



Office de la Propriété

Intellectuelle
du Canada

Un organisme
d'Industrie Canada

Canadian
Intellectual Property
Office

An agency of
Industry Canada

CA 2845510 A1 2012/12/20

(21) **2 845 510**

(12) **DEMANDE DE BREVET CANADIEN**
CANADIAN PATENT APPLICATION

(13) **A1**

(86) Date de dépôt PCT/PCT Filing Date: 2012/06/15
(87) Date publication PCT/PCT Publication Date: 2012/12/20
(85) Entrée phase nationale/National Entry: 2014/02/14
(86) N° demande PCT/PCT Application No.: US 2012/042683
(87) N° publication PCT/PCT Publication No.: 2012/174387
(30) Priorité/Priority: 2011/06/17 (US61/498,169)

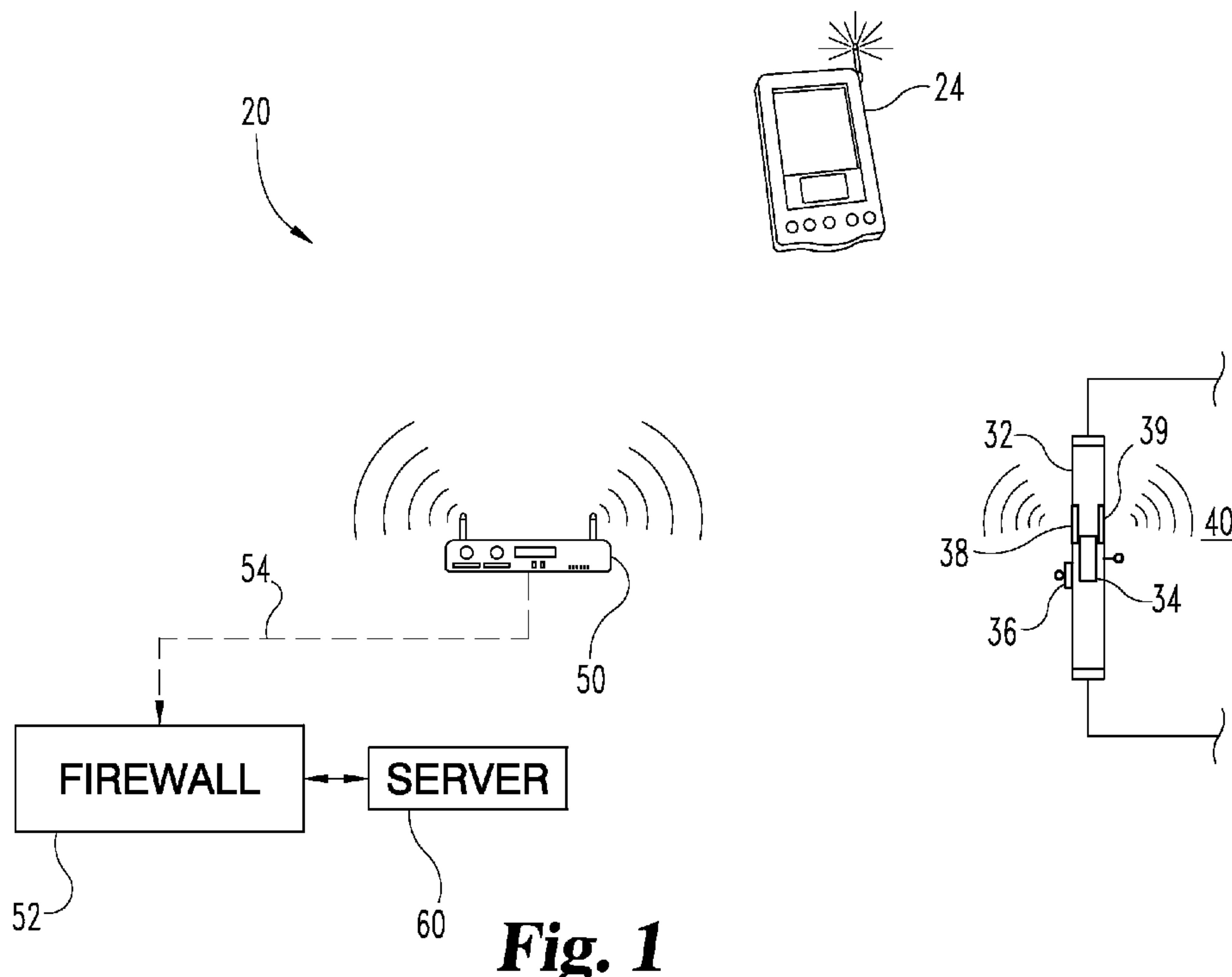
(51) Cl.Int./Int.Cl. *H04W 48/04* (2009.01),
E05B 53/00 (2006.01), *H04W 12/06* (2009.01)

(71) Demandeur/Applicant:
YIKES LLC, US

(72) Inventeurs/Inventors:
MCINTYRE, JIM E., US;
ROBERTSON, WILLIAM BENJAMIN, US;
ROBERTSON, ANDREW JOSEPH, US

(74) Agent: SMART & BIGGAR

(54) Titre : SYSTEME ET PROCEDE POUR ACCEDER A UNE STRUCTURE AU MOYEN D'ANTENNES DIRECTIVES
ET D'UN JETON SANS FIL
(54) Title: SYSTEM AND METHOD FOR ACCESSING A STRUCTURE USING DIRECTIONAL ANTENNAS AND A
WIRELESS TOKEN



(57) Abrégé/Abstract:

A wireless device access system that employs directional antennas for short-range wireless communication to detect the proximity and orientation of a user device with respect to a structure is disclosed. The access system receives and authenticates an unlock request and confirms the proximity and orientation of the user device prior to transmitting an unlock command to the structure. Additionally, the wireless device may require the proximity of a user token prior to operation and/or the access system may include an override within the structure blocking any unlock command.

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 December 2012 (20.12.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/174387 A3

(51) International Patent Classification:
H04W 48/04 (2009.01) *E05B 53/00* (2006.01)
H04W 12/06 (2009.01)

(21) International Application Number:
PCT/US2012/042683

(22) International Filing Date:
15 June 2012 (15.06.2012)

(25) Filing Language:
English

(26) Publication Language:
English

(30) Priority Data:
61/498,169 17 June 2011 (17.06.2011) US

(72) Inventors; and

(71) Applicants : **MCINTYRE, Jim, E.** [US/US]; 7245 N. Ridgeway Lane, Mooresville, IN 46158 (US). **ROBERTSON, Andrew, Joseph** [US/US]; 801 S. Main Street, Monticello, IN 47960 (US). **ROBERTSON, William, Benjamin** [US/US]; 801 S. Main Street, Monticello, IN 47960 (US).

(74) Agents: **MORIARTY, John, V.** et al.; Woodard, Emhardt, Moriarty, McNett & Henry LLP, 111 Monument Circle, Suite 3700, 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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.

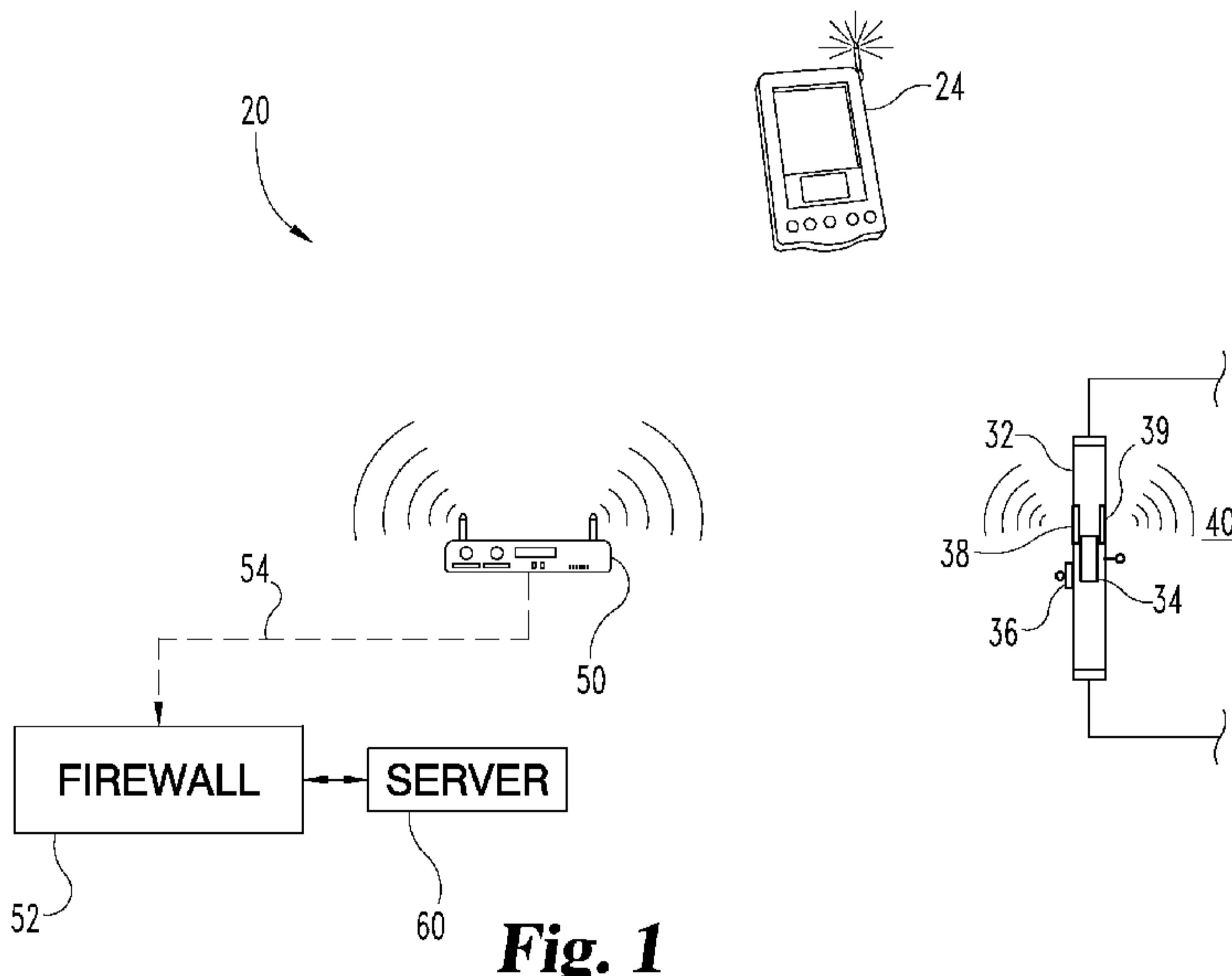
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, 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, ML, MR, NE, SN, TD, TG).

Published:

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

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR ACCESSING A STRUCTURE USING DIRECTIONAL ANTENNAS AND A WIRELESS TOKEN



(57) Abstract: A wireless device access system that employs directional antennas for short-range wireless communication to detect the proximity and orientation of a user device with respect to a structure is disclosed. The access system receives and authenticates an unlock request and confirms the proximity and orientation of the user device prior to transmitting an unlock command to the structure. Additionally, the wireless device may require the proximity of a user token prior to operation and/or the access system may include an override within the structure blocking any unlock command.

WO 2012/174387 A3

(88) Date of publication of the international search report:

21 February 2013

- *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))*

**SYSTEM AND METHOD FOR ACCESSING A STRUCTURE
USING DIRECTIONAL ANTENNAS AND A WIRELESS TOKEN**

CROSS REFERENCE TO RELATED APPLICATIONS

5

The present application claims the benefit of United States Provisional Patent Application Serial No. 61/498,169 filed June 17, 2011 entitled “A System and Method for Accessing a Structure using Directional Antennas and a Wireless Token” which is hereby incorporated by reference in its entirety to the extent not 10 inconsistent.

FIELD OF THE INVENTION

The present invention generally relates to an access system including a wireless token and a proximity and location verification device. More particularly, 15 the present invention pertains to a three point access system which includes a wireless token which transmits a request for access which ultimately results in a door being unlocked.

SUMMARY

20 Disclosed is a wireless device access system which employs short-range wireless communication and one or more directional antennas to require the presence of a user device within a designated area proximate to an entry point of a structure prior to providing access to the structure. The access system includes a wireless node having a wireless transmission area proximate to or covering the 25 entry point which authenticates a user device for a certain structure when the user device comes within range of the wireless node. In response to authenticating the user device, the wireless node sends a wake-up signal to an access device associated with the certain structure, such as a lock on an entry point. In response to the wake-up command, the access device will remain active for a predetermined 30 but limited period of time so as to be available to communicate with a user device. Additionally, in some forms, the wake-up command may also issue a notification triggering an in-room system to prepare the room, such as by turning on the lights or other user specified actions. In a further form, the wake-up command may

include a temporary security code for verifying an unlock command sent by a user device. When the user device comes within range of the recently activated access device, provided that the access device is still active, the user device will communicate its credential information to the access device for confirmation. In 5 addition, the access device utilizes a pair of directional antennas to confirm that the requesting user device is within a designated area, such as a 2 foot semi-circular area outside of a door. Such a location confirmation ensures that access to a structure won't ever be improperly granted based upon a user device within the structure. Upon confirming the authorization associated with the provided access 10 code and confirming that the user device is within the designated area, the access device grants the user access to the structure by unlocking the entry.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagrammatic view of an access system according to one implementation of the present invention.

FIG. 2 is a process flow diagram illustrating one set of steps performed in 5 enabling a user to access a structure using the novel access system, including a wireless token.

FIG. 3 is a mock floor plan illustrating the coverage areas of the access node and the two door lock antennas in a typical multi-room hotel setting.

DETAILED DESCRIPTION

For the purposes of promoting and understanding of the principles of the invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will

5 nevertheless be understood that no limitation of the scope of the invention is thereby intended. Any alterations and further modifications in the described embodiments, and any further applications of the principles of the invention as described herein are contemplated as would normally occur to one skilled in the art to which the invention relates.

10 Currently, systems exist, such as the Signature RFID/NFC system from VingCard, which provide a user access to a hotel room using their mobile phone. Alternatively, other point-to-point systems exist which provide access to an office, lab, or other secured area using a wireless token, such as an RFID tag or card. However, such systems are limited in that the token is limited to a single identifier

15 which leaves open a crucial security flaw which would allow for duplication of the token's responsive signal. Additionally, given the wireless range of these tokens, an undesirable situation may arise in which the token is within range of the lock or RFID reader when inside of the secured area. This presents the possibility that access may be granted to anyone seeking entry at that time.

20 As shown in FIG. 1, one embodiment of an access system 20 advantageously permits a user to access a structure 40 using a wireless token 24. In addition to lodging and workplace access systems, it will be appreciated that similar embodiments of the access system to be described also encompass systems for controlling access to other structures or openings/doors thereof. In particular,

25 the access system 20 is particularly well suited to providing access to structures in which the authorized users are frequently changes, such as a hotel. As such, in the illustrated embodiment, according to FIG. 1, the described system comprises an access system 20 for allowing a hotel guest to access their assigned hotel room 40 using a wireless token 24, which in the preferred form, is an electronic device

30 capable of short range wireless communication, such as a device implementing Bluetooth®, Zigbee®, or some other low-power wireless communication protocol/standard. It shall be understood that many of the descriptions herein are made with respect to a hotel environment and are meant for illustrative purposes

and that the concepts herein are generally applicable to a general safety and security access system and are not limited to only a hotel room access system.

Examples of other structures for which the novel access system may be adapted include other rooms within a hotel (i.e. workout rooms, pools, VIP 5 lounges), office buildings, school/university buildings, laboratories, warehouses, and portions thereof, event ticket gates/turnstiles, movie theatres, safety deposit boxes, mailboxes, lockers, or other enclosures for which providing selective user access is desired.

As shown in FIG. 1, according to the illustrative embodiment, the access 10 system 20 includes one or more wireless tokens 24 which allow a user to access their assigned hotel room without a traditional key or card. Illustratively, in some embodiments, the access system 20 includes a data network 54. Data network 54 is preferably a private local area network (LAN) and may comprise the Internet, which is a TCP/IP based global network; however, the user of the term “Internet” 15 herein shall be understood to refer to at least a portion of any public interconnected electronic network which interchanges data by packet-switching.

Access system 20 additionally comprises a mechanical lock 34 for locking and unlocking a structure 40 (partially shown). In the illustrated embodiment, a user gains access to the structure 40 via door 32. In the illustrative embodiment, 20 mechanical lock 34 is a mechanical door lock, which includes a locking mechanism similar to a common entry or exterior lock, but is further capable of self-unlocking in response to an electronic signal, in addition to other functionality described herein. For purposes of non-limiting example, mechanical lock 34 may include a cam lock, rotary latch, electro-mechanical lock, magnetic lock, or the like. According to the preferred form, lock 34 unlocks in response to an electrical 25 signal sent from a wireless token 24 and/or access node 50. In one form, the electrical signal is sent wirelessly, such as over a low-power RF connection, such as a Zigbee® connection. In a further preferred form, the lock 34 returns to a locked state following the passage of a predetermined time period or a user 30 opening and closing the door following the receipt of an unlock signal. In some additional forms, lock 34 or door 40 may also include a mechanical key slot, key card, or other entry permitting authentication means 36 in addition to, or as backup for, that described herein with respect to lock 34. In addition, it shall be

appreciated that system 20 may be applied to access restrictions other than locks including, for example, an elevator control system providing limited access, a garage door, or others access barriers, as described later.

Access system 20 also utilizes at least one access node 50 to interface with 5 wireless token 24 and lock 34. Access node 50, as illustrated, is a wireless node implementing a common short-range wireless standard, such as Bluetooth® or ZigBee®, to those implemented by wireless token 24 and lock 34. Access node 50 is also connected to server 60 via firewall 52 and network 54.

In the illustrative form, access system 20 includes a plurality of access 10 nodes, such as access node 50, where each node is strategically positioned near a specified structure (i.e. a hotel room). The access nodes are preferably always in a active mode so that wireless tokens 24 may be connected with them on demand in the event the wireless token 24 is authorized, such as by having an authorized MAC address or some other selected security mechanism. In a further form, the 15 access nodes 50 are not in a discoverable mode and the pairing of the access nodes 50 with wireless token 24 occurs prior to the user's arrival programmatically. Illustratively, in some embodiments, access node 50 is operatively connected to server 60 to process and authenticate electronic unlock requests from wireless tokens 24. Firewall 52 includes at least a hardware or software implemented 20 firewall or other selected security features to prevent external access to server 60 or access node 50.

The location information maintained by access node 50 is linked to the present/assigned location of the node and is used in processing any unlock request. For example, an access node on the fourth floor of a hotel in downtown Chicago 25 may be assigned a unique hotel identifier coupled with a hotel zone identifier. Alternatively, the node may be assigned a single identifier which is then linked to its location by the wireless token 24 or server 60. For purposes of illustrating the hierarchical relationship between access nodes 50 and the structures which fall within their range, a mock floor plan is shown in FIG 3. The mock floor plan 30 illustrates a number of complete circles which denote the wireless range of a number of access nodes 50 for purposes of covering the entryway/hallway of a hotel floor and one or more doors.

According to the illustrated embodiment, server 60 operates in conjunction with access node 50 over internal network 54 to authenticate any wireless token 24 which comes within its range. In one form, when a wireless token 24 comes within range of an access node 50, the access node 50 receives information from the 5 wireless token 24 and seeks to identify one or more structures within its coverage area to which the wireless token 24 is authorized to enter. The server 60 serves to authenticate the request or a portion thereof using a reservations and occupancy database, while in other forms, the access node 50 may perform at least a portion of the authentication. In the illustrative embodiment, server 60 processes each 10 request corresponding to an authentication request received by access node 50 from wireless token 24, and upon proper authentication, confirms the authentication for one or more structures to access node 50 which then transmits an electronic signal to the corresponding lock(s), such as lock 34, notifying the lock to wake-up for a predetermined period of time in order to communication with nearby 15 authorized wireless token 24. In a further form, the access node 50 not only notifies lock 34 that it should wake-up, but also communicates information to lock 34 regarding which wireless token 24 it should be expecting.

While server 60 is described and illustrated as being a server, it should be understood that server 60 may be any computer, including a client server 20 arrangement. Server 60 may interface with access node 50 by either a wireless or hardwired interconnection. Preferably, the connection is a secured connection. A non-limiting example list of potential interfaces includes IR, optical, RF, serial port, IP network, and USB. Additionally, the functions of server 60 and access node 50 may be integrated into one computer system.

Once access node 50 as authenticated wireless token 24 and woken-up a selected lock 34, the process proceeds to a second level authentication between the wireless token 24 and lock 34. In the illustrated embodiment, wireless token 24 connects to lock 34 and provides authorization information. In one form, the authorization information provided may be the same as the authorization 25 information provided by wireless token 24 to access node 50, described above. Alternatively, in another form, the authorization information provided by wireless node 24 may be unlock information provided to wireless node 24 by access node 50 earlier in the process. Furthermore, in this form as well as other, upon receiving

the authorization information from wireless token 24, lock 34 may communicate with access node 50 to confirm the authorization or wireless token 24. In the event the authorization information received by lock 34 is authorized, by whatever means selected, lock 34 determines that a legitimate unlock request is present.

5 Additionally, either prior to or simultaneous with, lock 34 assesses the location of wireless token 24 to determine whether it is within a designated area. For making this determination, lock 34 includes two directional antennas 38 and 39 which are operable to communicate with wireless token 24 over a low power wireless transmission protocol. As illustrated in FIG. 1, according to the illustrated 10 form, lock 34 and antennas 38 and 39 are located within the mortise of door 32. According to the described form, antenna 38 faces outward from door 32 and structure 40 while antenna 39 faces inward from door 32 and into structure 40. These antennas enable lock 34 to determine an approximate location of wireless token 24 with respect to door 32 (i.e. inside or outside of structure 40) based upon 15 a received signal strength indication (RSSI) determined by each of directional antennas 38 and 39. Furthermore, lock 34 can confirm that the requesting user device is within a designated area, such as an 2 foot semi-circular area on the outside of a door, based upon the signal strength received as well as the differential of the signal strength between the two opposite facing directional antennas. Such a 20 confirmation ensures that access to a structure won't ever be improperly granted based upon a user device within the structure. For example, the mock floor plan shown in FIG. 3 illustrates a number of desired areas as small half circles outside of hotel room doors, which area the effective coverage areas for the required signal strength to be detected by antenna 38 with respect to wireless token 24. It is only 25 when a wireless token 24 is within these areas that their respective doors may be opened if authorized. Furthermore, a number of larger half circles in the interior of the hotel rooms show the field of coverage of antennas 39 which are used to detect when wireless token is within the corresponding hotel room.

Only after the authentication information received from wireless token 24 30 is verified and the location of wireless token 24 has been determined to be in the designated area will lock 34 unlock to permit the user access to the structure.

In still other embodiments, lock 34 is operably coupled to an override switch (not shown) having an access disable state. Asserting the override switch

prevents the access system 20 from permitting access to corresponding structure 40. As one non-limiting example, the override switch may be asserted when a guest engages a deadbolt or bar latch within their hotel room. In some embodiments of the access system 20, the override switch is incorporated into an 5 electronic control, not shown here, accessible to the user within structure 40.

A flowchart illustrating one set of steps performed in configuring a wireless token 24 for use in accessing a structure 40 according to one embodiment of the present invention is shown in FIG. 2. The process involves a wireless token 24 and the various other components of access system 20. The following description is 10 with continuing reference to access system 20 of FIG. 1. As shown in FIG. 1, the wireless token 24 may be a dedicated wireless token or another device, such as a mobile telephone, laptop, tablet, or other portable electronic device; however, it is understood that numerous other networked appliances are also intended.

It shall be appreciated that initial reservation, check-in, and configuration 15 information must be populated within server 60 to enable to access methods described herein to be performed. For example, confirmation information stored by server 60 preferably identifies the hotel and the user and includes a check-in/check-out date along with details of the type of room requested/reserved. In the preferred form, this confirmation information is received by server 60 as a result of 20 a hotel booking being made for a user either online, in person, or over the phone.

Upon checking into the hotel, or being authorized to access some other structure in other adaptations of the system 20, the wireless token 24 is automatically configured to pair with or otherwise connect to access nodes located 25 near the structure 40. Additionally, the details of the assigned room or structure, including its number and location, are then stored by server 60 in association with wireless token 24. This ensures that access nodes 50 will properly identify the room wireless token 24 is assigned to access and be able to authenticate its request for access. It shall be appreciated that this process may be modified to accommodate more than one authorized hotel guest per room, such as having two wireless 30 devices authorized to enter the same hotel room, or allowing a current guest to authorize the wireless device of another to access the hotel room for any portion of their remaining stay.

In continuing the description of the embodiment described with respect to FIG. 2, a flowchart illustrating one set of steps performed in allowing a user to access structure 40 using wireless token 24 and the various other components of access system 20 is shown. The following description is with continuing reference 5 to access system 20 of FIG. 1

As shown in FIG. 2, the process begins at start point 200 with the user along with the wireless token 24 arriving in a location within range of an access node 50. In step 202 or 204, a user device, such as either a mobile telephone or wireless token 24, are detected by the access node 50 respectively. Upon detecting 10 the user device, the access node determines whether or not the user is authorized to enter one of the structure entrances that is proximate to access node 50 (step 206). If the user is not authorized, the process ends at point 208. If the user is authorized, the user device connects to the access node 50 (step 210). Next, in order to ensure that the user is on the proper floor, the access node 50 compares its 15 perceived signal strength from the nearest access nodes of the floor above and below (if available) to ensure that its signal is the strongest (step 212). If the user is determined to be on another floor, the process proceeds to and ends at step 214. Alternatively, if the access node 50 determines that the user is on its associated floor, the process proceeds to step 216. In step 216 the access node 50 collaborates 20 with server 60 to confirm the credentials provided by the user device. In the event the credentials are not confirmed, the process ends at step 218. If the credentials of the user device are confirmed, the process proceeds to step 220 where access node 50 sends a wake-up signal to the lock, such as lock 34, associated with the structure, such as structure 40, to which the user is authorized. Additionally, the 25 access node 50 may detect the type of wireless standard the user device is capable of such that the proper wireless standard may be activated by the selected door lock 34 in step 220. The wake-up signal may also include an access code, such as a temporary alphanumeric code or the like, which must be matched by the user device in order to cause the lock to open.

30 The second stage of the process begins in step 226 where the user device connects to the now active lock 34. The dual antennas 38 and 39 of lock 34 detect a RSSI from the user device (step 228). In the preferred form, the central focus of the antennas 38 and 39 are directly opposite of one another. However, in an

alternate form, the central focus of the antennas 38 and 39 may only be offset by at least 130 degrees. In yet another form, the central focus may differ by 150 degrees or more. If the user device is determined to be inside of the structure, such as by having a stronger signal strength via the internally facing antenna 39, the process

5 proceeds through steps 232, and 234, whereby it is determined that the user is already in the room and the process ends subject to starting over. Alternatively, if is determined to be outside of the structure, such as by having a stronger signal strength via the externally facing antenna 38 or a suitable ration, and at least a certain signal strength to indicate the desired proximity to lock 34 (step 236), the

10 process proceeds to authenticate the request by comparing the security code provided by the user device to the stored access code received from node 50 (step 238) until lock 34 unlocks either provides the user with access to structure 40 (step 240) upon a successful authentication or the process ends at point 242.

In a further form, door lock 34 takes appropriate samples of RSSI relative

15 to wireless token 24 on either side of door, using antennas 38 and 39. For example, the samples may include several periodic RSSI readings which are then averaged or otherwise combine to reduce interference, noise, or the like from a single reading. Based upon these readings, lock 34 makes a determination of whether wireless token 24 is inside and outside of door 32. Additionally, the lock

20 34 may use the RSSI samples of antenna 38 to determine the distance wireless token 24 is from lock 34 for purposes of determining its presence within the defined proximity range outside of the door 32 as well. Once measurements averages are conducted, and presence of token/device and it is determined that he is in the proper unlock zone (range of outside proximity), the unlock of step 242 is

25 granted.

In yet another form, lock 34 may periodically transmit information to access node 50 for passing along to server 60 which indicates the user is still in the hotel room. This information may trigger the in-room temperature to be maintained, and upon detecting that the user is no longer in the room, the

30 temperature may be raised to a user-specified or standard level or it may trigger the lights to be turned off, as described in U.S. Patent Application 10/126,486 to Sunyich entitled "Personalized Smart Room", which is hereby incorporated by reference to the extent not inconsistent.

While the invention has been illustrated and described in detail in the drawings and foregoing description with respect to a hotel access system, the same is to be considered as illustrative and not restrictive in character, it being understood that only the preferred embodiment has been shown and described and

5 that all equivalents, changes, and modifications that come within the spirit of the inventions as described herein and/or by the following claims are desired to be protected. By way of non-limiting example, the system described herein may be applied to other enclosed areas where selective access is desired, including, other structures such as offices, amusement parks, military bases, restricted areas,

10 vehicles, homes, etc.

What is claimed is:

1. An access system allowing a user to access an enclosed area using a wireless user device, the access system comprising:
 - a database storing access permissions identifying at least one wireless user device authorized to access said enclosed area;
 - a mechanical locking device securing a point of entry to said enclosed area, said locking device operably connected to at least one short-range wireless receiver suitable for receiving an unlock request from said wireless user device and subsequently responding by granting access through said point of entry when said unlock request is authorized using said database,
 - wherein said at least one short-range wireless receiver includes a first and second directional antenna which are mounted to said point of entry and oriented such that the centers of their fields of reception are offset by an angle of at least 130 degrees, and
- 15 wherein said authorizing requires a comparison of the received signal strength indicator of said first directional antenna to that of said second directional antenna.
2. The access system according to claim 1, wherein said at least one short-range wireless radio is a Bluetooth radio.
- 20 3. The access system according to claim 1, wherein the centers of the fields of reception of said first and said second directional antennas are offset by an angle of at least 150 degrees.
4. The access system according to claim 1, wherein said at least one short-range wireless radio is an 802.11 radio.
- 25 5. The access system according to claim 1, wherein said enclosed area is a structure and said point of entry is a door.
6. The access system according to claim 5, wherein said mechanical locking device is located in the mortise of said door.
7. The access system according to claim 5, wherein at least one of said first and said second directional antennas is located in the mortise of said door.
- 30 8. The access system according to claim 5, wherein said structure is a hotel room.

9. The access system according to claim 1, wherein said wireless user device is a mobile telephone.

10. The access system according to claim 2, wherein said wireless user device is a mobile telephone.

5 11. An method for granting access to an enclosed area based on a wireless user device, the method comprising the steps of:

maintaining a database storing access permissions identifying at least one wireless user device authorized to access one or more enclosed areas;

10 receiving a first unlock request for an identified enclosed area at an access node from a wireless user device, wherein at least one point of entry of said enclosed area is within the transmission range of said access node;

authenticating at least a portion of said unlock request using a said database;

15 transmitting a wake-up request and an access code from said access node to a short range wireless radio connected to said mechanical locking device securing a point of entry to said identified enclosed area;

receiving a second unlock request at said short range wireless radio from a wireless user device, wherein said second unlock request includes a security code; and

20 unlocking said mechanical lock device to provide access to said enclosed area in the event said security access code matches said access code.

12. The access system according to claim 12, further comprising the steps of :

determining a received signal strength indicator for said wireless user device for each of a first and second directional antenna positioned near said point of entry, wherein the centers of the fields of reception of said first and said second directional antennas are offset by an angle of at least 130 degrees; and

wherein said unlocking requires that the ratio of said first and said second received signal strength indicators indicates that said wireless user device is outside of said enclosed area.

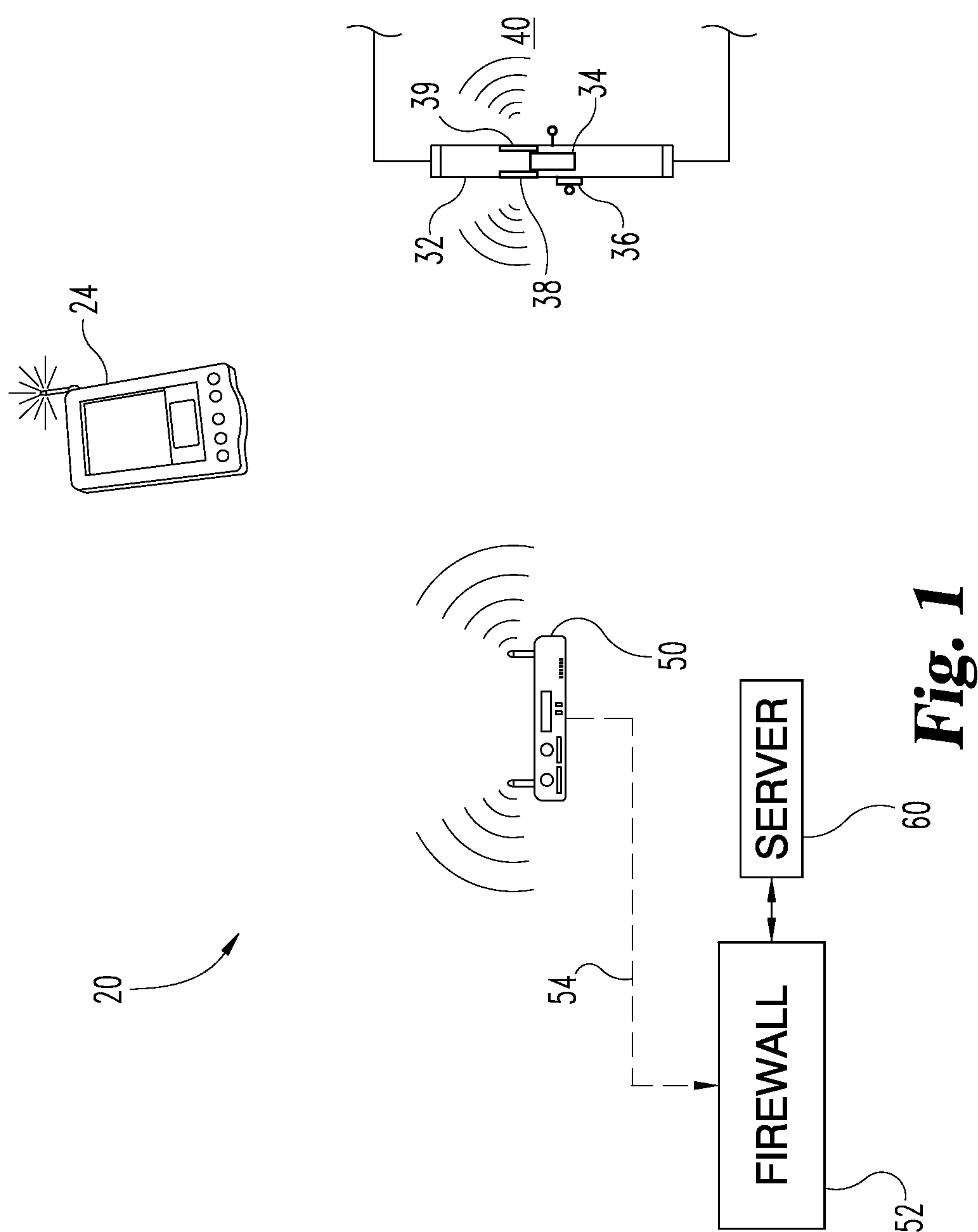
30 13. The access system according to claim 12, wherein said at least one short-range wireless radio is a Bluetooth radio.

14. The access system according to claim 12, wherein said at least one short-range wireless radio is a 915 MHz radio.

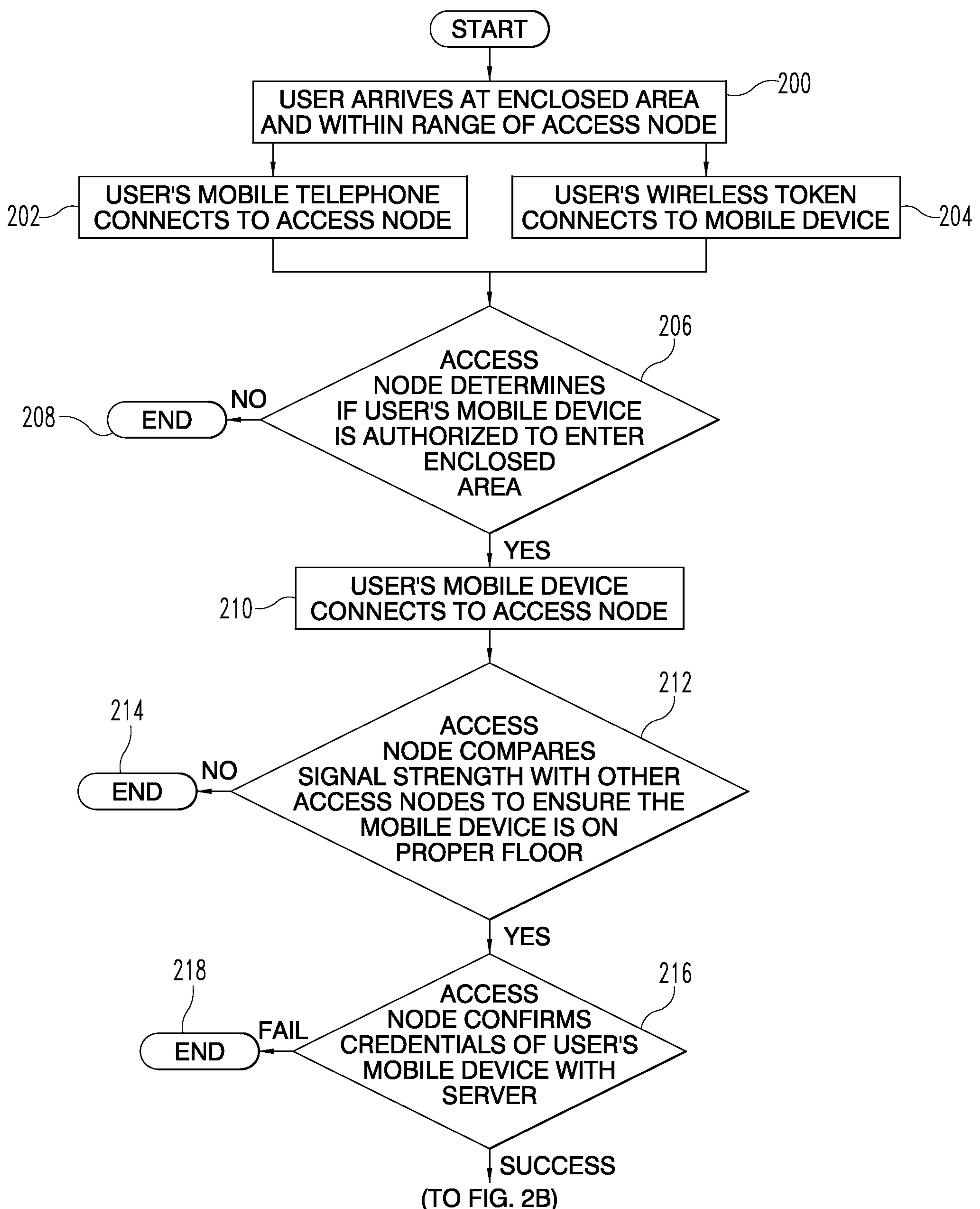
15. The access system according to claim 12, wherein said at least one short-range wireless radio is an 802.11 radio.
16. The access system according to claim 12, wherein the centers of the fields of reception of said first and said second directional antennas are offset by an angle of at least 150 degrees.
17. The access system according to claim 12, wherein said enclosed area is a structure and said point of entry is a door.
18. The access system according to claim 17, wherein said mechanical locking device is located in the mortise of said door.
- 10 19. The access system according to claim 18, wherein at least one of said first and said second directional antennas is located in the mortise of said door.
20. The access system according to claim 12, wherein said wireless user device is a mobile telephone.
- 15 21. An access system allowing a user to access a structure using a wireless user device, the access system comprising:
 - a database storing access permissions identifying at least one wireless user device authorized to access said structure and one access node authorized to permit access to said structure;
 - 20 a mechanical locking device securing a door of said structure, said locking device having at least one short-range wireless receiver suitable for receiving and authenticating an unlock command for a predetermined time after the receipt of a wireless wake-up command and responding to a properly authenticated unlock command by unlocking said door;
 - 25 wherein said at least one short-range wireless receiver includes a first and second directional antenna which are mounted to said door and oriented such that the centers of their fields of reception are offset by an angle of at least 130 degrees, and
 - 30 wherein said authorizing requires a comparison of the received signal strength indicator of said first directional antenna to that of said second directional antenna; and
 - an access node positioned near said structure comprising:
 - a first short-range wireless radio for receiving a wireless access request directly from a wireless user device; and

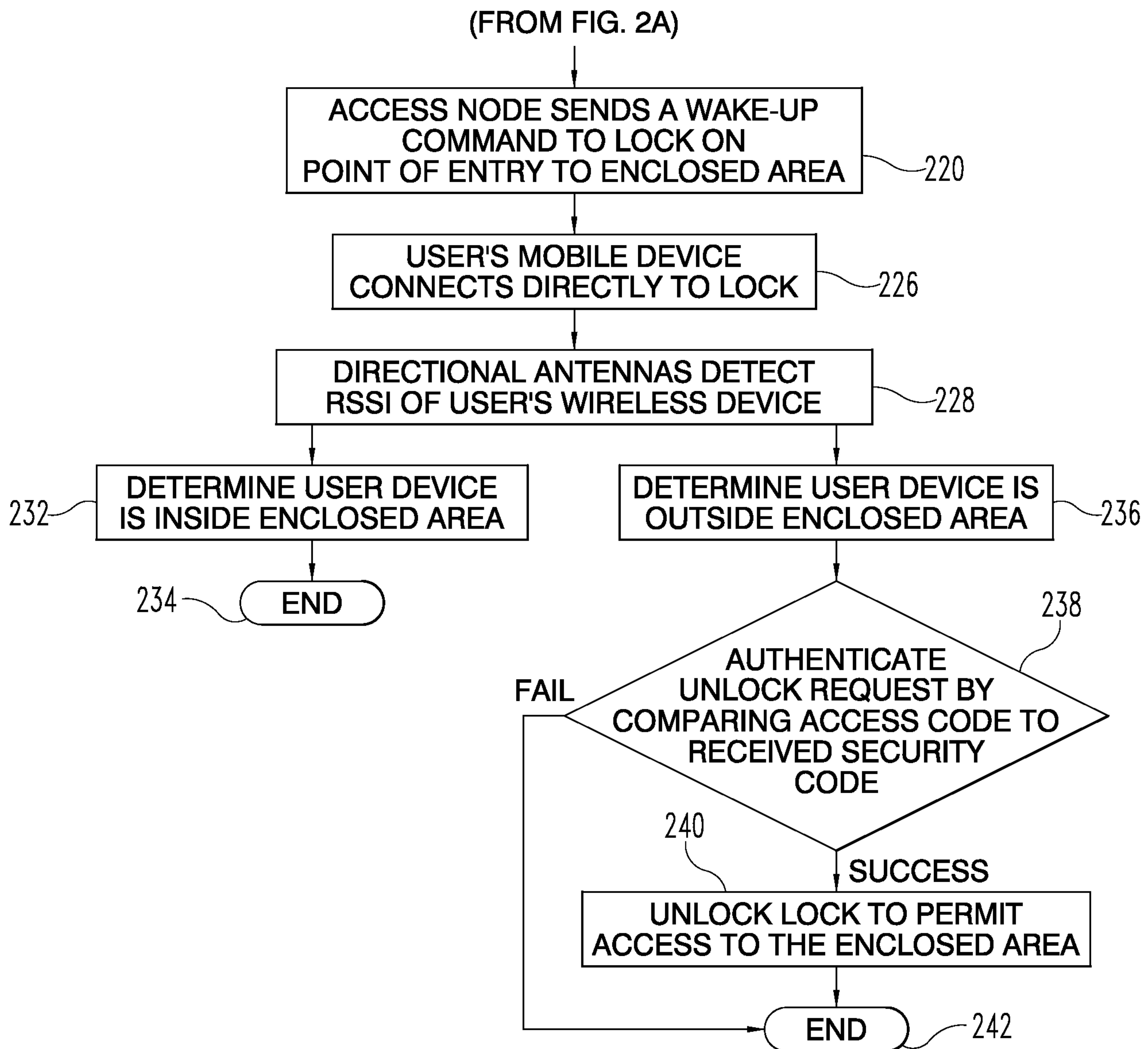
a second short-range wireless radio for transmitting a wake-up command to said mechanical locking device in response to receiving an authorized request.

1/4



2/4

**Fig. 2A**

**Fig. 2B**

4/4

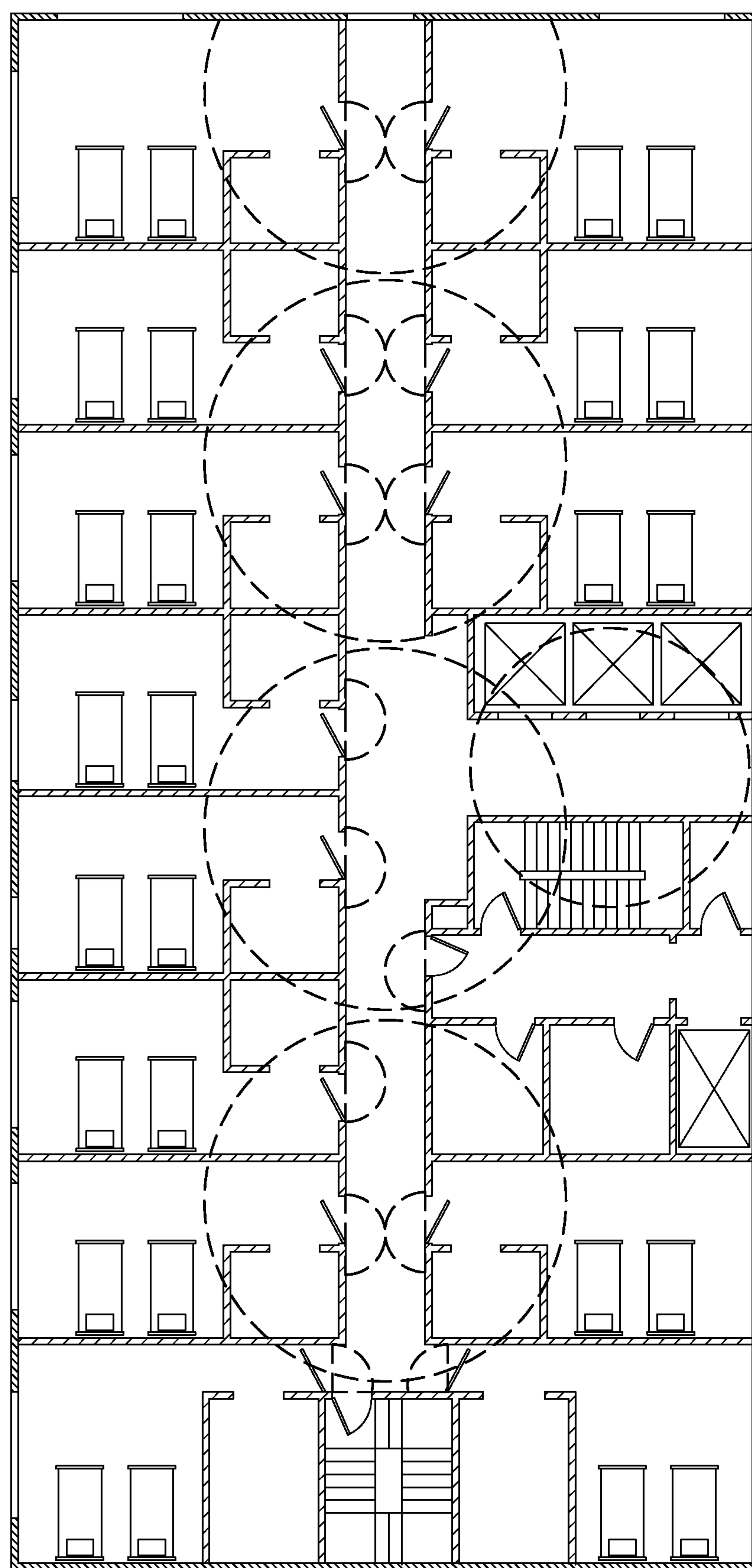


Fig. 3

