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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 June 2013 (27.06.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/096690 Al

(51) **International Patent Classification:**
H04L 12/28 (2006.01) ***H04L 29/06*** (2006.01)

(21) **International Application Number:**
PCT/US20 12/07 1077

(22) **International Filing Date:**
20 December 2012 (20. 12.2012)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
13/335,722 22 December 201 1 (22. 12.201 1) US
61/603,1 12 24 February 2012 (24.02.2012) US

(71) **Applicant: SILVER SPRING NETWORKS, INC.** [US/US]; 555 Broadway Street, Redwood City, California 94063 (US).

(72) **Inventors: FLAMMER, George H., Ill;** 575 Broadway Street, Redwood City, California 94063 (US). **DOYLE, John;** 575 Broadway Street, Redwood City, California 94063 (US). **HUGHES, Sterling;** 575 Broadway Street, Redwood City, California 94063 (US).

(74) **Agents: CAREY, John C.** et al; Patterson & Sheridan, LLP, 3040 Post Oak Blvd., Suite 1500, Houston, Texas 77056 (US).

(81) **Designated States** ***(unless otherwise indicated, for every kind of national protection available):*** AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** ***(unless otherwise indicated, for every kind of regional protection available):*** ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,

[Continued on nextpage]

(54) **Title:** SYSTEM AND METHOD FOR PROVIDING METERING DATA

(57) **Abstract:** One embodiment of the present invention sets forth a technique for efficiently interconnecting interrogator elements. The interrogator elements are configured to perform a read or write data operation to a second interrogator element. Two-way communications between interrogator elements is facilitated by read and write operations in this way. A data backhaul network may be advantageously implemented as a wireless mesh network, comprising a plurality of interrogator elements, to transmit data from each interrogator element to a server for processing. Transmitted data may be metering data.

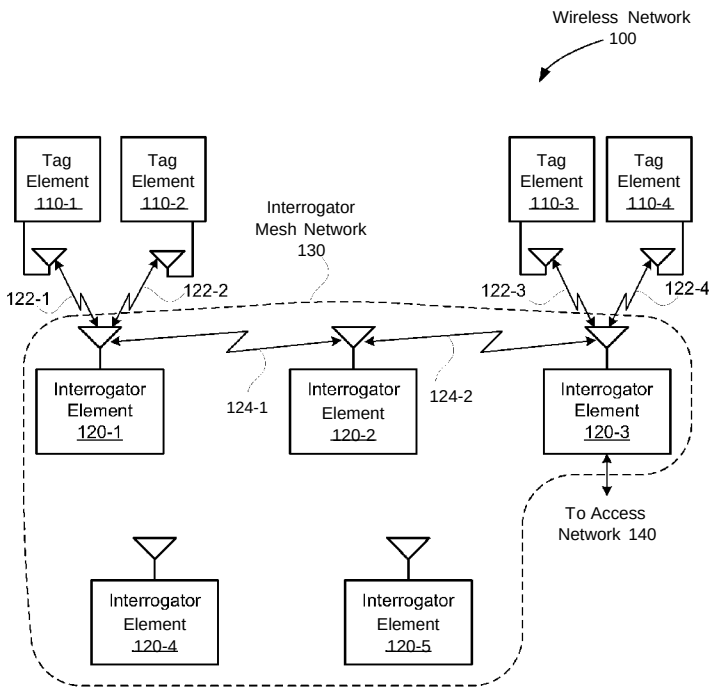

Figure 1A

WO 2013/096690 A1

UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

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

SYSTEM AND METHOD FOR PROVIDING METERING DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims benefit of United States patent application serial number 13/335,722, filed December 22, 2011, and United States provisional patent application serial number provisional 61/603,112, filed February 24, 2012, which are hereby incorporated herein by reference.

BACKGROUND

Technical Field

[0002] Embodiments of the present invention relate generally to wireless digital communication systems and, more specifically, to a system and method for providing metering data.

Description of the Related Art

[0003] A radio frequency identifier (RFID) network typically includes a plurality of RFID interrogators, each configured to read data from certain RFID tags that are positioned in sufficiently close proximity. This data is then conventionally transmitted upstream via a backhaul network to a server configured to process the data or log the data for later processing. Each RFID tag is configured to store certain data, which may comprise read-only, writeable, or measured data. For example, an RFID tag may store a product code or serial number for an associated article of manufacture. An RFID interrogator retrieves data stored within the RFID tag via a radio frequency (RF) communication transaction.

[0004] Certain RFID tags are referred to as "passive," and typically derive operating power by harvesting ambient RF energy. When the RFID interrogator attempts to read a passive RFID tag, sufficient ambient RF energy is provided to the passive RFID tag to power up and operate. To transmit stored data to the RFID interrogator, passive RFID tags typically employ backscatter techniques, which modulate reflected RF energy originating from the RFID interrogator. Certain other RFID tags are referred to as "active," and typically derive operating power from a battery or other robust power source. To transmit stored data to the RFID interrogator, active RFID tags typically generate a modulated RF signal. In both cases, the RFID interrogator conventionally

transmits data to the RFID tag, and the RFID tag transmits stored data back to the RFID interrogator. In both cases, RFID interrogators are typically configured to avoid interference with each other, for example by remaining inactive while nearby RFID interrogators transmit RF energy to perform read transactions with associated RFID tags.

[0005] One challenge in deploying an RFID network is implementing the backhaul network, which must be connected to each RFID interrogator. One approach to implementing the backhaul network involves coupling a wired data network, such as a wired Ethernet network, to each RFID interrogator. Implementing a conventional wired backhaul network for the RFID interrogators is generally expensive and complex, with each different RFID interrogator requiring that a separate cable be routed and coupled to the RFID interrogator from a wired data switch. Alternatively, the backhaul network may be conventionally implemented using a standard wireless data networking technology, such as the industry standard "WiFi" or related technologies. Implementing a backhaul network using conventional wireless data networking technologies generally eliminates much of the cost and complexity associated with a wired data network, but introduces different problems, such as potential interference from other legitimate users of the wireless data networking technology.

[0006] As the foregoing illustrates, what is needed in the art is a more efficient technique for interconnecting RFID interrogators.

SUMMARY

[0007] One embodiment of the present invention sets forth a computer-implemented method for transmitting and receiving data via a radio signal, the method comprising: transmitting a first interrogation request to a first interrogator element, receiving a first interrogation reply from the first interrogator element, receiving a second interrogation request from a second interrogator element, and transmitting a second interrogation reply to the second interrogator element in response to the second interrogation request.

[0008] Another embodiment of the present invention sets forth a computer-implemented method for transmitting and receiving metering data via a metering network. The method comprises recording metering data, receiving queries for data from a back office, and sending meter data to a back office in response to the queries.

[0009] Other embodiments include, without limitation, a computer-readable medium that includes instructions that enable a processing unit to implement one or more aspects of the disclosed methods as well as a system configured to implement one or more aspects of the disclosed methods.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] So that the manner in which the above recited features of the present invention can be understood in detail, a more particular description of the invention, briefly summarized above, may be had by reference to embodiments, some of which are illustrated in the appended drawings. It is to be noted, however, that the appended drawings illustrate only typical embodiments of this invention and are therefore not to be considered limiting of its scope, for the invention may admit to other equally effective embodiments.

[0011] Figure 1A illustrates a wireless network, configured to implement one or more aspects of the present invention;

[0012] Figure 1B illustrates an interrogator element configured to operate within the wireless network of Figure 1A, according to one embodiment of the invention;

[0013] Figure 2 illustrates a digital radio transceiver configured to implement one or more aspects of the present invention;

[0014] Figure 3A is a flow diagram of a method for bidirectional communication performed by an interrogator element, according to one embodiment of the invention; and

[0015] Figure 3B is a flow diagram of a method for bidirectional communication performed by an interrogator element, according to one embodiment of the invention.

[0016] Figure 4 illustrates a metering network, according to one embodiment of the present invention.

[0017] Figure 5 is a flow diagram of method steps for transmitting metering data via a metering network, according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0018] In the following description, numerous specific details are set forth to provide a more thorough understanding of the present invention. However, it will be apparent to one of skill in the art that the present invention may be practiced without one or more

of these specific details. In other instances, well-known features have not been described in order to avoid obscuring the present invention.

[0019] Figure 1A illustrates a wireless network 100, configured to implement one or more aspects of the present invention. The wireless network 100 includes interrogator elements 120 configured to both communicate with tag elements 110 and present as tags to other interrogator elements 120. For example interrogator element 120-1 may interrogate tag elements 110-1 and 110-2 via communications links 122-1 and 122-2, respectively. Each communications link 122 implements an RFID communications protocol employing a certain RF channel, or channels, and appropriate modulation techniques. The RFID communications protocol may also specify a specific range of frequencies organized as available RFID channels. Interrogator element 120-1 may also interrogate interrogator element 120-2, configured to temporarily operate as an RFID tag, via communications link 124-1 . Similarly, interrogator element 120-2 may interrogate interrogator element 120-1 , also configured to temporarily operate as an RFID tag. In one embodiment, communications links 124 operate within available RFID channels to implement a substantially identical RFID protocol as that implemented for communications links 122. In an alternative embodiment, communications links 124 implement a different protocol than the RFID protocol, for example to facilitate higher performance communications than enabled within the RFID protocol, but still utilizing an available RFID channel and adhering to regulatory requirements of the RFID channel.

[0020] Certain passive RFID tags utilize a backscatter modulation technique in which an interrogator element 120 transmits significantly more energy than an amount of backscatter energy received back from a tag element 110. The ratio of transmitted energy versus backscattered energy may be many orders of magnitude in some settings. Receiver sensitivity limitations and regulations defining maximum transmission power levels for RFID interrogators together limit a maximum distance from an interrogator element 120 to a tag element 110.

[0021] However, an interrogator element 120 configured to transmit data within maximum transmission power levels over an RFID channel may be located relatively far away from another interrogator element 120 configured to receive the data. Furthermore, two interrogator elements 120, each with an independent power source and each able to generate a unique RF signal for transmission, may be located relatively far apart compared to the maximum distance between an interrogator element

120 and a tag element 110 while achieving two-way communication and operating within the maximum transmission power level. Certain active RFID tags transmit a small amount of energy relative to a companion interrogator, creating a similar scenario, in which two interrogator elements 120 may be located relatively far apart while achieving two-way communication.

[0022] In one embodiment, pairs of interrogator elements 120 within an interrogator mesh network 130 are configured to perform two-way communications by taking turns alternately operating as either an RFID reader or an RFID tag. With two-way communication between interrogator elements 120, data may be routed between arbitrary source and destination interrogator elements 120 within interrogator mesh network 130. In an alternative embodiment, pairs of interrogator elements 120 achieve two-way communication within the interrogator mesh network 130 by transmitting data to each other via one or more RFID channels and within maximum transmission power levels, but without specific regard to RFID protocols.

[0023] One or more interrogator elements 120 may be coupled to an access network 140, providing access to interrogator elements 120. For example, interrogator element 120-3 may be coupled to an access network 130 via one or more suitable technologies, such as the technologies known in the art as wired Ethernet, WiFi, Bluetooth, or ZigBee.

[0024] Figure 1B illustrates an interrogator element 120 configured to operate within the wireless network 100 of Figure 1A, according to one embodiment of the invention. The interrogator element 120 comprises a processing unit 160, a digital radio subsystem 162, a power subsystem 164, an antenna 166, a non-volatile memory 154, and volatile memory 156. Certain embodiments also comprise one or more additional elements, such as a metrology subsystem 150, a control subsystem 152, and a local area network (LAN) interface 158.

[0025] Processing unit 160 includes a processor core configured to retrieve and execute programming instructions from non-volatile memory 154. During the course of executing the programming instructions, the processor core may also store and retrieve data residing within the volatile memory 156. Digital radio subsystem 162 may include a radio receiver circuit configured to demodulate and digitize incoming RF electrical signals. Digital radio subsystem 162 may also include a radio transmitter circuit configured to modulate a digital signal to generate RF electrical signals for

transmission. Antenna 166 converts incident electromagnetic energy into the incoming RF electrical signals and also converts the RF electrical signals for transmission into radiated electromagnetic energy. Power subsystem 164 comprises regulation and power conversion circuitry configured to provide electrical voltage sources to each circuit and subsystem within the interrogator element 120. Power subsystem 164 may also include an energy source such as a photovoltaic system, a battery or fuel cell. In one embodiment, LAN interface 158 includes circuitry to implement wired Ethernet, WiFi, Bluetooth, or ZigBee, or any combination thereof.

[0026] Metrology subsystem 150 comprises circuitry configured to perform one or more measurements, such as voltage, current, power, accumulated power, flow rate, accumulated flow, temperature, humidity, vibration, or any other quantifiable physical value or metric. Metrology subsystem 150 quantizes measured results into a digital value for processing and storage by processing unit 160. In one embodiment, metrology subsystem 150 comprises a power meter for measuring accumulated utilization of power. The control system 152 comprises one or more switches for controlling electrical signals. In one embodiment, control system 152 is a power switch for turning electrical power on or off.

[0027] Figure 2 illustrates a digital radio transceiver 200 configured to implement one or more aspects of the present invention. In one embodiment, digital radio transceiver 200 implements digital radio subsystem 162 of Figure 1B. In another embodiment, digital radio transceiver 200 implements digital radio subsystem 162, MPU 210 implements processing unit 160, and memory 212 implements one or both of non-volatile memory 154 and volatile memory 156.

[0028] The digital radio transceiver 200 may include, without limitation, a microprocessor unit (MPU) 210, a digital signal processor (DSP) 214, digital to analog converters (DACs) 220, 221, analog to digital converters (ADCs) 222, 223, analog mixers 224, 225, 226, 227, a phase shifter 232, an oscillator 230, a power amplifier (PA) 242, a low noise amplifier (LNA) 240, an antenna switch 244, and an antenna 246. A memory 212 may be coupled to the MPU 210 for local program and data storage. Similarly, a memory 216 may be coupled to the DSP 214 for local program and data storage.

[0029] In one embodiment, the MPU 210 implements procedures for processing IP packets transmitted or received as payload data by the digital radio transceiver 200.

The procedures for processing the IP packets may include, without limitation, wireless routing, encryption, authentication, protocol translation, and routing between and among different wireless and wired network ports.

[0030] The DSP 214 implements signal processing procedures for modulating a serialized representation of payload data comprising packets, such as IP packets or RFID protocol data, for wireless transmission, for example within the frequency range of available RFID channels. The serialized representation may encode one or more bits of payload data per modulation symbol or less than one bit per modulation symbol. A receiver may demodulate each modulation symbol to recover the one or more bits of payload data. In one embodiment the one or more bits of payload data are used to generate a corresponding IP packet. In another embodiment, the one or more bits of payload data are used to form an RFID interrogation message or an RFID interrogation response message.

[0031] The DSP 214 may also implement multi-channel modulation for simultaneous transmission of independent units of payload data via multiple, independent channels. Each independent channel occupies a different frequency range in a frequency domain representation of a transmitted radio signal. The DSP 214 also implements signal processing procedures for receiving payload data. The procedures may include, without limitation filtering, energy detection, signal characterization, and simultaneous demodulation of multiple, independent channels.

[0032] In one embodiment, the DSP 214 is configured to modulate data within a given channel using a particular modulation technique that is selected form a set of different modulation techniques, based on prevailing channel requirements. For a given packet of data, a particular transmission bit rate may be implemented using one of the different modulation techniques, based on channel conditions. For example, if a selected channel is subjected to a relatively large amount of noise, then a lower bit rate modulation technique that is more tolerant of noise may be selected. Alternatively, if a selected channel is subjected to relatively low noise and low loss, then a higher bit rate modulation technique may be selected despite a potentially reduced noise tolerance. Exemplary modulation techniques known in the art include, without limitation, frequency shift keying (FSK) and quadrature amplitude modulation (QAM). FSK may be implemented as a robust, but relatively low bit rate technique for representing one or more bits of data per modulation symbol as signal energy in at least one of two or more

defined frequency bands. QAM may be implemented as a relatively high bit rate technique for representing a set of two or more bits per modulation symbol within an amplitude-phase space. Each possible value represented by the two or more bits is mapped to a unique region within the amplitude-phase space. A collection of regions within the amplitude-phase space is known as a constellation. During modulation, each set of two or more bits comprising a modulation symbol is encoded and mapped to an appropriate region within a corresponding constellation. Persons skilled in the art will understand that quadrature encoded signal pairs may be used to conveniently implement QAM modulation. Furthermore, any technically feasible modulation, demodulation, filtering, energy detection, and signal characterization techniques may be implemented by the DSP 214 without departing the scope and spirit of embodiments of the present invention.

[0033] The DSP 214 is coupled to DAC 220 and DAC 221 . Each DAC 220, 221 is configured to convert a stream of outbound digital values into a corresponding analog signal. The outbound digital values are computed by the signal processing procedures for modulating one or more channels. The DSP 214 is also coupled to ADC 222 and ADC 223. Each ADC 222, 223 is configured to sample and quantize an analog signal to generate a stream of inbound digital values. The inbound digital values are processed by the signal processing procedures to demodulate and extract payload data from the inbound digital values.

[0034] In one embodiment, the DSP 214 generates two modulated streams of outbound digital values, which are converted to corresponding analog quadrature signals by DACs 220, 221 . The analog quadrature signals are separately mixed with a radio frequency (RF) carrier signal by analog mixers 224, 225 to generate corresponding quadrature RF signals, each having a frequency domain image centered about the frequency of the RF carrier signal. Oscillator 230 generates the RF carrier signal and phase shifter 232 generates a 90-degree shifted representation of the RF carrier signal for generating quadrature RF signals. The PA 242 combines the quadrature RF signals to generate a modulated RF signal, which is coupled through the antenna switch 244 to the antenna 246. The antenna 246 converts the modulated RF signal from an electrical representation to an electromagnetic representation for wireless transmission. The wireless transmission may be directed to a different instance of the digital radio transceiver 200, residing within a different node of the

wireless mesh network 102.

[0035] When the digital radio transceiver 200 is receiving data, the antenna 246 converts an incoming electromagnetic RF signal to an electrical RF signal, which is coupled through the antenna switch 244 to the LNA 240. The LNA 240 amplifies the electrical RF signal and couples the amplified RF signal to analog mixers 226 and 227. The amplified RF signal is characterized as having a signal image centered about an RF carrier frequency. The analog mixer 227 shifts the signal image down in frequency to an in-phase baseband component of the signal image. The signal is in-phase with respect to the RF carrier signal generated by oscillator 230. The analog mixer 226 shifts the signal image down in frequency to a 90-degree shifted baseband component of the signal image. The in-phase and 90-degree shifted baseband signals comprise a quadrature representation of one or more channels within the electrical RF signal. A plurality of different frequency channels may be represented within the baseband signals. The DSP 214 is configured to map the stream of inbound digital values, comprising a time domain representation of the baseband signals, to a frequency domain representation of the baseband signals. Persons skilled in the art will recognize that the frequency domain representation may be used to efficiently isolate one data bearing signal within one channel from a signal within a different channel. Similarly, the frequency domain representation may be used to detect noise and interfering transmissions within a given channel.

[0036] In one embodiment, the oscillator 230 can be programmed to generate one selected frequency from a plurality of possible frequencies. Each of the plurality of frequencies corresponds to a different channel. The selected frequency determines a center channel for a range of channels that are concurrently available for processing by the DSP 214 to receive or transmit data. For example, if a frequency range of 4 MHz defines ten channels, then each channel is allocated a bandwidth of 400 kHz. In this example, a frequency range of 2,000 kHz representing five channels is processed by the DSP 214 for transmitting or receiving data on one or more of the five channels. If the oscillator 230 is programmed to generate a different selected frequency, then a different set of five concurrently available channels may be used for transmitting or receiving data. The center channel may be changed arbitrarily by programming the oscillator 230 independently of the DSP 214 operating on the concurrently available channels. The digital radio transceiver 200 may be configured with an arbitrary number

of concurrently available channels, each having an arbitrary bandwidth without departing the scope and spirit of embodiments of the present invention.

[0037] Figure 3A is a flow diagram of a method 300 for bidirectional communication performed by an interrogator element, according to one embodiment of the invention. Although the method steps are described in conjunction with the systems of Figures 1A, 1B and 2, persons skilled in the art will understand that any system configured to perform the method steps, in any order, is within the scope of the present invention. This method 300 may be performed by the interrogator element 120 of Figure 1A.

[0038] The method 300 begins in step 310, where the interrogator element 120 transmits an interrogation request to a first RF ID device. In one embodiment, the interrogation request is structured according to any technically feasible RFID protocol, such as the well-known ISO 15693, or ISO 18000-7 protocols. In another embodiment, the interrogation request is structured according to a standard short-distance data protocol such as the well-known IEEE 802.1 1 (WiFi) standards or IEEE 802.1 5 (Bluetooth) standards. Prior to transmitting the interrogation request, the interrogator element 120 may configure the digital radio subsystem 162 of Figure 1B to operate according to a particular protocol and on a selected frequency, for example within an available RFID channel. The interrogation request may comprise a read request to retrieve data from the first RFID device or a write request to transmit data to the RFID device. In step 312, the interrogator element 120 receives an interrogation reply from the first RFID device. The interrogation reply may include data from the interrogation element 120 or confirmation that a write operation was successful. In one embodiment, the interrogation reply conforms to the protocol of the interrogation request. After receiving the interrogation reply, the interrogator element 120 may configure the digital radio subsystem 162 to operate in a mode that is receptive to an incoming interrogation request.

[0039] In step 314, the interrogator element 120 receives an interrogation request from a second RFID device. In one embodiment, the interrogation request is structured according to an RFID protocol. The interrogation request may comprise a read request to retrieve data within the interrogator element 120 or a write request to transmit data to the interrogator element 120. In step 316, the interrogation element 120 replies to the interrogation request from the second RFID device in accordance with protocol requirements of the interrogation request. The reply may comprise data from the

interrogator element 120 or confirmation that a write operation was successful within the interrogator element 120. The method 300 terminates in step 316.

[0040] In one embodiment, the first RFID device comprises an RFID tag, such as tag element 110, and the second RFID device comprises a different interrogator element 120. In this embodiment, interrogator element 120-1 may perform method steps 310 and 312 to read a first set of data from tag element 110-1, and method steps 314 and 316 to transmit a second set of data to interrogator element 120-2. The second set of data may include the first set of data or a derivative thereof.

[0041] In another embodiment, the first RFID device and the second RFID device both comprise interrogator elements 120. For example, interrogator element 120-2 may perform method steps 310 and 312 to read a first set of data from interrogator element 120-1 and method steps 314 and 316 to transmit a second set of data to interrogator element 120-3. The second set of data may include the first set of data or a derivative thereof. Alternatively, the interrogator element 120-2 may perform method steps 310 and 312 to write a first set of data to interrogator element 120-1 and method steps 314 and 316 to receive a second set of data from interrogator element 120-3. Persons skilled in the art will recognize that data may be pushed from one interrogator element 120 to another using a write mechanism or pulled from one interrogator element 120 to another using a read mechanism. Both read and write mechanisms of communication with RFID tags are known in the art and may be advantageously combined in certain embodiments of the present invention.

[0042] In yet another embodiment, the first RFID device and the second RFID device comprise the same type of device, such as interrogator device 120, configured to operate as both an RFID interrogator and an RFID tag. The method steps 310 through 316 may be performed for two-way communication between the two interrogator devices 120.

[0043] Figure 3B is a flow diagram of a method 302 for bidirectional communication performed by an interrogator element, according to one embodiment of the invention. Although the method steps are described in conjunction with the systems of Figures 1A, 1B and 2, persons skilled in the art will understand that any system configured to perform the method steps, in any order, is within the scope of the present invention. This method 302 may be performed by the interrogator element 120 of Figure 1A.

[0044] The method 302 begins in step 320, where the interrogator element 120

receives an interrogation request from a first RF ID device. In one embodiment, the interrogation request is structured according to any technically feasible RFID protocol, such as the well-known ISO 15693, or ISO 18000-7 protocols. In another embodiment, the interrogation request is structured according to a standard short-distance data protocol such as the well-known IEEE 802.1 1 (WiFi) standards or IEEE 802.1 5 (Bluetooth) standards. Prior to receiving the interrogation request, the interrogator element 120 may configure the digital radio subsystem 162 of Figure 1B to operate according to a particular protocol and on a selected frequency, for example within an available RFID channel. The interrogation request may comprise a read request to retrieve data from the interrogator element 120 or a write request to transmit data to the interrogator element 120.

[0045] In step 322, the interrogator element 120 replies to the interrogation request by transmitting an interrogation reply from the first RFID device. In one embodiment, the interrogation reply conforms to the protocol of the interrogation request. The interrogation reply may include data from the interrogation element 120 or confirmation that a write operation was successful within the interrogation element 120. The interrogator element 120 may configure the digital radio subsystem 162 to confirm to a particular protocol, such as an RFID protocol, prior to transmitting the interrogation reply. After transmitting the interrogation reply, the interrogator element 120 may configure the digital radio subsystem 162 to operate in a mode that is receptive to another incoming interrogation request.

[0046] In step 324, the interrogator element 120 transmits an interrogation request to a second RFID device. In one embodiment, the interrogation request is structured according to an RFID protocol. The interrogation request may comprise a read request to retrieve data within the second RFID device or a write request to transmit data to the second RFID device. In step 326, the interrogation element 120 replies to the interrogation request from the second RFID device in accordance with protocol requirements of the interrogation request. The reply may comprise data from the second RFID device or confirmation that a write operation was successful within the second RFID device. The method 302 terminates in step 326.

[0047] In one embodiment, the first RFID device and the second RFID device both comprise interrogator elements 120. For example, interrogator element 120-2 may perform method steps 320 and 322 to receive a first set of data from interrogator

element 120-1 and method steps 314 and 316 to transmit a second set of data to interrogator element 120-3. The second set of data may include the first set of data or a derivative thereof. Alternatively, the interrogator element 120-2 may perform method steps 310 and 312 to transmit a first set of data to interrogator element 120-1 and method steps 314 and 316 to receive a second set of data from interrogator element 120-3. Persons skilled in the art will recognize that data may be pushed from one interrogator element 120 to another using a write mechanism or pulled from one interrogator element 120 to another using a read mechanism. Both read and write mechanisms of communication with RFID tags are known in the art and may be advantageously combined in certain embodiments of the present invention.

[0048] In another embodiment, the first RFID device comprises interrogator element 120-2, and the second RFID device comprises tag element 110-1. In this embodiment, interrogator element 120-1 may perform method steps 320 and 322 to receive a first set of data from interrogator element 120-2, and method steps 324 and 326 to read a second set of data from tag element 110-1.

[0049] In yet another embodiment, the first RFID device and the second RFID device comprise the same device, such as another interrogator device 120. The method steps 320 through 326 may be performed for two-way communication between the two interrogator devices 120.

[0050] In certain embodiments, the interrogator element 120 implements a power meter configured to measure accumulated power consumption and report the accumulated power consumption via the interrogator mesh network 130 of Figure 1A to a server coupled to the access network 140. In such embodiments, each interrogator element 120 may operate independently to measure a corresponding sample of accumulated power consumption and report the sample of accumulated power consumption via a push regime or a pull regime, or a combination thereof through the interrogator mesh network 130. In this way, accumulated power consumption samples for all interrogator elements 120 may be gathered by the server.

Metering Network

[0051] Figure 4 illustrates a metering network 400, according to one embodiment of the present invention. As shown, metering network 400 comprises back office 402, access points 404, relays 406, and smart meters 408. Smart meters 408 take readings and send the readings through other smart meters 408, relays 406, and access points

404, to back office 402. Relays 406 are present to extend the range of smart meters 408. Access points 404 provide an interface between smart meters 408 and back office 402. Back office 402 queries smart meters 408, analyzes, and integrates readings from smart meters 408. Relays 406, smart meters 408, and access points 404 may implement a mesh network 130 as described above.

[0052] Smart meter 408 comprises data meter 410 and interrogator element 120, as described above. Access points 404 and relays 406 may also have interrogator elements 120 for communication between elements in network 400. Data meter 410 may be any type of meter for providing readings, such as utility readings, including a gas meter for measuring gas consumption, an electricity meter for measuring electricity consumption, and the like. Data meter 410 may collect and store data. If data meter 410 measures electricity, it may collect data such as customer usage, distribution network voltage, instantaneous current, power factor, device tamper and alarms. Data meter 410 may be any of a large number of types of devices, such as electric meters, fault indicators, capacitor banks and switch re-closures. Interrogator element 120 is coupled to data meter 410 and can transmit readings from data meter 410 to network 400. Interrogator element 120 therefore acts as a "transmitter" for data recorded by data meter 410. In one embodiment, interrogator element 120 in data meter 410 is a class 4 active RFID module.

[0053] To obtain data from smart meters 408, back office 402 sends requests for information ("data queries"), through access points 404, to smart meters 408. Smart meters 408 respond to the requests for information with data regarding the smart meter's 408 readings. Back office 402 may send data queries periodically, so that back office 402 receives a constant stream of data from smart meters 408 in order to perform analysis on the data. Back office 402 may store a database of data and update the database each time data is received from smart meters 408. Back office 402 may comprise a distributed web-based computer system that provides web-based access to meter data for a client.

[0054] Smart meters 408 are configured to send "alerts" to back office 402 if specific events occur. For example, if smart meter 408 detects certain sensor conditions or alarms, smart meter 408 sends an alert through network 400 to back office 402. The alert sent contains information regarding the specific alert. "Alerts" may indicate conditions that require immediate attention.

[0055] Network 400 is scalable in that new smart meters 408 may be added to the network. If a new smart meter 408 is not connected to network 400, the new smart meter 408 periodically sends "discovery" signals permitting network 400 to "discover" the new smart meter. When a new smart meter 408 is within range of another network 400 component such as a smart meter 408, access point 404, or relay 406, discovery signals may be detected by the new smart meter 408. To add the new smart meter 408 to the network 400, an authentication procedure begins in which the new smart meter 408 is authenticated, identified, and added to the network 400.

[0056] In one embodiment, smart meters 408 may authenticate utilizing three security credentials: a private key unique to the interrogator element 120, a "birth certificate" containing a public key corresponding to the private key, wherein the public key is derived from the X.509 Digital Certificate of the manufacturer of the RFID tag in the interrogator element 120, and the manufacturing station certificate. These certificates correspond to a securely held root key token, through intermediate certificates, as is known.

[0057] Together, the birth certificate and private key of the interrogator element 120 constitute the cryptographic identity (CI) of the interrogator element 120. In one embodiment, the birth certificate and private key of the interrogator element 120 may not be changed and thus uniquely and immutably identify the interrogator element 120. In addition to uniquely identifying the device, the cryptographic identity also defines the specific usage or role of the device. In other words, back office 402 may keep track of all cryptographic identities and their corresponding roles (type of meter, such as electric, gas, and the like). Additional information that is operationally useful can also be kept track of and can correspond to unique cryptographic identities.

[0058] The cryptographic identity may be used during establishment of a link between smart meter 408 and the rest of the network 400, may be used to identify the smart meter 408 to the back office 402, and may be used to validate data sent from smart meter 408 to the back office 402.

[0059] Additional information may be used to identify interrogator elements 120 and smart meters 408. For example, each interrogator element 120 in smart meter 408 has an RFID Tag Identifier (TID). In one embodiment, the TID of an interrogator element 120 may be fixed at manufacturing and does not change for the life of the product. In one embodiment, the TID is formatted as a EUI-64 unique identifier. Interrogator

elements 120 may also have a meter ID that identifies the data meter 410 with which interrogator element 120 is associated. In one embodiment, meter IDs are unique by regulatory region.

[0060] Each smart meter 408 may also periodically send out maintenance information to devices operating in the communications range of the smart meter 408 to maintain network 400. The maintenance information allows other devices to communicate with the smart meter 408. The maintenance information may include information regarding communication paths from the smart meter 408 through other smart meters 408 and relays 406, to access points 404, including indications of which specific smart meters 408, relays 406, and access points 404 constitute the communication paths. Sending out periodic maintenance information also allows smart meters 408 to re-configure the network 400, in case of any changes to elements within the network (location, malfunction, removal, and the like), by allowing elements to determine new communication paths to access points 404.

[0061] All elements within network 400 may be powered in any number of ways, including by battery or by drawing on power from the utility grid (e.g., electric grid) to which they are attached.

[0062] In one embodiment, interrogator elements 120 may transmit information exclusively utilizing RFID interrogator channels identified by applicable regulatory requirements. In one embodiment, interrogator elements 120 may be equipped with UHF transmitters to permit transmission of data.

[0063] Figure 5 is a flow diagram of method steps for transmitting metering data via a metering network, according to one embodiment of the present invention. Although the method steps are described in conjunction with Figures 1-4, persons skilled in the art will understand that any system configured to perform the method steps, in any order, falls within the scope of the present invention.

[0064] The method 500 begins at step 502, where the smart meter 408 records meter data. At step 504, the smart meter 408 receives queries from the network 400 to provide the data recorded at step 502. At step 506, the smart meter 408 sends meter data to the back office 402 in response to the queries.

[0065] In sum, a technique for implementing two-way communication between interrogator elements in a wireless network is disclosed. An interrogator element is configured to operate as both an RFID reader and an RFID tag to achieve two-way

communication with a different interrogator element. Each interrogator element may participate in an interrogator mesh network configured to route data between the participating interrogator elements. Each interrogator element may also act as a conventional RFID interrogator that communicates with RFID tag devices.

[0066] One advantage of the disclosed systems and methods is that a backhaul network that interconnects RFID interrogators may be efficiently implemented by combining interrogator and tag behavior within a single interrogator element device.

[0067] While the forgoing is directed to embodiments of the present invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof. For example, aspects of the present invention may be implemented in hardware or software or in a combination of hardware and software. One embodiment of the invention may be implemented as a program product for use with a computer system. The program(s) of the program product define functions of the embodiments (including the methods described herein) and can be contained on a variety of computer-readable storage media. Illustrative computer-readable storage media include, but are not limited to: (i) non-writable storage media (e.g., read-only memory devices within a computer such as CD-ROM disks readable by a CD-ROM drive, flash memory, ROM chips or any type of solid-state non-volatile semiconductor memory) on which information is permanently stored; and (ii) writable storage media (e.g., floppy disks within a diskette drive or hard-disk drive or any type of solid-state random-access semiconductor memory) on which alterable information is stored. Such computer-readable storage media, when carrying computer-readable instructions that direct the functions of the present invention, are embodiments of the present invention.

[0068] In view of the foregoing, the scope of the present invention is determined by the claims that follow.

What is claimed is:

1. A computer-implemented method for transmitting and receiving data via a radio signal, the method comprising:

transmitting a first interrogation request to a first interrogator element;

receiving a first interrogation reply from the first interrogator element;

receiving a second interrogation request from a second interrogator element; and

transmitting a second interrogation reply to the second interrogator element in response to the second interrogation request.

2. The method of claim 1, wherein the first interrogation request comprises a read request for a first set of data residing within the first interrogator element, and the first interrogation reply comprises a first message that includes the first set of data.

3. The method of claim 1, wherein the first interrogation request comprises a write request for a second set of data to be written to the first interrogator element, and the first interrogation reply comprises a second message that confirms a successful write operation for the second set of data within the first interrogator element.

4. The method of claim 1, wherein the second interrogation request comprises a read request for a third set of data residing within the interrogator element, and the second interrogation reply comprises a third message that includes the third set of data.

5. The method of claim 1, wherein the second interrogation request comprises a write request for a fourth set of data to be written to the interrogator element, and the second interrogation reply comprises a fourth message that confirms a successful write operation for the fourth set of data within the interrogator element.

6. The method of claim 1, further comprising:

receiving a third interrogation request from a third interrogator element;

transmitting a third interrogation reply to the third interrogator element in response to the third interrogation request;

transmitting a fourth interrogation request to a fourth interrogator element; and

receiving a fourth interrogation reply from the fourth interrogator element.

7. The method of claim 6, wherein the third interrogation request comprises a read or write request for data residing with the interrogator element, and the fourth interrogation request comprises a read or write request for data residing within the fourth interrogator element.

8. The method of claim 2, wherein the first set of data comprises metrology data measured by the first interrogator element.

9. The method of claim 8, wherein the metrology data comprises accumulated power consumption data.

10. The method of claim 1, wherein the first interrogator element and the second interrogator element are configured to transmit data using one or more radio frequency identification (RFID) channels.

11. The method of claim 10, wherein the first interrogator element and the second interrogator element are further configured to transmit data using RFID protocols.

12. A computer-readable storage medium including instructions that, when executed by a processing unit, cause the processing unit to transmit one or more data packets via a radio signal by performing the steps:

transmitting a first interrogation request to a first interrogator element;

receiving a first interrogation reply from the first interrogator element;

receiving a second interrogation request from a second interrogator element; and

transmitting a second interrogation reply to the second interrogator element in response to the second interrogation request.

13. The computer-readable storage medium of claim 12, wherein the first interrogation request comprises a read request for a first set of data residing within the

first interrogator element, and the first interrogation reply comprises a first message that includes the first set of data.

14. The computer-readable storage medium of claim 12, wherein the first interrogation request comprises a write request for a second set of data to be written to the first interrogator element, and the first interrogation reply comprises a second message that confirms a successful write operation within the first interrogator element.

15. The computer-readable storage medium of claim 12, wherein the second interrogation request comprises a read request for a third set of data residing within the interrogator element, and the second interrogation reply comprises a third message that includes the third set of data.

16. The computer-readable storage medium of claim 12, wherein the second interrogation request comprises a write request for a fourth set of data to be written to the interrogator element, and the second interrogation reply comprises a fourth message that confirms a successful write operation within the interrogator element.

17. The computer-readable storage medium of claim 12, further comprising:

receiving a third interrogation request from a third interrogator element;

transmitting a third interrogation reply to the third interrogator element in response to the third interrogation request;

transmitting a fourth interrogation request to a fourth interrogator element; and

receiving a fourth interrogation reply from the fourth interrogator element.

18. The computer-readable storage medium of claim 17, wherein the third interrogation request comprises a read or write request for data residing with the interrogator element, and the fourth interrogation request comprises a read or write request for data residing within the fourth interrogator element.

19. The computer-readable storage medium of claim 13, wherein the first set of data comprises accumulated power consumption data measured by the first interrogator element.

20. The computer-readable storage medium of claim 12, wherein the first interrogator element and the second interrogator element are configured to transmit data using one or more radio frequency identification (RFID) channels.

21. The method of claim 20, wherein the first interrogator element and the second interrogator element are further configured to transmit data using RFID protocols.

22. A wireless network device, comprising:

a digital radio circuit configured to generate a radio signal for data transmission and to receive a signal for data reception; and

a processing unit that is coupled to the radio transmitter circuit and configured to:

transmit first interrogation request to a first interrogator element;

receive a first interrogation reply from the first interrogator element;

receive a second interrogation request from a second interrogator element;

transmit a second interrogation reply to the second interrogator element in response to the second interrogation request;

receive a third interrogation request from a third interrogator element;

transmit a third interrogation reply to the third interrogator element in response to the third interrogation request;

transmit a fourth interrogation request to a fourth interrogator element; and

receive a fourth interrogation reply from the fourth interrogator element.

23. The wireless network device of claim 22, wherein the first set of data comprises accumulated power consumption data measured by the first interrogator element.

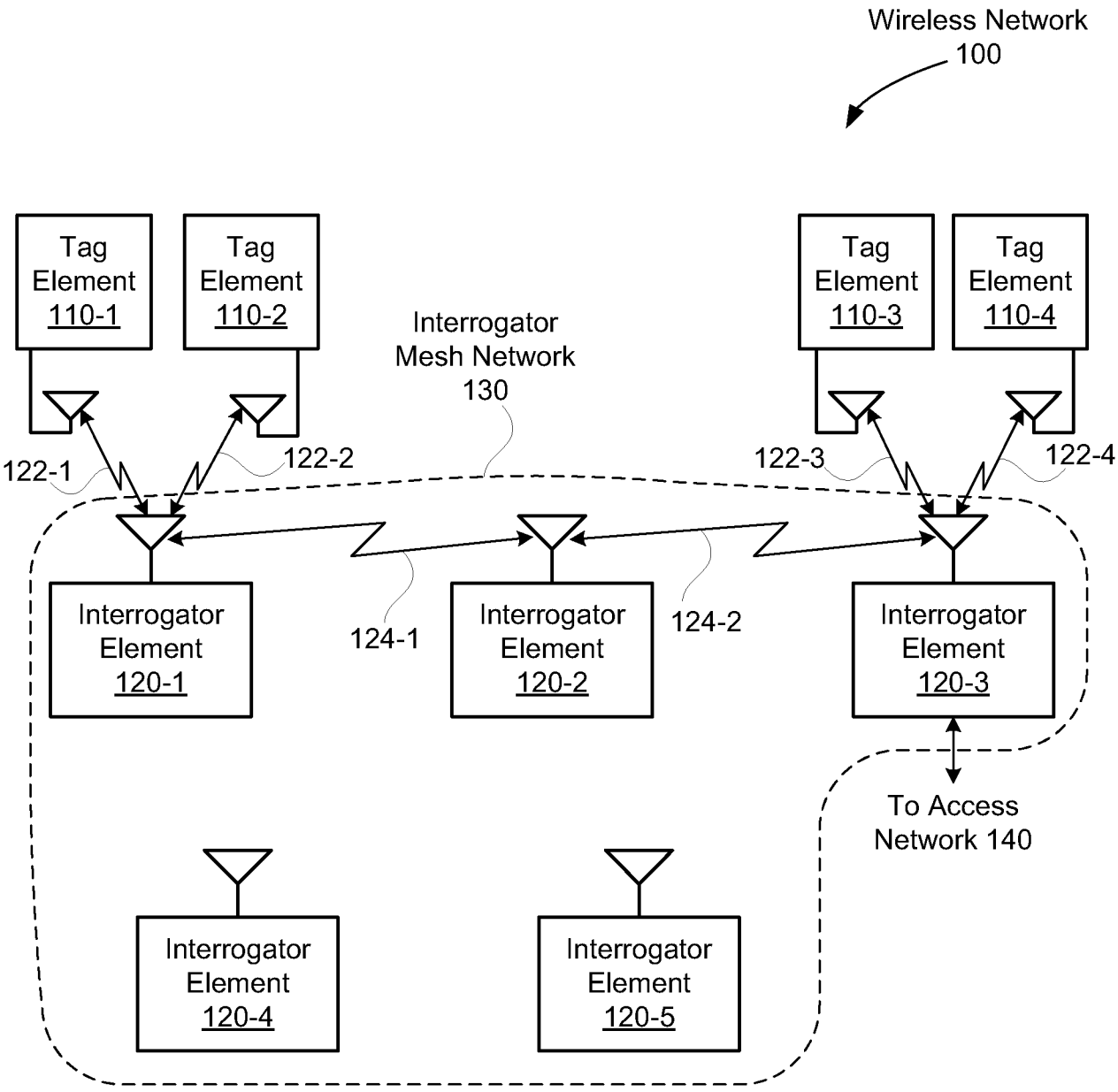
Wireless Network
100
Tag Element 110-1
Tag Element 110-2
Tag Element 110-3
Tag Element 110-4
Interrogator Mesh Network 130
122-1
122-2
122-3
122-4
Interrogator Element 120-1
Interrogator Element 120-2
Interrogator Element 120-3
124-1
124-2
To Access Network 140
Interrogator Element 120-4
Interrogator Element 120-5

Figure 1A

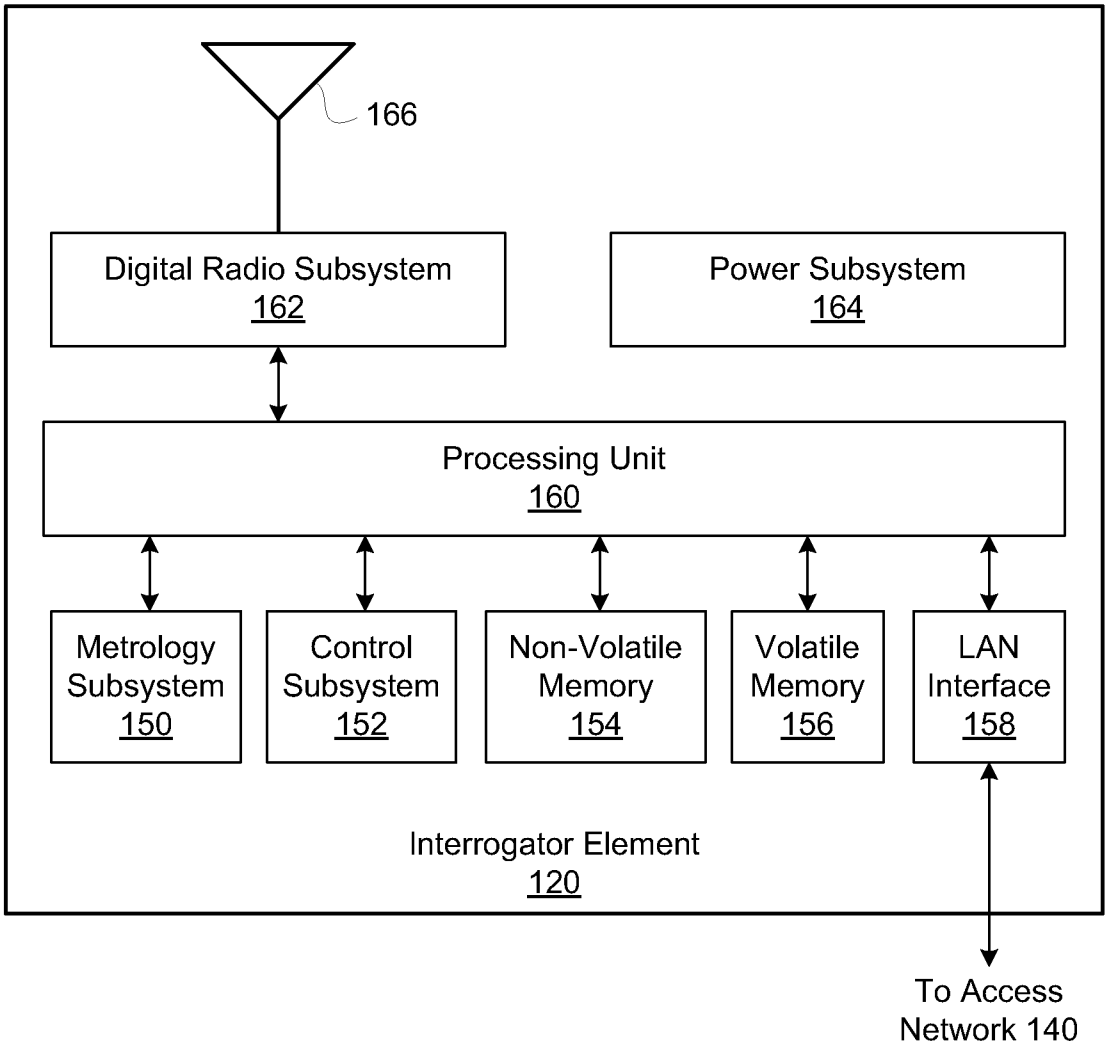
166
Digital Radio Subsystem
162
Power Subsystem
164
Processing Unit
160
Metrology
Subsystem
150
Control
Subsystem
152
Non-Volatile
Memory
154
Volatile
Memory
156
LAN
Interface
158
Interrogator Element
120
To Access
Network 140

Figure 1B

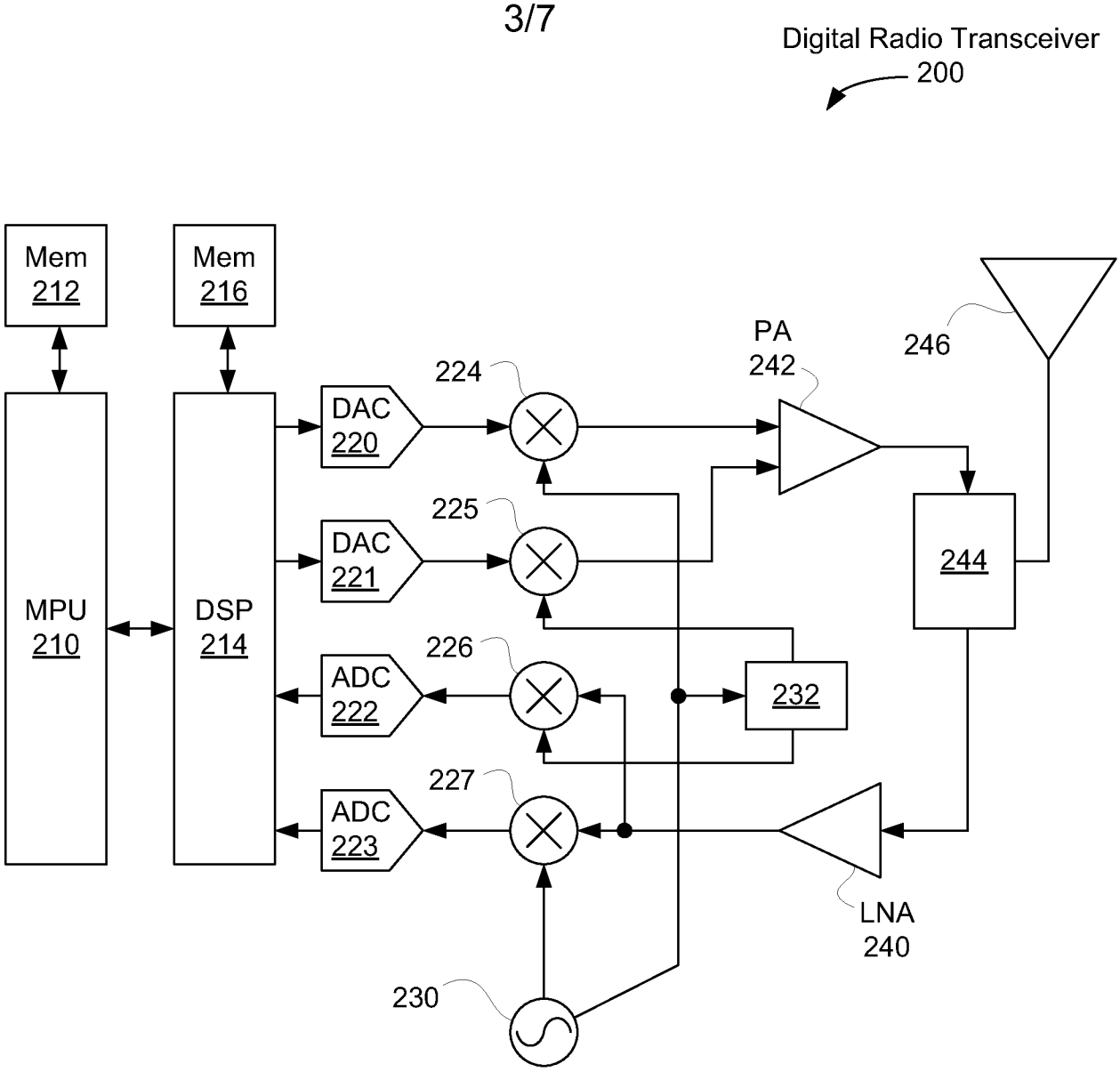
Digital Radio Transceiver
200
Mem
212
Mem
216
MPU
210
DSP
214
DAC
220
DAC
221
ADC
222
ADC
223
224
225
226
227
230
PA
242
246
244
232
LNA
240

Figure 2

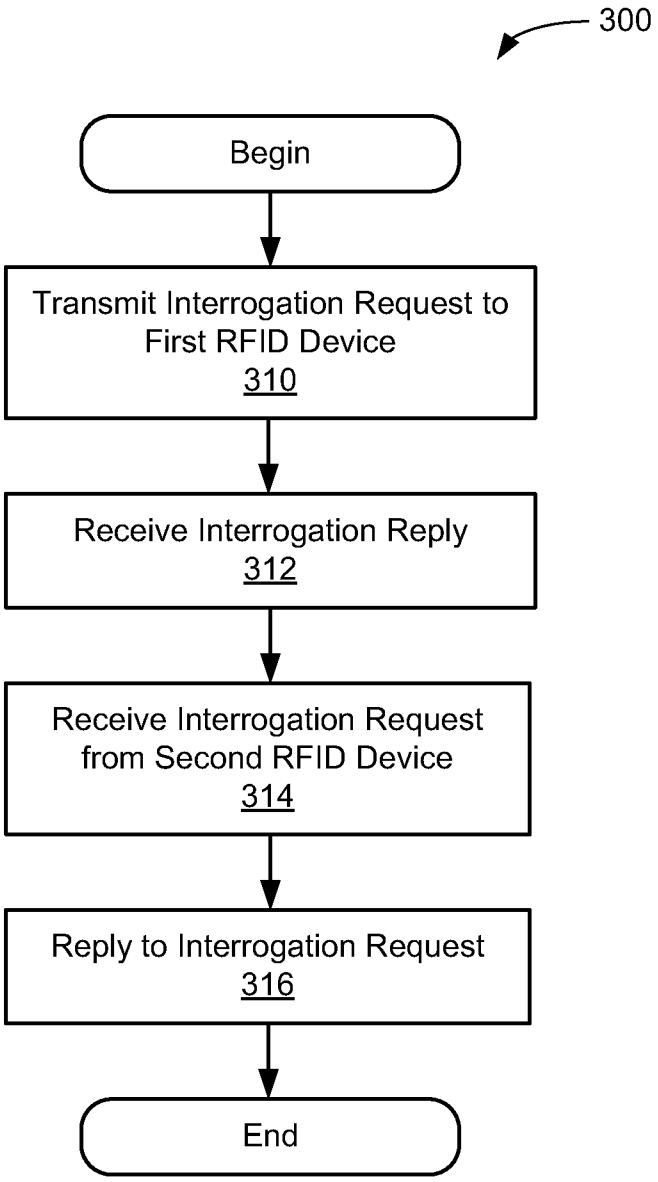
300
Begin
Transmit Interrogation Request to First RFID Device
310
Receive Interrogation Reply
312
Receive Interrogation Request from Second RFID Device
314
Reply to Interrogation Request
316
End

Figure 3A

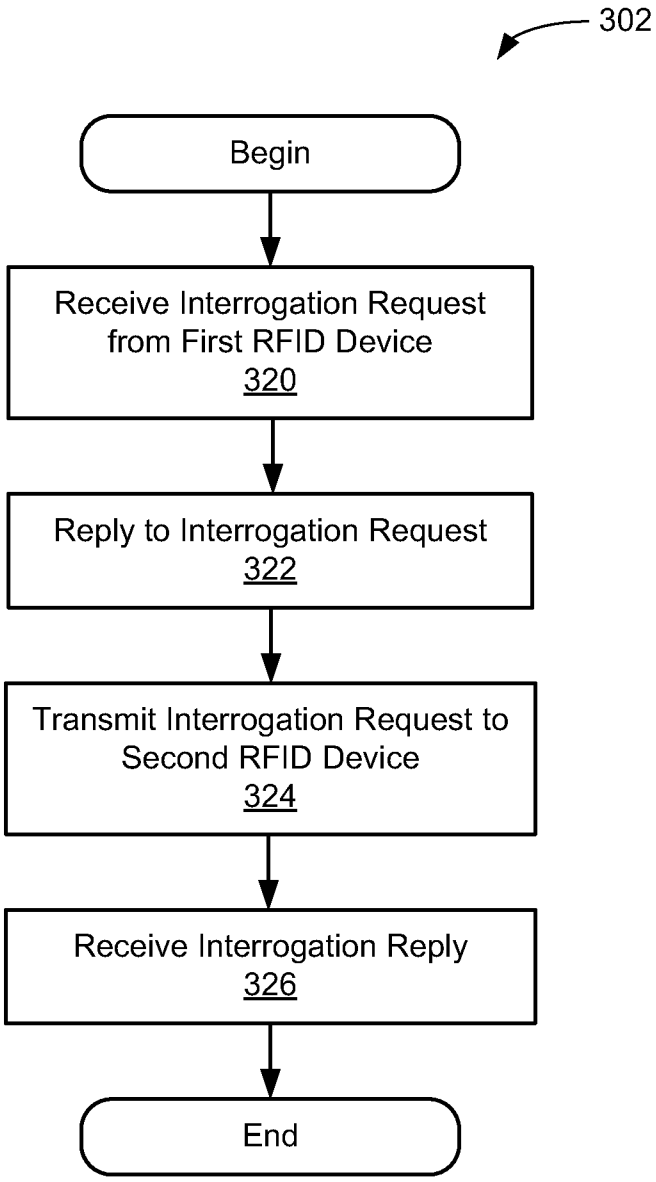
302
Begin
Receive Interrogation Request from First RFID Device 320
Reply to Interrogation Request 322
Transmit Interrogation Request to Second RFID Device 324
Receive Interrogation Reply 326
End

Figure 3B

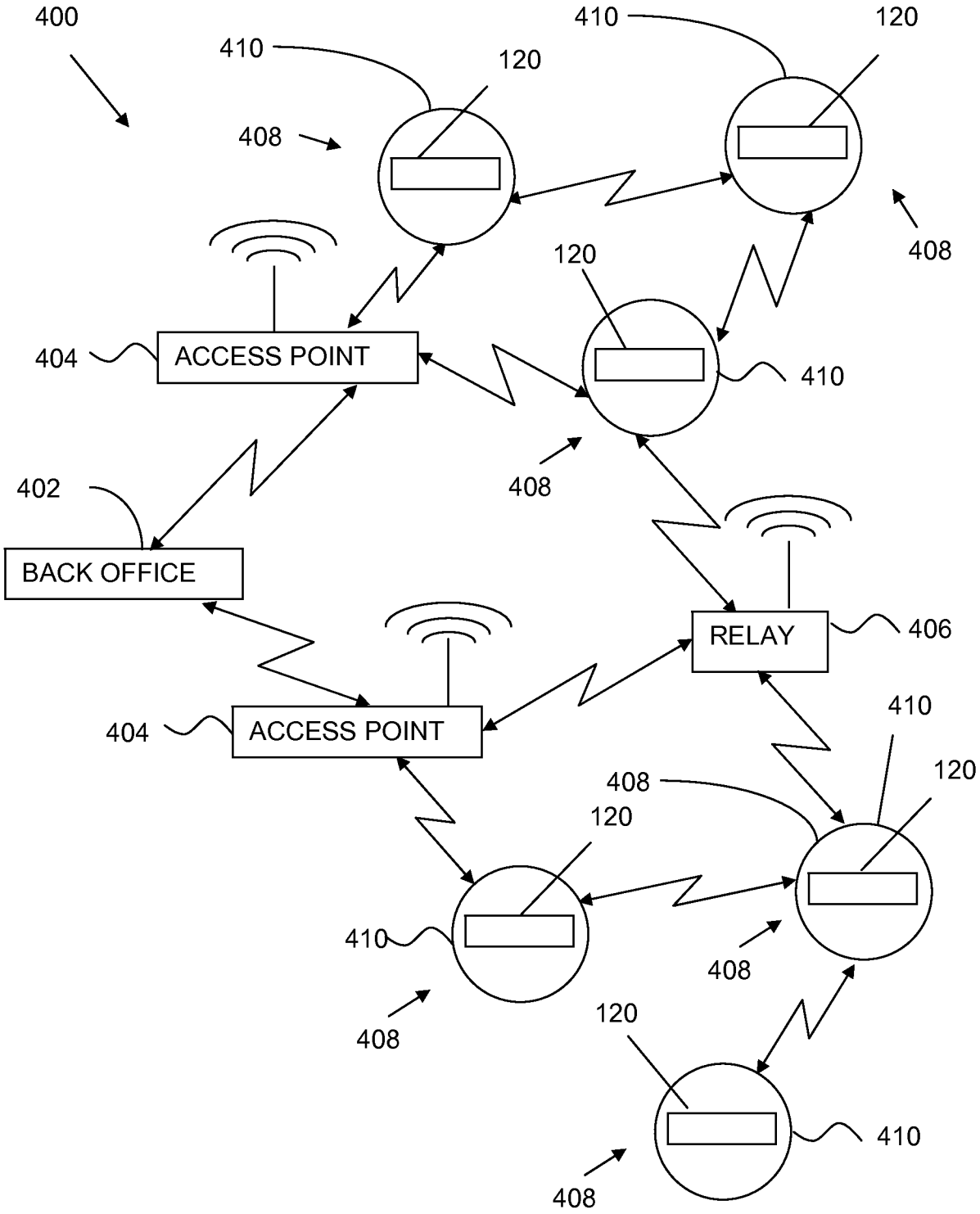
400
410
120
408
410
120
408
120
404
ACCESS POINT
410
408
402
BACK OFFICE
RELAY
406
404
ACCESS POINT
410
120
408
120
410
408
408
120
410
408

Figure 4

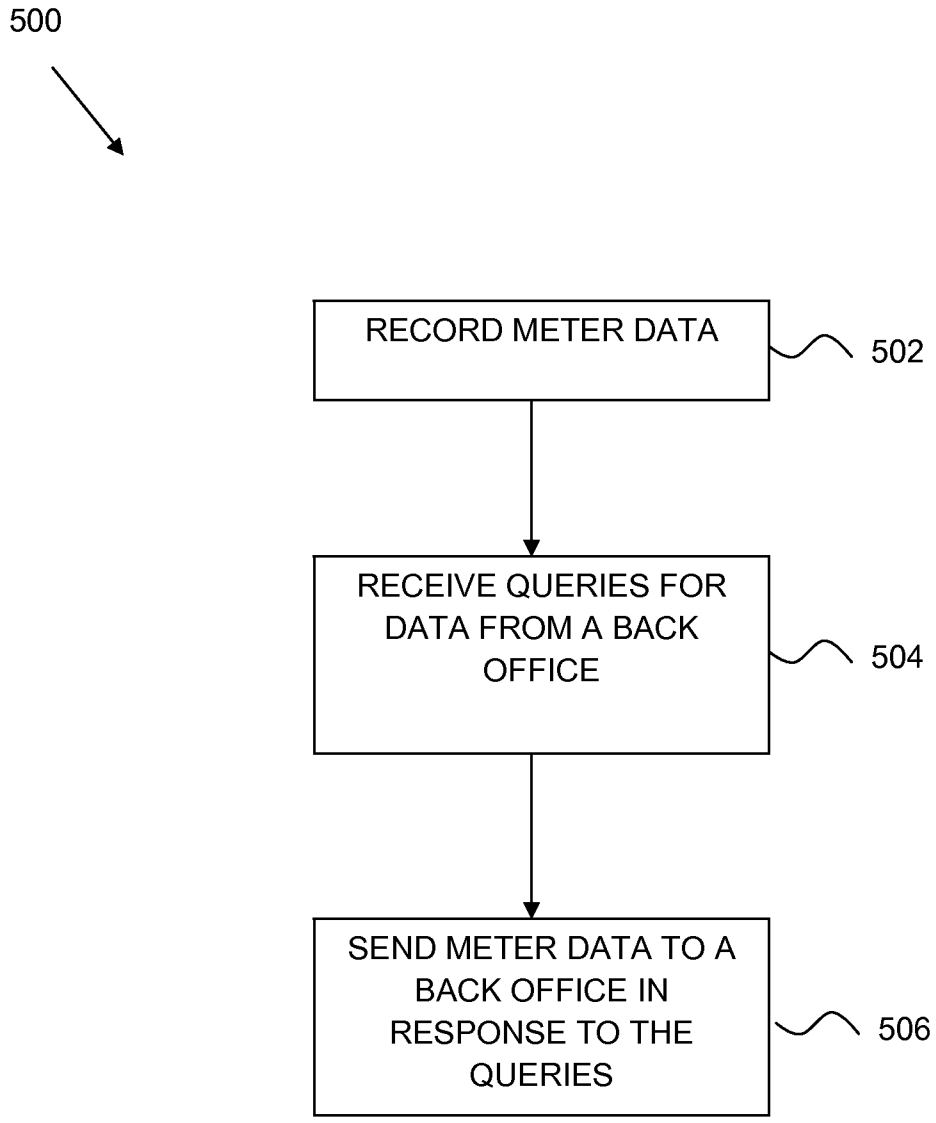
500
RECORD METER DATA
502
RECEIVE QUERIES FOR DATA FROM A BACK OFFICE
504
SEND METER DATA TO A BACK OFFICE IN RESPONSE TO THE QUERIES
506

Figure 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/071077

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/28(2006.01)i, H04L 29/06(2006.01)1

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/28; H04B 5/00; H04B 7/00; H04B 5/02; H04Q 5/22

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: RFID, interrogator, reader, request, query, radio, back- scattering

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008-0186145 Al (MANLEY, JATHAN W. et al.) 07 August 2008 See abstract ; paragraphs 9, 22-24, 33, 37-38 ; claim 9; and figures 1, 3, 5-7.	1-2,4,6-7,10-13,15,17-18,20-22
Y		8-9,19,23
A		3,5,14,16
Y	US 2009-0184804 Al (SEPPA, HEIKKI) 23 July 2009 See abstract ; paragraphs 62-63 ; and figure 1.	8-9,19,23
A	US 2007-0139163 Al (POWELL, KEVIN J. et al.) 21 June 2007 See abstract ; paragraphs 11-22 ; and figures 4-5.	1-23
A	KR 10-2009-0045001 A (BROADCOM CORPORATION) 07 May 2009 See abstract ; paragraphs 80-84 ; and figure 1.	1-23
A	US 2008-0297312 Al (MOSHFEGHI, MEHRAN) 04 December 2008 See abstract ; paragraphs 33, 75; and figure 4.	1-23

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 April 2013 (23.04.2013)	**24 April 2013 (24.04.2013)**

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-70 1, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

KANG, Hee Gok

Telephone No. 82-42-481-8264

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/071077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0186145 A1	07.08.2008	None	
US 2009-0184804 A1	23.07.2009	EP 2021737 A1	11.02.2009
		JP 2009-538013 A	29.10.2009
		WO 2007-135233 A1	29.11.2007
us 2007-0139163 A1	21.06.2007	EP 1964416 A2	03.09.2008
		US 2007-0139162 A1	21.06.2007
		US 7969282 B2	28.06.2011
		WO 2007-078440 A2	12.07.2007
KR 10-2009-0045001 A	07.05.2009	CN 101425148 A	06.05.2009
		CN 101425148 B	20.04.2011
		CN 101441702 A	27.05.2009
		EP 1998468 A2	03.12.2008
		EP 1998468 A3	06.06.2012
		EP 2056234 A2	06.05.2009
		EP 2056234 A3	30.01.2013
		KR 10-0988813 B1	20.10.2010
		US 2008-0238621 A1	02.10.2008
		US 2008-0238679 A1	02.10.2008
		US 2010-0123556 A1	20.05.2010
		US 7679514 B2	16.03.2010
		US 8022825 B2	20.09.2011
US 2008-0297312 A1	04.12.2008	US 2011-0267175 A1	03.11.2011
		US 2013-0015957 A1	17.01.2013
		US 7978050 B2	12.07.2011
		US 8284031 B2	09.10.2012