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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
05 March 2020 (05.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/047060 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *H04B 7/26* (2006.01)
H04L 12/26 (2006.01)

(21) International Application Number:
PCT/US2019/048515

(22) International Filing Date:
28 August 2019 (28.08.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/115,837 29 August 2018 (29.08.2018) US

(71) Applicant: LANDIS+GYR INNOVATIONS, INC. [US/US]; 30000 Mill Creek Avenue, Suite 100, Alpharetta, Georgia 30022 (US).

(72) Inventor: LOWELL, Alan Blair; 4082 Leprechan Way, Duluth, Georgia 30097 (US).

(74) Agent: HOLMES, Brenda O. et al.; Kilpatrick Townsend & Stockton LLP, Suite 2800, 1100 Peachtree Street, Atlanta, Georgia 30309 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

(54) Title: DETECTING NETWORK DEVICES WITHOUT JOINING A NETWORK

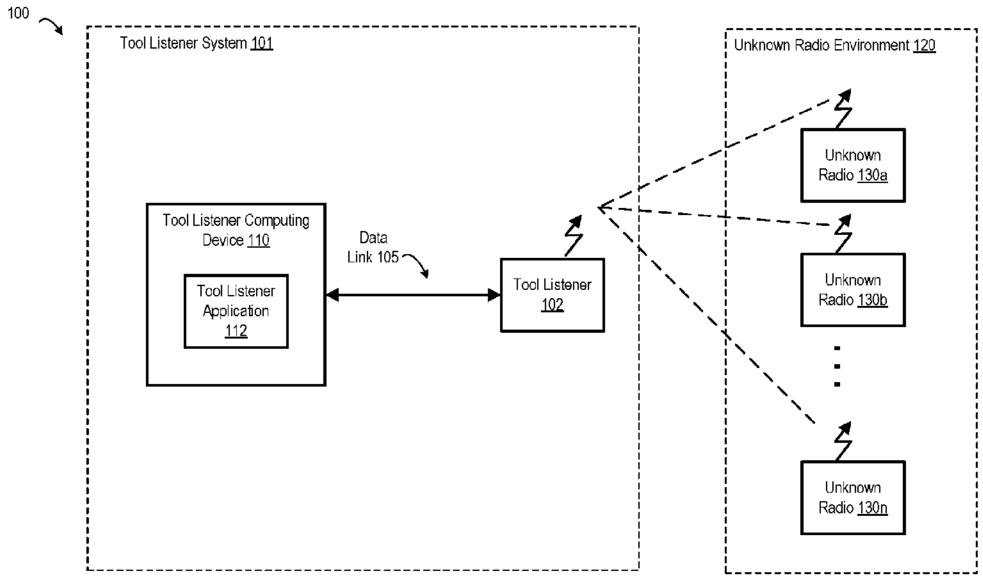

FIG. 1

(57) Abstract: A tool listening device comprising a transceiver is configured to listen on a radio channel selected from a discovery channel hopping sequence. The tool listening device is configured to identify a preamble, indicating a start of a packet. The tool listening device continues to listen until a packet header is received. The tool listener extracts, from the packet header, a source address, a destination address and a frame type. The tool listening device adds the source address, the destination address, and the frame type to a data structure, and transmits the data structure to an external device, where the data may be visualized. The tool listening device is further configured select another radio channel from the discovery channel hopping sequence.

[Continued on next page]

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

DETECTING NETWORK DEVICES WITHOUT JOINING A NETWORK

TECHNICAL FIELD

[0001] Aspects described herein relate generally to radio frequency network diagnostic tools and more specifically to identifying network devices that are configurable to operate on wireless mesh networks.

BACKGROUND

[0002] Resource distribution networks such as power, gas, or water distribution networks can use smart meters to collect and aggregate resource consumption data. Smart meters can help automate billing, reduce cost, and provide advanced analytics tools to utility companies. Smart meters can be configured to operate on a mesh network. A mesh network can be a short-range wireless network with or without a central node.

[0003] Before a smart meter is added to an existing network, the smart meter is configured for proper operation, for example, by configuring a set of network parameters. When configured and placed in the field, the smart meter can then automatically establish a connection with a mesh network.

[0004] Various diagnostic tools can be used to identify faults with smart meters. Defective smart meters are brought back from the field to a meter repair facility where a technician performs a diagnosis, repair, or reconfiguration. A technician may use a diagnostic tool to determine whether a smart meter is configured for a particular network, is attempting to connect to a network, or is non-operational. Further, a technician may use a diagnostic tool to configure a smart meter to communicate with a test network to enable further analysis or network reconfiguration.

[0005] But existing diagnostic tools suffer from deficiencies. Specifically, existing diagnostic tools are either limited to detecting one device at a time, requiring an identifier such as network or device address in order to search for a meter, or unnecessarily storing entire packets, thereby overloading a visual interface of the diagnostic tool with unnecessary information.

[0006] Hence, new solutions are needed.

SUMMARY

[0007] Certain aspects and features include a system and method for detecting a radio frequency device. In an example, a tool listening device comprising a transceiver is configured to listen on a radio channel selected from a discovery channel hopping sequence. The discovery channel hopping sequence uses a different sequence from a channel hopping sequence used by the radio frequency device and includes radio channels used by the channel hopping sequence of the radio frequency device. The tool listening device identifies a preamble of a packet. The packet includes a header. The tool listening device continues to listen until the header is received. The tool listening device extracts a source address, a destination address, and a frame type from the header and adds the source address, the destination address, and the frame type to a data structure. The tool listening device transmits the data structure to an external device, which can cause the external device to visualize the data structure. The tool listening device, responsive to either receiving a packet or determining that a predetermined amount of time has lapsed, is configured to select a next radio channel from the discovery channel hopping sequence and listen on that channel.

[0008] These illustrative examples are mentioned not to limit or define the disclosure, but to provide examples to aid understanding thereof. Additional examples and further description are provided in the Detailed Description.

BRIEF DESCRIPTION OF THE FIGURES

[0009] These and other features, aspects, and advantages of the present disclosure are better understood when the following Detailed Description is read with reference to the accompanying drawings, where:

Figure 1 illustrates an example of a tool listener environment, according to an aspect.

Figure 2 illustrates an implementation of a tool listener system, according to an aspect.

Figure 3 is a flowchart illustrating a process used by a tool listening device to detect a presence of another device, according to an aspect.

Figure 4 is a table illustrating data relating to radio devices detected by a tool listening device, according to an aspect.

Figure 5 illustrates a computing device used to implement certain functions of a tool listener, according to an aspect.

DETAILED DESCRIPTION

[0010] Aspects of the present invention relate to using a tool listening device to detect wireless devices such as smart meters. The tool listening device, or tool listener, is configured to listen for devices operating or attempting to operate on a wireless network such as a mesh network. The tool listener does not need to join a mesh network in order to detect network communications and does not need to use parameters with identical configuration as the network. For example, the tool listener may use a discovery channel hopping sequence that is different from a channel hopping sequence of a mesh network and may listen for a predetermined amount of time that differs from a time slot of the mesh network.

[0011] Mesh networks, such as Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 networks, are wireless personal area networks that are typically short-range, low-bitrate, and self-identifying networks. Advanced Metering Infrastructure (AMI) or smart meters can use mesh networks to communicate resource consumption or diagnostic information. Once connected to a network, devices on a mesh network operate within specified time slots and according to a particular channel-hopping sequence.

[0012] A channel hopping sequence includes a list of valid channels, a channel spacing, a bit rate, and a modulation index. The channel hopping sequence of a particular network can be a subset of the available channels of the region or country of operation. For example, if a regulatory body permits channels 1-10 for operation, a particular network, and therefore radios configured to operate on that network might use a channel hopping sequence that includes channels 1, 5, and 8. Additionally, devices on a mesh network utilize various communications features such as synchronization (or sync) words, beacon requests, and different frame types such as data frames, beacon frames, acknowledgement frames, and Media Access Control (MAC) command frames. Mesh devices may or may not emit a signal when they power on or reset such as a birth chirp.

[0013] The tool listener can listen on a set of radio channels for network activity, detect network activity without storing entire packets, save detected activity in a data structure, and provide the data to an external device such as a computer or tablet. The external device can visualize the data. Examples of visualization include displaying the data in a table, graph, chart, or as raw text. The tool listener can detect a presence of a specific device or can perform an inventory of unknown devices. Unknown devices can include wireless devices that are joined to a mesh network or are not joined to a mesh network, e.g., are attempting to communicate with a mesh network.

[0014] The following non-limiting examples are introduced for illustrative purposes. In a first example, the tool listening device is deployed in a meter repair facility to diagnose a particular smart meter that is defective or needs reconfiguration. The tool listener selects an initial channel according to a discovery channel hopping sequence and listens for communications for a predetermined amount of time. The predetermined amount of time can differ from the length of a time slot on a mesh network. Upon receiving communications, the tool listener filters out communications from the particular smart meter (or attempts at communications from the smart meter), stores the communications in a data structure, and then optionally provides the data to an external device. In an aspect, the tool listener can cause the particular device to join a temporary or diagnostic network in order to receive reprogramming commands.

[0015] In a second example, the tool listener is provided with a discovery channel hopping configuration including channels of a channel hopping sequence used by a particular network of meters. The tool listener selects an initial channel from the channel hopping sequence on which to listen and listens for a particular amount of time. If the tool listener detects activity on the channel, the tool listener attempts to receive a packet. A packet includes a preamble, a sync word, a header and a payload. The tool listener discards the payload of the packet and analyzes the header.

[0016] The tool listener stores the contents of the header, specifically a source address, a destination address, and a frame type, and provides this information to a tool listening application, which can visualize the information. The tool listener then selects a different channel in the discovery channel hopping sequence and continues to listen. Over time, the tool listener gathers information on previously unknown devices and networks and amasses an inventory of the number and type of devices within a certain range. Additionally, by querying an external database, the tool listener can determine whether any devices were removed or are no longer attempting to join a network.

[0017] Turning now to the figures, Figure 1 illustrates an example of a tool listener environment, according to an aspect. Tool listener environment 100 includes tool listener system 101 and unknown radio environment 120. Tool listener system 101 includes one or more of tool listener 102, tool listener computing device 110, tool listener application 112, and data link 105. Unknown radio environment 120 includes one or more unknown radios 130a-n. Unknown radios 130a-n can be within smart meters or other grid devices.

[0018] By listening for traffic on different channels, tool listener 102 can determine whether any of unknown radios 130a-n are present in a wireless environment. Tool listener 102 can operate on wireless networks such as mesh networks, IEEE 802.15.4 networks, WiFi networks, Bluetooth networks, or other wireless networks.

[0019] In an example, tool listener 102 listens on a particular channel for a predetermined amount of time to detect the presence of any unknown radios 130a-n. Unknown radios 130a-n can operate within a channel hopping sequence that can be specific to a particular network. Tool listener 102 can operate in conjunction with tool listener computing device 110 and tool listener application 112 to detect the presence of one or more unknown radios 130a-n. For example, tool listener 102 can transmit data obtained by listening such as packets, headers, source addresses or destination addresses, or frame types across data link 105 to tool listener computing device 110 for further analysis and visualization.

[0020] Data link 105 can be a Universal Serial Bus (USB) connection, a Bluetooth connection, an Ethernet connection, a wireless connection, serial or parallel connection, or any suitable data link. Tool listener computing device 110 can be a laptop, desktop, tablet computer, mobile phone, or any other computing device. Tool listener application 112 executes on tool listener computing device 110 and which can perform some or all of the functionality described herein.

[0021] Figure 2 illustrates an implementation of a tool listener system, according to an aspect. Figure 2 depicts tool listener system 200, which includes tool listener 201 and tool listener computing device 110. Tool listener 201 is an example of an implementation of tool listener 102. Tool listener 201 includes one or more of radio 220, processor 230, antenna 240, and data transceiver 250.

[0022] Radio 220 is a radio receiver or transmitter/receiver combination configured to operate according to a particular protocol such as IEEE 802.15.4. Radio 220 is connected to antenna 240. Antenna 240 can be any kind of antenna. Examples of suitable antennas include directional antennas or omnidirectional antennas. A directional antenna allows tool listener 201 to gather stronger signals from a particular area where smart meters are expected to be located. An omnidirectional antenna can be useful if a general location of unknown devices is not known. Radio 220 can receive commands from processor 230 such as when to listen, move to a different channel, power on, or power off, and can send received packet data back to processor 230.

[0023] Processor 230 can be any suitable microcontroller, microprocessor, signal processor, or embedded processor such as an Intel®-based processor, ARM®-based processor, etc. Processor 230 can execute firmware or software that performs the functions described herein such as processing packets and issuing commands to radio 220. Data transceiver 250 is a communications device that can send data and commands over data link 105 to tool listener computing device 110 and receive data and commands from tool listener computing device 110 over data link 105.

[0024] Processor 230 performs various functionality related to diagnostics of wireless networks. For example, processor 230 can access a particular discovery channel hopping sequence, configure radio 220 to operate at a particular channel for a particular amount of time, receive data from radio 220 or send data from radio 220.

[0025] Figure 3 is a flowchart illustrating a process used by a tool listening device to detect a presence of another device, according to an aspect. Process 300 can be implemented by tool listener 102, tool listener 201, or by another device. Process 300 can be used to detect the presence of one or more unknown radio devices such as smart meters.

[0026] At block 301, process 300 involves listening on a radio channel selected from a discovery channel hopping sequence. Smart meters on a mesh network synchronize to an agreed-upon time slot and operate according to a channel hopping sequence. A channel hopping sequence as used by a mesh network device includes a list of valid channels, a channel spacing, a bit rate, and a modulation index. In contrast, the discovery channel sequence used by tool listener 102 can be a different sequence from a sequence used by a channel hopping sequence used by the radio frequency device and can include radio channels used by the channel hopping sequence of the radio frequency device.

[0027] Further, tool listener 102 operates asynchronously from broadcasts from unknown radios 130a-n and any other mesh networks. Tool listener 102 need not synchronize with or join a mesh network. Rather, tool listener 102 remains on a channel for a predetermined amount of time unless a packet is detected. The predetermined amount of time need not equal the amount of time of a network time slot, and can be adjusted by configuring the tool listener.

[0028] In an example, processor 230 accesses a particular discovery channel hopping sequence. Processor 230 causes radio 220 to operate at a first channel in the sequence. In turn, radio 220 operates at the first channel and listens for radio transmissions via antenna 240. If a preamble is not detected during the predetermined duration, processor 230 control is passed to block 306. Alternatively, if a preamble is detected, control is passed to block 302.

[0029] At block 302, process 300 involves continuing to listen until the header is received. A packet can include a preamble, a sync word, a packet header, and a payload. Tool listener 102 listens for a preamble, a sync word, and the header of a packet from one of unknown radios 130a-n on the selected channel. A header is received by radio 220 and sent to processor 230.

[0030] Processor 230 can discard the payload information, which is typically not needed, to save memory space. Even though tool listener 102 may not be configured to analyze the payload of the packet, tool listener 102 can receive and inspect the entire packet in order to check for errors. Processor 230 can cause radio 220 to continue to listen until the packet is received and can be checked for errors, even if the predetermined duration has lapsed.

[0031] At block 303, process 300 involves extracting a source address, a destination address, and a frame type from the header. More specifically, processor 230 extracts the packet header and extracts a source address, destination address, and frame type. If the IEEE 802.15.4 Personal Area Network (PAN) ID is present, the Network ID can also be captured. If the IEEE 802.15.4 Header Information Elements (IEs) contain the Network ID, the Network ID can also be captured. A network ID is used to distinguish between networks operated by different utilities e.g. when utility networks are adjacent.

[0032] At block 304, process 300 involves adding the source address, the destination address, the frame type and optional PAN ID and Network ID to a data structure. Tool listener 102 adds the captured information to a data structure.

[0033] In an aspect, processor 230 can aggregate identifiers or flags in the data structure indicating whether the frame type is an acknowledgement, data, beacon, or MAC command, etc. over time for a specific unknown radio 130a-n. The data structure can be stored locally, i.e., in memory connected to processor 230, or stored on tool listening computing device 110.

[0034] Processor 230 can use error detection to check for errors in the received packet. If errors are detected that cannot be recovered, then processor 230 can discard the erroneous packet or cause data transceiver 250 to send a message to the tool listener computing device 110 with any remaining useful information.

[0035] In an aspect, the tool listener receives a particular network address (e.g., a LAN identifier) or a particular Media Access Control (MAC) address of a meter and filter out or ignore other communications. For example, in the case of a specified network address, processor 230 checks the source address in the packet header against a network address corresponding to the specific device. If the network address does not match, then the entire packet is discarded. In this manner, the tool listener can focus on particular networks or devices of interest such as communications from a particular defective meter in a repair shop and ignore other meters that may be in the repair shop.

[0036] In another aspect, tool listener 102 can acquire a location signal from a Global Positioning Systems (GPS) or other location device. Tool listener 102 can access a database of smart devices expected at the location and verify network addresses detected against expected devices from the database to determine a presence of new or erroneous devices.

[0037] At block 305, process 300 involves transmitting the data structure to an external device causing the external device to visualize the data structure. Processor 230 sends the data structure to data transceiver 250 and causes data transceiver 250 to send the information across data link 105 to tool listener computing device 110. Tool listener 102 can maintain the data structure locally and periodically transmit the data structure to the tool listener computing device 110, which can perform further visualization and analysis. Optionally, tool listener computing device 110 periodically queries the radio for this information table and updates the visualization accordingly. In an aspect, tool listener computing device 110 can aggregate, display, or visualize data that indicates whether the frame type is an acknowledgement, data, beacon, or MAC command, etc. over time for a specific unknown radio 130a-n.

[0038] Tool listener computing device 110 can display the data in real-time. Over time, tool listener 102 can capture multiple packets received from a particular unknown radio 130a-n. In this manner, tool listener 102 adds new data and frame types to the table over time to build an aggregate image of the traffic from neighboring radios. In order to visualize a large number of data packets, data can be indexed by MAC address and/or network ID. An example table showing an example of data presented by tool listening computing device 110 is shown in Figure 4.

[0039] At block 306, process 300 involves selecting a next radio channel from the discovery channel hopping sequence. Process 300 continues at block 301, using the next channel. If no network activity is detected during the predetermined amount of time, then processor 230 cycles through the discovery channel hopping sequence, remaining on each channel for the predetermined amount of time. Processor 230 need not cycle through the channels of the discovery channel hopping sequence in the same order defined by the channel hopping sequence; different orders of channels are possible.

[0040] Figure 4 is a table illustrating data relating to radio devices detected by a tool listening device, according to an aspect. Figure 4 depicts table 400. Table 400 can be populated by tool listener system 101, tool listener system 200, or by another suitable system or device executing process 300 or a similar process.

[0041] Table 400 includes entries 401a-n. Each entry can correspond to a detected packet from a wireless network. For example, each entry 401a-n includes a LAN address (address of a particular device), PAN ID (or network address), ACK (acknowledgement), MAC Command, DATA, and BEACON.

[0042] The ACK field refers to whether the packet is an acknowledgement packet. The DATA field refers to whether the packet includes a data field. A BEACON field in a packet indicates that the packet includes a beacon request. A MAC COMMAND beacon request packet may indicate that a particular radio has not been successful in establishing a connection with a network and is attempting to communicate. Other fields are possible. A technician may use information gathered from the tool listener to determine that the radio is not properly configured or is defective.

[0043] As depicted, entry 401a includes LAN address ab:cd:ef:01:02:03, PAN ID 10:01, ACK 0, DATA 1, BEACON 0, MAC COMMAND 1. Entry 401b includes LAN address ab:cd:ef:10:20:30, PAN ID 10:01, ACK 0, DATA 0, BEACON 1 and MAC COMMAND 0. Entry 401c includes LAN address ac:99:88:77:11:22, PAN ID 20:21, ACK 1, DATA 0, BEACON 0 and MAC COMMAND 1. Entry 401d includes LAN address ac:99:88:66:22:33, PAN ID 20:11, ACK 0, DATA 0, BEACON 0 and MAC COMMAND 1.

[0044] As can be seen, entries 401a and 401b have the same PAN ID and are likely communicating on the same network. In an aspect, entries originating from or destined for the same address can be aggregated to enable easier viewing.

Exemplary Computing Environment

[0045] Figure 5 illustrates computing environment 500 used to implement certain functions of a tool listener, according to an aspect. Any suitable computing system or device may be used for performing the operations described herein such as implementing the functions of tool listener 102, tool listener external computing device 110, or process 300. The depicted computing device 501 includes a processor 502 communicatively coupled to one or more memory devices 504. The processor 502 executes computer-executable program code 530 stored in a memory device 504, accesses data 520 stored in the memory device 504, or both. Examples of the processor 502 include a microprocessor, an application-specific integrated circuit (“ASIC”), a field-programmable gate array (“FPGA”), or any other suitable processing device. The processor 502 can include any number of processing devices or cores, including a single processing device. The functionality of the computing device may be implemented in hardware, software, firmware, or a combination thereof.

[0046] The memory device 504 includes any suitable non-transitory computer-readable medium for storing data, program code, or both. A computer-readable medium can include any electronic, optical, magnetic, or other storage device capable of providing a processor with computer-readable instructions or other program code. Non-limiting examples of a computer-readable medium include a flash memory, a ROM, a RAM, an ASIC, or any other medium from which a processing device can read instructions. The instructions may include processor-specific instructions generated by a compiler or an interpreter from code written in any suitable computer-programming language, including, for example, C, C++, C#, Visual Basic, Java, or scripting language.

[0047] The computing device 501 may also include a number of external or internal devices, such as input or output devices. For example, the computing device 501 is shown with one or more input/output ("I/O") interfaces 508. An I/O interface 508 can receive input from input devices or provide output to output devices. One or more busses 506 are also included in the computing device 501. The bus 506 communicatively couples one or more components of a respective one of the computing device 501.

[0048] The computing device 501 executes program code 530 that configures the processor 502 to perform one or more of the operations described herein. For example, the program code 530 causes the processor to perform the operations described in Figures 3.

[0049] The computing device 501 also includes a network interface device 510. The network interface device 510 includes any device or group of devices suitable for establishing a wired or wireless data connection to one or more data networks. The network interface device 510 may be a wireless device and have an antenna 514. The computing device 501 can communicate with one or more other computing devices implementing the computing device or other functionality via a data network using the network interface device 510.

[0050] The computing device 501 can also include a display device 512. Display device 512 can be a LCD, LED, touch-screen or other device operable to display information about the computing device 501. For example, information could include an operational status of the computing device, network status, etc.

[0051] While the present subject matter has been described in detail with respect to specific aspects thereof, it will be appreciated that those skilled in the art, upon attaining an understanding of the foregoing, may readily produce alterations to, variations of, and equivalents to such aspects. Accordingly, it should be understood that the present disclosure has been presented for purposes of example rather than limitation and does not preclude inclusion of such modifications, variations, and/or additions to the present subject matter as would be readily apparent to one of ordinary skill in the art.

CLAIMS

What is claimed is:

1. A device for detecting communication from a radio, the device comprising a transceiver configured to:

listen on a radio channel selected from a discovery channel hopping sequence, wherein the discovery channel hopping sequence (i) uses a different sequence from a sequence used by a channel hopping sequence used by the radio and (ii) comprises a plurality of radio channels used by the channel hopping sequence of the radio;

responsive to identifying a preamble of a packet, the packet comprising a header:

continue to listen until the header is received,

extract, from the header, a source address, a destination address and a frame type,

add the source address, the destination address, and the frame type to a data structure, and

transmit the data structure to an external device, wherein transmitting the data structure causes the external device to visualize the data structure; and

responsive to either (i) receiving a packet or (ii) determining that a predetermined amount of time has lapsed, select a next radio channel from the discovery channel hopping sequence.

2. The device of claim 1, wherein the predetermined amount of time differs from a slot time used by the radio.

3. The device of claim 1, wherein the transceiver is further configured to identify a particular radio by identifying a device identifier corresponding to the particular radio from the preamble.

4. The device of claim 1, wherein the external device identifies, from the data structure, a first packet and a second packet, wherein the first packet and the second packet originate from a particular radio, and displays information from the first packet and the second packet together in a visualization.

5. The device of claim 1, wherein the packet further comprises a cyclic redundancy check, and wherein the device is further configured to determine, based on the cyclic redundancy check, that the packet is valid.

6. The device of claim 1, wherein the packet comprises a payload and wherein the device is further configured to discard the payload of the packet.

7. The device of claim 1, wherein the packet is (i) an acknowledgement packet, (ii) a beacon packet, (iii) a beacon request packet, or (iv) a data packet.

8. The device of claim 1, wherein the discovery channel hopping sequence comprises all of the plurality of radio channels used by the channel hopping sequence of the radio.

9. The device of claim 1, wherein the packet further comprises (i) a PAN ID or (ii) a network ID, and wherein the device is further configured to extract the (i) PAN ID or (ii) network ID and provide the (i) PAN ID or (ii) network ID to the external device.

10. A system for detecting radio frequency communication from a radio, the system comprising:

a transceiver configured to:

listen on a radio channel selected from a discovery channel hopping sequence, wherein the discovery channel hopping sequence (i) uses a different sequence from a sequence used by a channel hopping sequence used by the radio and (ii) comprises a plurality of radio channels used by the channel hopping sequence of the radio;

responsive to identifying a preamble of a packet, the packet comprising a header:

continue to listen until the header is received,

extract, from the header, a source address, a destination address and a frame type,

add the source address, the destination address, and the frame type to a data structure, and

transmit the data structure to an external device; and responsive to either (i) receiving a packet or (ii) determining that a predetermined amount of time has lapsed, select a next radio channel from the discovery channel hopping sequence,

wherein the external device is configured to:

receive, from the transceiver, the data structure;

extract, from the data structure, a packet comprising a source address, a network address, and a frame type, wherein the frame type comprises acknowledgement, data, or beacon; and

visualize the source address, network address, and frame type on a display device.

11. The system of claim 10, wherein the transceiver is further configured to identify a particular radio by identifying a device identifier corresponding to the particular radio from the preamble.

12. The system of claim 10, wherein the external device identifies, from the data structure, a first packet and a second packet, wherein the first packet and the second packet originate from a particular radio, and displays information from the first packet and the second packet together in a visualization.

13. The system of claim 10, wherein the packet further comprises a cyclic redundancy check, and wherein the transceiver is further configured to determine, based on the cyclic redundancy check, that the packet is valid.

14. The system of claim 10, wherein packet comprises a payload and wherein the transceiver is further configured to discard the payload of the packet.

15. The system of claim 10, wherein the discovery channel hopping sequence comprises all of the plurality of radio channels used by the channel hopping sequence of the radio.

16. A computer-readable storage medium storing non-transitory computer-executable program instructions, wherein when executed by a processing device, the program instructions cause the processing device to perform operations comprising:

listening on a radio channel selected from a discovery channel hopping sequence, wherein the discovery channel hopping sequence (i) uses a different sequence from a sequence used by a channel hopping sequence used by a radio and (ii) comprises a plurality of radio channels used by the channel hopping sequence of the radio;

responsive to identifying a preamble of a packet, the packet comprising a header :

continuing to listen until the header is received,

extracting, from the header, a source address, a destination address and a frame type,

adding the source address, the destination address, and the frame type to a data structure, and

transmitting the data structure to an external device, wherein transmitting the data structure causes the external device to visualize the data structure; and

responsive to either (i) receiving a packet or (ii) determining that a predetermined amount of time has lapsed, selecting a next radio channel from the discovery channel hopping sequence.

17. The computer-readable storage medium of claim 16, the operations further comprising identifying a particular radio by identifying a device identifier corresponding to the particular radio from the preamble.

18. The computer-readable storage medium of claim 16, wherein transmitting the data structure to an external device causes the external device to identify, from the data structure, a first packet and a second packet, wherein the first packet and the second packet originate from a particular radio, and displays information from the first packet and the second packet together in a visualization.

19. The computer-readable storage medium of claim 16, wherein the packet comprises a payload and wherein the operations further comprise discarding the payload of the packet.

20. The computer-readable storage medium of claim 16, wherein the discovery channel hopping sequence comprises all of plurality of the radio channels used by the channel hopping sequence of the radio.

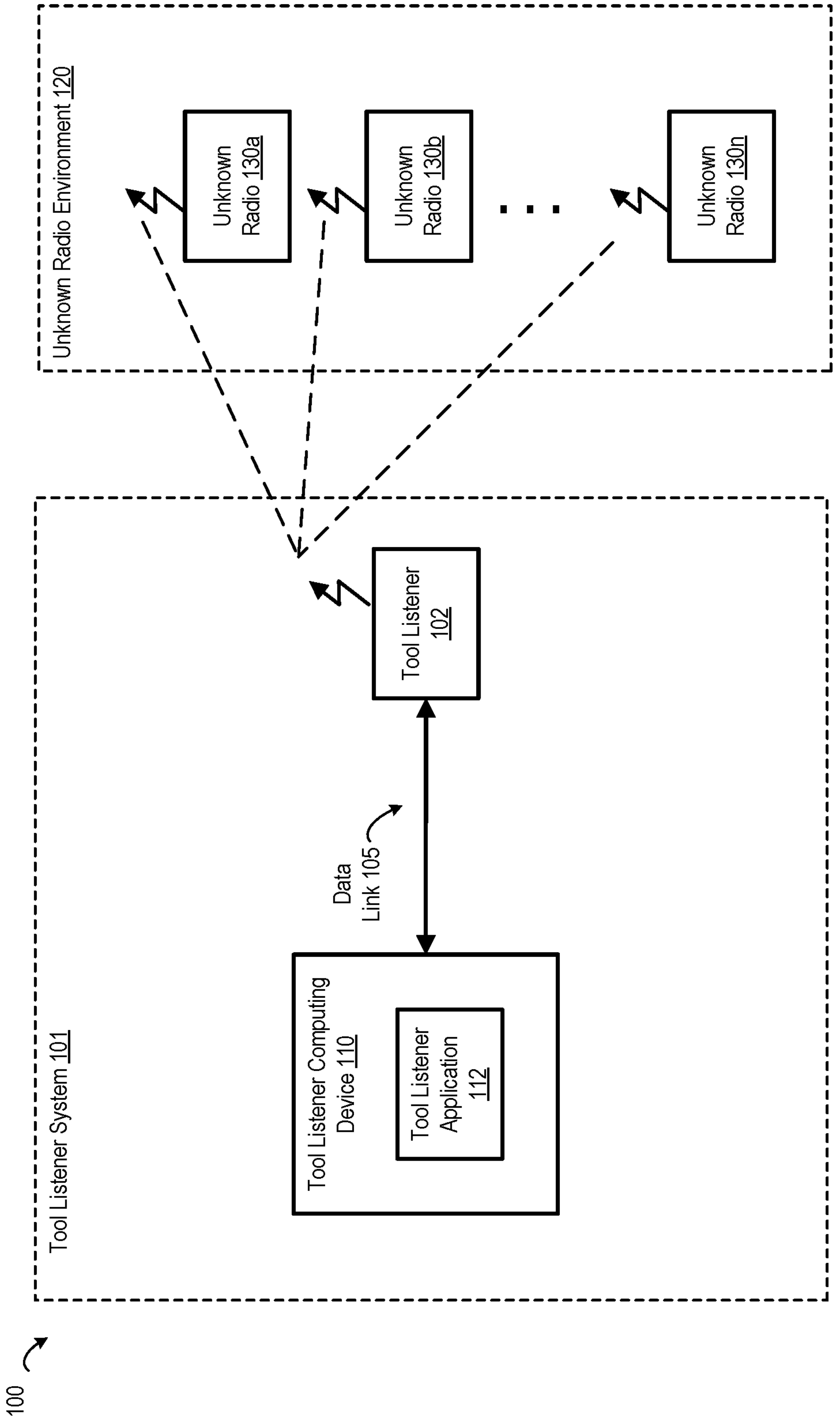
Unknown Radio Environment 120
Unknown Radio 130a
Unknown Radio 130b
. . .
Unknown Radio 130n
Tool Listener System 101
Tool Listener 102
Data Link 105
Tool Listener Computing Device 110
Tool Listener Application 112
100

FIG. 1

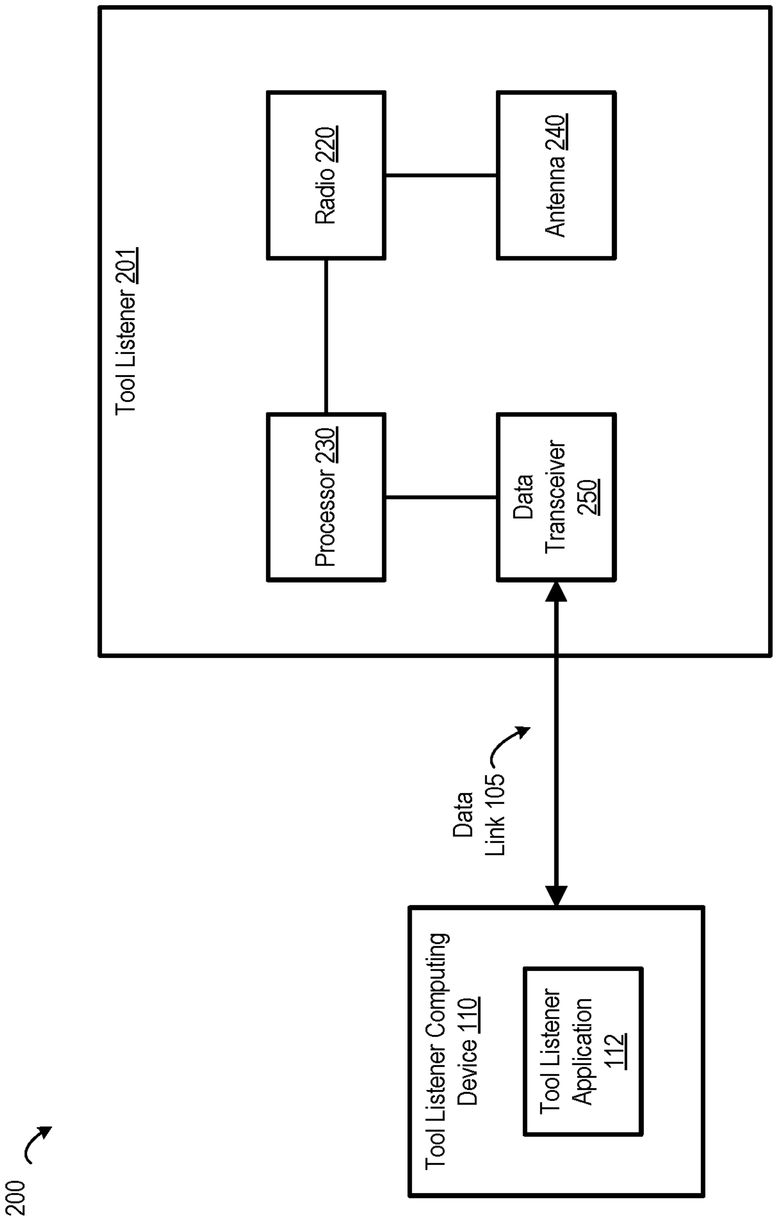
200
Tool Listener Computing Device 110
Tool Listener Application 112
Data Link 105
Tool Listener 201
Radio 220
Antenna 240
Processor 230
Data Transceiver 250

FIG. 2

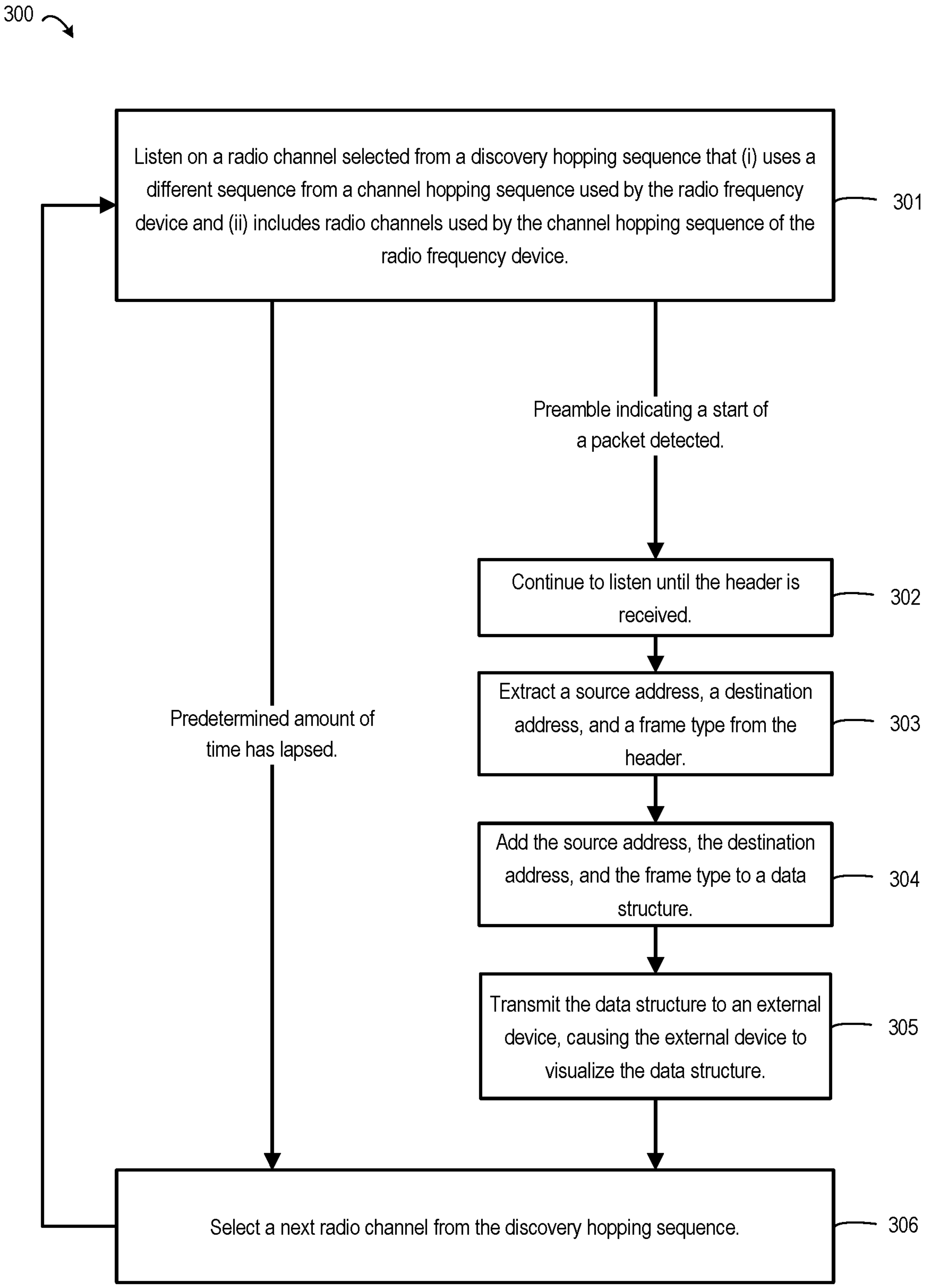
300
Listen on a radio channel selected from a discovery hopping sequence that (i) uses a different sequence from a channel hopping sequence used by the radio frequency device and (ii) includes radio channels used by the channel hopping sequence of the radio frequency device.
301
Preamble indicating a start of a packet detected.
Continue to listen until the header is received.
302
Extract a source address, a destination address, and a frame type from the header.
303
Predetermined amount of time has lapsed.
Add the source address, the destination address, and the frame type to a data structure.
304
Transmit the data structure to an external device, causing the external device to visualize the data structure.
305
Select a next radio channel from the discovery hopping sequence.
306

FIG. 3

400

401a
401b
401c
401d
401n

LAN address	PAN ID	TYPE			
		ACK	DATA	BEACON	MAC COMMAND
ab:cd:ef:01:02:03	10:01	0	1	0	1
ab:cd:ef:01:20:30	10:01	0	0	1	0
ac:99:88:77:11:22	20:21	1	0	0	1
ac:99:88:66:22:33	22:11	0	0	0	1

FIG. 4

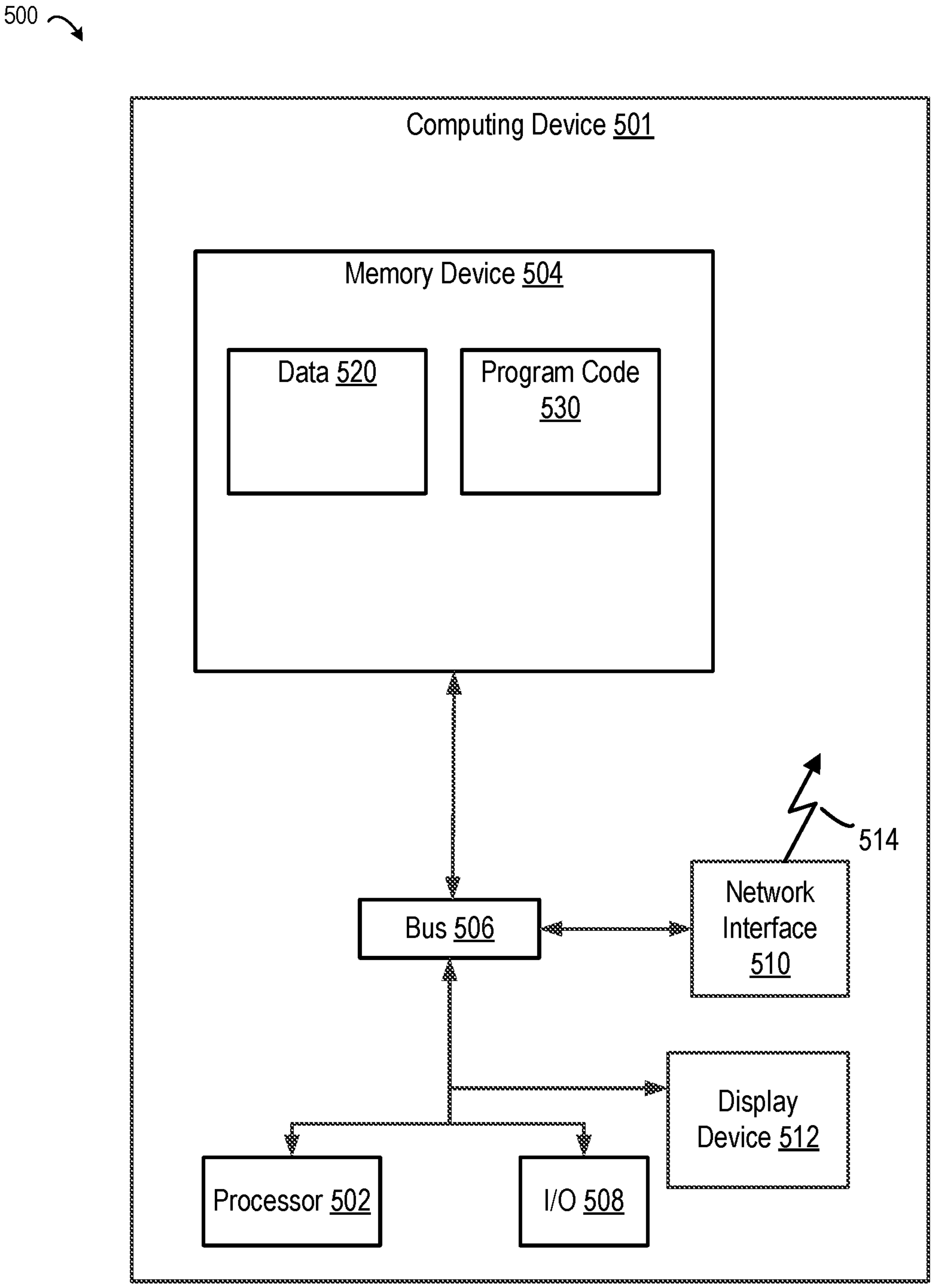
500
Computing Device 501
Memory Device 504
Data 520
Program Code 530
514
Bus 506
Network Interface 510
Display Device 512
Processor 502
I/O 508

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/048515

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/24 H04L12/26 H04B7/26
ADD.

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)
H04B H04L H04W

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)", IEEE STANDARD; [IEEE STANDARD], IEEE, PISCATAWAY, NJ, USA, 1 January 2005 (2005-01-01), pages _1-580, XP017694296, ISBN: 978-0-7381-4707-9 page 28, paragraph 6.4.3 Generic packet structure - page 117, paragraph 8.8.4.2 Inquiry substate page 224, paragraph 11.3 Overview of commands and events - page 229, paragraph 11.3.8 Remote information -/--	1-20

☒ 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 another citation or other special reason (as specified)

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search 4 November 2019	Date of mailing of the international search report 12/11/2019
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Fischer, Erik

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2019/048515

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 566, paragraph B.6.1 General inquiry - page 570, paragraph B.6.3.3 Device discovery -----	
A	Naresh Gupta: "Inside Bluetooth Low Energy" In: "Inside Bluetooth Low Energy", 1 March 2013 (2013-03-01), Artech House, XP055623746, ISBN: 978-1-60807-579-9 pages ToC,Ch01-Ch10,Ch15,, page 60, paragraph 3.5 Host Controller Interface (HCI) - page 128, paragraph 5.4.3 Code page 356, paragraph 16.3 Advertising and Scanning - page 358, paragraph 16.3 Advertising and Scanning -----	1-20
A	CA 2 717 641 A1 (ELSTER SOLUTIONS LLC [US]) 30 April 2011 (2011-04-30) paragraph [0029] - paragraph [0098]; figures 1-5 -----	1-20
A	MIKE RYAN ISEC PARTNERS: "Bluetooth: With Low Energy comes Low Security", USENIX, USENIX, THE ADVANCED COMPUTING SYSTEMS ASSOCIATION, 26 September 2013 (2013-09-26), pages 1-7, XP061008598, [retrieved on 2013-09-26] page 1, paragraph 2 Bluetooth Low Energy - page 4, paragraph 5 Injection -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2019/048515

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
CA 2717641	A1	30-04-2011	NONE	