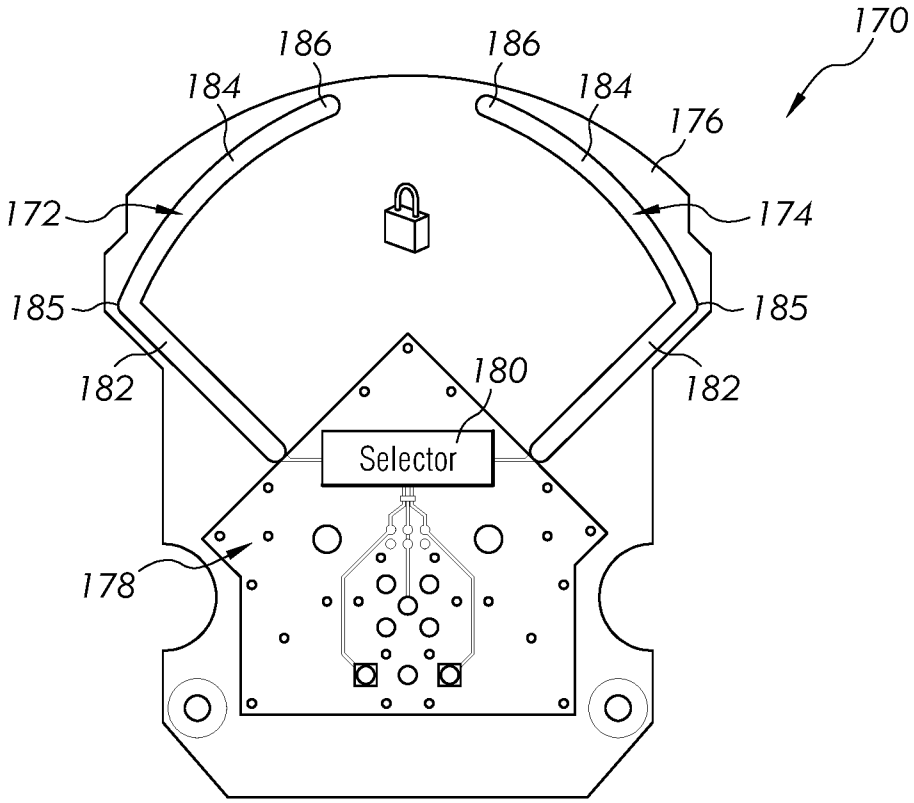
170
186
186
184
184
176
172
174
185
185
182
182
180
Selector
178

FIG. 6

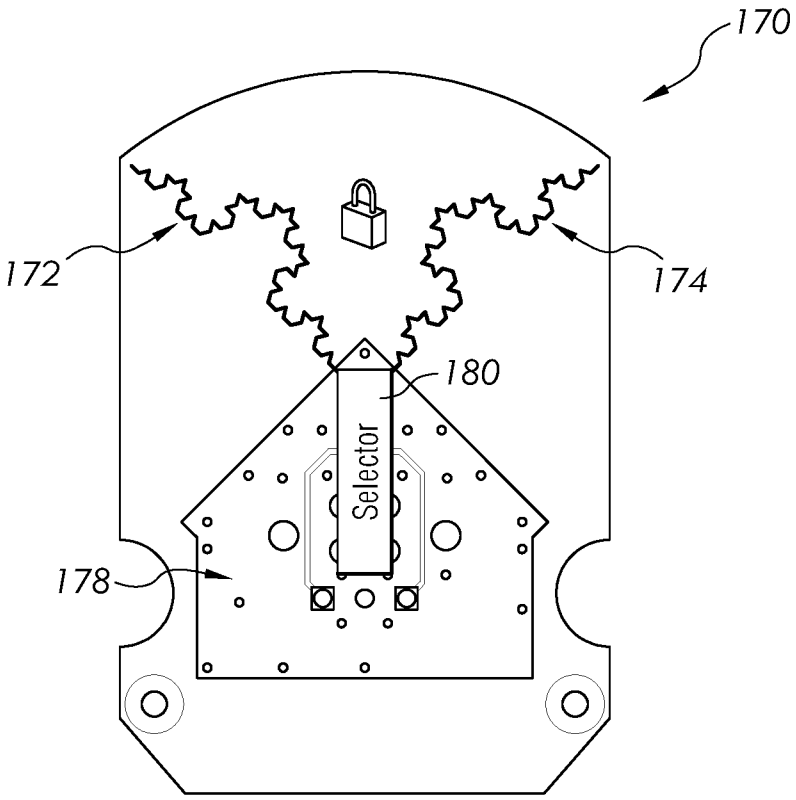
170
172
174
180
Selector
178

FIG. 7

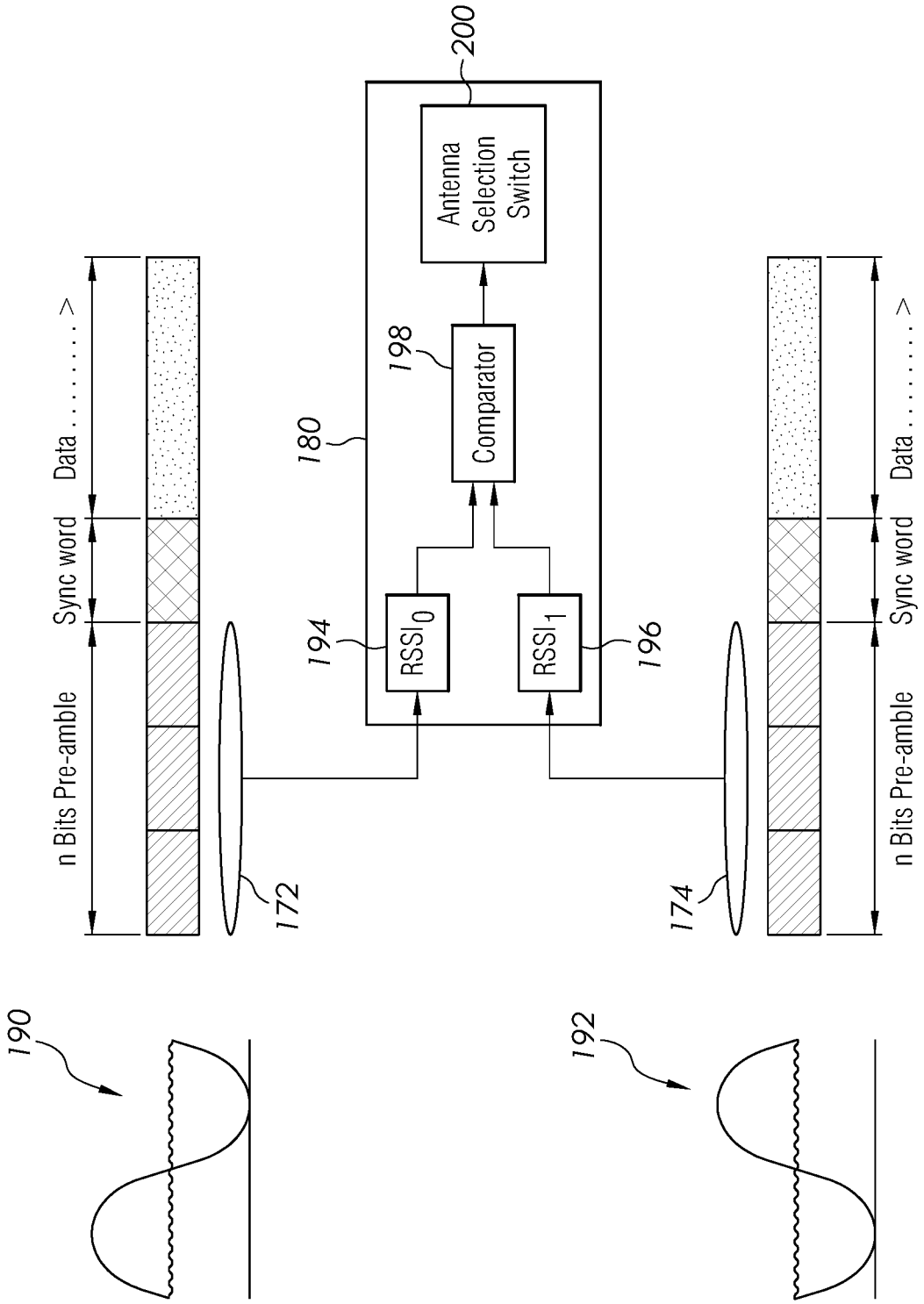
200
Antenna Selection Switch
198
Comparator
180
194
RSSI0
RSSI1
196
n Bits Pre-amble
Sync word
Data . . . . . >
172
174
190
192

FIG. 8

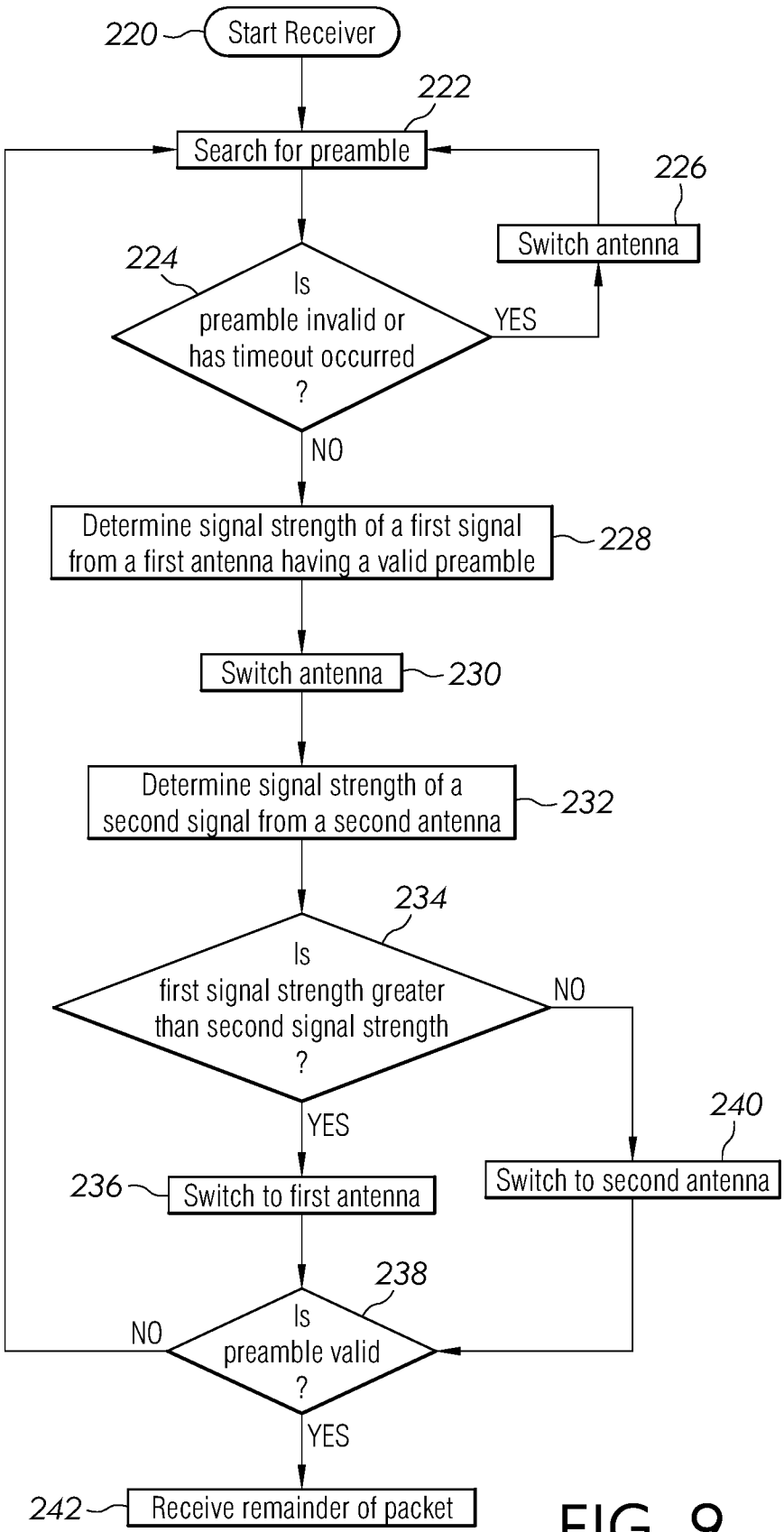
220
Start Receiver
222
Search for preamble
226
Switch antenna
224
Is preamble invalid or has timeout occurred ?
YES
NO
Determine signal strength of a first signal from a first antenna having a valid preamble
228
Switch antenna
230
Determine signal strength of a second signal from a second antenna
232
234
Is first signal strength greater than second signal strength ?
NO
YES
240
Switch to second antenna
236
Switch to first antenna
238
Is preamble valid ?
NO
YES
242
Receive remainder of packet

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/35045

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G08C 17/02; E05B 49/02, E05F 15/70 (2016.01)
CPC - G08C 17/02, G07C 9/00309, 9/00174
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(8) Classifications: G08C 17/02; E05B 49/02, E05F 15/70 (2016.01)
CPC Classifications: G08C 17/02, G07C 9/00309, 9/00174

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)
PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, Other Countries, (INPADOC), RU, AT, CH, TH, BR, PH); Google Patent, Google, IEEE, EBSCO.
Keywords: wireless, door, locks, antenna, diversity, preamble, frame, electronic, valid, invalid, fractal, second, signal, strength.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0292481 A1 (UNIKEY TECHNOLOGIES INC.) October 02, 2014; figures 7a, 7b, 10, 15, paragraphs [0040], [0053], [0092], [0093].	1-10
Y	US 2013/0102316 A1 (QUALCOMM INCORPORATED) April 25, 2013; figure 6, paragraphs [0024], [0065].	1-10
Y	LEE, J et al. "Improved modeling of IEEE 802.11a PHY through finegrained measurements". (Abstract only) Advances in Wireless and Mobile Networks, Computer Networks. Volume 54, Issue 4, 19 March 2010, Pages 641–657. < URL: http://www.sciencedirect.com/science/article/pii/S1389128609002436> DOI:10.1016/j.comnet.2009.08.003.	3, 7
Y	US 7,088,965 B1 (NGAN, J) August 08, 2006; figure 1, column 3, lines 12-17, claims 1, 16.	5
Y	US 8,064,861 B2 (RUIJTER, H) November 22, 2011; abstract, figures 1, 3, 4, & 6, column 5, lines 53-67, column 6, lines 33-59, claims 1, 10, & 11.	8-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"I." 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
28 September 2016 (28.09.2016)	04 NOV 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/35045

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
Group I: Claims 1-10

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US16/35045

-***-Continued from Box No. III Observations where unity of invention is lacking-***-

Claims 1 & 11 are objected to under PCT Rule 66.2(a)(v) as lacking clarity under PCT Article 6 because claims 1 & 11 are indefinite for the following reasons:

In claim 1, there is a lack of antecedent basis for the limitation, "the signal strength". For the purposes of this opinion, as best understood, "the signal strength" has been interpreted to read "a signal strength".

In claim 11, there is a lack of antecedent basis for the limitation, "determine the content of the greater". For the purposes of this opinion, as best understood, "determine the content of the greater" has been interpreted to read, "determining content of the greater".

Group I: Claims 1-10 appear to be directed towards selecting one of the first antenna and the second antenna to receive one of the first signal and the second signal based on the determined signal strength.

Group II: Claims 11-17 appear to be directed towards determining content of the greater of the first signal and the second signal based on the compared first signal strength and the second signal strength.

Group III: Claims 18-21 appear to be directed towards an interface module electrically coupled to a access control device and configured to transmit RF signals in response to system instructions received from the access control device.

The inventions listed as Groups I-III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features.

The special technical features of Group I are at least selecting one of the first antenna and the second antenna to receive one of the first signal and the second signal based on the determined signal strength, which are not present in Groups II & III.

The special technical features of Group II are at least an interface module including a wireless transmitter, the wireless transmitter configured to transmit wireless signals configured to modify an operating condition of the door lock, compare the first signal strength to the second signal strength to determine which is greater; and determine a content of the greater of the first signal and the second signal based on the compared first signal strength and the second signal strength, which are not present in Groups I & III.

The special technical features of Group III are at least an access control device configured to provide system instructions; an interface module electrically coupled to the access control device and configured to transmit RF signals in response to system instructions received from the access control device; and a plurality of wireless electronic door locks each configured to wirelessly communicate with the interface module, which are not present Groups I & II.

The common technical features of Groups I-III are at least an electronic door lock including a controller, a wireless receiver operatively connected to the controller, an interface module, wherein the controller is configured to execute stored program instructions to: determine a first signal strength of a first RF signal received by a first antenna; determine a second signal strength of a second RF signal received by a second antenna; compare the first signal strength to the second signal strength.

US 2014/0292481 A1 to UNIKEY TECHNOLOGIES, Inc. discloses an electronic door lock including a controller (lock 11, which is an electronic door lock, includes a controller 21; paragraph [0053], claim 1), a wireless receiver operatively connected to the controller (external antenna 52, which is a wireless receiver, connects to a controller; figure 1, paragraph [0093]), an interface module (a remote access device; paragraph [0114]), wherein the controller is configured to execute stored program instructions to: determine a first signal strength of a first RF signal received by a first antenna (a RF signal (first wireless signal) is received when in in-signal range 90 by external antenna 52 of lock 11, an RSSI is determined; figure 7b, paragraphs [0092], [0093], [0096]); determine a second signal strength of a second RF signal received by a second antenna (when a user of remote access device 915 is within activation range 91 a signal reaches internal antenna 50 of lock 11, an RSSI is determined for the signal; figure 7b, paragraph [0093]); compare the first signal strength to the second signal strength (controller 21 determines RSSI of both the exterior facing antenna 52 and the interior antenna 50; paragraph [0093]).

Since these common features are previously disclosed by UNIKEY, these features are not special and Groups I-III lack unity.