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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 May 2009 (28.05.2009)

PCT

(10) International Publication Number
WO 2009/066324 A2

(51) International Patent Classification:
G08B 25/10 (2006.01)

(21) International Application Number: PCT/IN2008/000693

(22) International Filing Date: 20 October 2008 (20.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2679/CHE/2007 19 November 2007 (19.11.2007) IN

(71) Applicant *(for all designated States except US)*: **SERIAL INNOVATIONS INDIA PRIVATE LIMITED** [IN/IN]; #38, II Floor, K.H. Circle, Hosur Road, Bangalore 560 027, Karnataka (IN).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **DATTATRAYA, Chandrakant, Bathe** [IN/IN]; Flat No. 211, B Block, Himagiri Enclave, Khagadaspura C.V. Raman Nagar, Bangalre 560 093, Karnataka (IN). **SUNAY, Narkar** [IN/IN]; 305, Gauray Arcade-1, 1st Main, Manorayanplaya, Bangalore, Karnataka (IN). **ANIL, Kumar, Ram, Rakhyani** [IN/IN]; 424/1, Shastri Nagar, Kanpur 208 012, Uttra Pradesh (IN). **ANURADHA, Raju** [IN/IN]; A3, Lakshmi Nivas, #22, Souuth Street, Radha Nagar, Chromepet, Chennai 600 044, Tamil Nadu (IN).

(74) Agent: ARUNACHALAM, Appaji, Mohan; Mohan Associates, D-4, IIIRD Floor, Ceebros Building, New N°.32.(OLD N°11), Cenetoph Road, Teynampet, Chennai 600 018 Tamil Nadu (IN).

(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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *of inventorship (Rule 4.17(iv))*

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: POWER SAVING SECURITY SYSTEM BASED ON PROGRAMMABLE RANGE

(57) Abstract: A method and system for managing power consumption of devices that undergo extended periods of inactivity while the user is away from such a device. The system is also capable of identifying an authentic user and responds to the arrival and departure of only authentic users. The system, by incorporating means for the authentication of users as they enter the proximity of the device, secures the device against access by unauthentic users. The system comprises of a sensor, at least one sensing device and a power options controller.

WO 2009/066324 A2

TITLE: POWER SAVING SECURITY SYSTEM BASED ON PROGRAMMABLE RANGE

FIELD OF THE INVENTION

The present invention relates generally to a system for controlling power consumption of a device. More specifically it relates to a system for enabling a device to save power based on the proximity of an authentic user and securing the device against unauthentic access.

BACKGROUND

Electrical and electronic devices and systems such as computers, computer monitors, fans, air-conditioners, lighting equipment, televisions, motors, machines and the like are used only when a user is present in the proximity of such devices. The devices may remain switched ON even when the user has stopped using them or when the user has temporarily gone away from the device. Since such devices are used extensively and are high on power consumption, it is imperative that they be switched OFF while the user is away. For example, 17" CRT and the LCD monitors consume power in the range of 35 and 60 watts. Leaving the computer or the computer monitor turned ON during periods of inactivity can, therefore, be a source of considerable power wastage.

Conventionally, the problem is approached by advising each user to turn OFF the computer monitor when not using it. The major disadvantage of this approach is that it requires user intervention in the form of the user pressing the power button on the monitor's operating panel. It is unreasonable to expect the user to remember to turn OFF the monitor every time he/she steps away from the computer. Further, in the user's absence, the monitor can be turned ON by anyone. This approach, therefore, requires user intervention to turn the monitor ON and further does not prevent access by unauthentic users.

Another approach to conserve power is to make use of power-saving schemes present in many modern computers. One such scheme allows the user to set a predetermined time after which the monitor will automatically be turned OFF while not in use. Although such an approach does not require user intervention to turn the monitor OFF, it still suffers from many shortcomings. First, the monitor shuts down only after the predetermined time which might be much longer than the time the user left the PC unattended. Second, the monitor can be turned ON by anyone in the user's absence; and third, turning the monitor ON requires user intervention, for example, in the form of a key being pressed or a mouse being moved.

Such power-saving schemes further allow the user to set the time after which the computer system will automatically go into standby or hibernation mode while not in use. Since the user can set a password requirement for logging into a system returning from standby, the monitor can be secured against unauthentic users. The major shortcoming of this approach, however, is that user intervention is still required to turn the computer on. Moreover, the user is required to wait while the system transitions to its active state.

U.S. Patent number 5396443, titled "Information processing apparatus including arrangements for activation to and deactivation from a power-saving state" discloses an apparatus which may be used to automatically switch OFF a device such as a computer monitor based on the presence of a user in the proximity of the device. When the apparatus determines that the user has left the proximity of the device, it switches OFF the device. Similarly, on determining that the user has returned to the proximity of the device, the apparatus switches the device on. However, the apparatus does not have the capability of authenticating users. As a consequence, it may switch the device ON even when an unauthentic user comes close to the device.

The existing solutions for optimizing power consumption of devices such as computer monitors, fans, air conditioners, and the like suffer from limitations. Some solutions require user intervention to switch the device ON and OFF, while others do not provide the desirable level of security for the device in the user's absence. There is a need, therefore, for a system that overcomes all of the above mentioned limitations by fully automating the process of controlling power consumption and securing the device against unauthentic access in the absence of authentic users.

SUMMARY OF THE INVENTION

A system and a method used to control the power options of a device have been disclosed. The system controls the power options of the device based on the proximity of an authentic user to the device and secures the device against unauthentic access in the absence of authentic users.

The usage of the device requires at least one authentic user in the proximity of the device. The device undergoes extended periods of inactivity while no authentic user is present in the proximity of the device. According to an embodiment of the invention, the system of the invention hereinafter referred to as the Watt saver sensor (WSS) system switches ON the device only when an authentic user is near the device and switches OFF the device when no authentic user is near the device. The WSS system is capable of distinguishing authentic users from unauthentic users such that the device is turned ON only when an authentic user comes near the device.

The WSS system can be based on any wireless technology including, Radio frequency Identification (RFID) technology, Ultra wide band RF, Bluetooth, infrared, WiFi, ultrasound, GPS, GPRS, wireless ethernet or a combination thereof. The WSS system comprises a power options controller, a sensory detector associated with the device, and a plurality of slave units associated with the users of the device. The sensory detector is capable of detecting the slave units based on the distance of the slave units from the sensory detector. The sensory detector incorporates a slave unit authenticator capable of authenticating slave units as they enter the proximity of the device. According to an embodiment of the invention, the sensory detector informs the power options controller when a first authentic slave unit enters the proximity of the device. Accordingly, the power options controller switches the device ON. The sensory detector also informs the power options controller when the last authentic slave unit leaves the proximity of the device. Accordingly, the power options controller switches the device OFF. Further, the WSS system provides for the association of new slave units in addition to the existing slave units.

For the purpose of explanation, the case where the WSS system is based on RFID technology has been described in detail in the detailed description of the drawings. The sensory detector is hereinafter referred to as the RFID detector and the slave units are hereinafter referred to as RFID slave units.

The RFID link between the RFID detector and the RFID slave units may be implemented to be: (a) full duplex active, (b) simplex and (c) full duplex passive. The WSS system prescribes different protocols for each of these cases. For example, the WSS system-Full Duplex Active (WSS-FDA) protocol prescribes the various modes the WSS system can be in, the conditions for transitioning from one mode to another, and the procedures for associating new slave units with an existing WSS system.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram showing the associations between the WSS system, the user, and the device;

FIG. 2 is the block diagram of an exemplary embodiment of the WSS system;

FIG. 3 is a flow diagram illustrating the transitions from Wake Up mode to other modes prescribed under the WSS-FDA protocol for the RFID detector;

FIG. 4 is a flow diagram illustrating the transitions between the three modes prescribed under the WSS-FDA protocol for the RFID slave units;

FIG. 5 is a flow diagram illustrating the details of the Wake Up mode for the RFID detector under the WSS-FDA protocol;

FIG. 6 is a flow diagram illustrating the details of the Wake Up mode for RFID slave units under the WSS-FDA protocol;

FIG. 7 is a flow diagram illustrating the details of the Within Range mode for the RFID detector under the WSS-FDA protocol;

FIG. 8 is a flow diagram illustrating the details of the Within Range mode for RFID slave units under the WSS-FDA protocol;

FIG. 9 is a flow diagram illustrating the details of the Out Of Range mode for the RFID detector under the WSS-FDA protocol;

FIG. 10 is a flow diagram illustrating the details of the Out Of Range mode for RFID slave units under the WSS-FDA protocol;

FIG. 11 is a flow diagram illustrating the details of the Association Phase for the RFID detector under the WSS-FDA protocol;

FIG. 12 is a flow diagram illustrating the details of the Association Phase for RFID slave units under the WSS-FDA protocol;

FIG. 13 is a flow diagram illustrating the transitions between the two modes prescribed under the WSS-SA protocol for the RFID detector on turning the PC on;

FIG. 14 is a flow diagram illustrating the transitions between the two states prescribed under the WSS-SA protocol for the RFID detector;

FIG. 15 is a flow diagram illustrating the details of the Within Range mode for the RFID detector under the WSS-SA protocol;

FIG. 16 is a flow diagram illustrating the details of the Out Of range mode for the RFID detector under the WSS-SA protocol;

FIG. 17 is a diagram illustrating the details of the PRESENT packet prescribed under the WSS-SA protocol;

FIG. 18 is a flow diagram illustrating the details of the Association Phase for RFID detector under the WSS-SA protocol;

FIG. 19 is a flow diagram illustrating the transitions from Wake Up mode to other modes prescribed under the WSS-FDP protocol for the RFID detector;

FIG. 20 is a flow diagram illustrating the transitions between the two states prescribed under the WSS-FDP protocol for RFID slave units;

FIG. 21 is a flow diagram illustrating the details of the Wake Up mode for the RFID detector under the WSS-FDP protocol;

FIG. 22 is a flow diagram illustrating the details of the Within Range mode for the RFID detector under the WSS-FDP protocol;

FIG. 23 is a flow diagram illustrating the details of the Out Of Range mode for the RFID detector under the WSS-FDP protocol; and

FIG. 24 is a flow diagram illustrating the details of the Association Phase for the RFID detector under the WSS-FDP protocol.

DETAILED DESCRIPTION

The detailed description set forth below in connection with the appended drawings is intended as a description of exemplary embodiments and is not intended to represent the only forms in which the exemplary embodiments may be constructed and/or utilized. The description sets forth the functions and the sequence of steps for constructing and operating the exemplary embodiments in connection with the illustrated embodiments. However, it is to be understood that the same or equivalent functions and sequences may be accomplished by different embodiments that are also intended to be encompassed within the spirit and scope of the invention.

FIG. 1 is a schematic diagram showing the associations between a device 102, a WSS system 104, and a user 106 according to an embodiment of the invention. A device 102 consumes power and WSS system 104 is used to manage the power consumption of device 102 as well as for security of device 102 such that only a user 106 authenticated to use device 102 is given access to device 102.

The usage of device 102 requires the presence of a user 106 in device 102's proximity. Device 102 typically undergoes extended periods of inactivity while user 106 is away from device 102's proximity. For example, device 102 may be a computer, a computer server, a computer monitor, a television, a fan, an air conditioner, lighting equipment or the like. According to an embodiment of the invention, WSS system 104 switches device 102 OFF when user 106 leaves the proximity of device 102. Likewise, WSS system 104 switches device 102 ON when user 106 returns to the proximity of device 102. Furthermore, WSS system 104 responds to the arrival and departure of user 106 only if user 106 is authenticated to use device 102. Moreover WSS system 104 can be designed to authenticate a plurality of users 106 to use device 102. WSS system 104 has been described in detail in conjunction with FIG. 2.

FIG. 2 is a block diagram illustrating WSS system 104 in accordance with an embodiment of the invention.

WSS system 104 comprises of components associated with device 102 and components associated with user 106. According to an embodiment of the invention, the communication between the two sets of components is based on Radio Frequency Identification (RFID) technology. However the communication between the two sets of components is not limited to only RFID technology and can also be based on other wireless technologies like Bluetooth, infrared, WiFi, ultrasound, GPS, GPRS, wireless Ethernet or a combination thereof.

The components associated with device 102 include a power options controller 202, an RFID detector 204, and a slave unit authenticator 208. According to an embodiment of the invention, the components associated with device 102 are located inside or around device 102. For example, if device 102 is a computer system, RFID detector 204 may be connected to the computer system using a USB port, a power line, fire-wire, PCI connector, RS232 cable, RS485 port, RS422 port, PCI express connector, PCMCI, camera link, optic fiber, SPI link, I2C link, CAN connector, parallel port, serial port, VGA port, LVDS, HEART devices, 4-20mA, Ethernet (10baseT, 100baseT, 10GbaseT), SCSI, EISA, GPIB, ISA, Audio port, SATA. ATA or any other wired digital or analog communication.

The components associated with user 106 include at least one RFID slave unit 206. According to an embodiment of the invention, each RFID slave unit 206 is associated with one user 106. For example, RFID slave unit 206 may be in the form of a name-tag, a wrist-band, and the like which the user may wear, carry, etc. Further, RFID slave unit 206 may be powered by a battery, solar power, mechanical energy, electromagnetic induction, capacitive energy, gravitational energy, thermal energy or a combination thereof.

A region of pre-specified radius, centering on device 102 is defined as the proximity of device 102. Full duplex active RFID link and simplex RFID link can provide a programmable range of radius 0-200 meters based on the frequency used and the programmed output power. According to an embodiment of the invention, the pre-specified radius is programmed in the range of 0 to 10 meters. Any RFID slave unit 206 within the region of pre-specified radius centering on device 102 is hereinafter referred as being within the proximity of device 102. Further, any RFID slave unit 206 leaving the region is hereinafter referred to as departing from the proximity of device 102. Similarly, any RFID slave unit 206 entering the region is hereinafter referred to as entering the proximity of device 102.

According to an embodiment of the invention, RFID detector 204 receives a radio frequency (RF) packet from RFID slave unit 206 only if RFID slave unit 206 is within the proximity of device 102. Based on the reception of the RF packet from RFID slave unit 206, RFID detector can determine if RFID slave unit 206 has entered the proximity of device 102 or has departed from it.

According to an embodiment of the invention, power options controller 202 is a software component and manages the power options of device 102. For example, power options controller 202 is a software installed in a computer. Power options controller 202 can be integrated either with device 102 or with RFID detector 204. RFID detector 204 alerts power options controller 202 about the approach and departure of RFID slave unit 206 in the proximity of device 102. Based on the alerts received from RFID detector 204, power options controller 202 selects an appropriate power option for device 102. For example, power options controller 202 may switch OFF device 102 based on RFID slave unit 206 departing from the proximity of device 102. According to another embodiment of the invention, power options controller 202 is a hardware component and is placed between device 102 and the power supply to device 102. For example, power options controller 202 is a hardware component like a relay, semi-conductor switch etc. placed between an air-conditioner and the power supply to device 102. According to another embodiment of the invention, power options controller 202 is integrated within RFID detector 204 as a firmware module and sends commands to device 102 like a computer to switch ON or OFF.

According to an embodiment of the invention, WSS system 104 responds to the approach and departure of authentic RFID slave unit 206 only. Slave unit authenticator 208 authenticates RFID slave unit 206 present within the proximity of device 102. According to an embodiment of the invention, slave unit authenticator 208 is incorporated within power options controller 202. In an alternate embodiment, slave unit authenticator 208 is incorporated within RFID detector 204. Slave unit authenticator 208 authenticates RFID slave units 206 based on unique identifications assigned to RFID detector 204 and each of the plurality of RFID slave units 206. The unique identification assigned to RFID detector 206 is hereinafter referred to as Master ID MID. The unique identification assigned to RFID slave unit 206 is hereinafter referred to as Slave ID (SID). During the Association Phase described in detail in conjunction with FIG. 11 and FIG. 12, RFID detector 204 and RFID slave unit 206 exchange RDID and SID information. As an example of this scheme of authentication, RFID detector 204 may accept only the packets from RFID slave unit 206 which have the MID of RFID detector 204 as destination address and a known SID as source address.

According to another embodiment of the invention, WSS system 104 may be used to switch ON device 102 as soon as user 106, authenticated to use device 102 enters the office wherein device 102 lies. As such, RFID detector 204 is located at the entrance of the office in order to detect the arrival of user 106. Similarly, RFID detector 204 can also detect the departure of user 106 and based on the departure of user 106, switch OFF device 102. RFID detector 204 sends an alert to power options controller 202 through a network to switch device 102 ON or OFF based on the arrival or departure of user 106. According to an embodiment of the invention, a plurality of power options controllers 202 can receive alerts from RFID detector 204 through the network to control the power options of a plurality of devices 202. RFID detector 204 sends the alert to appropriate power option controller 202 controlling the power options of device 102, based on the arrival or departure of user 106 authenticated to use device 102.

According to another embodiment of the invention, WSS system 104 may be used to switch OFF device 102 upon detecting an unauthenticated user 106 in the proximity of device 102.

According to an embodiment of the invention, WSS system 104 may be designed to operate in the general case where a plurality of RFID slave units 206 are associated with device 102. RFID detector 204 can receive RF packets from a plurality of RFID slave units 206 simultaneously. As such, RFID detector 204 determines when a first of the plurality of RFID slave units 206 authenticated by slave unit authenticator 208 enters the proximity of device 102, and alerts power options controller 202 to select an appropriate power option, for example, to switch ON device 102. Similarly, RFID detector 204 determines when a last of the plurality of RFID slave units 206 authenticated by slave unit authenticator 208 leaves the proximity of device 102, and alerts power options controller 202 to select an appropriate power option, for example, to switch OFF device 102.

Device 102 may include, but is not limited to computes, computer monitors, televisions, fans, air conditioners, and the like. For the purpose of explanation, the case where device 102 is a personal computer (PC) is considered hereinafter. Device 102 is hereinafter referred to as PC. According to an embodiment of the invention, WSS system 104 may be deployed to automatically switch PC ON or OFF based on the presence of user 106 in the proximity of PC. According to another embodiment of the invention, WSS system 104 may be used to automatically switch the monitor of PC ON or OFF based on the presence of user 106 in the proximity of PC. For the purpose of explanation, the latter case wherein WSS system 104 is deployed to manage the power consumption of the monitor of PC is considered hereinafter.

Further, in the embodiments described below, power options controller 102 may conveniently be implemented as a software application. Power options controller 102 is hereinafter referred to as WSS application software and can be installed on PC or integrated with RFID detector 204.

FIG. 3 is a flow diagram illustrating the transitions of RFID detector 204 from Wake Up mode to other modes prescribed under the Watt Saver Sensor – Full Duplex Active (WSS-FDA) protocol according to an embodiment of the invention. WSS system 104 may be implemented using Full Duplex Active RFID technology wherein RFID detector 204 and RFID slave unit 206 communicate as per the WSS-FDA protocol. Under the WSS-FDA protocol, both RFID detector 204 and RFID slave unit 206 can transmit and receive radio frequency (RF) packets. Consequently, under this protocol, RFID detector 204 and RFID slave unit 206 can be in one of three states: transmit, receive, and idle. Further, the WSS-FDA protocol prescribes three modes of operation for WSS system 104: the Wake Up (WU) mode, the Within Range (WIR) mode, and the Out Of Range (OOR) mode. These modes cover all possible operating conditions of WSS system 104 under the WSS-FDA protocol. FIG. 3-10 illustrate the details of these modes while FIG. 11-12 describe the method prescribed for associating new slave units under the WSS-FDA protocol.

At step 302, PC is switched on. According to an embodiment of the invention, switching ON PC automatically boots up WSS application software. According to another embodiment of the invention, the WSS application software needs to be manually turned ON. Further, the monitor of PC is, by default, ON immediately after PC is switched ON. At step 304, RFID detector 204 is switched ON. When switched ON, RFID detector 204 enters the WU mode at step 306. At step 308, RFID detector 204 enquires for RFID slave unit 206 as per the WSS-FDA protocol. At step 310, RFID detector determines if any RFID slave unit 206 authenticated by slave unit authenticator 208 is present in the proximity of PC.

If it is determined at step 310 that no RFID slave unit 206 authenticated by slave unit authenticator 208 is present in the proximity of PC, RFID detector 204 proceeds to step 312. At step 312, RFID detector enters the OOR mode. At step 314, RFID detector 204, while remaining in the OOR mode, sends an alert to WSS application software to switch the monitor of PC OFF. If it is determined at step 310 that at least one RFID slave unit 206 authenticated by slave unit authenticator 208 is present in the proximity of PC, RFID detector 204 proceeds to step 316. At step 316, RFID detector enters the WIR mode.

FIG. 4 is a flow diagram illustrating the transitions of RFID slave unit 206 between the modes prescribed under WSS-FDA protocol according to an embodiment of the invention.

At step 402, RFID slave unit 206 is switched ON. When switched ON, RFID slave unit 206 enters the WU mode at step 404. At step 406, while remaining in the WU mode, RFID slave unit 206 starts enquiring for packets from RFID detector 204. At step 408, RFID slave unit 206 determines if a valid packet is received from RFID detector 204. If it is determined as step 408 that no valid packet is received from RFID detector 204, RFID slave unit 206 proceeds to step 410. At step 410, RFID slave unit 206 enters the OOR mode.

After step 410, while remaining in the OOR mode, RFID slave unit 206 returns to step 406 and enquires for packets from RFID detector 204.

If it is determined as step 408 that a valid packet is received from RFID detector 204, RFID slave unit 206 proceeds to step 412. At step 412, RFID slave unit 206 enters the WIR mode. After step 412, while remaining in the WIR mode, RFID slave unit 206 returns to step 406 and enquires for packets from RFID detector 204.

FIG. 5 is a flow diagram illustrating the WU mode for RFID detector 204 under the WSS-FDA protocol according to an embodiment of the invention. Immediately after PC is switched ON, WSS application software causes RFID detector 204 to enter the WU mode.

At step 502, RFID detector 204 enters the WU mode. At step 504, RFID detector 204 enters the transmit state. At step 506, RFID detector 204 transmits a wake-up enquiry (WU_ENQ) packet of a pre-specified time period (MT1). At step 508, RFID detector 204 enters the receive state in which it waits for another pre-specified time period (MT2) period for a wake-up response (WU_RESP) packet from RFID slave unit 206. At step 510, RFID detector 204 determines if a WU_RESP packet is received within the MT2 time period.

If it is determined at step 510 that a WU_RESP packet is received within the MT2 time period, RFID detector 204 proceeds to step 512. At step 512, RFID detector 204 checks the received WU_RESP packet for validity. In case the WU_RESP packet is found to be invalid, RFID detector 204 proceeds to step 514. At step 514, RFID detector 204 increments the wake-up positive-response (WU_POS_RESP) counter by one. The WU_POS_RESP counter indicates the number of successful responses received by RFID detector 204 while in the WU mode, i.e. the number of WU_ENQ packets transmitted that resulted in a valid WU_RESP packet being received.

At step 516, RFID detector 204 determines if the WU_POS_RESP counter exceeds the WU_POS_RESP limit. The WU_POS_RESP limit is the minimum number of successful responses required by RFID detector 204 to transition from the WU mode to the WIR mode. If it is determined at step 516 that the WU_POS_RESP counter is greater than or equal to the WU_POS_RESP limit, RFID detector 204 proceeds to step 518. At step 518, RFID detector 204 enters the WIR mode.

If it is determined at step 516 that the WU_POS_RESP counter is less than the WU_POS_RESP limit, RFID detector 204 returns to step 504 and prepares to transmit further WU_ENQ packets.

If it is determined at step 510 that a WU_RESP packet is not received within the MT2 time period, RFID detector 206 proceeds to step 520. RFID detector 206 also proceeds to step 520 if it is determined at step 512 that the received WU_RESP packet is invalid. At step 520, RFID detector 204 increments the wake-up negative-response (WU_NEG_RESP) counter by one. The WU_NEG_RESP counter indicates the number of unsuccessful responses required by RFID detector 204 in the WU mode, i.e. the number of WU_ENQ packets transmitted that did not result in a valid WU_RESP packet being received. At step 522, RFID detector 204 determines if the WU_NEG_RESP counter exceeds the WU_NEG_RESP limit. The WU_NEG_RESP limit is the minimum number of unsuccessful responses required for RFID detector to transition from the WU mode to the OOR mode. If it is determined at step 522 that the WU_NEG_RESP counter is greater than or equal to the WU_NEG_RESP limit, then at step 524, RFID detector 204 enters the OOR mode. In case the WU_NEG_RESP counter is less than the WU_NEG_RESP limit, RFID detector returns to step 504 and prepares to transmit further WU_ENQ packets.

FIG. 6 is a flow diagram illustrating the WU mode for RFID slave unit 206 under the WSS-FDA protocol according to an embodiment of the invention. Immediately after RFID slave unit 206 is switched ON for the first time, it enters the WU mode. According to an embodiment of the invention, RFID slave unit 206 may not enter the WU mode again during its life cycle. Once in the WU mode, RFID slave unit 206 can transition to either the WIR mode or the OOR mode.

At step 602, RFID slave unit 206 is switched ON. At step 604, RFID slave unit 206 enters the WU mode. At step 606, RFID slave unit 206 enters the receive state and waits for a pre-specified time period (ST1) period for a WU_ENQ packet from RFID detector 204. At step 608, RFID slave unit 206 determines if a WU_ENQ packet is received within the ST1 time period.

If it is determined at step 608 that a WU_ENQ packet is received within the ST1 time period, RFID slave unit 206 proceeds to step 610. At step 610, RFID slave unit 206 checks the received WU_ENQ packet for validity. If it is determined at step 610 that the received WU_ENQ packet is valid, RFID slave unit 206 proceeds to step

612. At step 612, RFID slave unit 206 enters the transmit state. At step 614, RFID slave unit 206 transmits a WU_RESP packet of a pre-specified time period (ST2). At step 616, RFID slave unit 206 determines if the change of mode recommended by the WU_ENQ packet is valid. If at step 616, it is determined that the change of mode is valid, RFID slave unit 206 proceeds to step 618. At step 618, RFID slave unit 206 enters the WIR mode.

If at step 616, it is determined that the change of mode recommended by the WU_ENQ packet is invalid, RFID slave unit 206 returns to step 606 to wait for further WU_ENQ packets. If at step 610, it is determined that the received WU_ENQ packet is invalid, RFID slave unit 206 returns to step 606 to wait for further WU_ENQ packets. If at step 608, it is determined that no WU_ENQ packet is received within the ST1 time period, RFID slave unit 206 returns to step 606 to wait for WU_ENQ packets.

FIG. 7 is a flow diagram illustrating the WIR mode for RFID detector 204 prescribed under the WSS-FDP protocol according to an embodiment of the invention. RFID detector 204 enters the WIR mode on having ascertained the presence of at least one authenticated RFID slave unit 206 within the proximity of device 102.

At step 702, RFID detector 204 enters the WIR mode. At step 704, RFID detector informs WSS application software to switch ON the monitor of PC. If the monitor of PC is already not on, the WSS application software switches on the monitor of PC. At step 706, RFID detector 204 enters the transmit state. At step 708, RFID detector 204 transmits a within-range enquiry (WIR_ENQ) packet of a pre-specified time period (MT3). At step 710, RFID detector 204 enters the receive state in which it waits for another pre-specified time period (MT4) for a within-range response (WIR_RESP) packet from RFID slave unit 206. At step 712, RFID detector 204 determines if a WIR_RESP packet is received within the MT4 time period. If at step 712, it is determined that no WIR_RESP packet is received within the MT4 time period, RFID detector 204 proceeds to step 714. At step 714, RFID detector 204 increments the within-range negative-response (WIR_NEG_RESP) counter by one. The WIR_NEG_RESP counter indicates the number of unsuccessful enquiries made by RFID detector 204 while in the WIR mode, i.e. the number of WIR_ENQ packets transmitted that did not result in a valid WIR_RESP packet being received. At step 716, RFID detector 204 determines if the WIR_NEG_RESP counter exceeds the

WIR_NEG_RESP limit. The WIR_NEG_RESP limit is the minimum number of unsuccessful enquiries required for RFID detector to transition from the WIR mode to the OOR mode. If at step 716, it is determined that the WIR_NEG_RESP counter is greater than or equal to the WIR_NEG_RESP limit, RFID detector 204 proceeds to step 718. At step 718, RFID detector enters the OOR mode.

If at step 716, it is determined that the WIR_NEG_RESP counter is less than the WIR_NEG_RESP limit, RFID detector 204 proceeds to step 720. At step 720, RFID detector 204 enters the idle state. At step 722, RFID detector 204 waits in the idle state for a pre-specified time period (MT5). After step 722, RFID detector 204 returns to step 706 to transmit further WIR_ENQ packets.

If at step 712, it is determined that a WIR_RESP packet is received within the MT4 time period, RFID detector 204 proceeds to step 724. At step 724, RFID detector 204 checks the received WIR_RESP packet for validity. If at step 724, it is determined that the received WIR_RESP packet is valid, RFID detector 204 proceeds to step 720 and enters the idle state. If at step 724, it is determined that the received WIR_RESP packet is invalid, RFID detector 204 proceeds to step 714 and increments the WIR_NEG_RESP counter.

FIG. 8 is a flow diagram illustrating the WIR mode for RFID slave unit 206 under the WSS-FDA protocol according to an embodiment of the invention.
At step 802, RFID slave unit 206 enters the WIR mode. At step 804, RFID slave unit 206 enters the receive state and waits for a pre-specified time period (ST3) for a WIR_ENQ packet from RFID detector 204. At step 806, RFID slave unit 206 determines if a WIR_ENQ packet is received within the ST3 time period. If at step 806, it is determined that a WIR_ENQ packet is received within the ST3 time period, RFID slave unit 206 proceeds to step 808. At step 808, RFID slave unit 206 checks the received WIR_ENQ packet for validity. If at step 808, the received WIR_ENQ packet is found to be invalid, RFID slave unit 206 proceeds to step 810. At step 810, RFID slave unit 206 increments the WIR_NEG_ENQ counter by one. The WIR_NEG_ENQ counter indicates the number of cycles during which the RFID slave unit 206 has waited unsuccessfully, i.e. the number of cycles for which no valid WIR_ENQ packets were received. At step 812, RFID slave unit 206 determines if the within-range negative-response (WIR_NEG_ENQ) counter exceeds the WIR_NEG_ENQ limit. The WIR_NEG_ENQ limit is the minimum number of unsuccessful waiting cycles required for RFID slave unit 206 to transition from the

WIR mode to the OOR mode. If at step 812, it is determined that the WIR_NEG_ENQ counter is greater than or equal to the WIR_NEG_ENQ limit, RFID slave unit 206 enters the OOR mode.

If at step 812, it is determined that the WIR_NEG_ENQ counter is less than the WIR_NEG_ENQ limit, RFID slave unit 206 proceeds to step 816. At step 816, RFID slave unit 206 enters the idle state. At step 818, RFID slave unit 206 waits in the idle state for a pre-specified time period (ST5). After step 818, RFID slave unit 206 returns to step 804 to wait for WIR_ENQ packets.

If at step 808, it is determined that the received WIR_ENQ packet is valid, RFID slave unit proceeds to step 820. At step 820, RFID slave unit 206 enters the transmit state. At step 822, RFID slave unit 206 transmits a WIR_RESP packet of a pre-specified time period (ST4). After step 822, RFID slave unit proceeds to step 816 and enters the idle state.

If at step 806, it is determined that no WIR_ENQ packet is received within the ST3 time period, RFID slave unit 206 proceeds to step 810 where it increments the WIR_NEG_ENQ counter.

FIG. 9 is a flow diagram illustrating the OOR mode for RFID detector 204 under the WSS-FDA protocol according to an embodiment of the invention. RFID detector 204 enters the OOR mode on having ascertained that no authenticated RFID slave unit is present within the proximity of device 102.

At step 902, RFID detector 204 enters the OOR mode. At step 904, RFID detector informs WSS application software to switch OFF the monitor of PC. At step 906, RFID detector 204 enters the transmit state. At step 908, RFID detector 204 transmits an out-of-range enquiry (OOR_ENQ) packet of a pre-specified time period (MT6). At step 910, RFID detector 204 enters the receive state in which it waits for another pre-specified time period (MT7) for an out-of-range response (OOR_RESP) packet from RFID slave unit 206. At step 912, RFID detector 204 determines if an OOR_RESP packet is received within the MT7 time period. If at step 912, it is determined that an OOR_RESP packet is received within the MT7 time period, RFID detector 204 proceeds to step 914. At step 914, RFID detector 204 checks the received OOR_RESP packet for validity. If at step 914, the received OOR_RESP packet is found to be valid, RFID detector 204 proceeds to step 916. At step 916, RFID detector 204 increments the out-of-range positive-response (OOR_POS_RESP) counter by one. The OOR_POS_RESP counter indicates the number of successful enquiries made by RFID detector 204 while in the OOR mode, i.e. the number of OOR_ENQ packets transmitted that resulted in a valid OOR_RESP packet being received. At step 918, RFID detector 204 determines if the OOR_POS_RESP counter exceeds the OOR_POS_RESP limit. The OOR_POS_RESP limit is the minimum number of successful enquiries required for RFID detector to transition from the OOR mode to the WIR mode. If at step 918, it is determined that the OOR_POS_RESP counter is greater than or equal to the OOR_POS_RESP limit, RFID detector 204 proceeds to step 920. At step 920, RFID detector 204 enters the WIR mode.

If at step 918, it is determined that the OOR_POS_RESP counter less than the OOR_POS_RESP limit, RFID detector 204 proceeds to step 922. At step 922, RFID detector enters the idle state. At step 924, RFID detector 204 waits in the idle state for a pre-specified time period (MT8). After step 924, RFID detector 204 returns to step 906 and prepares to transmit further OOR_ENQ packets.

If at step 914, it is determined that the received OOR_RESP packet is invalid, RFID detector 204 proceeds to step 922 and enters the idle state.

If at step 912, it is determined that no OOR_RESP packet is received within the MT7 time period, RFID detector 204 proceeds to step 922 and enters the idle state.

FIG. 10 is a flow diagram illustrating the OOR mode for RFID slave unit 206 under the WSS-FDA protocol according to an embodiment of the invention.

At step 1002, RFID slave unit 206 enters the OOR mode. At step 1004, RFID slave unit 206 enters the receive state and waits for a pre-specified time period (ST6) for an OOR_ENQ packet from RFID detector 204. At step 1006, RFID slave unit 206 determines if an OOR_ENQ packet is received within the ST6 time period. If at step 1006, it is determined that an OOR_ENQ packet is received within the ST6 time period, RFID slave unit 206 proceeds to step 1008. At step 1008, RFID slave unit checks the received OOR_ENQ packet for validity. If at step 1008, it is determined that the received OOR_ENQ packet is valid, RFID slave unit 206 proceeds to step 1010. At step 1010, RFID slave unit 206 enters the transmit state. At step 1012, RFID slave unit 206 transmits an OOR_RESP packet of a pre-specified time period (ST7). At step 1014, RFID slave unit 206 increments the OOR_POS_ENQ counter by one. The OOR_POS_RESP counter indicates the number of cycles during which the RFID slave unit 206 has waited successfully, i.e.

the number of cycles for which a valid OOR_ENQ packet was received. At step 1016, RFID slave unit 206 determines if the OOR_POS_ENQ counter exceeds the OOR_POS_ENQ limit. The OOR_POS_ENQ limit is the minimum number of successful waiting cycles required for RFID slave unit 206 to transition from the OOR mode to the WIR mode. At step 1018, RFID slave unit 206 determines if the change of mode recommended by the OOR_ENQ packet is valid. If at step 1018, the change of mode is found to be valid, RFID slave unit 206 proceeds to step 1020. At step 1020, RFID slave unit 206 enters the WIR mode.

If at step 1018, the change of mode is found to be invalid, RFID slave unit 206 proceeds to step 1022. At step 1022, RFID slave unit 206 enters the idle state. At step 1024, RFID slave unit 206 waits in the idle state for a pre-specified time period (ST8). After step 1024, RFID slave unit 206 returns to step 1004 to wait for further OOR_ENQ packets.

If at step 1008, it is determined that the received OOR_ENQ packet is invalid, RFID slave unit 206 proceeds to step 1022 and enters the idle state.

If at step 1006, it is determined that no OOR_ENQ packet is received within the ST6 time period, RFID slave unit 206 proceeds to step 1022 and enters the idle state.

FIG. 11 is a flow diagram illustrating the Association Phase for RFID detector 204 under the WSS-FDA protocol according to an embodiment of the invention. A new RFID slave units 206 may be associated with RFID detector 204 by invoking the Association Phase functionality of WSS system 104. For the association to be formed, RFID slave unit 206 is placed within the proximity of RFID detector 206 by user 106. User 106 calls the Association Phase functionality of WSS application software. According to an embodiment of the invention, only an authentic user 106, for example, a system administrator is capable of calling the Association Phase functionality of WSS application software. WSS application software responds by requesting user 106 to enter the product identification information for new RFID slave unit 206. Subsequently, WSS application software places RFID detector 204 in Association Phase. Further, WSS application software extracts the SID of new RFID slave unit 206 from its product identification information, and sends the SID to RFID detector 204.

At step 1102, RFID detector 204 enters the Association Phase. At step 1104, RFID detector 204 enters the transmit state. At step 1106, RFID detector 204 transmits the association request (ASSOCIATION_REQUEST) packet for a pre-specified time period (MAT1). At step 1108, RFID detector 204 enters the receive state in which it waits for another pre-specified time period (MAT2) for an association-request reply (ASSOCIATION_REQUEST_REPLY) packet. At step 1110, RFID detector 204 determines if an ASSOCIATION_REQUEST_REPLY packet is received within the MAT2 time period. If at step 1110, it is determined that an ASSOCIATION_REQUEST_REPLY packet is received within the MAT2 time period, RFID detector 204 proceeds to step 1112. At step 1112, RFID detector 204 determines if the received ASSOCIATION_REQUEST_REPLY packet is valid. If at step 1112, it is determined that the received ASSOCIATION_REQUEST_REPLY packet is valid, RFID detector 204 proceeds to step 1114. At step 1114, RFID detector 204 informs the WSS application software of the successful association of new RFID slave unit 206 and saves the SID of RFID slave unit 206 extracted from the received ASSOCIATIOM_REQUEST_REPLY packet as an authentic SID code. At step 1116, RFID detector 204 waits for the instruction from WSS application software to exit the Association Phase. On receiving the instruction from WSS application software to exit the Association phase, at step 1118, user 106 is informed about the successful association. At step 1820 RFID detector 204 exits the Association Phase.

If at step 1112, it is determined that the received ASSOCIATION_REQUEST_REPLY packet is invalid, RFID detector 204 proceeds to step 1120. At step 1120, RFID detector 204 increments the association negative-response (ASSOCIATION_NEG_RESP) counter by one. The ASSOCIATION_NEG_RESP counter indicates the number of unsuccessful association cycles, i.e. the number of cycles during which no valid ASSOCIATION_REQUEST_REPLY packet was received. At step 1122, RFID detector 204 determines if the ASSOCIATION_NEG_RESP counter has exceeded the slave-association (SLAVE_ASSOCIATION) limit. The SLAVE_ASSOCIATION limit is the maximum number of unsuccessful association cycles allowed during the Association Phase. If at step 1122, it is determined that the ASSOCIATION_NEG_RESP counter is greater than or equal to the SLAVE_ASSOCIATION limit, RFID detector 204 proceeds to step 1124. At step 1124, RFID detector 204 informs WSS application software of the failure in associating RFID slave unit 206. After step 1124, RFID detector 204 proceeds to step 1116 and waits for the instruction from WSS application software to exit the Association Phase. On receiving the instruction from WSS application software to exit the Association phase, at step 1118, user 106 is informed about the unsuccessful association. At step 1820 RFID detector 204 exits the Association Phase.

If at step 1122, it is determined that the ASSOCIATION_NEG_RESP counter is less than the SLAVE_ASSOCIATION limit, RFID detector 204 proceeds to step 1104 and prepares to transmit further ASSOCIATION_REQUEST packets.

If at step 1110, it is determined that no ASSOCIATION_REQUEST_REPLY packet is received within the MAT2 time period, RFID detector proceeds to step 1120.

FIG. 12 is a flow diagram illustrating the response from RFID slave unit 206 during the Association Phase under the WSS-FDA protocol according to an embodiment of the invention.

At step 1202, RFID slave unit 206 enters receive state. At step 1204, RFID slave unit 206 determines if the packet received is an ASSOCIATION_REQUEST packet. If at step 1204, it is determined that the ASSOCIATION_REQUEST packet is received, RFID slave unit 206 proceeds to step 1206. At step 1206, RFID slave unit 206 checks the received ASSOCIATION_REQUEST packet for validity. If at step 1206, it is determined that the received ASSOCIATION_REQUEST packet is valid, RFID slave unit 206 proceeds to step 1208. At step 1208, RFID slave unit 206 enters the transmit state. At step 1210, RFID slave unit 206 transmits the ASSOCIATION_REQUEST_REPLY packet for a pre-specified time period (SAT1) and stores the MID of RFID detector 204 extracted from the ASSOCIATION_REQUEST packet.

If at step 1206, it is determined that the received ASSOCIATION_REQUEST packet is invalid, RFID slave unit 206 returns to step 1202 and enters the receive state.

If at step 1208, it is determined that no ASSOCIATION_REQUEST packet is received, RFID slave unit 206 returns to step 1202 and enters the receive state.

Fig 13 is a flow diagram describing the transitions of RFID detector 204 between the modes prescribed under the Watt Saver Sensor - Simplex Active (WSS-SA) protocol on turning PC on in accordance with an embodiment of the invention.

According to another embodiment of the invention, the WSS system 104 may be implemented using Simplex Active RFID wherein RFID detector 204 and RFID slave unit 206 communicate as per the WSS-SA protocol. Under the WSS-SA protocol, RFID detector 204 can only receive RF packets, whereas RFID slave unit 206 can only transmit RF packets. Consequently, under WSS-SA protocol, RFID detector 204 can be in one of the two states: receive and idle. Likewise, RFID slave unit 206 can be in either of two states: transmit and idle. Further, the WSS-SA protocol prescribes two modes of operation for RFID detector 204 of WSS system 104: the Within Range (WIR) mode.and the Out Of Range (OOR) mode. The WR mode and OOR mode cover all possible operating conditions of WSS system 104 under the WSS-SA protocol. FIG. 13-17 illustrate the details of the modes while FIG. 18 describes the method prescribed for associating new RFID slave units 206 under the WSS-SA protocol. Under the WSS-SA protocol, RFID slave unit 206 requires less power as compared to that under WSS-FDA protocol. WSS-SA protocol has reduced enquiry and response times for RFID detector 204 and RFID slave unit 206.

At step 1302, PC is switched ON. According to an embodiment of the invention, switching ON PC automatically boots up WSS application software. According to another embodiment of the invention, the WSS application software needs to be manually turned ON. Further, the monitor of PC is, by default, ON immediately after PC is switched ON At step 1304, RFID detector 204 is switched ON. When switched ON, RFID detector 204 enters the WIR mode at step 1306. At step 1308, RFID detector 204 enquires for RFID slave units 206 as per the WSS-SA protocol. At step 1310, a determination is made if any RFID slave unit 206 is within the proximity of PC. Any RFID slave unit 206 within the proximity of PC is further authenticated by slave unit authenticator 208. If it is determined at step 1310 that no RFID slave unit 206 authenticated by slave unit authenticator 208 is within the proximity of PC, then at step 1314, RFID detector 204 enters the OOR mode. RFID detector 204, while remaining in the OOR mode, sends an alert to WSS application software to switch OFF the monitor of PC.

If it is determined at step 1310 that at least one RFID slave unit 206 authenticated by slave unit authenticator 208 is present within the proximity of PC, then RFID detector 204 remains in WIR mode.

Fig 14 is a flow diagram describing the transitions of RFID slave unit 206 between two states under the WSS-SA protocol in accordance with an embodiment of the invention.

At step 1402, RFID slave unit 206 is switched ON. .According to an embodiment of the invention, RFID slave unit 206 cannot be switched OFF once it is switched ON. At step 1404, RFID slave unit 206 enters Transmit (TX) state. In TX State, RFID slave unit 206 transmits a PRESENT packet of a pre specified (ST1) time period at step 1406. The PRESENT packet is received by RFID detector 204 in accordance with the WSS-SA protocol. The PRESENT packet is an information packet which informs about the presence of a RFID slave unit 206 within the proximity of PC. The WSS-SA PRESENT packet format has been described in detail in conjunction with FIG. 17. At step 1408, RFID slave unit 206 enters idle (IDL) state. On entering IDL state, RFID slave unit 206 waits in IDL state for another pre-specified time period (ST2) at step 1410. RFID slave unit 206 on waiting in IDL state for ST2 time period again enters the TX state at step 1404.

FIG. 15 is a flow diagram illustrating the WIR mode for RFID detector 204 prescribed under the WSS-SA protocol according to an embodiment of the invention. RFID detector 204 enters the WIR mode on having ascertained the presence of at least one RFID slave unit 206 authenticated by slave unit authenticator 208 within the proximity of device 102.

On being switched ON, RFID detector 204 enters WIR mode at step 1502. On entering the WIR mode, RFID detector 204 alerts the WSS application software to switch ON the monitor of PC at step 1504. At step 1506, RFID detector 204 enters Receive (RX) state. On entering the RX state, RFID detector 204 waits in RX state for a pre-specified (MT1) time period. At step 1508 a determination is made by RFID detector 204 if a PRESENT packet from at least one RFID slave unit 206 authenticated by the slave unit authenticator 208 is received.

If it is determined that RFID detector 204 has received a PRESENT packet then at step 1510 a validation check is made by RFID detector 204 for validating the received PRESENT packet. If the PRESENT packet is determined to be valid then RFID detector 204 then at step 1512, it enters the IDL state. On entering the IDL state, RFID detector 204 waits in IDL state for a pre-specified (MT2) time period at step 1514. On waiting in IDL state for MT2 time period, again step 1506 is executed where RFID detector 204 again enters RX state to receive further PRESENT packets.

If at step 1510, it is determined that RFID detector 204 received an invalid PRESENT packet, or at step 1508 it is determined that RFID detector 204 has not received a PRESENT packet, then at step 1516, a counter (WIR_SLAVE_NOT_PRESENT) for RFID slave unit 206 not present is incremented by one count. The WIR_SLAVE_NOT_PRESENT counter indicates that RFID slave unit 206 authenticated by slave unit authenticator 208 is not present within the proximity of PC. If the count of the WIR_SLAVE_NOT_PRESENT counter exceeds a limit, it may be interpreted as no authentic RFID slave unit 206 is present within the proximity of PC and as such the monitor of PC needs to be switched OFF. At step 1518 a determination is made if WIR_SLAVE_NOT_PRESENT counter has exceeded the limit for RFID slave unit 206 being not present within range (WIR_SLAVE_NOT_PRESENT limit). If it is determined that WIR_SLAVE_NOT_PRESENT counter has exceeded WIR_SLAVE_NOT_PRESENT limit, then RFID detector 204 enters OOR mode at step 1520. If it is determined that WIR_SLAVE_NOT_PRESENT counter has not exceeded WIR_SLAVE_NOT_PRESENT limit, then RFID detector again enters the RX state at step 1506 to attempt to receive PRESENT packets.

FIG. 16 is a flow diagram illustrating the OOR mode for RFID detector 204 prescribed under the WSS-SA protocol according to an embodiment of the invention.

RFID detector 204 enters OOR mode at step 1602 if a plurality of PRESENT packets from a RFID slave unit 206 authenticated by slave unit authenticator 208 are not received implying that RFID slave unit 206 is not within the proximity of PC and as such is out of range. On entering OOR mode, RFID detector 204 alerts the WSS application software to turn OFF the monitor of PC at step 1604. At step 1606, RFID detector 204 enters Receive (RX) state. On entering RX state, RFID detector 204 waits in RX state for a pre-specified (MT3) time period. At step 1608 a determination is made by RFID detector 204 if any PRESENT packet has been received from a RFID slave unit 206 authenticated by slave unit authenticator 208.

If it is determined at step 1608 that a PRESENT packet has not been received, then RFID detector 204 proceeds to step 1610. At step 1610, RFID detector 204 enters the idle (IDL) state. On entering IDL state, RFID detector 204 waits in IDL state for another pre-specified time period (MT4) at step 1612. After

Step 1612, RFID detector 204 again enters RX state at step 1606 in order to be able to receive any PRESENT packet.

If it is determined at step 1608 that a PRESENT packet has been received then at step 1614 a determination is made by RFID detector 204 for the validity of the received PRESENT packet.

If it is determined at step 1614 that RFID detector 204 has not received a valid PRESENT packet, it again enters the IDL state at step 1610 and proceeds to step 1612.

If it is determined at step 1614 that RFID detector 204 has received a valid PRESENT packet, then at step 1616 RFID detector 204 increments a counter (OOR_SLAVE_PRESENT) for RFID slave unit 206 being out of range by one count. At step 1618, a determination is made if OOR_SLAVE_PRESENT counter has exceeded the limit for out of range mode for RFID slave unit 206 (OOR_SLAVE_PRESENT limit).

If it is determined at step 1618 that OOR_SLAVE_PRESENT counter has exceeded the OOR_SLAVE_PRESENT limit, then at step 1620 RFID detector 204 enters WIR mode.

If it is determined at step 1618 that OOR_SLAVE_PRESENT counter has not exceeded the OOR_SLAVE_PRESENT limit, then RFID detector 204 again enters IDL state at step 1610.

Fig. 17 is a schematic describing the WSS-SA PRESENT packet format prescribed under the WSS-SA protocol in accordance with an embodiment of the invention.

According to an embodiment of the invention, the PRESENT packet comprises a sequence of fifteen bytes of information. However the invention is not limited to the PRESENT packet comprising of exactly fifteen bytes and may comprise of any number of bytes. The PRESENT packet comprises of a Preamble 1702, a Sync Word 1704, a Payload 1706 and a CRC-16 1708. Preamble 1702 comprises of four bytes of information which is a pattern of sequence of ones (1) and zeros (0) in digital format. Preamble 1702 fills the first four bytes i.e. byte 1 to byte 4 of the PRESENT packet format. Sync Word 1704 fills the next four bytes i.e. byte 5 to byte 8 of PRESENT packet and provides the byte synchronization information of an incoming packet. Payload 1706 fills the next five bytes i.e. byte 9 to byte 13 of the PRESENT packet. Byte number 9 has the command data and the coding for this byte is as given in Table -1 below. Byte 14 and byte 15 comprises the 16 bit Cyclic Redundancy Check data.

Byte Coding			Packet Type	Function	Initiator
Bit 7	Bit 6	Bit 5 - 0			
1	0	00_0010	WU_ENQUIRY	Pre-associated Master & Slave unit communication	Master Unit
0	0	00_0011	WU_RESPONSE	Pre-associated Master & Slave unit communication	Slave Unit
1	0	00_0100	WIR_ENQUIRY	Pre-associated Master & Slave unit communication	Master Unit
0	0	00_0101	WIR_RESPONSE	Pre-associated Master & Slave unit communication	Slave Unit
1	0	00_1000	OOR_ENQUIRY	Pre-associated Master & Slave unit communication	Master Unit
0	0	00_1001	OOR_RESPONSE	Pre-associated Master & Slave unit communication	Slave Unit
1	1	00_0010	WU_ENQUIRY	Non-Pre associated Master & Slave unit communication	Master Unit
0	1	00_0011	WU_RESPONSE	Non-Pre associated Master & Slave unit communication	Slave Unit
1	1	00_0100	WIR_ENQUIRY	Non-Pre associated Master & Slave unit communication	Master Unit
0	1	00_0101	WIR_RESPONSE	Non-Pre associated Master & Slave unit communication	Slave Unit
1	1	00_1000	OOR_ENQUIRY	Non-Pre associated Master & Slave unit communication	Master Unit

0	1	00_10 01	OOR_RESPONSE	Non-Pre associated Master & Slave unit communication	Slave Unit
1	0	01_00 00	ASSOCIATION_REQUEST	New slave unit association request communication	Master Unit
0	0	01_00 01	ASSOCIATION_REQUEST_REPLY	New slave unit association reply communication	Slave Unit
Remaining Byte coding are reserved					

Table 1 Coding for Byte 9

FIG. 18 is a flow diagram illustrating the Association Phase for RFID slave unit 206 under the WSS-SA protocol according to an embodiment of the invention.

At step 1802, RFID detector 204 enters the Association Phase. At step 1804, RFID detector 204 enters the Receive (RX) state. On entering RX state, RFID detector 204 waits for a PRESENT packet from a new RFID slave unit 206. At step 1806 a determination is made if RFID detector 204 has received a PRESENT packet within a certain time period. If it is determined at step 1806 that no PRESENT packet has been received within the certain time period, RFID detector 204 again enters RX state at step 1804.

If at step 1806, it is determined that a PRESENT packet has been received within the certain time period, then RFID detector 204 proceeds to step 1808. At step 1808 the validity of the received PRESENT is checked. If it is determined that the received PRESENT packet is not valid, RFID detector 204 again enters RX state at step 1804. If at step 1808, it is determined that the received PRESENT packet is valid, then at step 1810 RFID detector 204 extracts an SID code from the PRESENT packet and sends it to the WSS application software. An SID code is a pre-configured identification code associated with any RFID slave unit 206 which is identifiable under the prescribed WSS-SA protocol by RFID detector 204. After alerting the WSS application software, RFID detector 204 waits for a valid response from the WSS application software at step 1812. At step 1814 a determination is made by RFID detector 204 if the SID code has been accepted by WSS application software. If the SID code is accepted, WSS application software saves the SID code as an authentic SID code. If it is determined at step 1814 that the SID code has been accepted by WSS application software, then RFID detector 204 identifies the new RFID slave unit 206 as an authentic RFID slave unit 206 at step 1816. The association phase of new RFID slave unit 206 by RFID detector 204 is completed at step 1816. After step 1816 RFID detector 204 proceeds to step 1818. At step 1818, user 106 is informed about the successful association. At step 1820, RFID detector 204 exits from Association phase.

If it is determined at step 1814 that the extracted SID code has not been accepted by WSS application Software, the new RFID slave unit 206 is not identified to be authentic and at step 1818, user 106 is informed about the unsuccessful association. At step 1820, RFID detector 204 exits from Association phase.

FIG. 19 is a flow diagram illustrating the transitions between the three modes prescribed under the WSS-FDP protocol for the RFID detector 204, according to an embodiment of the invention.

WSS system 104 may be implemented using Full Duplex Passive RFID wherein RFID detector 204 and RFID slave unit 206 communicate as per the WSS-FDP protocol. Under the WSS-FDP protocol, both RFID detector 204 and RFID slave unit 206 can transmit and receive RF packets. According to an embodiment of the invention, RFID slave unit 206 used in accordance with the WSS-FDP protocol does not use battery power but uses energy from the received RF packets to transmit other RF packets. Consequently, under WSS-SA protocol, RFID detector 204 can be in one of the three states: transmit, receive and idle. Likewise, RFID slave unit 206 can be in either of two states: transmit and idle. Further, the WSS-FDP protocol prescribes three modes of operation for WSS system 104: the Wake Up (WU) mode, the Within Range (WIR) mode, and the Out Of Range (OOR) mode. The modes cover all possible operating conditions of WSS system 104 under the WSS-FDP protocol. FIG. 19-23 illustrate the details of the modes while FIG. 24 describe the method prescribed for associating new slave units under the WSS-FDP protocol.

At step 1902, PC is switched ON. According to an embodiment of the invention, switching ON PC automatically boots up WSS application software. According to another embodiment of the invention, the WSS application software needs to be manually turned ON. Further, the monitor of PC is, by default, ON immediately after PC is switched ON. At step 1904 RFID detector 204 is switched ON. On being switched ON, RFID detector 204 enters the WU mode at step 1906. At step 1908, RFID detector 204 enquires for RFID slave units 206 as per the WSS-FDP protocol. At step 1910, a determination is made if at least one RFID slave unit 206 authenticated by slave unit authenticator is within the proximity of PC.

If it is determined at step 1910 that at least one RFID slave unit 206 authenticated by slave unit authenticator has been detected in the proximity of PC, then RFID detector 204 proceeds to step 1912. At step 1912 RFID detector 204 enters WIR mode.

If it is determined at step 1910 that no RFID slave units 206 authenticated by slave unit authenticator is within the proximity of PC, then RFID detector 204 proceeds to step 1916. At step 1916 RFID detector 204 enters the OOR mode. On entering the OOR mode, RFID detector 204 sends an alert to WSS application software to switch OFF the monitor of PC. At step 1918 the monitor of PC is switched OFF.

FIG. 20 is a flow diagram illustrating the transition of RFID slave unit 206 between the two states prescribed under the WSS-FDP protocol according to an embodiment of the invention.

At step 2002, RFID slave unit 206 enters idle (IDL) state. At step 2004, it is determined if a packet is received from RFID detector 204. If it is determined that a valid packet has not been received, RFID slave unit 206 remains in IDL state and again returns to step 2004. According to an embodiment of the invention, RFID slave unit 206 keeps returning to step 2004 asynchronously on not receiving a valid packet from RFID detector 204. According to another embodiment of the invention, RFID slave unit 206 waits for a pre-specified (SP1) time period before returning to step 2004 on not receiving a valid packet from RFID detector 204.

If it is determined that a valid packet from RFID detector 204 has been received, then at step 2006, RFID slave unit 206 enters transmit (TX) state. RFID slave unit 206 uses the RF energy from the received packet to read the SID from RFID slave unit 206's memory. At step 2008, RFID slave unit 206 reads the SID and transmits the SID to RFID detector 206. After the SID has been transmitted, RFID slave unit 206 again enters IDL state at step 2002.

FIG. 21 is a flow diagram illustrating the WU mode for RFID detector 204 under the WSS-FDP protocol according to an embodiment of the invention. Immediately after PC is switched ON, WSS application software causes RFID detector 204 to enter the WU mode.

On entering the WU mode RFID detector 204 enters the Transmit (TX) state at step 2104. At step 2106, RFID detector 204 transmits a wake up enquiry (WU_ENQ) packet of a pre-specified (MT1) time period. After step 2106, RFID detector 204 enters the Receive (RX) state at step 2108. On entering RX state RFID detector 204 waits for a pre-specified (MT2) time period at step 2108.

RFID Slave unit 206 on receiving an RF signal from RFID detector 204, uses the stored RF energy of the RF signal to send its encrypted Slave Identification number (SID) over RF link. The encrypted SID packet is an information packet used as an identification data to identify each of RFID detector 204 and RFID slave unit 206 during communication between them over RF link.

At step 2110, a determination is made if a SID packet has been received from RFID slave unit 206 authenticated by slave unit authenticator 208 within a pre-specified (MT2) time period.

If it is determined at step 2110 that a SID packet has been received by RFID detector 204, then at step 2112 a validation check is performed to check the validity of received SID packet.

If it is determined at step 2112 that the received SID packet is valid, then at step 2114 RFID detector 204 increments a counter (WU_POS_RESPONSE) for positive response from RFID slave unit 206 under wake up mode by one count. At step 2116, a determination is made if WU_POS_RESPONSE counter has exceeded a limit for positive response from RFID slave unit 206 under WU mode (WU_POS_RESPONSE limit). If it is determined at step 2116 that WU_POS_RESPONSE counter has exceeded the WU_POS_RESPONSE limit, then at step 2118 RFID detector 204 enters the WIR mode. If it is determined at step 2116 that WU_POS_RESPONSE counter has not exceeded the WU_POS_RESPONSE limit, then RFID detector 204 again enters TX state at step 2104.

If it is determined at step 2112 that the received SID packet is not valid or if it is determined at step 2110 that no SID packet has been received, then at step 2120 a counter (WU_NEG_RESPONSE) for negative response from RFID slave unit 206 under Wake-up mode is incremented by one count. At step 2122 a determination is made if WU_NEG_RESPONSE counter has exceeded a limit for negative response from RFID slave unit 206 under WU mode (WU_NEG_RESPONSE limit). If it is determined that WU_NEG_RESPONSE counter has not exceeded WU_NEG_RESPONSE limit, then RFID detector 204 enters TX state at step 2104. If it is determined at step 2122 that WU_NEG_RESPONSE counter has exceeded WU_NEG_RESPONSE limit, then RFID detector 204 proceeds to step 2124. At step 2124 RFID detector 204 enters OOR mode.

FIG. 22 is a flow diagram illustrating the WIR mode for RFID detector 204 prescribed under the WSS-FDP protocol according to an embodiment of the invention.

RFID detector 204 enters the WIR mode at step 2202 on having ascertained the presence of at least one RFID slave unit 206 within the proximity of device 102. On entering the WIR mode, RFID detector 204 alerts the WSS application software to switch ON the monitor of PC at step 2204. If the monitor of PC is not already ON, the WSS application software switches ON the monitor of PC. RFID detector 204 enters the Transmit (TX) state at step 2206. At step 2208, RFID detector 204 transmits an enquiry packet for detecting RFID slave unit 206 in WIR mode (WIR_ENQUIRY) packet of a pre-specified (MT3) time period. After step 2208, RFID detector 204 enters the Receive (RX) state at step 2210. On entering RX state RFID detector 204 waits in RX state for another pre-specified (MT4) time period at step 2210. At step 2212 a determination is made if an SID packet has been received from a pre-associated RFID slave unit 206 within the MT4 time period.

If it is determined at step 2212 that an SID packet has been received, then RFID detector 204 proceeds to step 2214. At step 2214, a validation check is performed by RFID detector 204 to check the validity of received SID packet.

If it is determined at step 2214 that the received SID packet is valid, then RFID detector 204 at step 2216 enters the idle (IDL) state. On entering the IDL state, RFID detector 204 waits for another pre-specified (MT5) time period in the IDL state at step 2218. After step 2218, RFID detector 204 again enters TX state at step 2206.

If it is determined at step 2212 that an SID packet has not been received, or if it is determined at step 2214 that the received SID packet is not valid then at step 2220, RFID detector 204 increments a counter for negative response from RFID slave unit 206 in WIR mode (WIR_NEG_RESPONSE) by one count.

At step 2222 a determination is made if the WIR_NEG_RESPONSE counter has exceeded the limit for negative response from RFID slave unit 206 in WIR mode (WIR_NEG_RESPONSE limit). If it is determined at step 2222 that

WIR_NEG_RESPONSE counter has not exceeded the WIR_NEG_RESPONSE limit, then RFID detector 204 proceeds to step 2218 where it again enters the IDL state. If it is determined at step 2222 that WIR_NEG_RESPONSE counter has exceeded the WIR_NEG_RESPONSE limit, then RFID detector 204 proceeds to step 2224 where it enters the OOR mode.

FIG. 23 is a flow diagram illustrating the details of the OOR mode for RFID detector 204 under the WSS-FDP protocol according to an embodiment of the invention.

At step 2302, RFID detector 204 enters the OOR mode on having ascertained that no RFID slave unit 206 authenticated by slave unit authenticator 208 is present within the proximity of device 102. On entering the OOR mode, RFID detector 204 alerts the WSS application software to switch OFF the monitor of PC at step 2304. After step 2302, RFID detector 204 enters the Transmit (TX) state at step 2306. At step 2308, RFID detector 204 transmits an enquiry packet for detecting RFID slave unit 206 under OOR mode (OOR_ENQUIRY) of another pre-specified (MT6) time period. After step 2308, RFID detector 204 enters the Receive (RX) state at step 2310. On entering the RX state RFID detector 204 waits in RX state for another pre-specified (MT7) time period at step 2310. At step 2312, a determination is made if RFID detector 204 has received a valid SID packet from a RFID slave unit 206 authenticated by slave unit authenticator 208 within the MT7 time period.

If it is determined at step 2312 that a valid SID packet has been received, then RFID detector 204 proceeds to step 2314. At step 2314 RFID detector 204 increments a counter for positive response from RFID slave unit 206 in OOR mode (OOR_POS_RESPONSE) by one. After step 2314, a determination is made if OOR_POS_RESPONSE counter has exceeded the limit for positive response from RFID slave unit 206 in OOR mode (OOR_POS_RESPONSE limit) at step 2316. If it is determined at step 2316 that OOR_POS_RESPONSE counter has exceeded the OOR_POS_RESPONSE limit, then RFID detector 204 proceeds to step 2318. At step 2318 RFID detector 204 goes in WIR mode.

If it is determined at step 2312 that no valid SID packet has been received, or if it is determined at step 2316 that OOR_POS_RESPONSE counter has not exceeded the OOR_POS_RESPONSE limit then RFID detector 204 at step 2320 RFID detector 204 enters the Idle (IDL) state. On entering IDL state RFID detector 204 waits in IDL state for another pre-specified (MT8) time period at step 2322 and again enters transmit state at step 2306.

FIG. 24 is a flow diagram illustrating the Association Phase for RFID slave unit 206 under the WSS-FDP protocol according to an embodiment of the invention.

At step 2402 RFID detector 204 enters the Association Phase. At step 2404, RFID detector 204 enters the Transmit (TX) state. At step 2406, RFID detector 204 transmits an ASSOCIATION_REQUEST packet for a pre specified (MAT1) time period. An ASSOCIATION_REQUEST packet is an information data packet sent by RFID detector 204 for initiating the association process with a new valid RFID slave unit 206. At step 2408, RFID detector 204 enters the Receive (RX) state and waits for a certain time for an SID packet. At step 2410, a determination is made if RFID detector 204 has received an SID packet within the certain time period.

If it is determined at step 2410 that no SID packet has been received within the certain time period, then RFID detector 204 proceeds to step 2416. At step 2416 RFID detector 204 increments a counter for detecting the number of times the SID packet has been received (NUM_CYCLES) by one count. At step 2418, a determination is made if NUM_CYCLES counter has exceeded a counter for detecting the association of RFID slave unit 206 (SLAVE_ASSOCIATION). If it is determined that NUM_CYCLES counter has not exceeded SLAVE_ASSOCIATION, then RFID detector 204 again enters the TX state at step 2404. If it is determined that NUM_CYCLES counter has exceeded SLAVE_ASSOCIATION, then RFID detector 204 proceeds to step 2420 where it informs WSS Application Software of unsuccessful association. At step 2422, RFID detector 204 waits for the instruction from WSS application software to exit the Association Phase. On receiving the instruction from WSS application software to exit the Association phase, at step 2424, user 106 is informed about the unsuccessful association. At step 2426 RFID detector 204 exits the Association Phase.

If it is determined at step 2410 that an SID packet has been received within the certain time period, then RFID detector 204 performs a validation check to check the validity of the received SID packet at step 2412. If it is determined at step 2412 that the received SID packet is not valid, then RFID detector 204 again proceeds to step 2416 where it increments NUM_CYCLES counter by one.

If it is determined at step 2412 that the received SID packet is valid, then RFID detector 204 informs the WSS Application Software of a successful association at step 2414. After step 2414 RFID detector 204 waits for the instruction from WSS application software to exit the Association Phase. On receiving the instruction from WSS application software to exit the Association phase, at step 2424, user 106 is informed about the successful association. At step 2426 RFID detector 204 exits the Association Phase.

While example embodiments of the invention have been illustrated and described, it will be clear that the invention is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions and equivalents will be apparent to those skilled in the art without departing from the spirit and scope of the invention as described in the claims.

CLAIMS:

1. A system for controlling the power consumption of an equipment based on the proximity of a user from the equipment, the system comprising:

a) at least one RFID slave unit,

b) an RFID detector, the RFID detector being capable of detecting the RFID slave unit based on the proximity of the RFID slave unit to the equipment; and

c) a power options controlling device, the power option controlling device controlling the power option of the equipment based on the detection of the RFID slave unit, the power options controlling device further comprising a slave unit authenticator, the slave unit authenticator being capable of authenticating the RFID slave unit

2. The system of claim 1 wherein the RFID slave unit and the RFID detector are based on full duplex active RFID technology.

3. The system of claim 1 wherein the RFID slave unit and the RFID detector are based on Simplex Active RFID technology.

4. The system of claim 1 wherein the RFID slave unit and the RFID detector are based on Full Duplex Passive RFID technology.

5. The system of claim 1 wherein the RFID slave unit is powered by a battery

6. The system of claim 1 wherein the power option controlling device controls the power option of the equipment based on the detection of the RFID slave unit, the RFID slave unit having being authenticated by the slave unit authenticator.

7. The system of claim 1 wherein the power option controlling device switches on the equipment based on the RFID detector detecting a first of the at least one RFID slave unit approaching the proximity of the equipment.

8. The system of claim 1 wherein the power option controlling device switches off the equipment based on the RFID detector detecting a last of the at least one RFID slave unit departing from the proximity of the equipment.

9. The system of claim 1 wherein the power option controlling device switches off the equipment based on the RFID detector detecting at least one unauthenticated RFID slave unit in the proximity of the equipment.

10. The system of claim 1, wherein the slave unit authenticator is capable of associating new RFID slave units to the system.

11. A method for controlling the power consumption of equipment based on the proximity of a user, the method comprising the steps of:

a) detecting at least one RFID slave unit based on the proximity of the at least one RFID slave unit to the equipment;
b) authenticating the at least one RFID slave unit; and
c) controlling the power option of the equipment based on the detection of the at least one RFID slave unit.

12. The method of claim 11, wherein the step of controlling the power option of the equipment further comprises switching ON the equipment based on detecting a first of the at least one RFID slave unit approaching the proximity of the equipment.

13. The method of claim 11, wherein the step of controlling the power option of the equipment further comprises switching OFF the equipment based on detecting a last of the at least one RFID slave unit departing from the proximity of the equipment.

14. The method of claim 11, wherein the step of controlling the power option of the equipment further comprises switching OFF the equipment based on detecting at least one

15. An apparatus for managing power consumption based on the proximity of a user from the apparatus, the apparatus comprising:

a) a computer system;
b) at least one slave unit, the at least one slave unit being associated with the user of the computer system;

c) a sensory detector, the sensory detector being capable of detecting the at least one slave unit based on the proximity of the sensing unit to the equipment by wirelessly communicating with the at least one slave unit;

d) a power options controlling device, the power options controlling device controlling the power option of the computer system based on the detection of the at least one slave unit;

e) a slave unit authenticator, the slave unit authenticator being capable of authenticating the slave unit.

16. The system for controlling power consumption of an equipment as recited in claim 1 wherein the sensory detector communicates with the slave unit based on a wireless technology selected from the group consisting of Bluetooth, Ultra wide band RF, infrared, WiFi, ultrasound, GPS, GPRS and Wireless Ethernet.

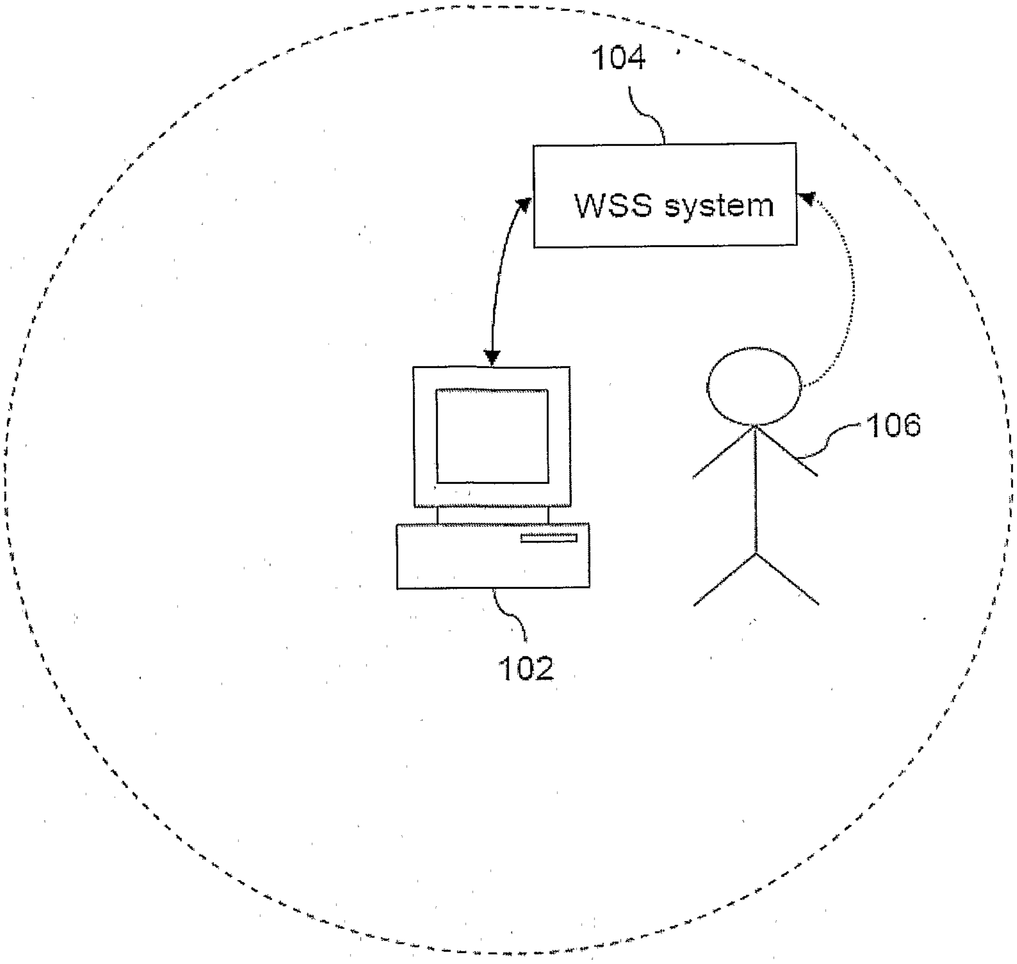

FIG. 1

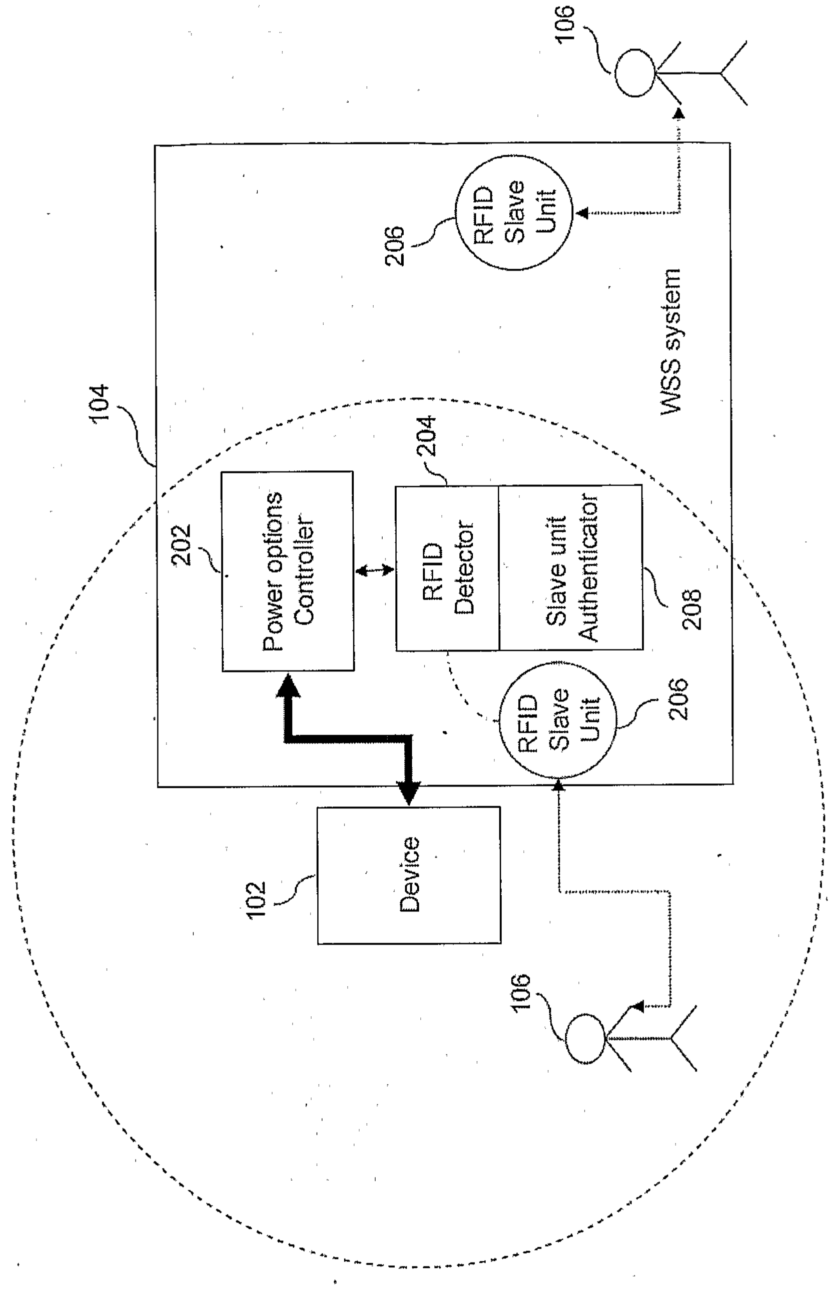
106
RFID Slave Unit
206
WSS system
104
204
RFID Detector
Slave unit Authenticator
208
202
Power options Controller
RFID Slave Unit
206
102
Device
106

FIG. 2

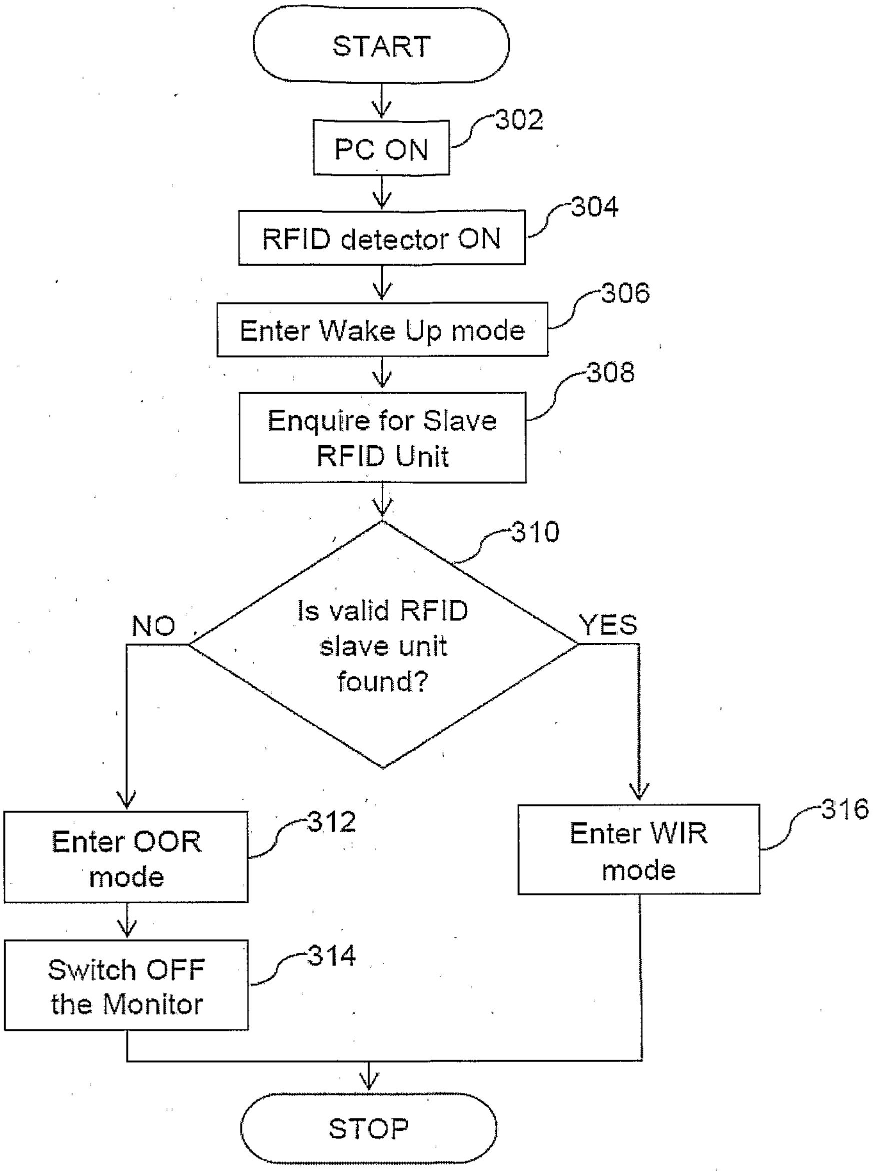
START
PC ON
302
RFID detector ON
304
Enter Wake Up mode
306
Enquire for Slave RFID Unit
308
Is valid RFID slave unit found?
310
NO
YES
Enter OOR mode
312
Switch OFF the Monitor
314
Enter WIR mode
316
STOP

FIG. 3

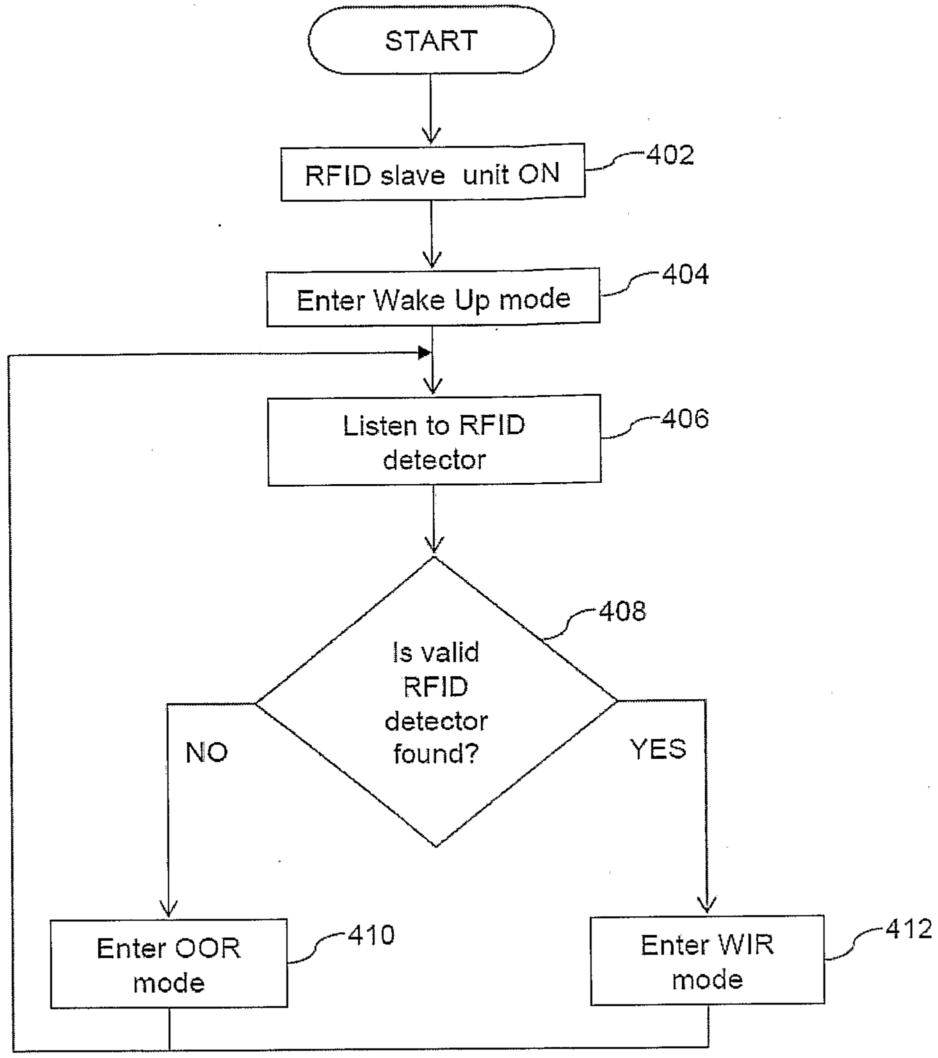
START
RFID slave unit ON
402
Enter Wake Up mode
404
Listen to RFID detector
406
Is valid RFID detector found?
408
NO
YES
Enter OOR mode
410
Enter WIR mode
412

FIG. 4

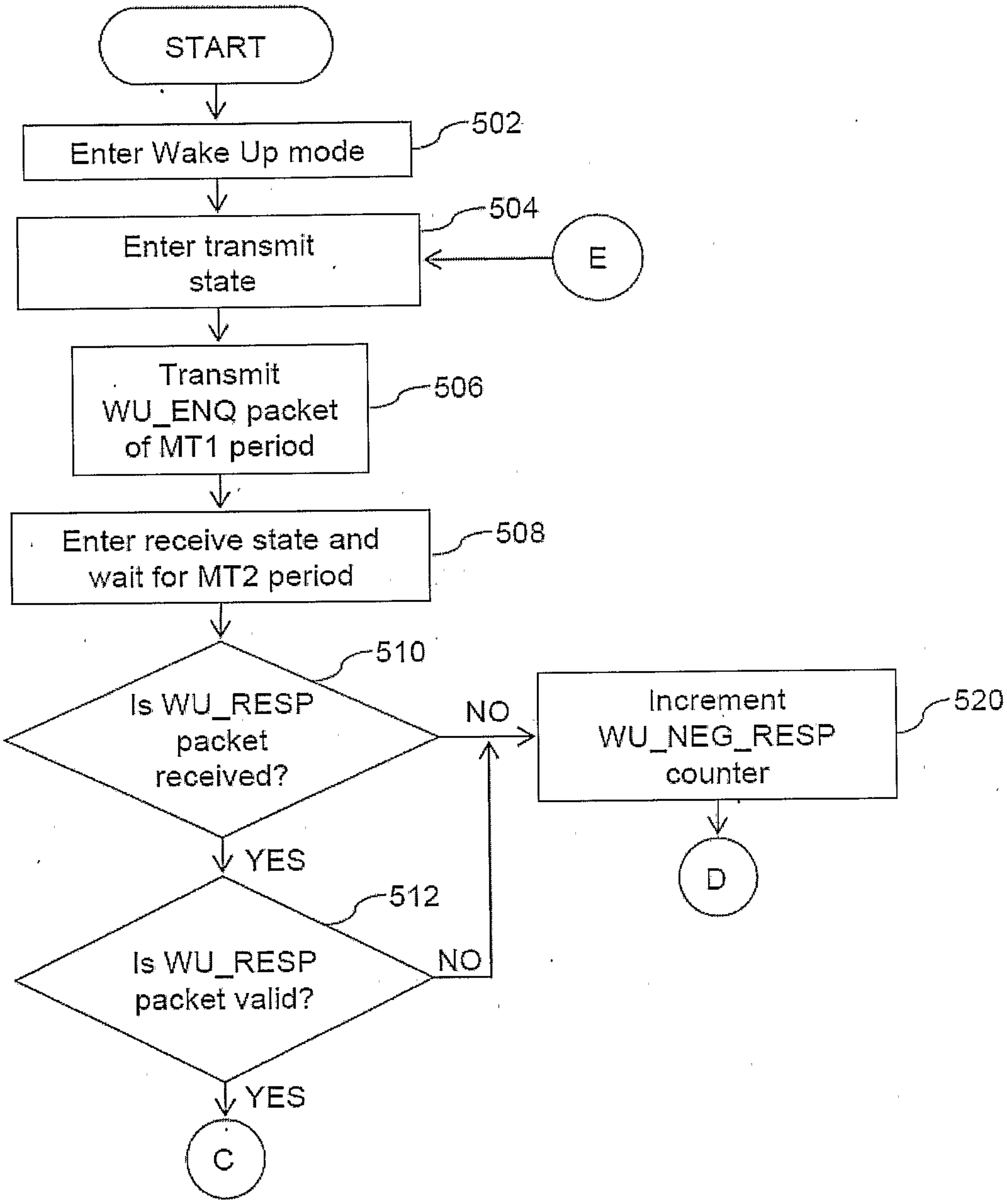
START
Enter Wake Up mode
502
Enter transmit state
504
E
Transmit WU_ENQ packet of MT1 period
506
Enter receive state and wait for MT2 period
508
Is WU_RESP packet received?
510
NO
Increment WU_NEG_RESP counter
520
D
YES
Is WU_RESP packet valid?
512
NO
YES
C

FIG. 5A

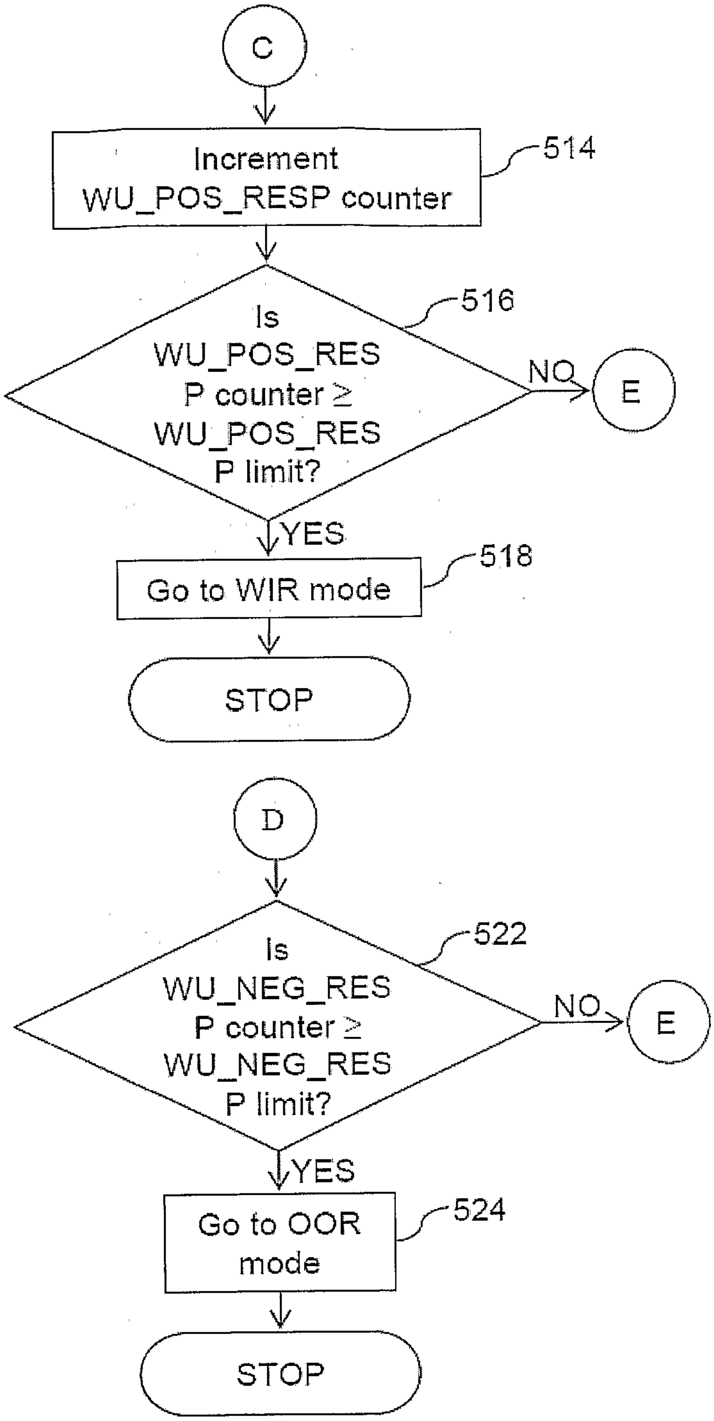
C
Increment WU_POS_RESP counter
514
Is WU_POS_RESP counter ≥ WU_POS_RESP limit?
516
NO
E
YES
Go to WIR mode
518
STOP
D
Is WU_NEG_RESP counter ≥ WU_NEG_RESP limit?
522
NO
E
YES
Go to OOR mode
524
STOP

FIG. 5B

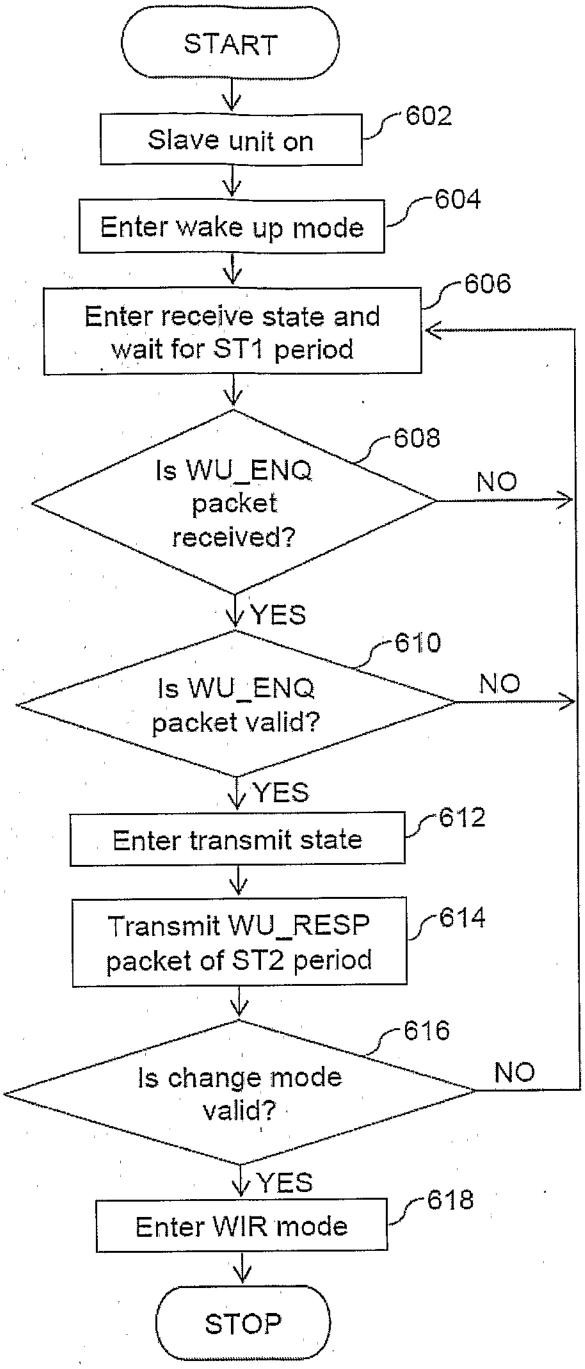
START
Slave unit on
602
Enter wake up mode
604
Enter receive state and wait for ST1 period
606
Is WU_ENQ packet received?
608
NO
YES
Is WU_ENQ packet valid?
610
NO
YES
Enter transmit state
612
Transmit WU_RESP packet of ST2 period
614
Is change mode valid?
616
NO
YES
Enter WIR mode
618
STOP

FIG. 6

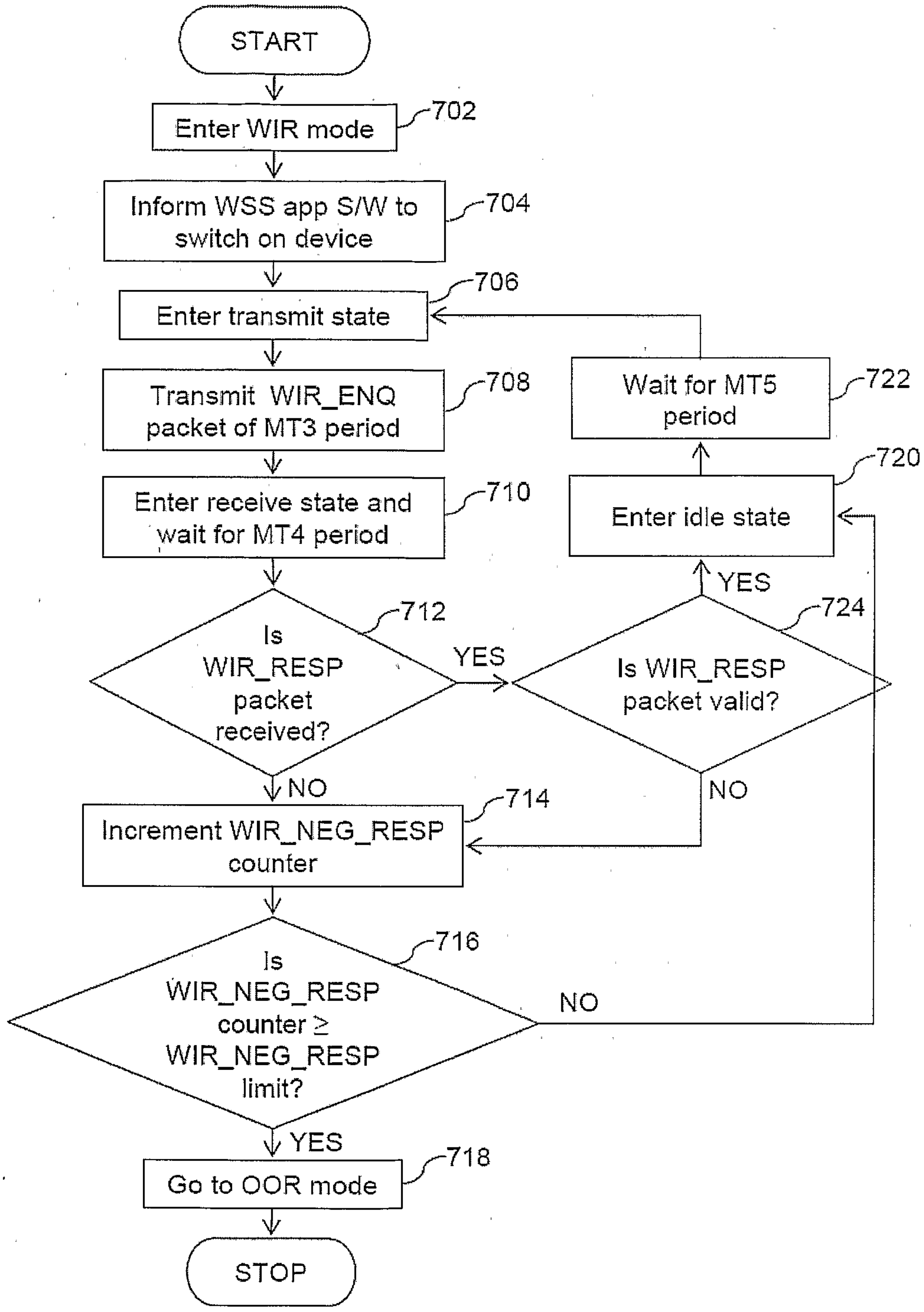
START
Enter WIR mode
702
Inform WSS app S/W to switch on device
704
Enter transmit state
706
Transmit WIR_ENQ packet of MT3 period
708
Enter receive state and wait for MT4 period
710
Is WIR_RESP packet received?
712
YES
NO
Increment WIR_NEG_RESP counter
714
Is WIR_NEG_RESP counter ≥ WIR_NEG_RESP limit?
716
NO
YES
Go to OOR mode
718
STOP
Is WIR_RESP packet valid?
724
YES
NO
Enter idle state
720
Wait for MT5 period
722

FIG. 7

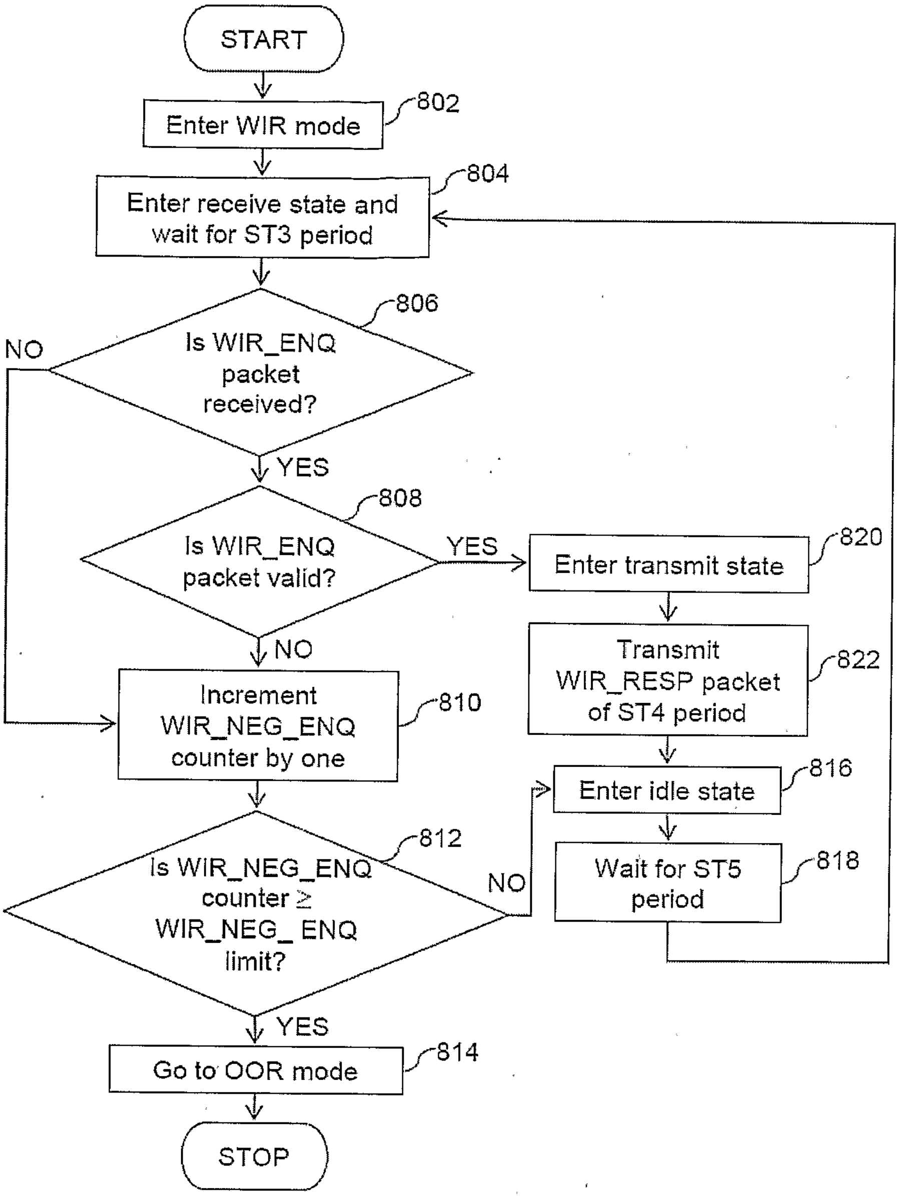
START
Enter WIR mode
802
Enter receive state and wait for ST3 period
804
Is WIR_ENQ packet received?
806
NO
YES
Is WIR_ENQ packet valid?
808
YES
NO
Enter transmit state
820
Transmit WIR_RESP packet of ST4 period
822
Increment WIR_NEG_ENQ counter by one
810
Enter idle state
816
Is WIR_NEG_ENQ counter ≥ WIR_NEG_ ENQ limit?
812
NO
Wait for ST5 period
818
YES
Go to OOR mode
814
STOP

FIG. 8

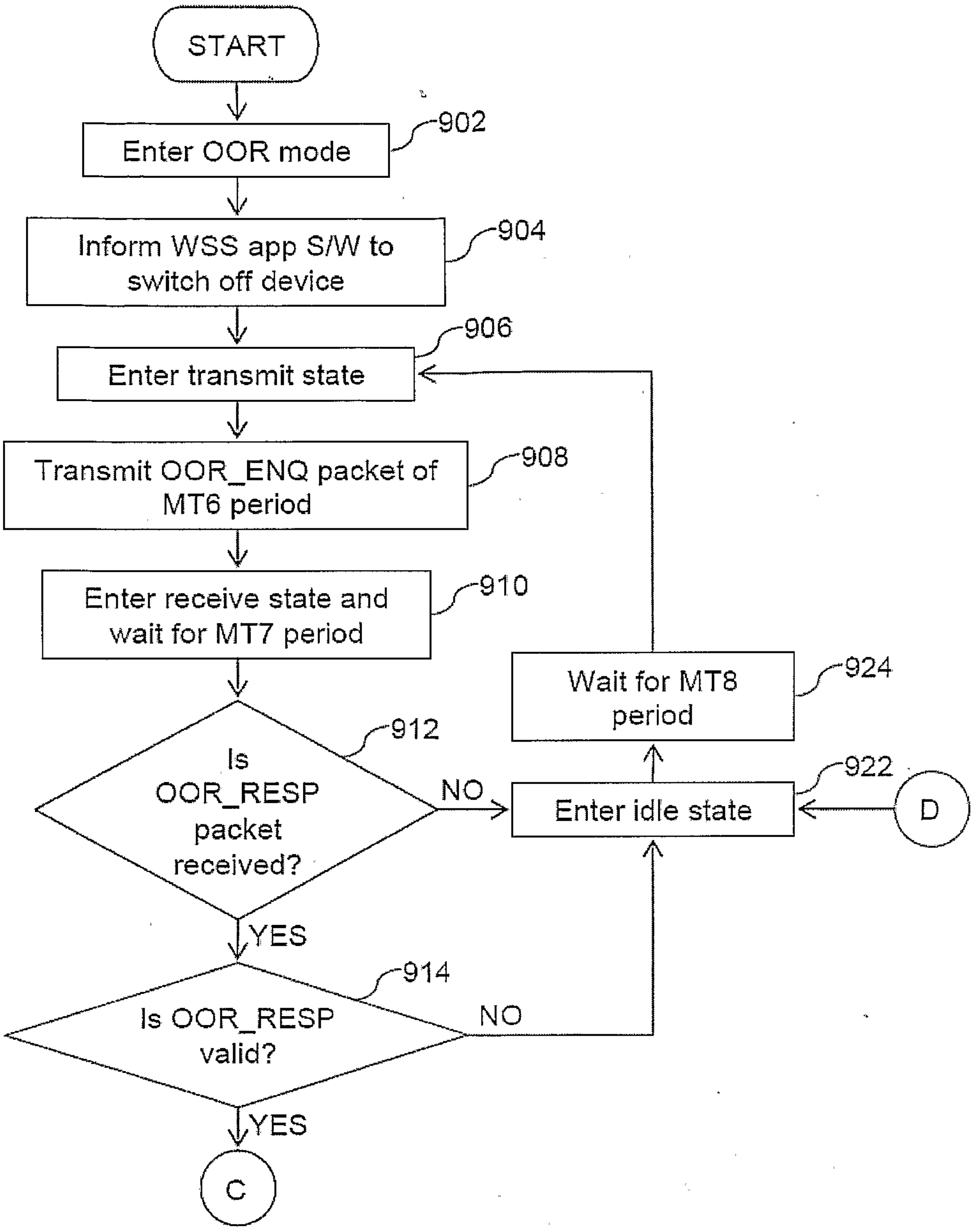
START
Enter OOR mode
902
Inform WSS app S/W to switch off device
904
Enter transmit state
906
Transmit OOR_ENQ packet of MT6 period
908
Enter receive state and wait for MT7 period
910
Is OOR_RESP packet received?
912
NO
YES
Is OOR_RESP valid?
914
NO
YES
C
Wait for MT8 period
924
Enter idle state
922
D

FIG. 9

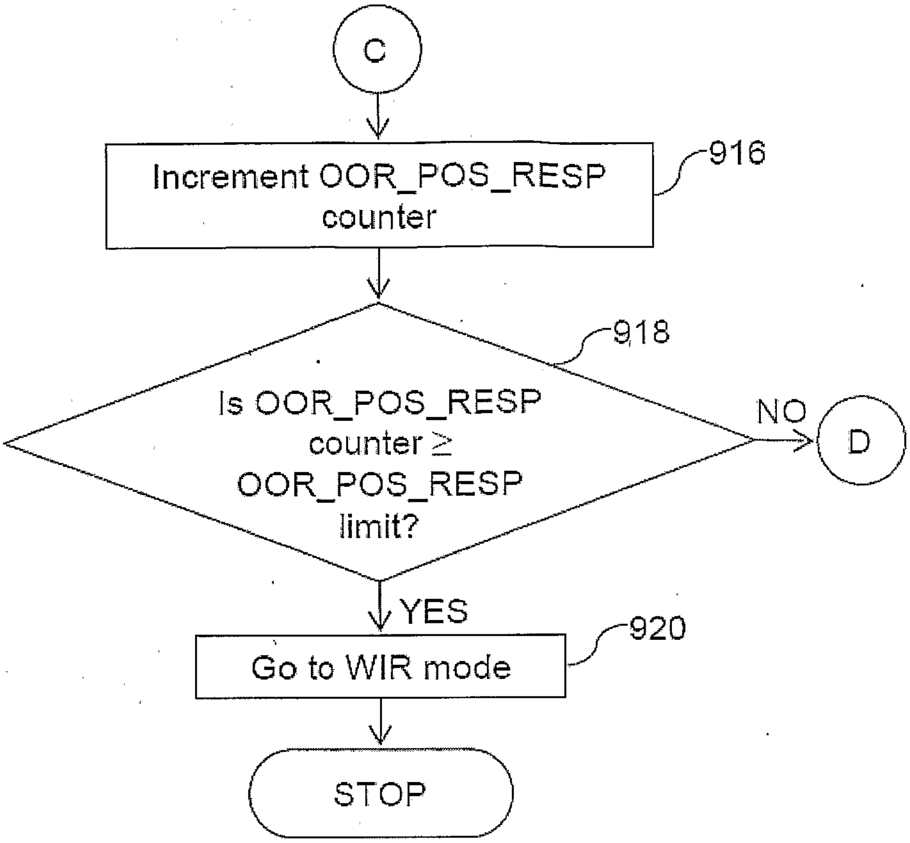
C
Increment OOR_POS_RESP counter
916
Is OOR_POS_RESP counter ≥ OOR_POS_RESP limit?
918
NO
D
YES
Go to WIR mode
920
STOP

FIG. 9B

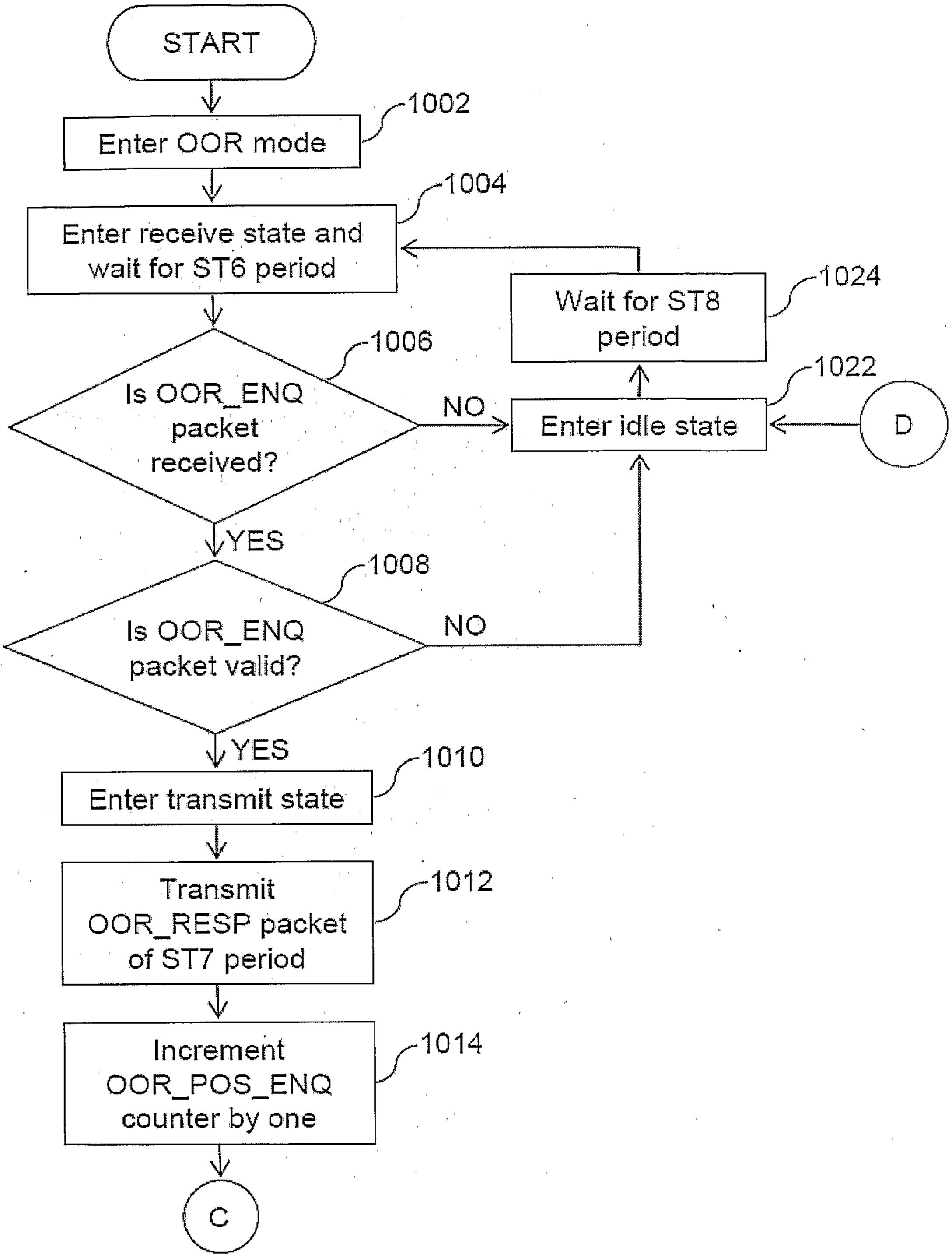
START
Enter OOR mode
1002
Enter receive state and wait for ST6 period
1004
Is OOR_ENQ packet received?
1006
NO
YES
Enter idle state
1022
D
Wait for ST8 period
1024
Is OOR_ENQ packet valid?
1008
NO
YES
Enter transmit state
1010
Transmit OOR_RESP packet of ST7 period
1012
Increment OOR_POS_ENQ counter by one
1014
C

FIG. 10A

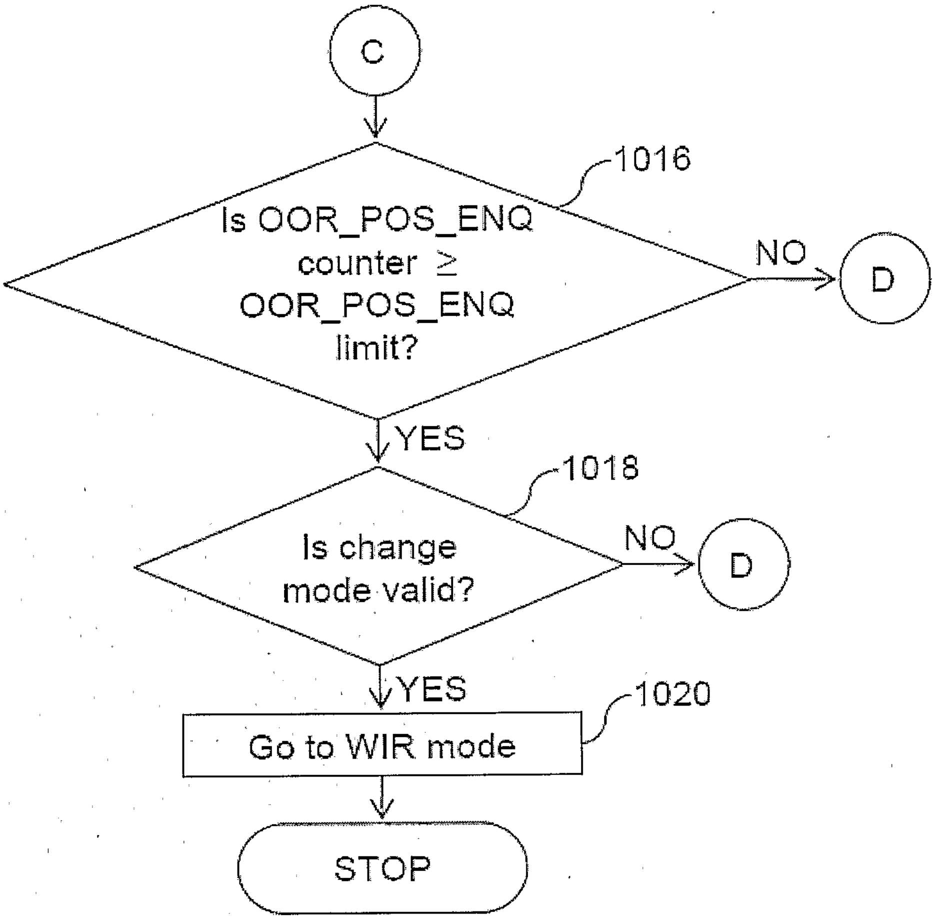
C
Is OOR_POS_ENQ counter ≥ OOR_POS_ENQ limit?
1016
NO
D
YES
1018
Is change mode valid?
NO
D
YES
1020
Go to WIR mode
STOP

FIG. 10B

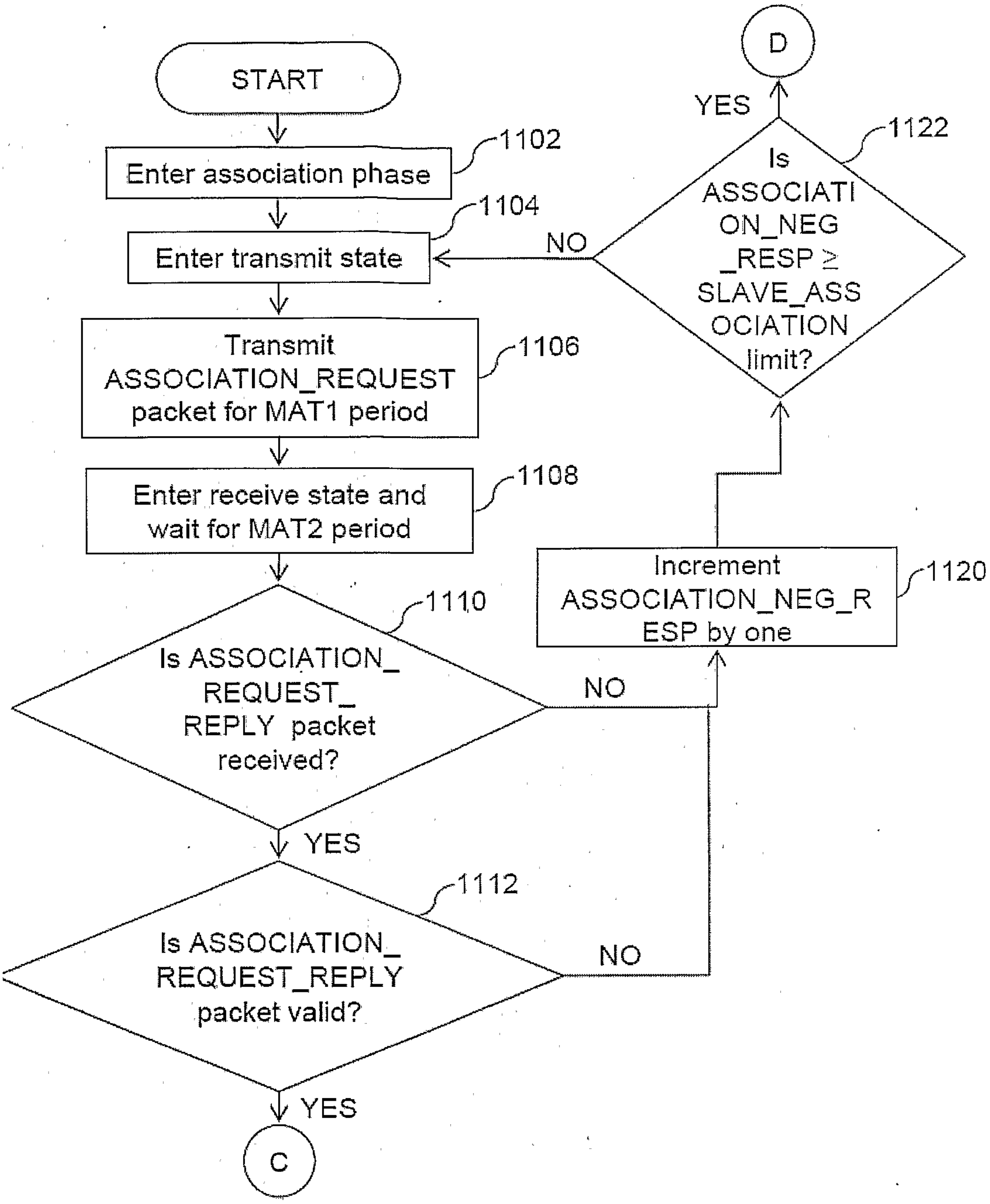
START
Enter association phase
1102
Enter transmit state
1104
Transmit ASSOCIATION_REQUEST packet for MAT1 period
1106
Enter receive state and wait for MAT2 period
1108
Is ASSOCIATION_REQUEST_REPLY packet received?
1110
YES
NO
Is ASSOCIATION_REQUEST_REPLY packet valid?
1112
YES
NO
C
Increment ASSOCIATION_NEG_RESP by one
1120
Is ASSOCIATION_NEG_RESP ≥ SLAVE_ASSOCIATION limit?
1122
YES
NO
D

FIG. 11A

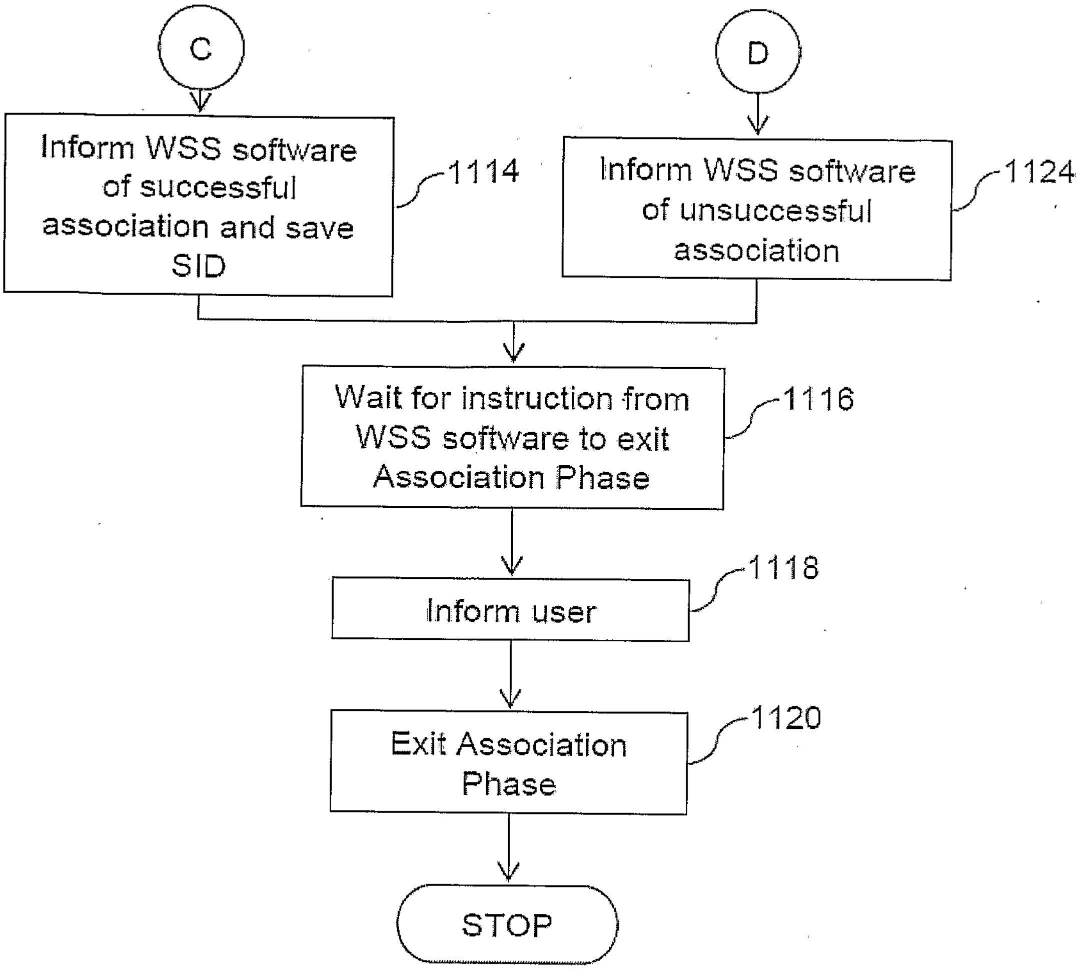
C
D
Inform WSS software of successful association and save SID
1114
Inform WSS software of unsuccessful association
1124
Wait for instruction from WSS software to exit Association Phase
1116
Inform user
1118
Exit Association Phase
1120
STOP

FIG. 11B

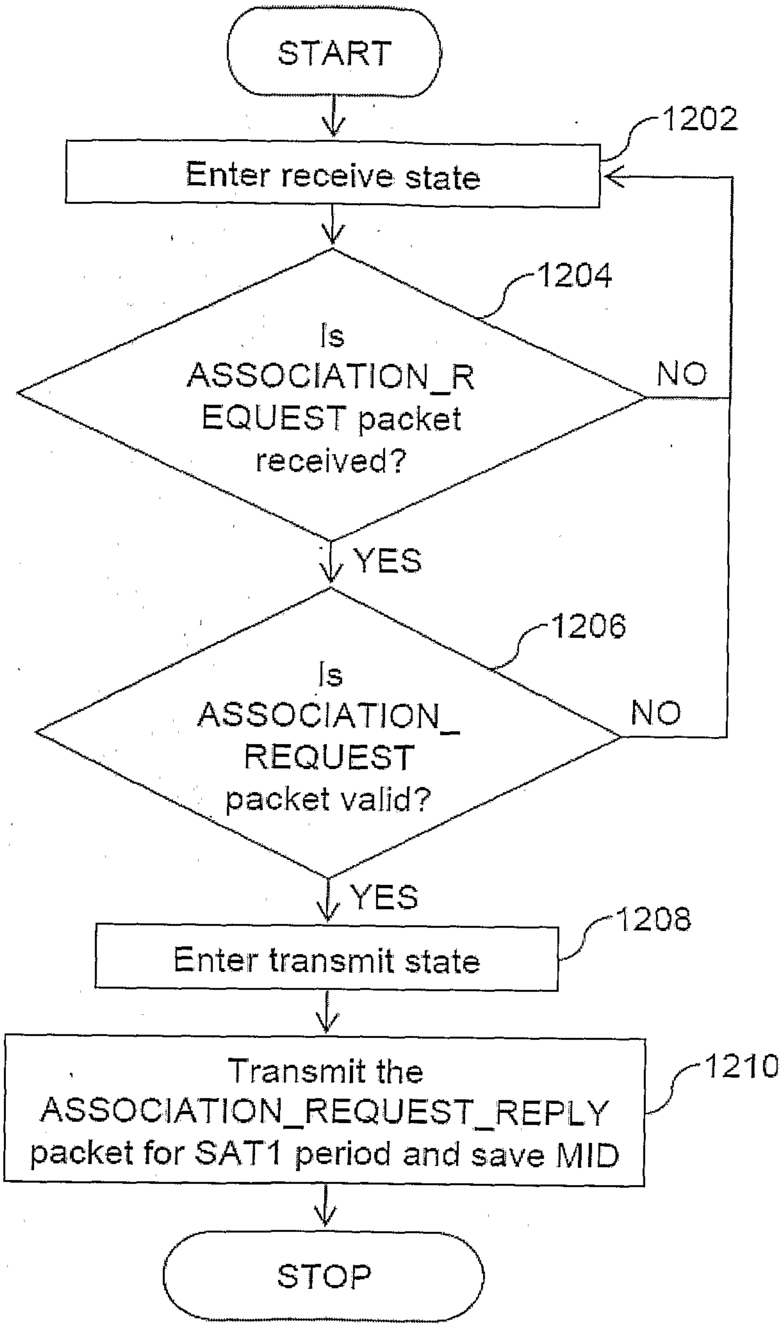
START
Enter receive state
1202
Is ASSOCIATION_R EQUEST packet received?
1204
NO
YES
Is ASSOCIATION_ REQUEST packet valid?
1206
NO
YES
Enter transmit state
1208
Transmit the ASSOCIATION_REQUEST_REPLY packet for SAT1 period and save MID
1210
STOP

FIG. 12

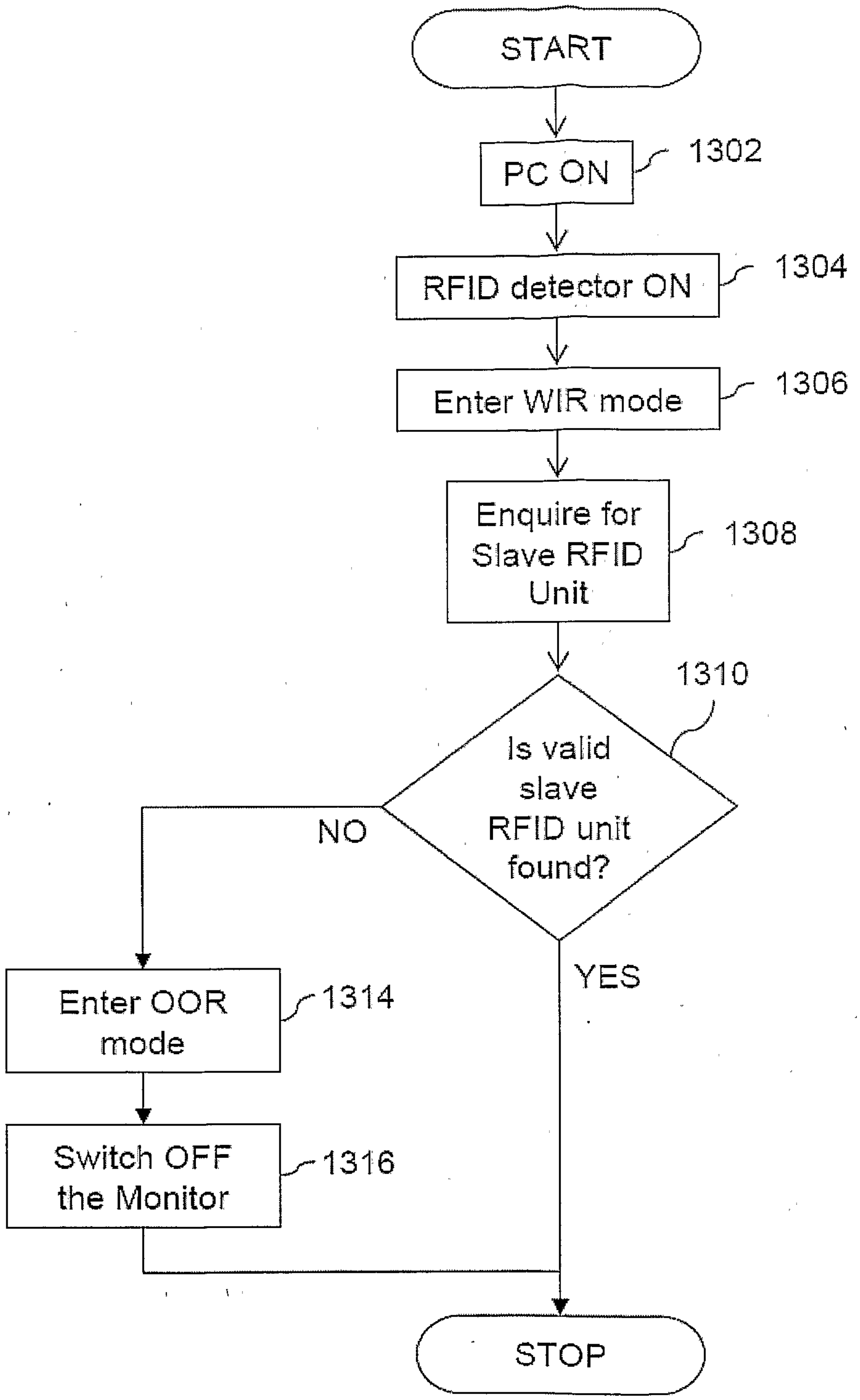
START
PC ON
1302
RFID detector ON
1304
Enter WIR mode
1306
Enquire for Slave RFID Unit
1308
1310
Is valid slave RFID unit found?
NO
YES
Enter OOR mode
1314
Switch OFF the Monitor
1316
STOP

FIG.13

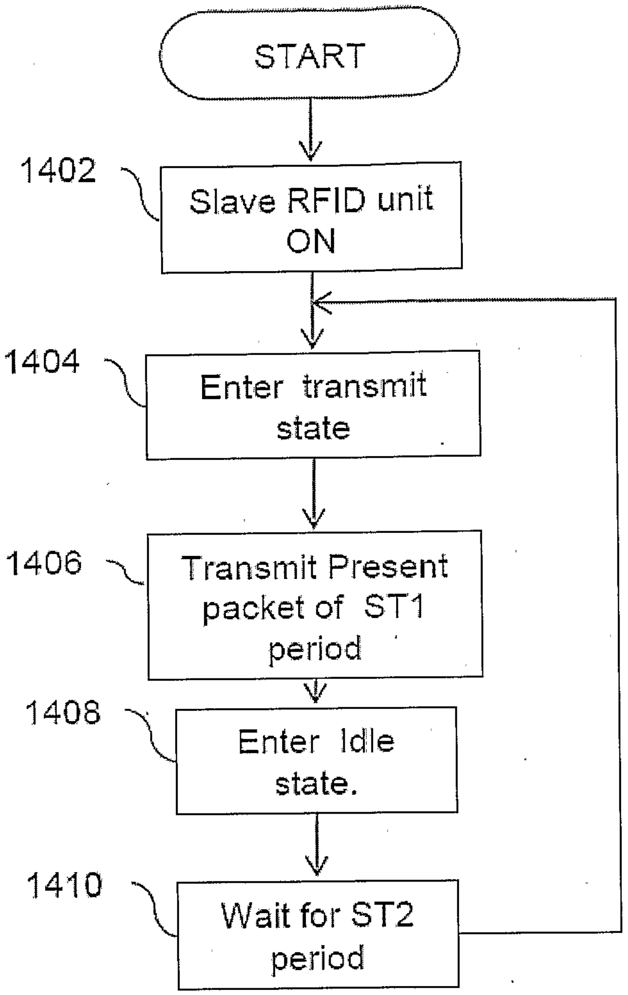
START
1402
Slave RFID unit ON
1404
Enter transmit state
1406
Transmit Present packet of ST1 period
1408
Enter Idle state.
1410
Wait for ST2 period

FIG. 14

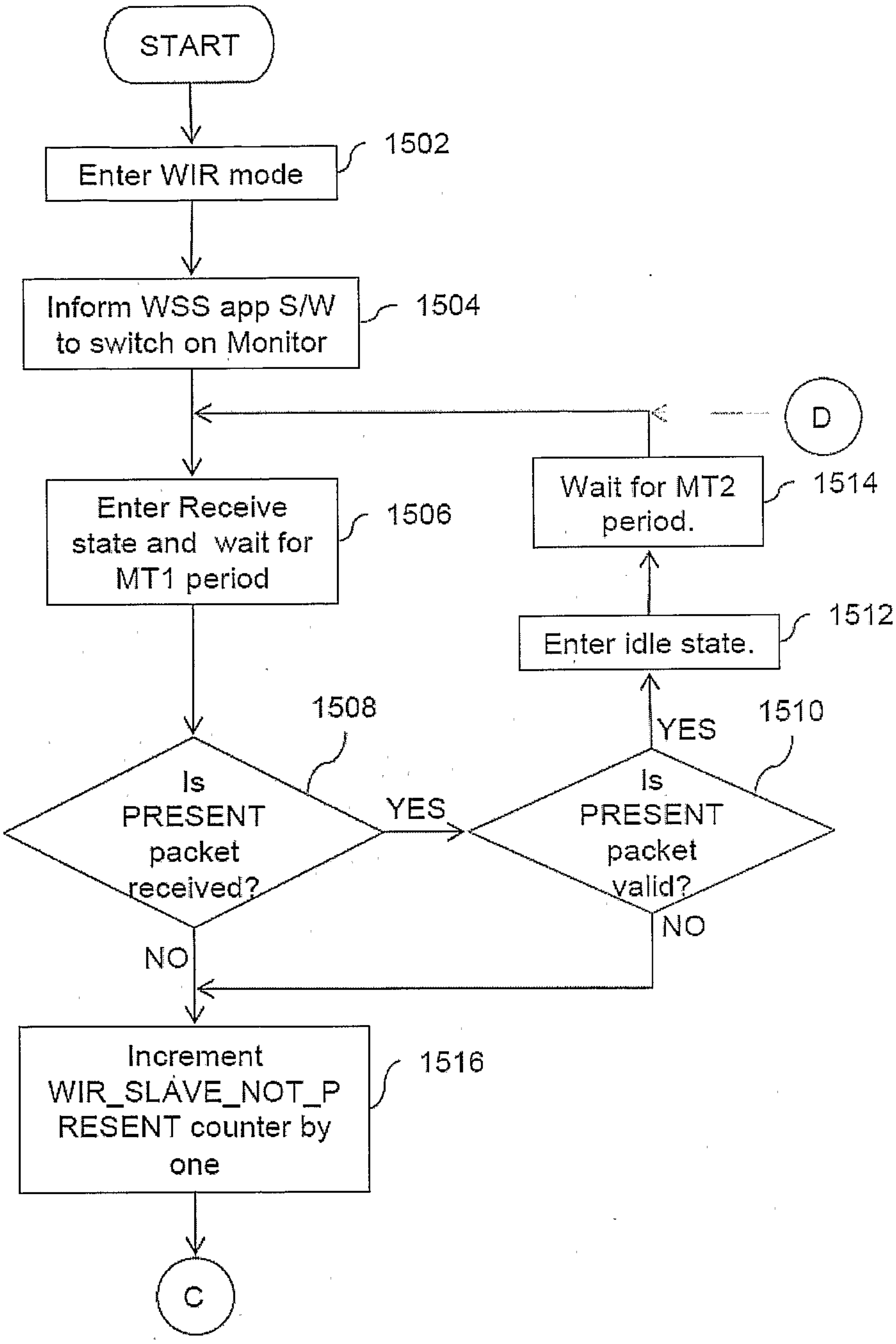
START
Enter WIR mode
1502
Inform WSS app S/W to switch on Monitor
1504
D
Wait for MT2 period.
1514
Enter Receive state and wait for MT1 period
1506
Enter idle state.
1512
1508
YES
1510
Is PRESENT packet received?
YES
Is PRESENT packet valid?
NO
NO
Increment WIR_SLAVE_NOT_PRESENT counter by one
1516
C

FIG. 15A

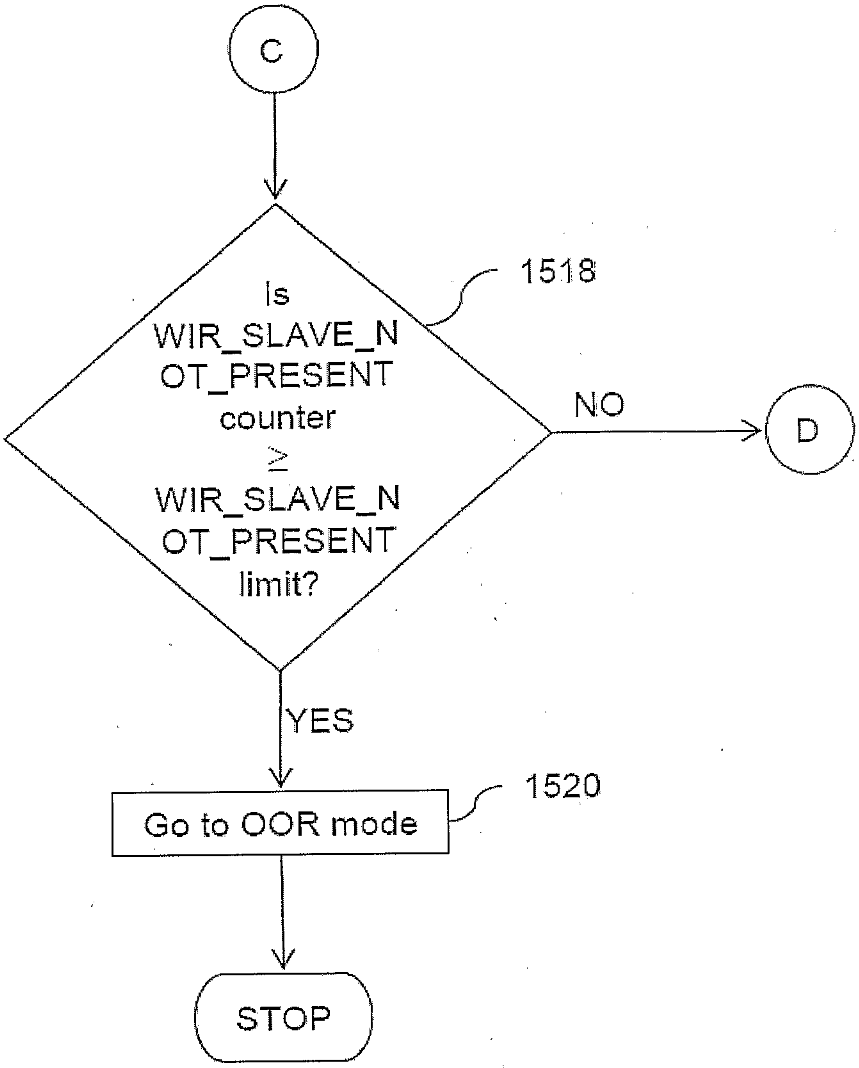
C
Is WIR_SLAVE_NOT_PRESENT counter ≥ WIR_SLAVE_NOT_PRESENT limit?
1518
NO
D
YES
Go to OOR mode
1520
STOP

FIG. 15B

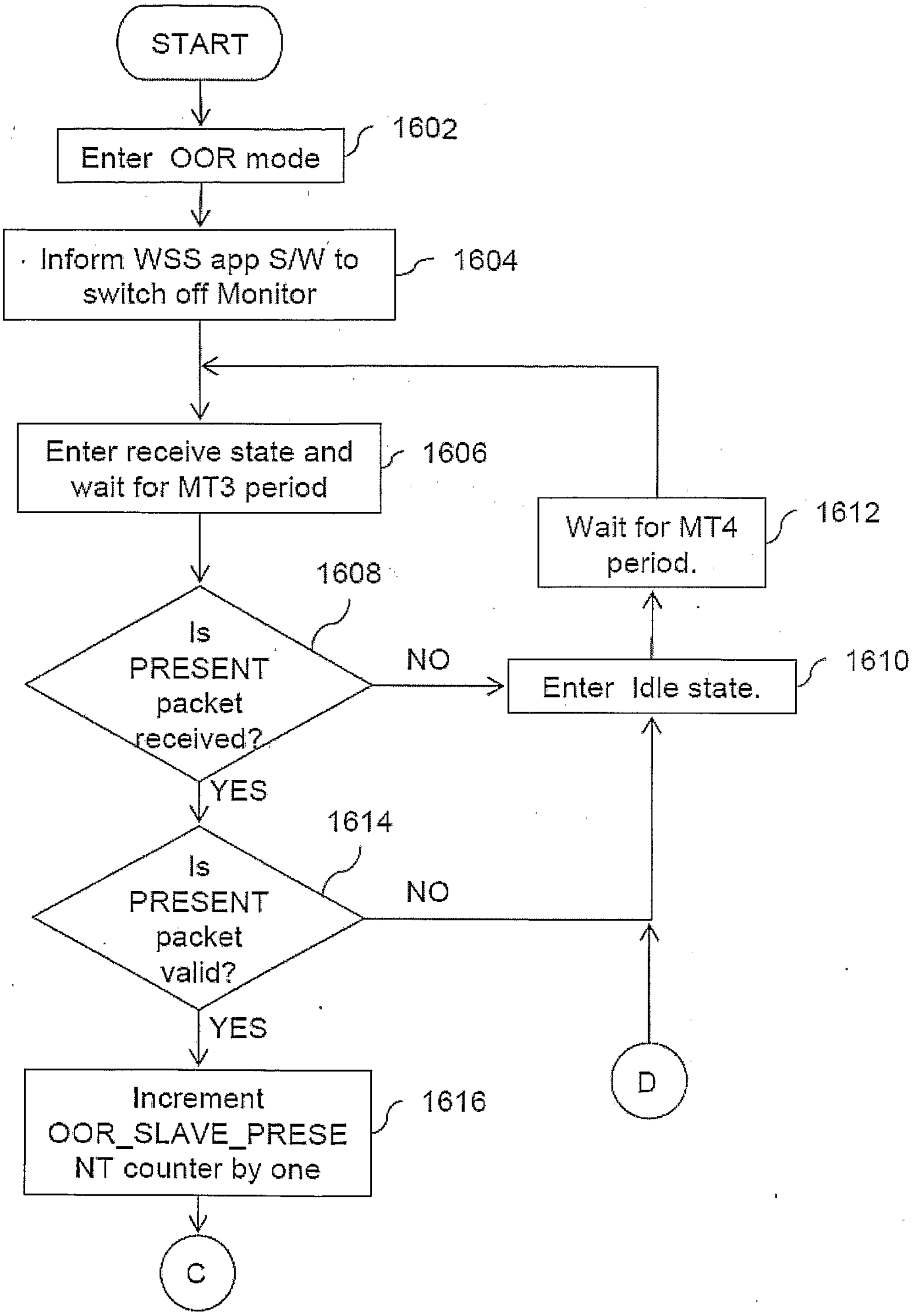
START
Enter OOR mode
1602
Inform WSS app S/W to switch off Monitor
1604
Enter receive state and wait for MT3 period
1606
Is PRESENT packet received?
1608
NO
YES
Enter Idle state.
1610
Wait for MT4 period.
1612
Is PRESENT packet valid?
1614
NO
YES
Increment OOR_SLAVE_PRESENT counter by one
1616
C
D

FIG. 16A

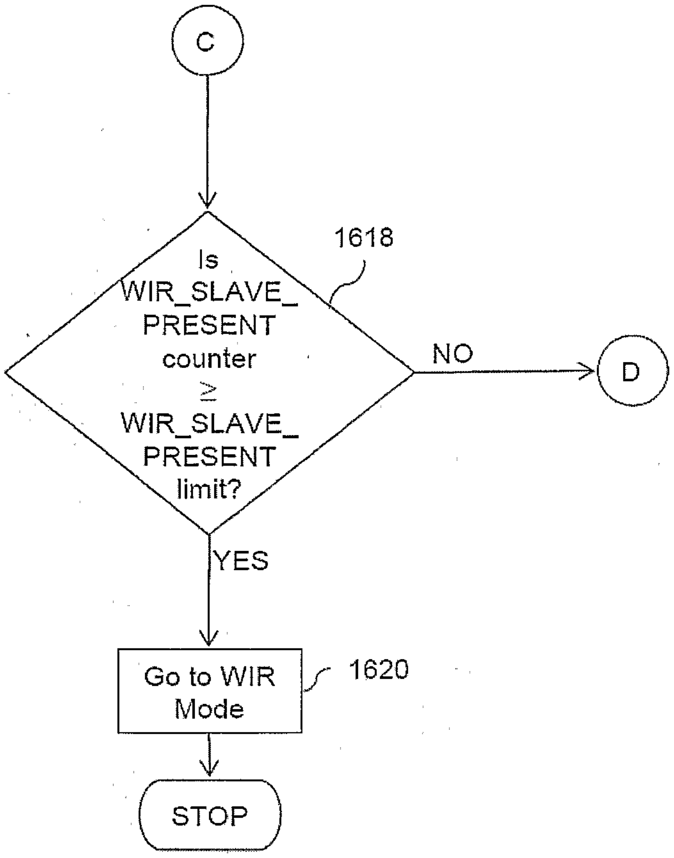
C
Is WIR_SLAVE_ PRESENT counter ≥ WIR_SLAVE_ PRESENT limit?
1618
NO
D
YES
Go to WIR Mode
1620
STOP

FIG. 16B

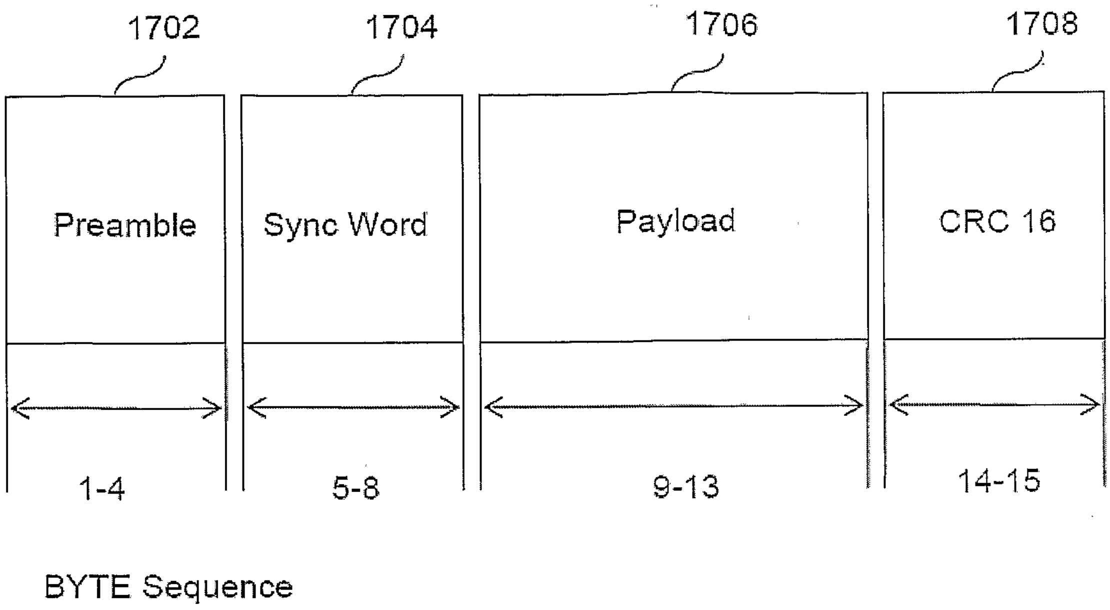
1702
1704
1706
1708
Preamble
Sync Word
Payload
CRC 16
1-4
5-8
9-13
14-15
BYTE Sequence

FIG. 17

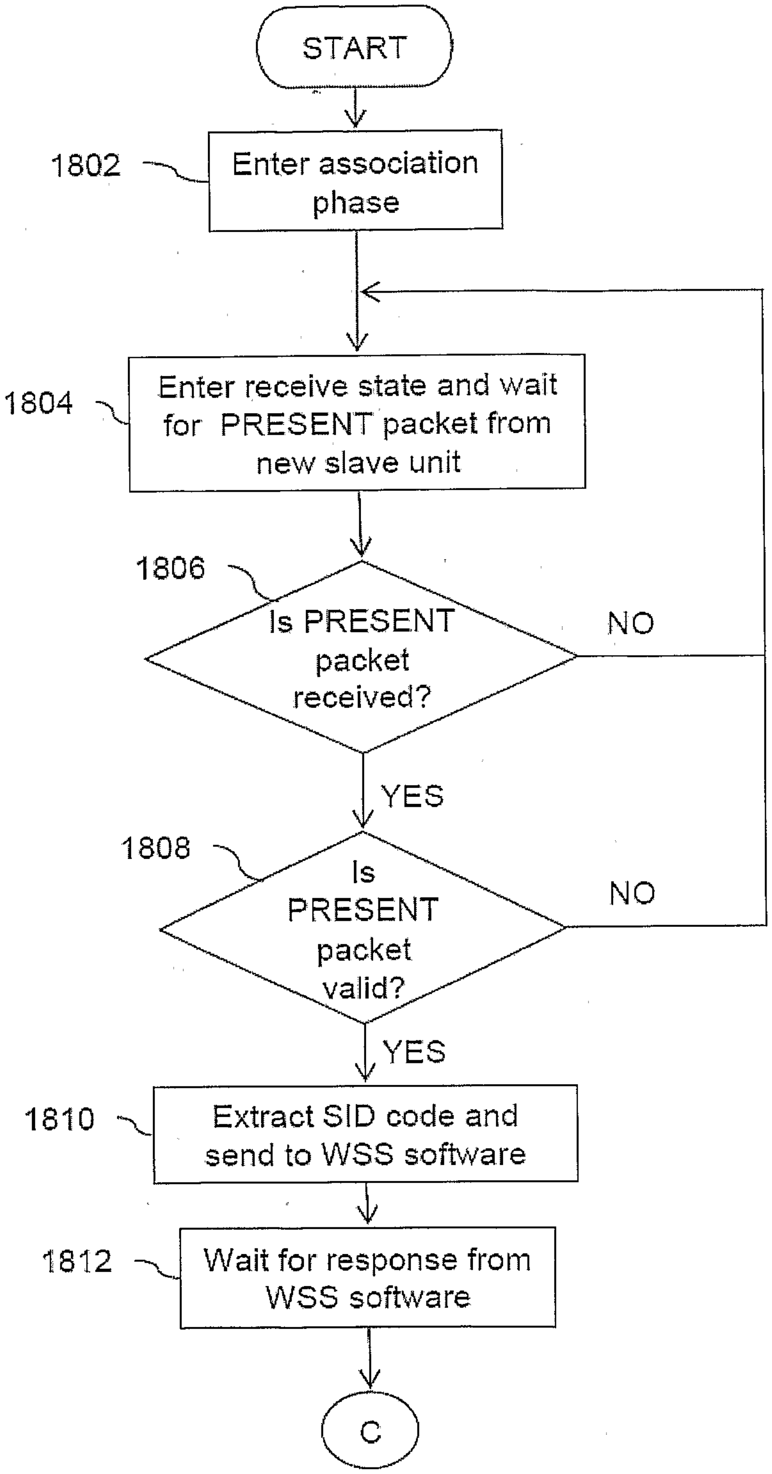
START
1802
Enter association phase
1804
Enter receive state and wait for PRESENT packet from new slave unit
1806
Is PRESENT packet received?
NO
YES
1808
Is PRESENT packet valid?
NO
YES
1810
Extract SID code and send to WSS software
1812
Wait for response from WSS software
C

FIG. 18A

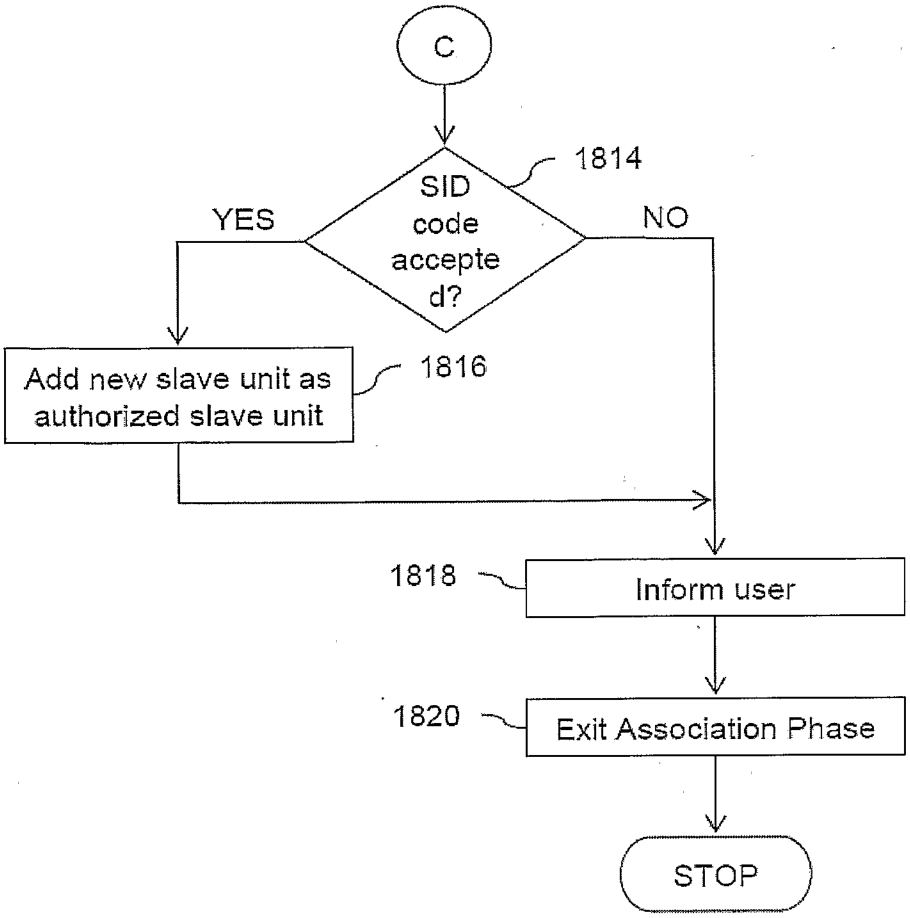
C
SID code accepte d?
1814
YES
NO
Add new slave unit as authorized slave unit
1816
1818
Inform user
1820
Exit Association Phase
STOP

FIG. 18B

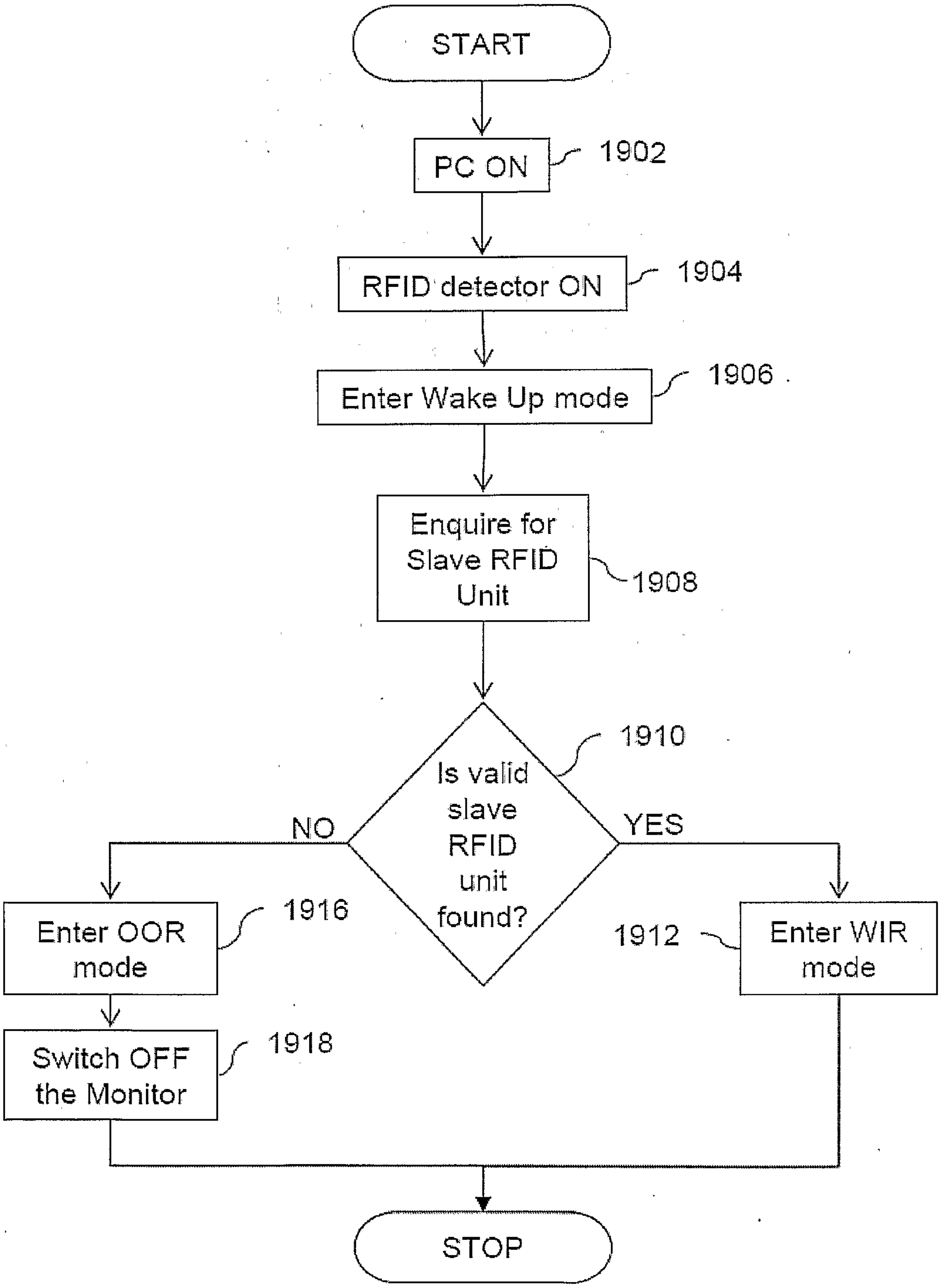
START
PC ON
1902
RFID detector ON
1904
Enter Wake Up mode
1906
Enquire for Slave RFID Unit
1908
Is valid slave RFID unit found?
1910
NO
YES
Enter OOR mode
1916
Switch OFF the Monitor
1918
1912
Enter WIR mode
STOP

FIG. 19

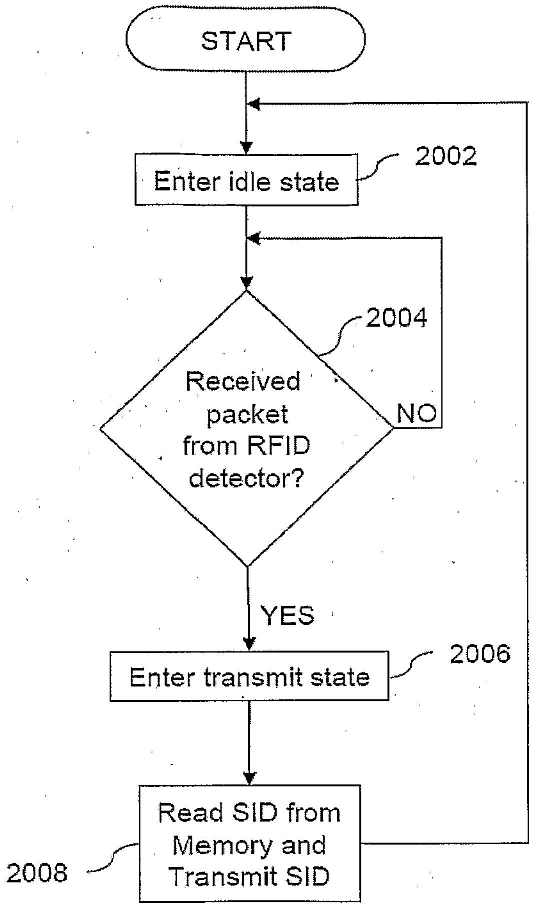
START
Enter idle state
2002
Received packet from RFID detector?
2004
NO
YES
Enter transmit state
2006
Read SID from Memory and Transmit SID
2008

FIG. 20

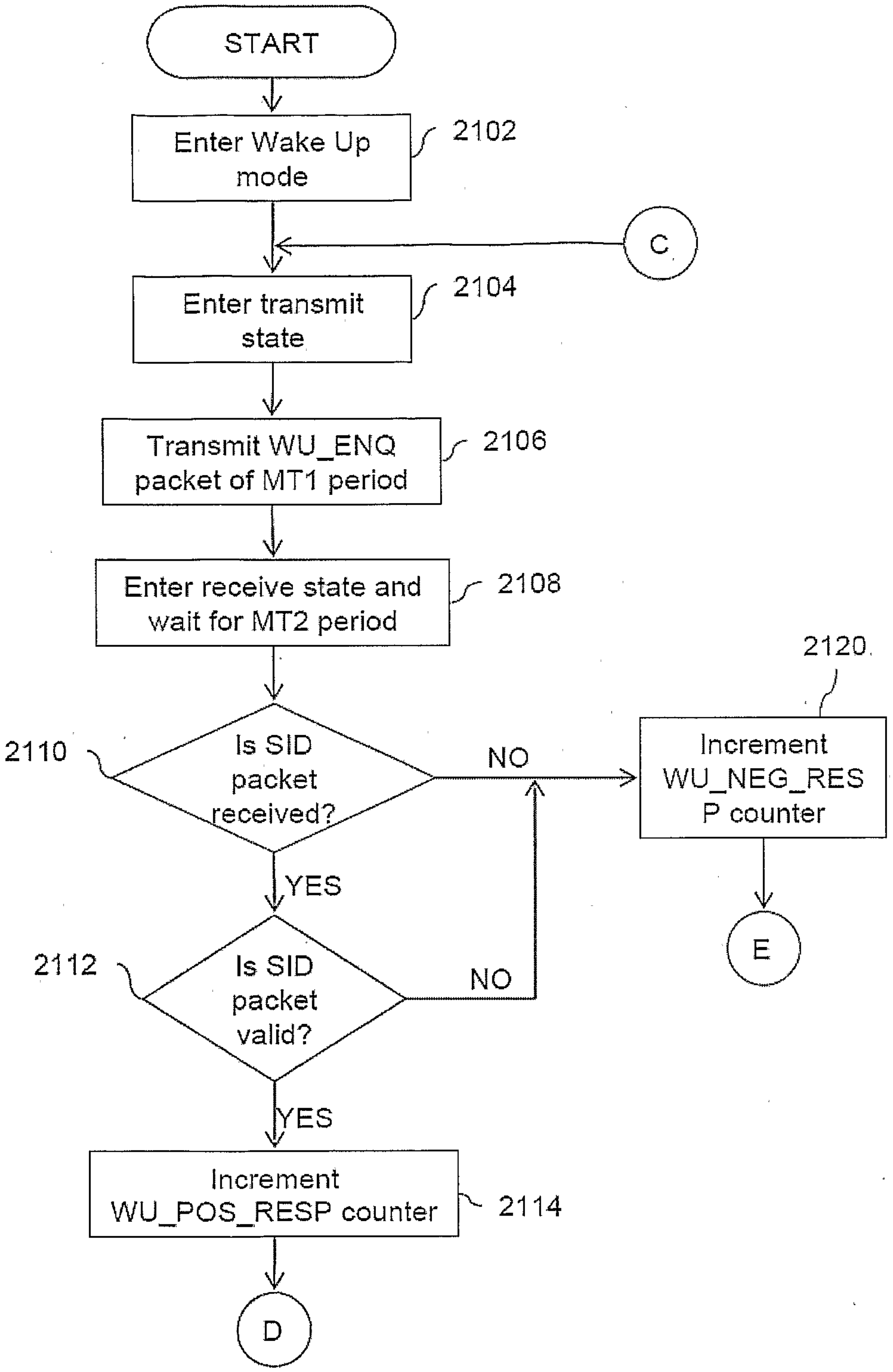
START
Enter Wake Up mode
2102
C
Enter transmit state
2104
Transmit WU_ENQ packet of MT1 period
2106
Enter receive state and wait for MT2 period
2108
2120
2110
Is SID packet received?
NO
Increment WU_NEG_RESP counter
YES
E
2112
Is SID packet valid?
NO
YES
Increment WU_POS_RESP counter
2114
D

FIG. 21A

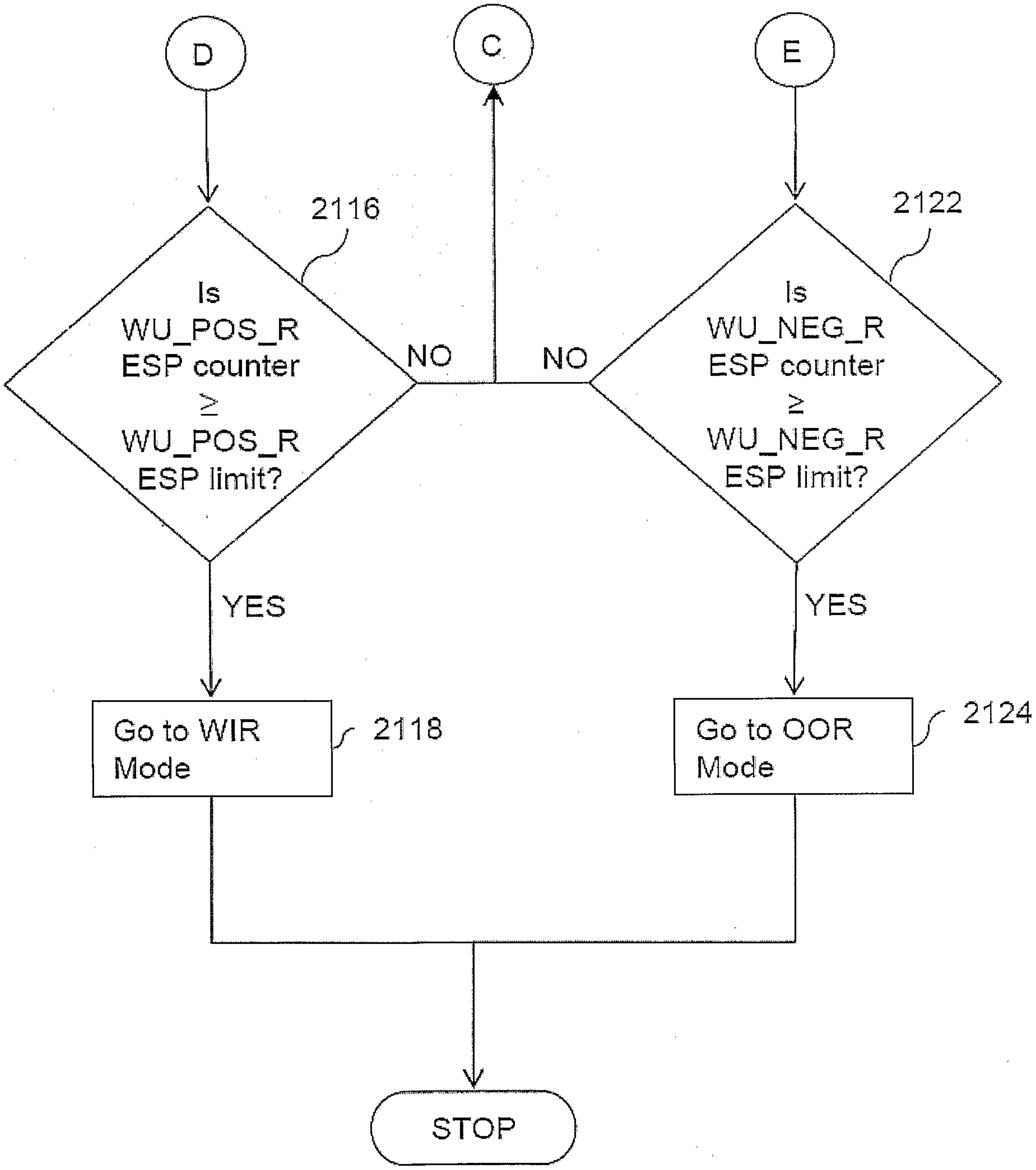
D
C
E
2116
Is
WU_POS_R
ESP counter
≥
WU_POS_R
ESP limit?
NO
NO
2122
Is
WU_NEG_R
ESP counter
≥
WU_NEG_R
ESP limit?
YES
YES
Go to WIR
Mode
2118
Go to OOR
Mode
2124
STOP

FIG. 21B

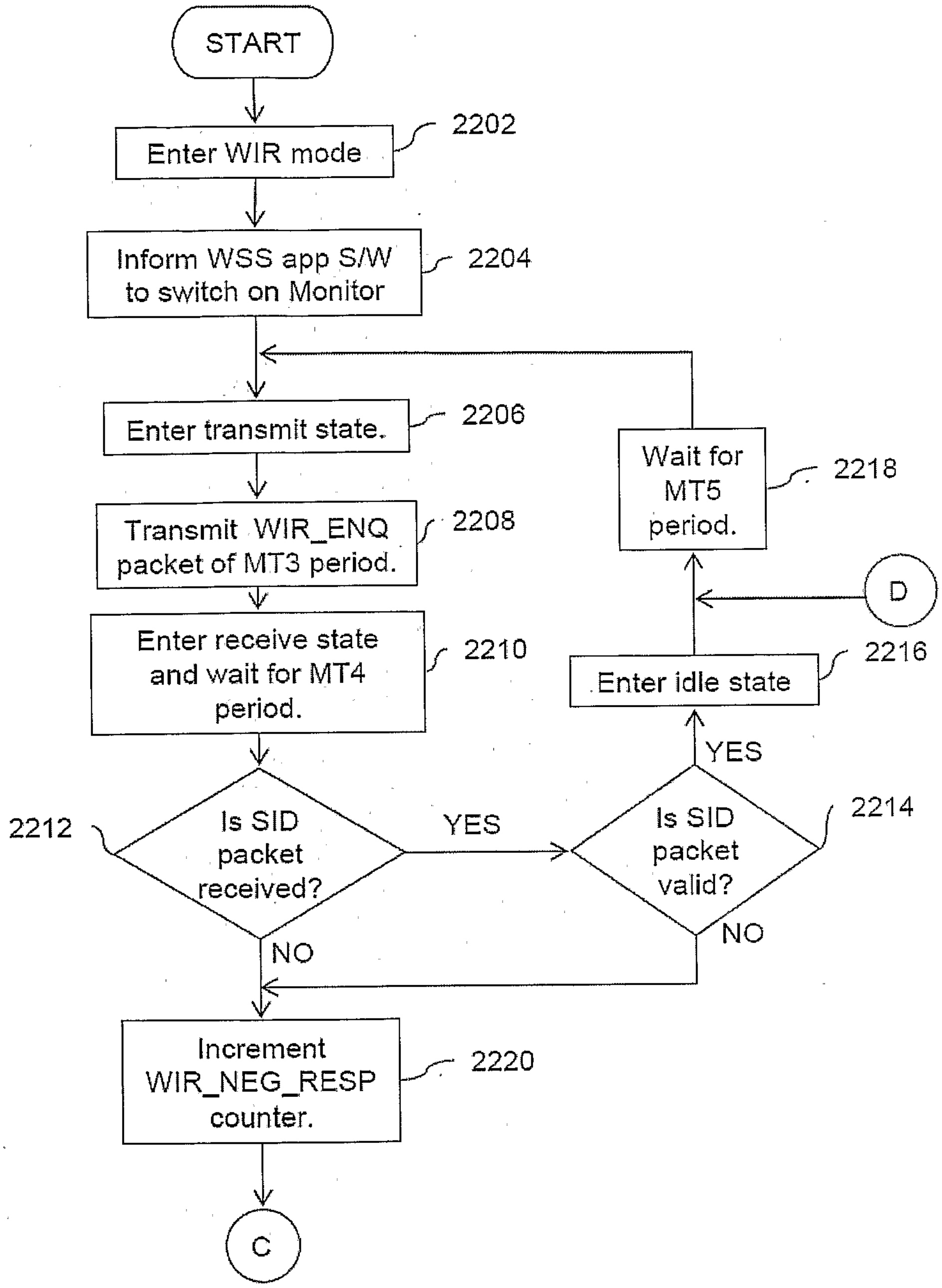
START
Enter WIR mode
2202
Inform WSS app S/W to switch on Monitor
2204
Enter transmit state.
2206
Transmit WIR_ENQ packet of MT3 period.
2208
Enter receive state and wait for MT4 period.
2210
2212
Is SID packet received?
YES
NO
Is SID packet valid?
2214
YES
NO
Enter idle state
2216
D
Wait for MT5 period.
2218
Increment WIR_NEG_RESP counter.
2220
C

FIG. 22A

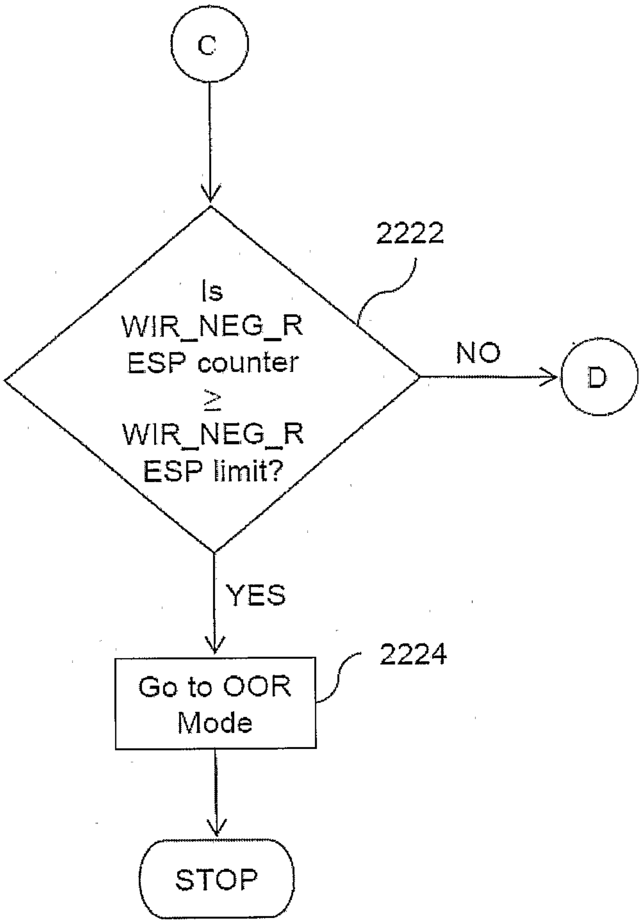
C
2222
Is
WIR_NEG_R
ESP counter
≥
WIR_NEG_R
ESP limit?
NO
D
YES
2224
Go to OOR
Mode
STOP

FIG. 22B

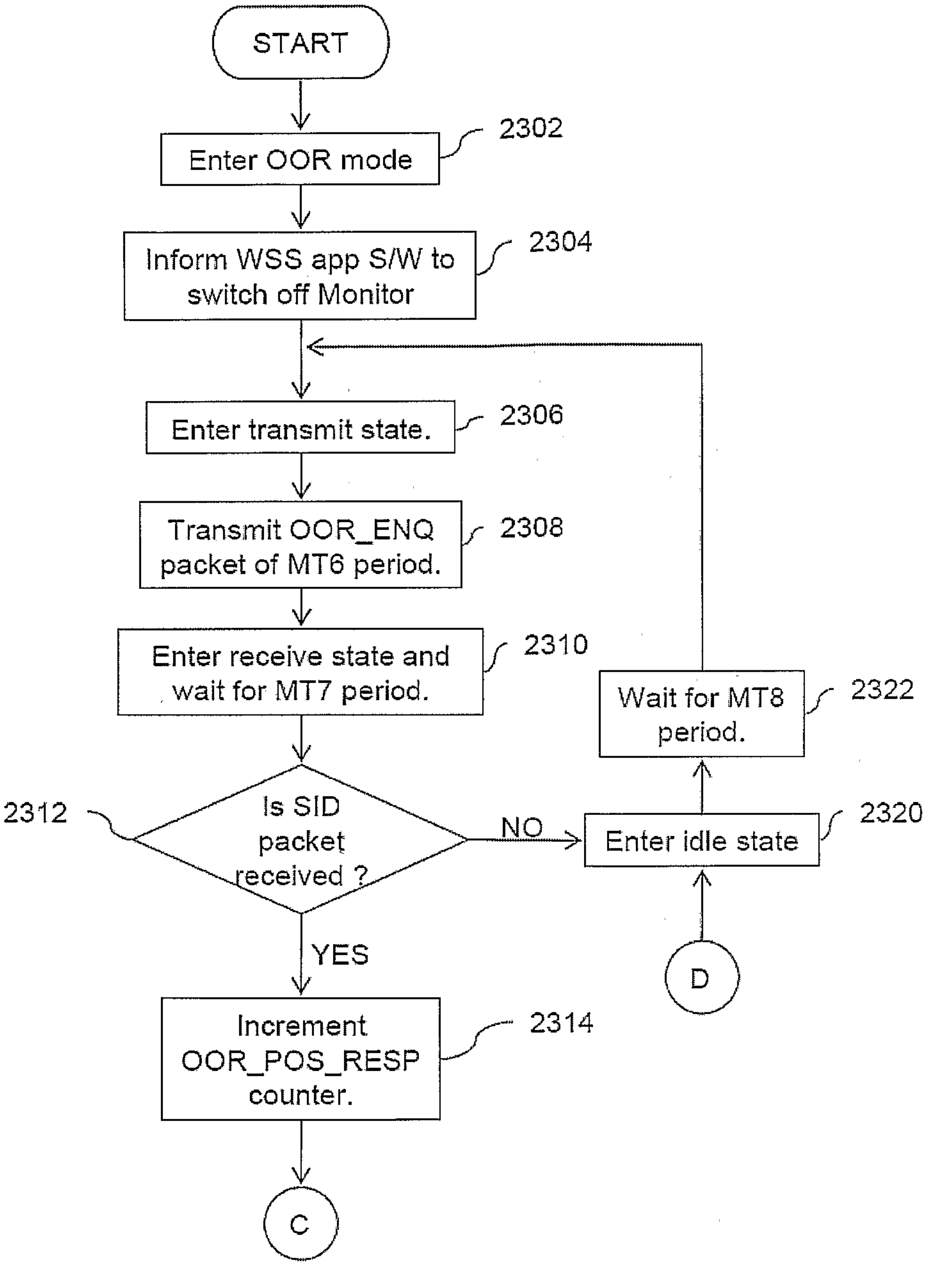
START
Enter OOR mode
2302
Inform WSS app S/W to switch off Monitor
2304
Enter transmit state.
2306
Transmit OOR_ENQ packet of MT6 period.
2308
Enter receive state and wait for MT7 period.
2310
Wait for MT8 period.
2322
2312
Is SID packet received ?
NO
Enter idle state
2320
YES
D
Increment OOR_POS_RESP counter.
2314
C

FIG. 23A

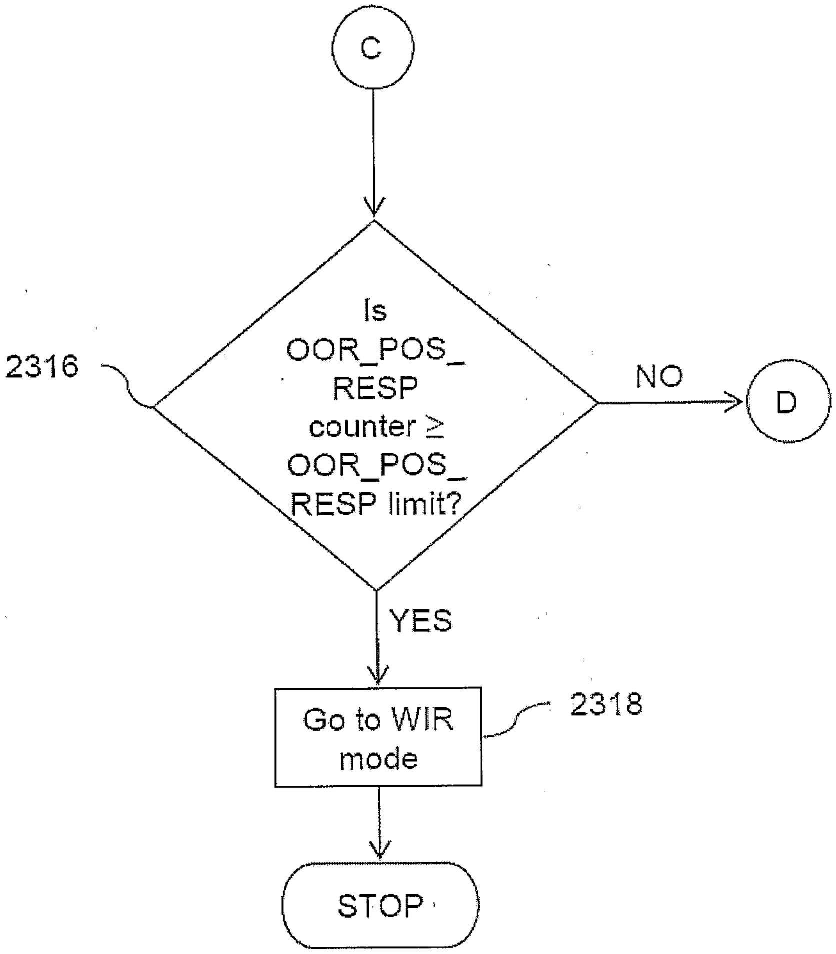
C
Is OOR_POS_RESP counter ≥ OOR_POS_RESP limit?
2316
NO
D
YES
Go to WIR mode
2318
STOP

FIG. 23B

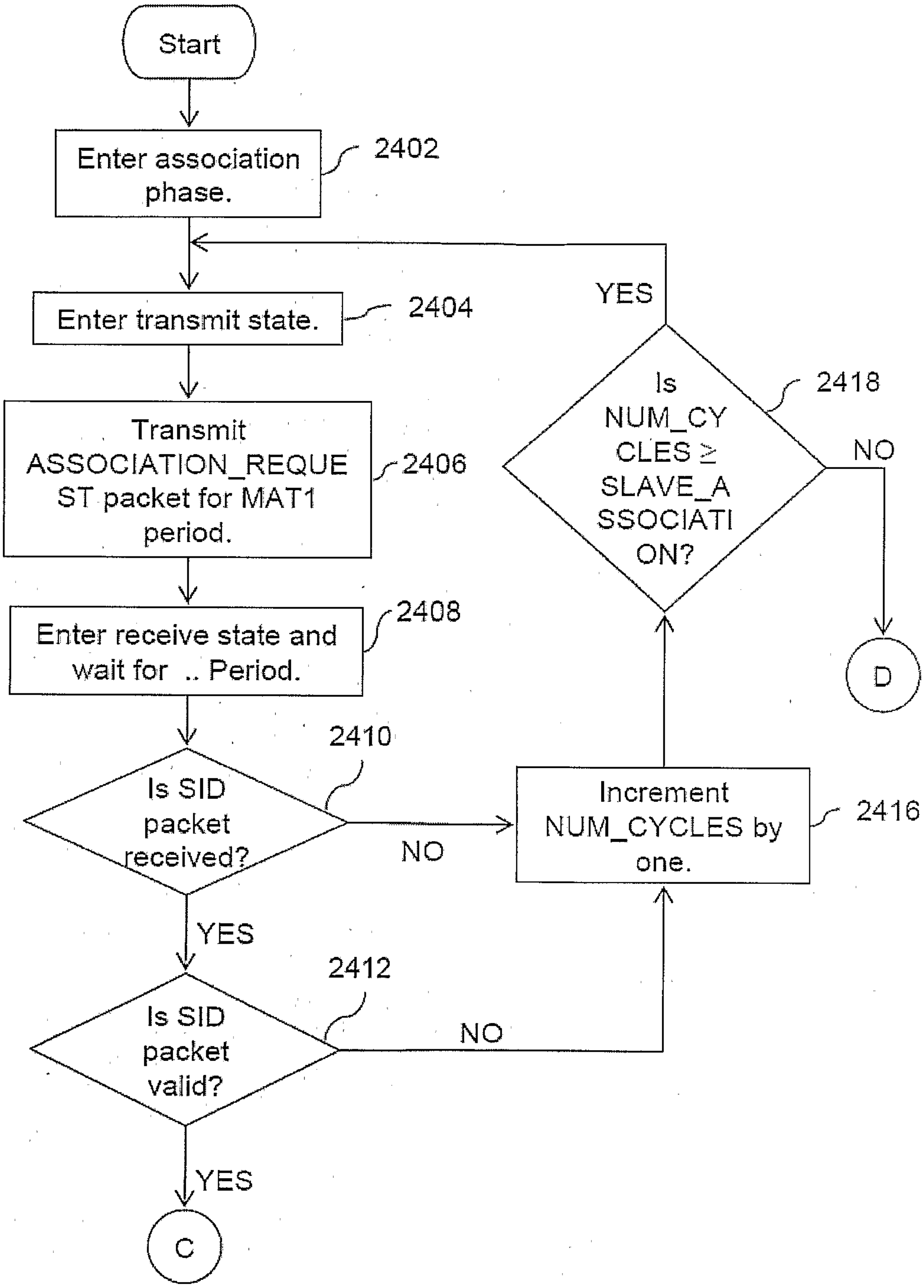
Start
Enter association phase.
2402
Enter transmit state.
2404
Transmit ASSOCIATION_REQUEST packet for MAT1 period.
2406
Enter receive state and wait for .. Period.
2408
Is SID packet received?
2410
NO
YES
Is SID packet valid?
2412
NO
YES
C
Increment NUM_CYCLES by one.
2416
Is NUM_CYCLES ≥ SLAVE_ASSOCIATION?
2418
YES
NO
D

FIG. 24A

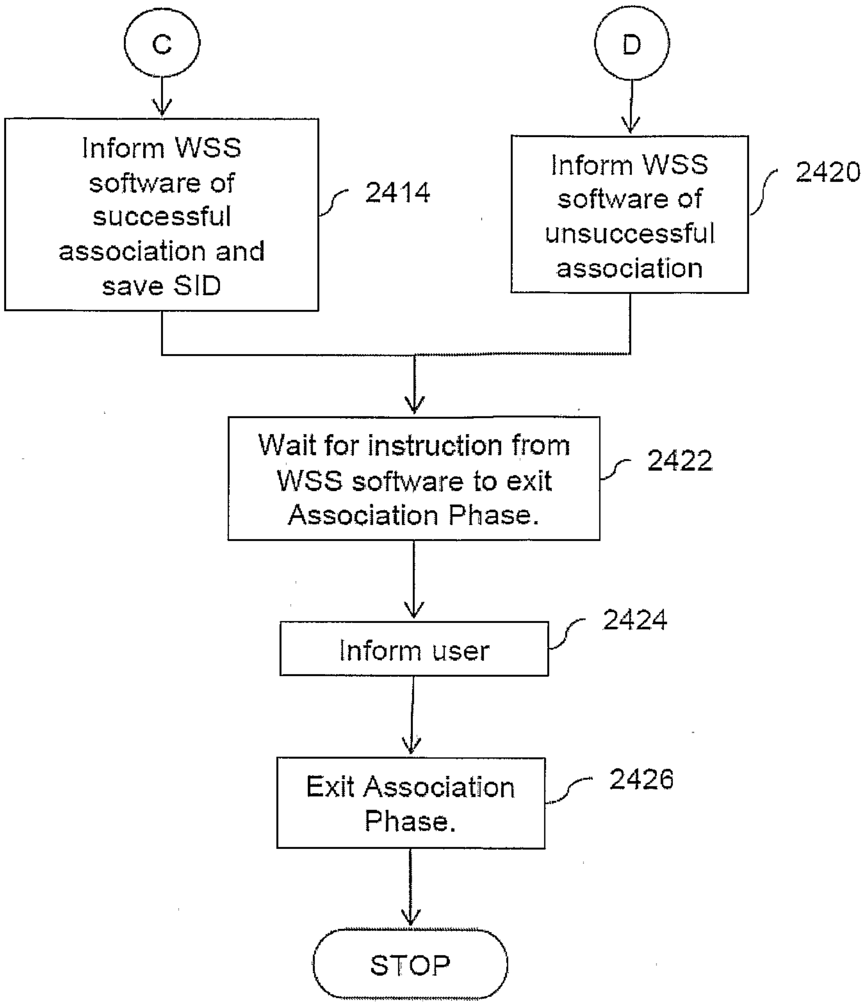
C
D
Inform WSS software of successful association and save SID
2414
Inform WSS software of unsuccessful association
2420
Wait for instruction from WSS software to exit Association Phase.
2422
Inform user
2424
Exit Association Phase.
2426
STOP

FIG. 24B