



(51) International Patent Classification:

H04W 4/50 (2018.01) H04W 8/00 (2009.01)
H04W 12/04 (2009.01) H04W 84/18 (2009.01)
H04W 72/12 (2009.01)

(21) International Application Number:

PCT/US2017/068482

(22) International Filing Date:

27 December 2017 (27.12.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/551,803 30 August 2017 (30.08.2017) US

(71) Applicant: **INTEL IP CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).

(72) Inventors: **QI, Emily H.**; 8407 104th St., Gig Harbor, Washington 98332 (US). **PEER, Ilan**; 24/1 Mivtza Yonatan

St., 71721 Modiin (IL). **OREN, Elad**; 2 Yohanan Horcanus St., 62493 Tel Aviv (IL).

(74) Agent: **SHICHRUR, Naim Avraham**; SHICHRUR & CO., Azrieli Business Center, 132 Menachem Begin Blvd., Triangle Tower, 38th Floor, 6701101 Tel Aviv (IL).

(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,

(54) Title: APPARATUS, SYSTEM AND METHOD OF SECURE NEIGHBOR AWARENESS NETWORKING (NAN) COMMUNICATION

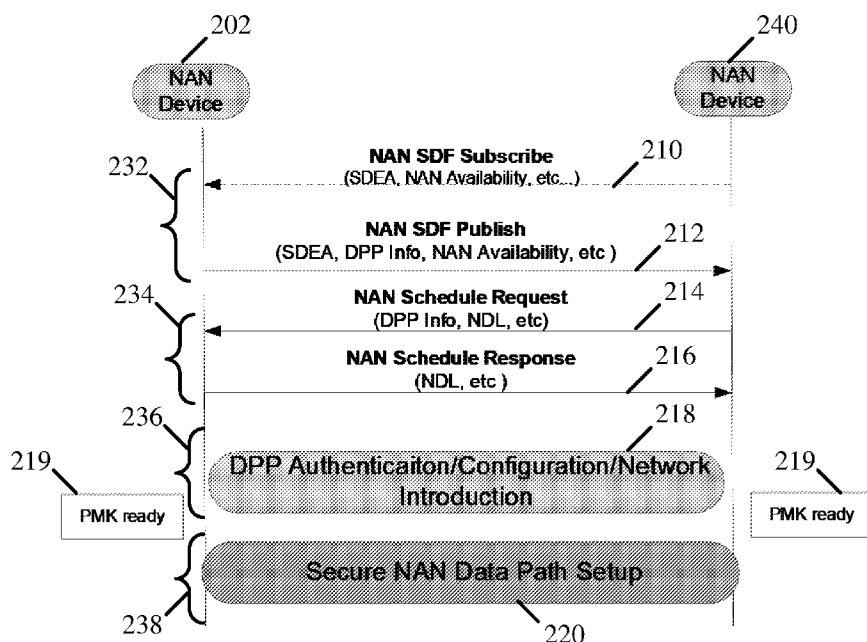


Fig. 2

(57) Abstract: Some demonstrative embodiments include apparatuses, systems and/or methods of secure Neighbor Awareness Networking (NAN) communication. For example, an apparatus may include logic and circuitry configured to cause a first NAN device to setup a NAN schedule with a second NAN device; to exchange with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and second NAN devices; and to setup a secure NAN Data Path (NDP) with the second NAN device based on the security key.

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

Declarations under Rule 4.17:

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

Published:

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

APPARATUS, SYSTEM AND METHOD OF SECURE NEIGHBOR AWARENESS NETWORKING (NAN) COMMUNICATION

5

CROSS REFERENCE

[001] This Application claims the benefit of and priority from US Provisional Patent Application No. 62/551,803 entitled “APPARATUS, SYSTEM AND METHOD OF SECURE NEIGHBOR AWARENESS NETWORKING (NAN) COMMUNICATION”, filed August 30, 2017, the entire disclosure of which is incorporated herein by reference.

10

TECHNICAL FIELD

[002] Embodiments described herein generally relate to secure Neighbor Awareness Networking (NAN) communication.

15

BACKGROUND

[003] Awareness networking, for example, according to a Wi-Fi Aware Specification, may enable wireless devices, for example, Wi-Fi devices, to perform device/service discovery, e.g., in their close proximity.

[004] The awareness networking may include forming a cluster, e.g., a Wi-Fi Aware cluster, for devices in proximity. Devices in the same Wi-Fi Aware cluster may be configured to follow the same time schedule, e.g., a discovery window (DW), for example, to facilitate cluster formation and/or to achieve low power operation.

20

BRIEF DESCRIPTION OF THE DRAWINGS

[005] For simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity of presentation. Furthermore, reference numerals may be repeated among the figures to indicate corresponding or analogous elements. The figures are listed below.

[006] Fig. 1 is a schematic block diagram illustration of a system, in accordance with some demonstrative embodiments.

[007] Fig. 2 is a schematic illustration of communications between Neighbor Awareness Networking (NAN) devices to setup a secure NAN Data Path (NDP), in accordance with some demonstrative embodiments.

[008] Fig. 3 is a schematic flow-chart illustration of a method of secure Neighbor Awareness Networking (NAN) communication, in accordance with some demonstrative embodiments.

[009] Fig. 4 is a schematic illustration of a product, in accordance with some demonstrative embodiments.

DETAILED DESCRIPTION

[0010] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of some embodiments. However, it will be understood by persons of ordinary skill in the art that some embodiments may be practiced without these specific details. In other instances, well-known methods, procedures, components, units and/or circuits have not been described in detail so as not to obscure the discussion.

[0011] Discussions herein utilizing terms such as, for example, “processing”, “computing”, “calculating”, “determining”, “establishing”, “analyzing”, “checking”, or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulate and/or transform data represented as physical (e.g., electronic) quantities within the computer’s registers and/or memories into other data similarly represented as physical quantities within the computer’s registers and/or memories or other information storage medium that may store instructions to perform operations and/or processes.

[0012] The terms “plurality” and “a plurality”, as used herein, include, for example, “multiple” or “two or more”. For example, “a plurality of items” includes two or more items.

[0013] References to “one embodiment”, “an embodiment”, “demonstrative embodiment”, “various embodiments” etc, indicate that the embodiment(s) so described may include a particular feature, structure, or characteristic, but not every embodiment necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrase “in one embodiment” does not necessarily refer to the same embodiment, although it may.

[0014] As used herein, unless otherwise specified the use of the ordinal adjectives “first”, “second”, “third” etc, to describe a common object, merely indicate that different instances of like objects are being referred to, and are not intended to imply that the objects so described must be in a given sequence, either temporally, spatially, in ranking, or in any other manner.

[0015] Some embodiments may be used in conjunction with devices and/or networks operating in accordance with existing (WiFi) Alliance (WFA) Specifications (including *Wi-Fi Neighbor Awareness Networking (NAN) Technical Specification, Version 1.0, May 1, 2015*) and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing WFA Peer-to-Peer (P2P) specifications (*WiFi P2P technical specification, version 1.7, July 6, 2016*) and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing IEEE 802.11 standards (including IEEE 802.11-2016 (*IEEE 802.11-2016, IEEE Standard for Information technology--Telecommunications and*

information exchange between systems Local and metropolitan area networks--Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, December 7, 2016)) and/or future versions and/or derivatives thereof, devices and/or networks operating in accordance with existing cellular specifications and/or protocols, e.g., 3rd Generation Partnership Project (3GPP), 3GPP Long Term Evolution (LTE) and/or future versions and/or derivatives thereof, units and/or devices which are part of the above networks, and the like.

[0016] Some embodiments may be used in conjunction with one way and/or two-way radio communication systems, cellular radio-telephone communication systems, a mobile phone, a cellular telephone, a wireless telephone, a Personal Communication Systems (PCS) device, a PDA device which incorporates a wireless communication device, a mobile or portable Global Positioning System (GPS) device, a device which incorporates a GPS receiver or transceiver or chip, a device which incorporates an RFID element or chip, a Multiple Input Multiple Output (MIMO) transceiver or device, a Single Input Multiple Output (SIMO) transceiver or device, a Multiple Input Single Output (MISO) transceiver or device, a device having one or more internal antennas and/or external antennas, Digital Video Broadcast (DVB) devices or systems, multi-standard radio devices or systems, a wired or wireless handheld device, e.g., a Smartphone, a Wireless Application Protocol (WAP) device, or the like.

[0017] Some embodiments may be used in conjunction with one or more types of wireless communication signals and/or systems, for example, Radio Frequency (RF), Infra Red (IR), Frequency-Division Multiplexing (FDM), Orthogonal FDM (OFDM), Orthogonal Frequency-Division Multiple Access (OFDMA), FDM Time-Division Multiplexing (TDM), Time-Division Multiple Access (TDMA), Multi-User MIMO (MU-MIMO), Extended TDMA (E-TDMA), General Packet Radio Service (GPRS), extended GPRS, Code-Division Multiple Access (CDMA), Wideband CDMA (WCDMA), CDMA 2000, single-carrier CDMA, multi-carrier CDMA, Multi-Carrier Modulation (MDM), Discrete Multi-Tone (DMT), Bluetooth®, Global Positioning System (GPS), Wi-Fi, Wi-Max, ZigBee™, Ultra-Wideband (UWB), Global System for Mobile communication (GSM), 2G, 2.5G, 3G, 3.5G, 4G, Fifth Generation (5G) mobile networks, 3GPP, Long Term Evolution (LTE), LTE advanced, Enhanced Data rates for GSM Evolution (EDGE), or the like. Other embodiments may be used in various other devices, systems and/or networks.

[0018] The term “wireless device”, as used herein, includes, for example, a device capable of wireless communication, a communication device capable of wireless communication, a

communication station capable of wireless communication, a portable or non-portable device capable of wireless communication, or the like. In some demonstrative embodiments, a wireless device may be or may include a peripheral that may be integrated with a computer, or a peripheral that may be attached to a computer. In some demonstrative embodiments, the term
5 “wireless device” may optionally include a wireless service.

[0019] The term “communicating” as used herein with respect to a communication signal includes transmitting the communication signal and/or receiving the communication signal. For example, a communication unit, which may be capable of communicating a communication signal, may include a transmitter to transmit the communication signal to at least one other
10 communication unit, and/or a communication receiver to receive the communication signal from at least one other communication unit. The verb communicating may be used to refer to the action of transmitting or the action of receiving. In one example, the phrase “communicating a signal” may refer to the action of transmitting the signal by a first device, and may not necessarily include the action of receiving the signal by a second device. In another example, the
15 phrase “communicating a signal” may refer to the action of receiving the signal by a first device, and may not necessarily include the action of transmitting the signal by a second device.

[0020] Some demonstrative embodiments may be used in conjunction with a WLAN, e.g., a WiFi network. Other embodiments may be used in conjunction with any other suitable wireless communication network, for example, a wireless area network, a “piconet”, a WPAN, a WVAN
20 and the like.

[0021] As used herein, the term "circuitry" may refer to, be part of, or include, an Application Specific Integrated Circuit (ASIC), an integrated circuit, an electronic circuit, a processor (shared, dedicated, or group), and/or memory (shared, dedicated, or group), that execute one or more software or firmware programs, a combinational logic circuit, and/or other suitable
25 hardware components that provide the described functionality. In some embodiments, the circuitry may be implemented in, or functions associated with the circuitry may be implemented by, one or more software or firmware modules. In some embodiments, circuitry may include logic, at least partially operable in hardware.

[0022] The term “logic” may refer, for example, to computing logic embedded in circuitry of a
30 computing apparatus and/or computing logic stored in a memory of a computing apparatus. For example, the logic may be accessible by a processor of the computing apparatus to execute the computing logic to perform computing functions and/or operations. In one example, logic may be embedded in various types of memory and/or firmware, e.g., silicon blocks of various chips

and/or processors. Logic may be included in, and/or implemented as part of, various circuitry, e.g. radio circuitry, receiver circuitry, control circuitry, transmitter circuitry, transceiver circuitry, processor circuitry, and/or the like. In one example, logic may be embedded in volatile memory and/or non-volatile memory, including random access memory, read only memory, programmable memory, magnetic memory, flash memory, persistent memory, and/or the like. Logic may be executed by one or more processors using memory, e.g., registers, buffers, stacks, and the like, coupled to the one or more processors, e.g., as necessary to execute the logic.

[0023] The term “antenna”, as used herein, may include any suitable configuration, structure and/or arrangement of one or more antenna elements, components, units, assemblies and/or arrays. In some embodiments, the antenna may implement transmit and receive functionalities using separate transmit and receive antenna elements. In some embodiments, the antenna may implement transmit and receive functionalities using common and/or integrated transmit/receive elements. The antenna may include, for example, a phased array antenna, a single element antenna, a set of switched beam antennas, and/or the like.

[0024] The phrase “peer to peer (PTP) communication”, as used herein, may relate to device-to-device communication over a wireless link (“peer-to-peer link”) between devices. The PTP communication may include, for example, a WiFi Direct (WFD) communication, e.g., a WFD Peer to Peer (P2P) communication, wireless communication over a direct link within a QoS basic service set (BSS), a tunneled direct-link setup (TDLS) link, a STA-to-STA communication in an independent basic service set (IBSS), or the like.

[0025] Some demonstrative embodiments are described herein with respect to WiFi communication. However, other embodiments may be implemented with respect to any other communication scheme, network, standard and/or protocol.

[0026] Reference may be now made to Fig. 1, which schematically illustrates a block diagram of a system 100, in accordance with some demonstrative embodiments.

[0027] As shown in Fig. 1, in some demonstrative embodiments system 100 may include a wireless communication network including one or more wireless communication devices, e.g., including wireless communication devices 102 and/or 140.

[0028] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may include, for example, a UE, an MD, a STA, an AP, a PC, a desktop computer, a mobile computer, a laptop computer, an UltrabookTM computer, a notebook computer, a tablet computer, a server computer, a handheld computer, a handheld device, an Internet of Things (IoT) device, a sensor device, a wearable device, a PDA device, a handheld PDA device, an on-board device, an

off-board device, a hybrid device (e.g., combining cellular phone functionalities with PDA device functionalities), a consumer device, a vehicular device, a non-vehicular device, a mobile or portable device, a non-mobile or non-portable device, a mobile phone, a cellular telephone, a PCS device, a PDA device which incorporates a wireless communication device, a mobile or portable GPS device, a DVB device, a relatively small computing device, a non-desktop computer, a “Carry Small Live Large” (CSLL) device, an Ultra Mobile Device (UMD), an Ultra Mobile PC (UMPC), a Mobile Internet Device (MID), an “Origami” device or computing device, a device that supports Dynamically Composable Computing (DCC), a context-aware device, a video device, an audio device, an A/V device, a Set-Top-Box (STB), a Blu-ray disc (BD) player, a BD recorder, a Digital Video Disc (DVD) player, a High Definition (HD) DVD player, a DVD recorder, a HD DVD recorder, a Personal Video Recorder (PVR), a broadcast HD receiver, a video source, an audio source, a video sink, an audio sink, a stereo tuner, a broadcast radio receiver, a flat panel display, a Personal Media Player (PMP), a digital video camera (DVC), a digital audio player, a speaker, an audio receiver, an audio amplifier, a gaming device, a data source, a data sink, a Digital Still camera (DSC), a media player, a Smartphone, a television, a music player, or the like.

[0029] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, one or more STAs. For example, device 102 may include at least one STA, and/or device 140 may include at least one STA.

[0030] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, one or more WLAN STAs.

[0031] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, one or more Wi-Fi STAs.

[0032] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, one or more Bluetooth (BT) devices.

[0033] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, one or more Neighbor Awareness Networking (NAN) STAs.

[0034] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, one or more location measurement STAs.

[0035] In one example, a station (STA) may include a logical entity that may be a singly addressable instance of a medium access control (MAC) and physical layer (PHY) interface to

the wireless medium (WM). The STA may perform any other additional or alternative functionality.

[0036] In some demonstrative embodiments, devices 102 and/or 140 may include, operate as, and/or perform the functionality of, any other devices and/or STAs.

5 [0037] In some demonstrative embodiments, devices 102 and/or 140 may be configured to operate as, and/or to perform the functionality of, an access point (AP) STA.

[0038] In some demonstrative embodiments, devices 102 and/or 140 may be configured to operate as, and/or to perform the functionality of, a non-AP STA.

10 [0039] In one example, an AP may include an entity that contains a station (STA), e.g., one STA, and provides access to distribution services, via the wireless medium (WM) for associated STAs. The AP may perform any other additional or alternative functionality.

[0040] In one example, a non-AP STA may include a STA that may be not contained within an AP. The non-AP STA may perform any other additional or alternative functionality.

15 [0041] In one example, device 102 may be configured to operate as, and/or to perform the functionality of, an AP STA, and/or device 140 may be configured to operate as, and/or to perform the functionality of, a non-AP STA.

[0042] In some demonstrative embodiments, device 102 may include, for example, one or more of a processor 191, an input unit 192, an output unit 193, a memory unit 194, and/or a storage unit 195; and/or device 140 may include, for example, one or more of a processor 181, an input unit 182, an output unit 183, a memory unit 184, and/or a storage unit 185. Devices 102 and/or 140 may optionally include other suitable hardware components and/or software components. In some demonstrative embodiments, some or all of the components of one or more of devices 102 and/or 140 may be enclosed in a common housing or packaging, and may be interconnected or operably associated using one or more wired or wireless links. In other embodiments, 25 components of one or more of devices 102 and/or 140 may be distributed among multiple or separate devices.

[0043] In some demonstrative embodiments, processor 191 and/or processor 181 may include, for example, a Central Processing Unit (CPU), a Digital Signal Processor (DSP), one or more processor cores, a single-core processor, a dual-core processor, a multiple-core processor, a microprocessor, a host processor, a controller, a plurality of processors or controllers, a chip, a 30 microchip, one or more circuits, circuitry, a logic unit, an Integrated Circuit (IC), an Application-Specific IC (ASIC), or any other suitable multi-purpose or specific processor or controller.

Processor 191 executes instructions, for example, of an Operating System (OS) of device 102 and/or of one or more suitable applications. Processor 181 executes instructions, for example, of an Operating System (OS) of device 140 and/or of one or more suitable applications.

[0044] In some demonstrative embodiments, input unit 192 and/or input unit 182 may include, for example, a keyboard, a keypad, a mouse, a touch-screen, a touch-pad, a track-ball, a stylus, a microphone, or other suitable pointing device or input device. Output unit 193 and/or output unit 183 includes, for example, a monitor, a screen, a touch-screen, a flat panel display, a Light Emitting Diode (LED) display unit, a Liquid Crystal Display (LCD) display unit, a plasma display unit, one or more audio speakers or earphones, or other suitable output devices.

[0045] In some demonstrative embodiments, memory unit 194 and/or memory unit 184 may include, for example, a Random Access Memory (RAM), a Read Only Memory (ROM), a Dynamic RAM (DRAM), a Synchronous DRAM (SD-RAM), a flash memory, a volatile memory, a non-volatile memory, a cache memory, a buffer, a short term memory unit, a long term memory unit, or other suitable memory units. Storage unit 195 and/or storage unit 185 includes, for example, a hard disk drive, a floppy disk drive, a Compact Disk (CD) drive, a CD-ROM drive, a DVD drive, or other suitable removable or non-removable storage units. Memory unit 194 and/or storage unit 195, for example, may store data processed by device 102. Memory unit 184 and/or storage unit 185, for example, may store data processed by device 140.

[0046] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may be capable of communicating content, data, information and/or signals via a wireless medium (WM) 103. In some demonstrative embodiments, wireless medium 103 may include, for example, a radio channel, a cellular channel, a Global Navigation Satellite System (GNSS) Channel, an RF channel, a WiFi channel, an IR channel, a Bluetooth (BT) channel, and the like.

[0047] In some demonstrative embodiments, wireless communication medium 103 may include a wireless communication channel over a 2.4 Gigahertz (GHz) frequency band, a 5GHz frequency band, a millimeterWave (mmWave) frequency band, e.g., a 60GHz frequency band, a Sub 1 Gigahertz (S1G) band, and/or any other frequency band.

[0048] In some demonstrative embodiments, devices 102 and/or 140 may include one or more radios including circuitry and/or logic to perform wireless communication between devices 102, 140 and/or one or more other wireless communication devices. For example, device 102 may include at least one radio 114, and/or device 140 may include at least one radio 144.

[0049] In some demonstrative embodiments, radio 114 may include one or more wireless receivers (Rx) including circuitry and/or logic to receive wireless communication signals, RF

signals, frames, blocks, transmission streams, packets, messages, data items, and/or data. For example, radio 114 may include at least one receiver 116, and/or radio 144 may include at least one receiver 146.

[0050] In some demonstrative embodiments, radios 114 and/or 144 may include one or more wireless transmitters (Tx) including circuitry and/or logic to transmit wireless communication signals, RF signals, frames, blocks, transmission streams, packets, messages, data items, and/or data. For example, radio 114 may include at least one transmitter 118, and/or radio 144 may include at least one transmitter 148.

[0051] In some demonstrative embodiments, radio 114 and/or radio 144, transmitters 118 and/or 148, and/or receivers 116 and/or 146 may include circuitry; logic; Radio Frequency (RF) elements, circuitry and/or logic; baseband elements, circuitry and/or logic; modulation elements, circuitry and/or logic; demodulation elements, circuitry and/or logic; amplifiers; analog to digital and/or digital to analog converters; filters; and/or the like. For example, radio 114 and/or radio 144 may include or may be implemented as part of a wireless Network Interface Card (NIC), and the like.

[0052] In some demonstrative embodiments, radios 114 and/or 144 may be configured to communicate over a 2.4GHz band, a 5GHz band, an mmWave band, a S1G band, and/or any other band.

[0053] In some demonstrative embodiments, radios 114 and/or 144 may include, or may be associated with, one or more antennas 107 and/or 147, respectively.

[0054] In one example, device 102 may include a single antenna 107. In another example, device 102 may include two or more antennas 107.

[0055] In one example, device 140 may include a single antenna 147. In another example, device 140 may include two or more antennas 147.

[0056] Antennas 107 and/or 147 may include any type of antennas suitable for transmitting and/or receiving wireless communication signals, blocks, frames, transmission streams, packets, messages and/or data. For example, antennas 107 and/or 147 may include any suitable configuration, structure and/or arrangement of one or more antenna elements, components, units, assemblies and/or arrays. Antennas 107 and/or 147 may include, for example, antennas suitable for directional communication, e.g., using beamforming techniques. For example, antennas 107 and/or 147 may include a phased array antenna, a multiple element antenna, a set of switched beam antennas, and/or the like. In some embodiments, antennas 107 and/or 147 may implement

transmit and receive functionalities using separate transmit and receive antenna elements. In some embodiments, antennas 107 and/or 147 may implement transmit and receive functionalities using common and/or integrated transmit/receive elements.

[0057] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may form, and/or may communicate as part of, a wireless local area network (WLAN).

[0058] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may form, and/or may communicate as part of, a WiFi network.

[0059] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may form, and/or may communicate as part of, a WiFi Direct (WFD) network, e.g., a WiFi direct services (WFDS) network, and/or may operate as and/or perform the functionality of one or more WFD devices.

[0060] In one example, wireless communication devices 102 and/or 140 may include, may operate as, and/or may perform the functionality of a WiFi Direct device.

[0061] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may be capable of performing awareness networking communications, for example, according to an awareness protocol, e.g., a WiFi aware protocol, and/or any other protocol, e.g., as described below.

[0062] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may be capable of forming, and/or communicating as part of, a Neighbor Awareness Networking (NAN) network, e.g., a WiFi NAN or WiFi Aware network, and/or may perform the functionality of one or more NAN devices (“WiFi aware devices”).

[0063] Some demonstrative embodiments are described herein with respect to one or more NAN devices communicating as part of a NAN network, e.g., a NAN cluster. However, embodiments are not limited to these demonstrative embodiments, and other embodiments may be implemented with respect to any other type of devices and/or STAs communicating as part of any other group, service set, and/or network.

[0064] In some demonstrative embodiments, wireless communication medium 103 may include a direct link, for example, a PTP link, e.g., a WiFi direct P2P link or any other PTP link, for example, to enable direct communication between wireless communication devices 102 and/or 140.

[0065] In some demonstrative embodiments, wireless communication devices 102 and/or 140 may operate as and/or perform the functionality of WFD P2P devices. For example, devices 102

and/or 140 may be able to operate as and/or perform the functionality of a P2P client device, and/or P2P group Owner (GO) device.

[0066] In other embodiments, wireless communication devices 102 and/or 140 may form, and/or communicate as part of, any other network, and/or may perform the functionality of any other wireless devices or stations.

[0067] In some demonstrative embodiments, devices 102 and/or 140 may include one or more applications configured to provide, to share, and/or to use one or more services, e.g., a social application, a file sharing application, a media application and/or the like, for example, using an awareness network, NAN network (“WiFi Aware network”), a PTP network, a P2P network, WFD network, or any other network.

[0068] In some demonstrative embodiments, device 102 may execute an application 125 and/or an application 126. In some demonstrative embodiments, device 140 may execute an application 145.

[0069] In some demonstrative embodiments, devices 102 and/or 140 may be capable of sharing, showing, sending, transferring, printing, outputting, providing, synchronizing, and/or exchanging content, data, and/or information, e.g., between applications and/or services of devices 102 and/or 140 and/or one or more other devices.

[0070] In some demonstrative embodiments, devices 102 and/or 140 may include a controller configured to control one or more operations and/or functionalities of devices 102 and/or 140, for example, one or more operations and/or functionalities of communication, e.g., awareness networking communications, WiFi Aware (NAN) communication and/or any other communication, between devices 102 and/or 140 and/or other devices, and/or any other functionality, e.g., as described below.

[0071] In some demonstrative embodiments, device 102 may include a controller 124, and/or device 140 may include a controller 154. Controller 124 may be configured to perform and/or to trigger, cause, instruct and/or control device 102 to perform, one or more communications, to generate and/or communicate one or more messages and/or transmissions, and/or to perform one or more functionalities, operations and/or procedures between devices 102, 140 and/or one or more other devices; and/or controller 154 may be configured to perform, and/or to trigger, cause, instruct and/or control device 140 to perform, one or more communications, to generate and/or communicate one or more messages and/or transmissions, and/or to perform one or more functionalities, operations and/or procedures between devices 102, 140 and/or one or more other devices, e.g., as described below.

[0072] In some demonstrative embodiments, controllers 124 and/or 154 may include, or may be implemented, partially or entirely, by circuitry and/or logic, e.g., one or more processors including circuitry and/or logic, memory circuitry and/or logic, Media-Access Control (MAC) circuitry and/or logic, Physical Layer (PHY) circuitry and/or logic, baseband (BB) circuitry and/or logic, a BB processor, a BB memory, Application Processor (AP) circuitry and/or logic, an AP processor, an AP memory, and/or any other circuitry and/or logic, configured to perform the functionality of controllers 124 and/or 154, respectively. Additionally or alternatively, one or more functionalities of controllers 124 and/or 154 may be implemented by logic, which may be executed by a machine and/or one or more processors, e.g., as described below.

[0073] In one example, controller 124 may include circuitry and/or logic, for example, one or more processors including circuitry and/or logic, to cause, trigger and/or control a wireless device, e.g., device 102, and/or a wireless station, e.g., a wireless STA implemented by device 102, to perform one or more operations, communications and/or functionalities, e.g., as described herein.

[0074] In one example, controller 154 may include circuitry and/or logic, for example, one or more processors including circuitry and/or logic, to cause, trigger and/or control a wireless device, e.g., device 140, and/or a wireless station, e.g., a wireless STA implemented by device 140, to perform one or more operations, communications and/or functionalities, e.g., as described herein.

[0075] In some demonstrative embodiments, at least part of the functionality of controller 124 may be implemented as part of one or more elements of radio 114, and/or at least part of the functionality of controller 154 may be implemented as part of one or more elements of radio 144.

[0076] In other embodiments, the functionality of controller 124 may be implemented as part of any other element of device 102, and/or the functionality of controller 154 may be implemented as part of any other element of device 140.

[0077] In some demonstrative embodiments, controller 124 may perform one or more one or more operations and/or functionalities of, and/or may cause device 102 to perform one or more operations and/or functionalities of, a NAN engine, e.g., a NAN Discovery Engine (DE), for example to process one or more service queries and/or responses, e.g., from applications and/or services on devices 102 and/or 140, and/or one or more other devices.

[0078] In some demonstrative embodiments, controller 154 may perform one or more one or more operations and/or functionalities of, and/or may cause device 140 to perform one or more

operations and/or functionalities of, a NAN engine, e.g., a NAN Discovery Engine (DE), for example to process one or more service queries and/or responses, e.g., from applications and/or services on devices 102 and/or 140, and/or one or more other devices.

[0079] In some demonstrative embodiments, device 102 may include a message processor 128 configured to generate, process and/or access one or messages communicated by device 102.

[0080] In one example, message processor 128 may be configured to generate one or more messages to be transmitted by device 102, and/or message processor 128 may be configured to access and/or to process one or more messages received by device 102, e.g., as described below. In one example, message processor 128 may be configured to process transmission of one or more messages from a wireless station, e.g., a wireless STA implemented by device 102; and/or message processor 128 may be configured to process reception of one or more messages by a wireless station, e.g., a wireless STA implemented by device 102.

[0081] In some demonstrative embodiments, device 140 may include a message processor 158 configured to generate, process and/or access one or messages communicated by device 140.

[0082] In one example, message processor 158 may be configured to generate one or more messages to be transmitted by device 140, and/or message processor 158 may be configured to access and/or to process one or more messages received by device 140, e.g., as described below. In one example, message processor 158 may be configured to process transmission of one or more messages from a wireless station, e.g., a wireless STA implemented by device 140; and/or message processor 158 may be configured to process reception of one or more messages by a wireless station, e.g., a wireless STA implemented by device 140.

[0083] In some demonstrative embodiments, message processors 128 and/or 158 may include, or may be implemented, partially or entirely, by circuitry and/or logic, e.g., one or more processors including circuitry and/or logic, memory circuitry and/or logic, Media-Access Control (MAC) circuitry and/or logic, Physical Layer (PHY) circuitry and/or logic, BB circuitry and/or logic, a BB processor, a BB memory, AP circuitry and/or logic, an AP processor, an AP memory, and/or any other circuitry and/or logic, configured to perform the functionality of message processors 128 and/or 158, respectively. Additionally or alternatively, one or more functionalities of message processors 128 and/or 158 may be implemented by logic, which may be executed by a machine and/or one or more processors, e.g., as described below.

[0084] In some demonstrative embodiments, controllers 124 and/or 154, and/or message processors 128 and/or 158 may perform one or more operations and/or functionalities of, and/or may cause a STA to perform one or more operations and/or functionalities of, a NAN MAC,

which may be configured to generate, process and/or handle one or more NAN messages, e.g., NAN Beacon frames and/or NAN Service Discovery Frames (SDFs).

[0085] In some demonstrative embodiments, at least part of the functionality of message processor 128 may be implemented as part of radio 114.

5 [0086] In some demonstrative embodiments, at least part of the functionality of message processor 128 may be implemented as part of controller 124.

[0087] In other embodiments, the functionality of message processor 128 may be implemented as part of any other element of device 102.

[0088] In some demonstrative embodiments, at least part of the functionality of controller 124,
10 radio 114, and/or message processor 128 may be implemented by an integrated circuit, for example, a chip, e.g., a System in Chip (SoC). In one example, the chip or SoC may be configured to perform one or more functionalities of radio 114. For example, the chip or SoC may include one or more elements of controller 124, one or more elements of message processor 128, and/or one or more elements of radio 114. In one example, controller 124, message
15 processor 128, and radio 114 may be implemented as part of the chip or SoC.

[0089] In some demonstrative embodiments, at least part of the functionality of message processor 158 may be implemented as part of radio 144.

[0090] In some demonstrative embodiments, at least part of the functionality of message processor 158 may be implemented as part of controller 154.

20 [0091] In other embodiments, the functionality of message processor 158 may be implemented as part of any other element of device 140.

[0092] In some demonstrative embodiments, at least part of the functionality of controller 154, radio 144, and/or message processor 158 may be implemented by an integrated circuit, for example, a chip, e.g., a SoC. In one example, the chip or SoC may be configured to perform one
25 or more functionalities of radio 144. For example, the chip or SoC may include one or more elements of controller 154, one or more elements of message processor 158, and/or one or more elements of radio 144. In one example, controller 154, message processor 158, and radio 144 may be implemented as part of the chip or SoC.

[0093] In some demonstrative embodiments, devices 102 and/or 140 may operate as and/or
30 perform the functionality of a device or station, for example, an awareness networking device, a NAN device, a WiFi device, a WiFi Aware device, a WFD device, a WLAN device, a Low

Power Long Range (LPLR) device, and/or any other device, capable of discovering other devices according to a discovery protocol and/or scheme.

[0094] In some demonstrative embodiments, radios 114 and/or 144 may communicate over wireless communication medium 103 according to an awareness networking scheme, for example, a discovery scheme, for example, a WiFi Aware discovery scheme (“NAN discovery scheme”), and/or any other awareness networking and/or discovery scheme, e.g., as described below.

[0095] In some demonstrative embodiments, the awareness networking scheme, e.g., NAN, may enable applications to discover services in their close proximity. For example, the NAN technology may be a low power service discovery, which may, for example, scale efficiently, e.g., in dense Wi-Fi environments.

[0096] In some demonstrative embodiments, a device, e.g., one or more of wireless communication devices 102 and/or 140, may include one or more blocks and/or entities to perform network awareness functionality. For example, a device, e.g., one or more of devices 102 and/or 140, may be capable of performing the functionality of a NAN device, which may include a NAN MAC and/or a Discovery Engine (DE). In one example, controllers 124 and/or 154, and/or message processors 128 and/or 158 may be configured to perform the functionality of the discovery engine; and/or controllers 124 and/or 154, and/or message processors 128 and/or 158 may be configured to perform the functionality of the NAN MAC, e.g., as described above. In another example, the functionality of the NAN MAC and/or the Discovery engine may be performed by any other element and/or entity of devices 102 and/or 140.

[0097] In some demonstrative embodiments, the awareness networking scheme may include a discovery scheme or protocol, e.g., as described below.

[0098] In some demonstrative embodiments, devices 102 and/or 140 may perform a discovery process according to the awareness networking scheme, for example, to discover each other and/or to establish a wireless communication link, e.g., a directional and/or high throughput wireless communication link and/or any other link.

[0099] In some demonstrative embodiments, devices 102 and/or 140 may be configured to enable time synchronization between devices 102, 140 and/or one or more other devices, e.g., performing the functionality of Wi-Fi stations (STAs), for example, such that STAs can discover each other more efficiently and/or quickly.

[00100] Some demonstrative embodiments are described below with respect to a NAN

discovery scheme, and to NAN discovery frames of the NAN discovery scheme. However, in other embodiments, any other discovery scheme and/or discovery frames may be used.

[00101] In some demonstrative embodiments, the discovery scheme may include a plurality of contention-based discovery windows (DWs).

- 5 [00102] In some demonstrative embodiments, communication during the DWs may be configured to enable time synchronization between Wi-Fi stations (STAs), e.g., devices 102 and/or 140, so that STAs can find each other more efficiently during a DW.

- [00103] In some demonstrative embodiments, devices of an awareness network, e.g., a NAN network, may form one or more clusters, e.g., in order to publish and/or subscribe for services. A
10 NAN cluster may be defined by an Anchor Master (AM) (also referred to as a “NAN master device” or “anchor device”). In one example, the AM may include a NAN device, which has the highest rank in the NAN cluster.

- [00104] In some demonstrative embodiments, NAN data exchange may be reflected by discovery frames, e.g., Publish, Subscribe and/or Follow-Up Service discovery frames (SDF).
15 These frames may include action frames, which may be sent by a device that wishes to publish a service/application, and/or to subscribe to a published service/application at another end.

- [00105] In one example, one of devices 102 and/or 140, e.g., device 102, may operate as and/or perform the functionality of an AM. The AM may be configured to transmit one or more beacons. Another one of devices 102 and/or 140, e.g., device 140, may be configured to receive
20 and process the beacons.

- [00106] In one example, devices 102 and/or 140 may operate as and/or perform the functionality of NAN devices, e.g., belonging to a NAN cluster, which may share a common set of NAN parameters, for example, including a common NAN timestamp, and/or a common time period between consecutive discovery windows (DWs). The NAN timestamp may be communicated,
25 for example, as part of a NAN beacon frame, which may be communicated in the NAN cluster. In one example, the NAN timestamp may include a Time Synchronization Function (TSF) value, for example, a cluster TSF value, or any other value.

- [00107] In some demonstrative embodiments, devices 102 and/or 140 may be configured to discover one another over a predefined communication channel (“the social channel”). In one
30 example, the Channel 6 in the 2.4GHz band may be defined as the NAN social channel. Any other additional or alternative channel may be used as the social channel.

[00108] In some demonstrative embodiments, devices 102 and/or 140 may transmit discovery

frames, e.g., SDFs, during the plurality of DWs, e.g., over the social channel and/or any other channel, which may be used for discovery. For example the NAN AM may advertize the time of the DW, during which NAN devices may exchange SDFs.

5 [00109] In one example, devices 102 and/or 140 may transmit the discovery frames to discover each other, for example, to enable using the one or more services provided by applications 125, 126 and/or 145.

[00110] In some demonstrative embodiments, devices 102 and/or 140 may communicate during a DW according to a contention mechanism. For example, devices 102 and/or 140 may check whether or not a channel may be unoccupied prior to an attempt to transmit a discovery frame
10 during the discovery window.

[00111] In some demonstrative embodiments, a device of devices 102 and/or 140, e.g., device 102, may not transmit the discovery frame during the DW, e.g., if the channel may be occupied. In some demonstrative embodiments, for example, device 102 may transmit the discovery frame during the DW, e.g., if the channel may be unoccupied.

15 [00112] In some embodiments, the discovery frame may be transmitted as a group addressed, e.g., broadcast or multicast, discovery frame. In other embodiments, the discovery frame may be transmitted as any other type of frame.

[00113] In some demonstrative embodiments, the discovery frame may not require an acknowledgement frame. According to these embodiments, a transmitter of the discovery frame
20 may not backoff a transmission of the discovery frame.

[00114] In some demonstrative embodiments, the discovery frame transmitted by device 102 during the DW may be configured to enable other devices or services that are running on other devices to discover the services on device 102.

[00115] In some demonstrative embodiments, devices of system 100 may utilize availability
25 information, e.g., in the form of an Availability Interval Bitmap and/or Further Availability Map, for example, to allow a device of devices 102 and/or 140, to advertise its availability, for example, in terms of at least one channel and one or more timeslots, during which the device may be available, e.g., active (“awake”), for example, to perform post NAN activities.

[00116] In one example, the availability information may be communicated as part of an
30 Availability Attribute, e.g., including a 32-bit bitmap for 32 timeslots, for example, wherein each timeslot may be 16 milliseconds (ms) long. For example, each bit that may be not zero may represent a timeslot, during which a device sending the Availability Attribute may be to be

awake and available to send and/or receive data in a specified method. In another example, the availability information may include any other additional or alternative information, and/or may be communicated and/or formatted in any other manner.

5 [00117] In some demonstrative embodiments, devices 102 and/or 140 may be part of an awareness cluster, e.g., a NAN cluster.

[00118] In some demonstrative embodiments, devices 102 and/or 140 may form the NAN cluster.

10 [00119] In some demonstrative embodiments, devices 102 and/or 140 may be configured to communicate according to a Wi-Fi Aware specification and/or any other awareness networking specification, which may be configured to allow a group of devices to discover other devices/services nearby and/or in close proximity, e.g., with low power.

[00120] In some demonstrative embodiments, devices 102 and/or 140 may form the NAN cluster and may synchronize to the same clock, e.g., as described above.

15 [00121] In one example, all devices of the NAN cluster, may converge on a time period and channel, e.g., one or more DWs, to facilitate the discovery of services of devices 102 and/or 140, and/or to achieve low power consumption, e.g., as described above.

20 [00122] In some demonstrative embodiments, devices 102 and/or 140 may be configured to utilize NAN as a power efficient, and/or scalable, peer to peer technology, for example, to enable Wi-Fi devices to discover devices and/or services in their close proximity, and/or to setup one or more data paths with one or more peer devices.

[00123] For example, devices 102 and/or 140 may be configured to form a NAN cluster for devices in proximity, and devices in the same NAN cluster may follow the same awake time schedule, e.g., the same DWs, to facilitate cluster formation and/or achieve low power operation, e.g., as described above.

25 [00124] In some demonstrative embodiments, devices 102 and/or 140 may transmit NAN Service Discovery frames, for example, during the DWs, e.g., to publish services that the devices are interested or provide and/or to subscribe to one or more published services, e.g., as described above.

30 [00125] In some demonstrative embodiments, two or more NAN devices may set up a NAN Data Path (NDP), for example, over a NAN Data Link (NDL) between the two NAN devices, which may enable to transmit data packets between the two or more NAN devices. For example, the two NAN devices may setup the NDL and/or NDP, for example, when a desired service is

discovered.

[00126] In some demonstrative embodiments, two or more devices, for example, devices 102 and/or 140, may wish to communicate with each other. The two or more devices may establish a Service Data Session (SDS), during which the two devices may set up an NDP and/or an NDL, e.g., to support this SDS or more SDSs.

[00127] In some demonstrative embodiments, devices 102 and/or 140 may be configured to perform one or more operations of a procedure, e.g., a data path setup procedure, for setting up a NAN service, e.g., a unicast service or a multicast service.

[00128] In some demonstrative embodiments, devices 102 and/or 140 may be configured to perform one or more operations of a procedure, e.g., an NDP negotiation procedure, for example, to setup a service, for example, to enable data transmission between two NAN devices, for example, NAN2 devices, e.g., between devices 102 and 140.

[00129] In some demonstrative embodiments, devices 102 and/or 140 may be configured to establish a connection, for example, a data path, e.g., a NAN data path, which may be configured to support communication, e.g., communication of data, between peer devices, e.g., between a first NAN device, e.g., device 102, and a second NAN device, e.g., device 140.

[00130] In one example, a pair of NAN devices, e.g., devices 102 and 140, may be configured to establish an NDP, which may include, for example, a data connection established between the pair of NAN Devices, e.g., for a service instance.

[00131] In some demonstrative embodiments, devices 102 and/or 140 may be configured to establish a secure data path, e.g., a secure NDP, between peers, e.g., as described below.

[00132] In some demonstrative embodiments, devices 102 and/or 140 may be configured to establish the secure data path, e.g., the secure NDP, for example, in accordance with a NAN Specification (WiFi Aware), e.g., a NAN2 Specification, for example, to allow and/or support addressing one or more technical aspects, for example, one or more privacy and/or security aspects of peer to peer communication.

[00133] In some demonstrative embodiments, the secure data path may be established between peers based on a security key, e.g., a Pairwise Master Key (PMK) and/or any other form of security key, which may be known to the peers, e.g., as described below.

[00134] In some demonstrative embodiments, devices 102 and/or 140 may be configured to perform one or more operations and/or communications, which may be configured to support

derivation and/or provisioning of a security key, e.g., PMK provisioning, between peer NAN devices, for example, in compliance with a NAN Specification, e.g., as described below.

[00135] In some demonstrative embodiments, devices 102 and/or 140 may be configured to implement a provisioning protocol, for example, a Device Provisioning Protocol (DPP) or any other protocol, which may be configured to provision security information, e.g., using a public key based identities and/or mechanism to derive a PMK, for example, from public key identities for two devices.

[00136] In other embodiments, any other additional or alternative provisioning protocol or procedure may be implemented to support deriving the PMK and/or any other security key.

[00137] In some demonstrative embodiments, configuring NAN devices, e.g., devices 102 and/or 140, to use a provisioning mechanism, e.g., a DPP mechanism, may provide one or more technical advantages, for example, at least to enable improved device interoperability and/or easy and/or simplified establishment of the PMK, e.g., as described below.

[00138] In some demonstrative embodiments, there may be a need to address one or more technical aspects, for example, when implementing a provisioning protocol, e.g., a DPP, for derivation of a security key, e.g., a PMK, to support a secure NDP, e.g., as described below.

[00139] In some demonstrative embodiments, for example, one technical aspect may relate to an availability of NAN devices. For example, due to power saving and availability, a NAN device may not be always available, e.g., for performing one or more operations and/or communications of a provisioning protocol.

[00140] In some demonstrative embodiments, devices 102 and/or 140 may be configured to perform one or more operations and/or communications, which may be configured to allow addressing, for example, at least a technical aspect of when and/or where the NAN devices are to exchange one or more provisioning messages, e.g., DPP messages, for example, provisioning authentication messages, provisioning configuration messages, and/or network authentication messages, e.g., as described below.

[00141] In some demonstrative embodiments, devices 102 and/or 140 may be configured to implement one or more operations of a mechanism, which may be configured, for example, to support provisioning of a security key, e.g., a PMK, between devices 102 and 140, e.g., as described below.

[00142] In some demonstrative embodiments, devices 102 and/or 140 may be configured to implement one or more operations of a mechanism, which may be configured, for example, to

use one or more provisioning messages, e.g., DPP messages, for provisioning of the PMK, e.g., as described below.

[00143] In some demonstrative embodiments, devices 102 and/or 140 may be configured to implement a mechanism for a DPP capability exchange and/or a public key exchange, for example, in one or more NAN messages, for example, a NAN Discovery message and/or an initiate setup message, e.g., as described below.

[00144] In some demonstrative embodiments, devices 102 and/or 140 may be configured to perform a DPP capability and public key exchange, for example, in a NAN Discovery and initiate setup message, e.g., as described below.

[00145] In some demonstrative embodiments, for example, the initiate setup message may include a NAN schedule request frame, e.g., as described below. In other embodiments, any other additional or alternative message may be implemented.

[00146] In some demonstrative embodiments, devices 102 and/or 140 may be configured to establish a NAN schedule, e.g., a common NAN availability or schedule, which may be configured to support an exchange of one or more provisioning messages, for example, an exchange of DPP messages, e.g., as described below.

[00147] In some demonstrative embodiments, devices 102 and/or 140 may be configured to setup a schedule, e.g., a NAN schedule (also referred to as “NAN Device Link”), to exchange one or more provisioning messages, e.g., DPP messages, e.g., as described below.

[00148] In some demonstrative embodiments, devices 102 and/or 140 may be configured to implement one or more operations of a mechanism to negotiate a NAN availability between devices 102 and 140, and to establish the NAN schedule for the DPP messages exchange, e.g., as described below.

[00149] In some demonstrative embodiments, devices 102 and/or 140 may be configured to implement a mechanism, which may be configured to setup the NAN schedule to exchange the provisioning messages, e.g., the DPP messages, between devices 102 and 140, e.g., as described below.

[00150] In some demonstrative embodiments, for example, once the NAN schedule for DPP operation is established, devices 102 and/or 140 may start the exchange of the DPP messages, for example, according to a common NAN availability, e.g., the NAN schedule, as described below.

[00151] In some demonstrative embodiments, devices 102 and/or 140 may be configured to provision and/or establish a security key, for example, a PMK or any other key, for example, based on the provisioning messages, for example, according to the provisioning protocol, e.g., DPP, as described below.

- 5 [00152] In some demonstrative embodiments, devices 102 and/or 140 may be configured to utilize the security key, e.g., the PMK, for example, to establish a secure data path, e., a secure NDP, e.g., as described below.

[00153] In some demonstrative embodiments, devices and/or 140 may be configured to setup a NAN schedule, to exchange DPP messages according to the NAN schedule, and to use a DPP to
10 establish a PMK for a secure NAN Data Path, e.g., as described below.

[00154] In some demonstrative embodiments, devices 102 and/or 140 may be configured to discover each other, for example, according to a NAN discovery scheme, e.g., as described below.

[00155] In some demonstrative embodiments, controller 124 may be configured to control
15 cause, and/or trigger device 102 to discover device 140, for example, during a DW of a NAN cluster, e.g., as described below.

[00156] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to discover device 102 during the DW of the NAN cluster, e.g., as described below.

20 [00157] In some demonstrative embodiments, devices 102 and/or 140 may be configured to communicate one or more NAN Service Discovery Frames (SDFs), e.g., during a DW, for example, to support the NAN discovery, e.g., as described below.

[00158] In some demonstrative embodiments, devices 102 and/or 140 may be configured to setup a NAN schedule, e.g., as described below.

25 [00159] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to setup a NAN schedule with device 140, e.g., as described below.

[00160] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to setup the NAN schedule device 102, e.g., as described below.

[00161] In some demonstrative embodiments, setting up the NAN schedule may include exchanging a NAN schedule request and/or a NAN schedule response, between devices 102 and 140, e.g., as described below.

5 [00162] In some demonstrative embodiments, devices 102 and/or 140 may be configured to exchange one or more provisioning messages of a provisioning protocol, for example, according to the NAN schedule, e.g., as described below.

[00163] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to exchange with device 140, e.g., according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security
10 key for devices 102 and 140, e.g., as described below.

[00164] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to exchange with device 102, e.g., according to the NAN schedule, the one or more provisioning messages of the provisioning protocol to provision the security key for devices 102 and 140, e.g., as described below.

15 [00165] In some demonstrative embodiments, the one or more provisioning messages may include one or more messages of a provisioning authentication exchange, a provisioning configuration exchange, and/or a provisioning network introduction exchange, e.g., as described below. In other embodiments, any other additional or alternative provisioning messages may be implemented.

20 [00166] In some demonstrative embodiments, the provisioning protocol may include a security-based provisioning protocol, e.g., as described below.

[00167] In some demonstrative embodiments, the provisioning protocol may include a DPP, e.g., as described below.

[00168] In other embodiments, any other provisioning protocol may be implemented.

25 [00169] In some demonstrative embodiments, the security key may include a PMK, e.g., as described below. in other embodiments, any other additional or alternative form of security key and/or security information may be implemented.

[00170] In some demonstrative embodiments, devices 102 and/or 140 may be configured to setup a secure NDP, for example, based on the security key, e.g., as described below.

[00171] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to setup a secure NDP with device 140, for example, based on the security key, e.g., as described below.

5 [00172] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to setup the secure NDP with device 102, for example, based on the security key, e.g., as described below.

[00173] In some demonstrative embodiments, devices 102 and/or 140 may be configured to communicate one or more messages, e.g., NAN SDFs, including an indication to indicate support of the provisioning protocol, for example, before setting up the NAN schedule to
10 exchange the provisioning messages, e.g., as described below.

[00174] In some demonstrative embodiments, a NAN device, e.g., device 102 or device 140, publishing a service which requires security, may indicate that a provisioning protocol, e.g., DPP, is to be used for security key provisioning, e.g., PMK provisioning, as described below.

[00175] In some demonstrative embodiments, for example, a NAN device, e.g., device 102 or
15 device 140, may be configured to include in a Service Descriptor Extension Attribute (SDEA) an indication that the device 102 supports DPP, e.g., as described below. In other embodiments, the indication may be included in any other additional or alternative attribute.

[00176] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to transmit a NAN SDF including an indication that the device
20 102 supports the provisioning protocol to setup the secure NDP, e.g., as described below.

[00177] In some demonstrative embodiments, device 140 may receive the NAN SDF from device 102, e.g., as described below.

[00178] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to receive from device 102 the NAN SDF including the
25 indication that device 102 supports the provisioning protocol, e.g., as described below.

[00179] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to transmit a NAN SDF including an indication that the device 140 supports the provisioning protocol to setup the secure NDP, e.g., as described below.

[00180] In some demonstrative embodiments, device 102 may receive the NAN SDF from
30 device 140, e.g., as described below.

[00181] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to receive from device 102 the NAN SDF including the indication that device 140 supports the provisioning protocol, e.g., as described below.

[00182] In some demonstrative embodiments, a NAN SDF sent by a NAN device, e.g., device 102 or device 140, may include a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported by the NAN device, e.g., as described below.

[00183] In some demonstrative embodiments, the NAN SDF may include an SDEA, e.g., as described below.

[00184] In some demonstrative embodiments, the SDEA may include a control field including the provisioning-supported field, e.g., as described below.

[00185] In some demonstrative embodiments, a NAN device, e.g., device 102 or device 140, publishing a service which requires security, may indicate that the NAN device supports a provisioning protocol, e.g., DPP, which is to be used for PMK provisioning.

[00186] In one example, device 102, may be configured to include in the SDEA of a NAN SDF an indication (“DPP supported indication”) that device 102 supports the provisioning protocol, for example, the DPP, e.g., as described below.

[00187] In other embodiments, the indication that the provisioning protocol is supported may be included in any other additional or alternative attribute, field, and/or message.

[00188] In some demonstrative embodiments, the provisioning-supported field (“DPP supported”) may be implemented in the form of a predefined bit or a new bit, which may be included, for example, in the SDEA attribute, for example, as part of an SDEA Control Field, e.g., as follows:

Field	Size (bits)	Value	Description
...	...	...	...
<u>DPP Supported</u>	<u>b10</u>	<u>Variable</u>	<u>1: DPP is supported for this service. 0: DPP is not supported.</u>
Reserved	b11-b15	NA	Reserved for future use

Table 1

[00189] For example, a NAN device, e.g., device 102, may transmit a NAN SDF, e.g., a NAN SDF Publish message, or any other frame or message, including the SDEA, which may include the DPP supported field, e.g., as part of the SDEA Control Field. According to this example, the DPP supported field of Table 1 may include the value “1” to indicate that device 102 supports the DPP for a published service, or the DPP supported field of Table 1 may include the value “0” to indicate that device 102 does not support the DPP for the published service.

[00190] In some demonstrative embodiments, the NAN SDF may include a service name to indicate that device 102 supports the provisioning protocol, e.g., as described below.

[00191] In some demonstrative embodiments, e.g., additionally or alternatively to using the indication of the support of the DPP, e.g., the DPP supported indication of Table 1, a NAN device may be configured to publish a service, e.g., ‘nan.dpp.device.service’, to indicate support for DPP provisioning/configuration for the device, e.g., for all services. For example, whether using DPP provisioning for a specific service, a subset of services, and/or all services in the NAN device may be based on a security policy.

[00192] In some demonstrative embodiments, the NAN SDF may include a provisioning information attribute including security-based provisioning information corresponding to a sender of the NAN SDF, e.g., as described below.

[00193] In some demonstrative embodiments, the provisioning information attribute may include a public key of the sender of the NAN SDF, e.g., as described below.

[00194] In one example, device 102 may be configured to generate the NAN SDF including the provisioning information attribute including the security-based provisioning information corresponding to device 102, and to transmit the provisioning information attribute.

[00195] In another example, device 140 may be configured to generate the NAN SDF including the provisioning information attribute including the security-based provisioning information corresponding to device 140, and to transmit the provisioning information attribute.

[00196] In some demonstrative embodiments, the provisioning information attribute may include a NAN DPP Information Attribute including one more fields, e.g., as follows:

Field	Size (Octets)	Value (Hex)	Description
Attribute ID	1	TBD	Identifies the type of NAN attribute

Length	2	Variable	Length of the following fields in the attribute.
Publish ID	1	Variable	Identifies the Publish Service Instance
Information	2	TBD	An unsigned two-octet integer defined in IANA, in little-endian format, that identifies a domain parameter set
Public Key	Variable	Variable	Public key is an octet string ; DER of ASN.1 SubjectPublicKeyInfo encoded in “base64” as per RFC 4648

Table 2

[00197] In some demonstrative embodiments, the NAN DPP Information Attribute may include some or all of the fields of Table 2, and/or one or more additional or alternative fields.

[00198] In some demonstrative embodiments, a NAN device, e.g., device 102 or device 140, may transmit the provisioning information attribute, e.g., including one or more fields of the NAN DPP Information Attribute of Table 2, as part of a NAN SDF, for example, a NAN SDF Publish message, a NAN schedule request, a NAN schedule response, and/or any other frame or message, e.g., as described below.

[00199] In some demonstrative embodiments, at least one of the provisioning messages may be based on the public key provided by the provisioning information attribute, e.g., as described below.

[00200] In one example, at least one message of the provisioning authentication exchange, the provisioning configuration exchange, and/or the provisioning network introduction exchange between devices 102 and 140 may be based on the public key of device 102 and/or the public key of device 140, e.g., as described below.

[00201] In some demonstrative embodiments, NAN Devices, e.g., devices 102 and 140, may be configured to negotiate their NAN availability, and to establish a NAN Device Link and/or a

NAN schedule for exchanging the provisioning messages, e.g., for a DPP exchange, as described below.

[00202] In some demonstrative embodiments, devices 102 and/or 140 may be configured to exchange NAN Schedule Request and/or Schedule Response frames to negotiate the schedule for DPP message exchanges, e.g., as described below. In other embodiments, any other additional or alternative types of messages may be used.

[00203] In some demonstrative embodiments, devices 102 and 140 may be configured to setup the NAN schedule to be used for the provisioning exchange, for example, by exchanging a NAN schedule request and a NAN schedule response, e.g., as described below.

10 [00204] In some demonstrative embodiments, devices 102 and/or 140 may be configured to setup the NAN schedule by exchanging the NAN schedule request and the NAN schedule response between devices 102 and 140, e.g., as described below.

[00205] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to setup the NAN schedule by exchanging with device 140 a NAN schedule request and/or a NAN schedule response, e.g., as described below.

[00206] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to setup the NAN schedule by exchanging with device 102 the NAN schedule request and the NAN schedule response, e.g., as described below.

20 [00207] In some demonstrative embodiments, the NAN schedule request and/or the NAN schedule response may include an indication that an NDL is to be set up for exchanging the provisioning messages, e.g., as described below.

[00208] In some demonstrative embodiments, the NAN schedule request and/or the NAN schedule response may include an NDL attribute, e.g., as described below.

25 [00209] In some demonstrative embodiments, the NDL attribute may include an NDL control field, e.g., as described below.

[00210] In some demonstrative embodiments, the NDL control field may include an NDL setup reason field having a predefined value, for example, to indicate that the NDL is to be set up for exchanging the provisioning messages, e.g., as described below. In other embodiments, any other field or attribute may be configured to indicate that the NDL is to be set up for exchanging the provisioning messages.

30

[00211] For example, devices 102 and/or 140 may be configured to include the NDL attribute in the NAN schedule request and/or response frames.

[00212] For example, the NDL Control field of the NDL attribute may be configured to include a predefined value, e.g., a value “2” or any other value, for example, in the NDL Setup Reason field and/or any other field, to indicate that the NDL is to be configured for exchanging one or more messages of the provisioning protocol, e.g., the DPP message exchange.

[00213] In one example, the NDL Setup Reason field may be configured, e.g., as follows:

Field	Size(bits)	Description
...	...	
NDL Setup Reason	2	00: NDP 01: FSD using GAS <u>10: DPP</u> 11: reserved

Table 3

[00214] In one example, the NDL Setup Reason field may be included as part of the NDL Control Field of the NDL attribute, e.g., as described above. In other embodiments, any other field, attribute and/or message format may be used.

[00215] In some demonstrative embodiments, the NAN schedule request may include a provisioning information attribute including security-based provisioning information corresponding to a sender of the NAN schedule request.

[00216] For example, the provisioning information attribute including the security-based provisioning information may include one more fields of the NAN DPP Information Attribute according to Table 2, e.g., as described above.

[00217] In one example, device 102 may transmit the NAN schedule request to device 140, and device 140 may transmit the NAN schedule response to device 102, e.g., in response to the NAN schedule request from device 102. According to this example, the NAN schedule request may include a provisioning information attribute, e.g., including one or more fields of the NAN DPP Information Attribute according to Table 2, for example, including the security-based

provisioning information corresponding to device 102. According to this example, the NAN schedule response may include a provisioning information attribute, e.g., including one or more fields of the NAN DPP Information Attribute according to Table 2, for example, including the security-based provisioning information corresponding to device 140.

5 [00218] In some demonstrative embodiments, devices 102 and/or 140 may be configured to cancel the NAN schedule, for example, after the provisioning of the security key, e.g., as described below.

[00219] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to cancel the NAN schedule after provisioning the security key
10 according to the provisioning protocol, e.g., as described below.

[00220] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to cancel the NAN schedule, for example, after provisioning the security key according to the provisioning protocol, e.g., as described below.

[00221] In some demonstrative embodiments, devices 102 and/or 140 may be configured to
15 implicitly cancel the NAN schedule, e.g., as described below.

[00222] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to implicitly, e.g., automatically, cancel the NAN schedule, for example, upon completion of the provisioning of the security key according to the provisioning protocol.

20 [00223] In some demonstrative embodiments, controller 154 may be configured to control cause, and/or trigger device 140 to implicitly, e.g., automatically, cancel the NAN schedule, for example, upon completion of the provisioning of the security key according to the provisioning protocol.

[00224] In some demonstrative embodiments, devices 102 and/or 140 may be configured to
25 explicitly cancel the NAN schedule, e.g., as described below.

[00225] In some demonstrative embodiments, controller 124 may be configured to control cause, and/or trigger device 102 to explicitly cancel the NAN schedule by transmission of a schedule update notification, e.g., which does not include a NAN availability attribute.

[00226] In some demonstrative embodiments, controller 154 may be configured to control
30 cause, and/or trigger device 140 to explicitly cancel the NAN schedule by transmission of the schedule update notification, e.g., which does not include the NAN availability attribute.

[00227] .In some demonstrative embodiments, configuring NAN devices, e.g., devices 102 and/or 140, to use a provisioning mechanism, e.g., the DPP mechanism, as described above, may provide one or more technical advantages, for example, at least to enable improved device interoperability and/or easy and/or simplified establishment of the PMK.

5 [00228] Reference is made to Fig. 2, which schematically illustrates communications between NAN devices, e.g., a first NAN device 202 and a second NAN device 240, to setup a secure NDP, in accordance with some demonstrative embodiments.

[00229] For example, device 102 (Fig. 1) may be configured to perform a role of, one or more operations of, and/or one or more functionalities of, a first NAN device of the NAN devices of 10 202 and 240, e.g., NAN device 202; and/or device 140 (Fig. 1) may be configured to perform a role of, one or more operations of, and/or one or more functionalities of, a second NAN device of the NAN devices of 202 and 240, e.g., NAN device 240.

[00230] In some demonstrative embodiments, devices 202 and 240 may be configured to use a provisioning protocol, e.g., a DPP, to establish a security key, e.g., a PMK, for setting up a 15 secure NDP, e.g., as described below.

[00231] In some demonstrative embodiments, setting up the secure NDP may include one or more stages, operations and/or steps, e.g., as described below.

[00232] In some demonstrative embodiments, devices 202 and 240 may perform a NAN Discovery and DPP information exchange 232, for example, at a first stage, e.g., as described 20 below.

[00233] In some demonstrative embodiments, for example, as shown in Fig. 2, device 202 may generate and transmit an NAN SDF publish message 212, for example, including the SDEA and the DPP information attribute element corresponding to device 202, e.g., as described above.

[00234] In some demonstrative embodiments, for example, as shown in Fig. 2, device 240 may 25 receive and process the NAN SDF publish message 212 from device 202.

[00235] In some demonstrative embodiments, for example, as shown in Fig. 2, device 240 may optionally generate and transmit a NAN SDF subscribe message 210, for example, including the SDEA including the information corresponding to device 240.

[00236] In one example, the SDEA may include the SDEA Control Field including one or more 30 fields of Table 1, and/or the DPP information attribute element may include one or more fields of Table 2.

[00237] In some demonstrative embodiments, for example, devices 202 and 240 may establish (234) a NAN Schedule (or NAN Device Link) for DPP messages exchange, for example, by negotiating a NAN schedule at a second stage, e.g., as described above.

[00238] In some demonstrative embodiments, for example, as shown in Fig. 2, device 240 may generate and transmit a NAN schedule request message 214, for example, including the DPP information attribute element, including provisioning information corresponding to device 240 and the NDL attribute including NAN availability and/or schedule information corresponding to device 240, e.g., as described above.

[00239] In some demonstrative embodiments, for example, as shown in Fig. 2, device 202 may receive and process the NAN schedule request message 214 from device 240, e.g., as described above.

[00240] In some demonstrative embodiments, for example, as shown in Fig. 2, device 202 may generate and transmit a NAN schedule response message 216, for example, including the NDL attribute including NAN availability and/or schedule information corresponding to device 202, e.g., as described above.

[00241] In some demonstrative embodiments, for example, as shown in Fig. 2, device 240 may receive and process the NAN schedule response message 216 from device 202, e.g., as described above.

[00242] In one example, the DPP information attribute element may include one or more fields of Table 2, and/or the NDL attribute may include the NDL Control field including the NDL Setup Reason field of Table 3.

[00243] In some demonstrative embodiments, for example, when the NAN Schedule for DPP operation is established, e.g., based on the exchange of messages 214 and 216, devices 202 and 240 may begin an exchange of DPP messages, for example, in the common NAN availability, e.g., according to the negotiated NAN schedule.

[00244] In some demonstrative embodiments, devices 202 and 240 may use the NAN DPP schedule to provision multiple PMKs for different services or for the device. For example, multiple DPP operations may occur in the agreed NAN DPP schedule. For example, a corresponding NAN Data Interface addresses (NDIs) shall be used in the DPP message exchanges.

[00245] In some demonstrative embodiments, as shown in Fig. 2, devices 202 and 240 may perform an exchange (236) of DPP messages, for example at a third stage, e.g., as described below.

[00246] In some demonstrative embodiments, for example, as shown in Fig. 2, devices 202 and 240 may exchange one or more DPP messages 218 according to the NAN schedule negotiated with messages 214 and 216.

[00247] In one example, DPP messages 218 may include, for example, messages of a DPP authentication exchange, a DPP configuration exchange, a DPP network introduction exchange, and/or an exchange of one or more additional or alternative DPP messages, e.g., in compliance with a DPP Specification and/or protocol.

[00248] In some demonstrative embodiments, for example, as shown in Fig. 2, devices 202 and 240 may determine a provisioned security key, e.g., a PMK 219, for example, based on the DPP messages 218.

[00249] In some demonstrative embodiments, as shown in Fig. 2, devices 202 and 240 may setup (238) a secure NDP, for example, at a fourth stage, e.g., as described below.

[00250] In some demonstrative embodiments, for example, as shown in Fig. 2, devices 202 and 240 may setup a secure NAN data path 220, for example, based on the PMK 219.

[00251] In one example, using a security key, e.g., a PMK, which is based on the DPP, for example, may be compliance with a NAN Specification, e.g., a NAN 2 Specification.

[00252] Reference is made to Fig. 3, which schematically illustrates a method of secure NAN communication, in accordance with some demonstrative embodiments. For example, one or more of the operations of the method of Fig. 3 may be performed by one or more elements of a system, system 100 (Fig. 1); a device, e.g., wireless communication devices 102 and/or 140 (Fig. 1); a controller, e.g., controller 124 (Fig. 1), and/or controller 154 (Fig. 1); a radio, e.g., radio 114 (Fig. 1) and/or radio 144 (Fig. 1); and/or a message processor, e.g., message processor 128 (Fig. 1) and/or message processor 158 (Fig. 1).

[00253] As indicated at block 302, the method may include setting up, at a first NAN device, a NAN schedule with a second NAN device. For example, controller 124 (Fig. 1) may control, cause and/or trigger device 102 (Fig. 1) to setup the NAN schedule with device 140 (Fig. 1), e.g., as described above.

[00254] As indicated at block 303, the method may include exchanging with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning

protocol to provision a security key for the first and second NAN devices. For example, controller 124 (Fig. 1) may control, cause and/or trigger device 102 (Fig. 1) to exchange with device 140 (Fig. 1) one or more provisioning messages of the provisioning protocol to provision the security key for devices 102 and 140 (Fig. 1), e.g., as described above.

5 [00255] As indicated at block 306, the method may include setting up a secure NDP with the second NAN device based on the security key. For example, controller 124 (Fig. 1) may control, cause and/or trigger device 102 (Fig. 1) to set up the secure NDP with device 140 (Fig. 1), for example, based on the security key, e.g., as described above.

[00256] Reference is made to Fig. 4, which schematically illustrates a product of manufacture
10 400, in accordance with some demonstrative embodiments. Product 400 may include one or more tangible computer-readable (“machine-readable”) non-transitory storage media 402, which may include computer-executable instructions, e.g., implemented by logic 404, operable to, when executed by at least one computer processor, enable the at least one computer processor to implement one or more operations at device 102, device 140 (Fig. 1), radio 114 (Fig. 1), radio
15 144 (Fig. 1), transmitter 118 (Fig. 1), transmitter 148 (Fig. 1), receiver 116 (Fig. 1), receiver 146 (Fig. 1), controller 124 (Fig. 1), controller 154 (Fig. 1), message processor 128 (Fig. 1), and/or message processor 158 (Fig. 1), to cause device 102, device 140 (Fig. 1), radio 114 (Fig. 1), radio 144 (Fig. 1), transmitter 118 (Fig. 1), transmitter 148 (Fig. 1), receiver 116 (Fig. 1), receiver 146 (Fig. 1), controller 124 (Fig. 1), controller 154 (Fig. 1), message processor 128 (Fig.
20 1), and/or message processor 158 (Fig. 1), to perform, trigger and/or implement one or more operations and/or functionalities, and/or to perform, trigger and/or implement one or more operations and/or functionalities described with reference to the Figs. 1, 2, and/or 3, and/or one or more operations described herein. The phrase “non-transitory machine-readable medium” may be directed to include all computer-readable media, with the sole exception being a transitory
25 propagating signal.

[00257] In some demonstrative embodiments, product 400 and/or machine-readable storage media 402 may include one or more types of computer-readable storage media capable of storing data, including volatile memory, non-volatile memory, removable or non-removable memory, erasable or non-erasable memory, writeable or re-writeable memory, and the like. For example,
30 machine-readable storage media 402 may include, RAM, DRAM, Double-Data-Rate DRAM (DDR-DRAM), SDRAM, static RAM (SRAM), ROM, programmable ROM (PROM), erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), Compact Disk ROM (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-

RW), flash memory (e.g., NOR or NAND flash memory), content addressable memory (CAM), polymer memory, phase-change memory, ferroelectric memory, silicon-oxide-nitride-oxide-silicon (SONOS) memory, a disk, a floppy disk, a hard drive, an optical disk, a magnetic disk, a card, a magnetic card, an optical card, a tape, a cassette, and the like. The computer-readable storage media may include any suitable media involved with downloading or transferring a computer program from a remote computer to a requesting computer carried by data signals embodied in a carrier wave or other propagation medium through a communication link, e.g., a modem, radio or network connection.

[00258] In some demonstrative embodiments, logic 404 may include instructions, data, and/or code, which, if executed by a machine, may cause the machine to perform a method, process and/or operations as described herein. The machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware, software, firmware, and the like.

[00259] In some demonstrative embodiments, logic 404 may include, or may be implemented as, software, a software module, an application, a program, a subroutine, instructions, an instruction set, computing code, words, values, symbols, and the like. The instructions may include any suitable type of code, such as source code, compiled code, interpreted code, executable code, static code, dynamic code, and the like. The instructions may be implemented according to a predefined computer language, manner or syntax, for instructing a processor to perform a certain function. The instructions may be implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language, such as C, C++, Java, BASIC, Matlab, Pascal, Visual BASIC, assembly language, machine code, and the like.

EXAMPLES

[00260] The following examples pertain to further embodiments.

[00261] Example 1 includes an apparatus comprising logic and circuitry configured to cause a first Neighbor Awareness Networking (NAN) device to setup a NAN schedule with a second NAN device; exchange with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and second NAN devices; and setup a secure NAN Data Path (NDP) with the second NAN device based on the security key.

[00262] Example 2 includes the subject matter of Example 1, and optionally, wherein the apparatus is configured to cause the first NAN device to transmit a NAN Service Discovery Frame (SDF) comprising an indication that the first NAN device supports the provisioning protocol.

5 [00263] Example 3 includes the subject matter of Example 2, and optionally, wherein the NAN SDF comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

[00264] Example 4 includes the subject matter of Example 3, and optionally, wherein the NAN SDF comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a
10 control field comprising the provisioning-supported field.

[00265] Example 5 includes the subject matter of any one of Examples 2-4, and optionally, wherein the NAN SDF comprises a service name to indicate that the first NAN device supports the provisioning protocol.

[00266] Example 6 includes the subject matter of any one of Examples 2-5, and optionally,
15 wherein the NAN SDF comprises a provisioning information attribute comprising security-based provisioning information corresponding to the first NAN device.

[00267] Example 7 includes the subject matter of Example 6, and optionally, wherein the provisioning information attribute comprises a public key of the first NAN device.

[00268] Example 8 includes the subject matter of Example 7, and optionally, wherein at least
20 one of the provisioning messages is based on the public key of the first NAN device.

[00269] Example 9 includes the subject matter of any one of Examples 1-8, and optionally, wherein the apparatus is configured to cause the first NAN device to receive a NAN Service Discovery Frame (SDF) from the second NAN device, the NAN SDF from the second NAN device comprising an indication that the second NAN device supports the provisioning protocol.

25 [00270] Example 10 includes the subject matter of Example 9, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

[00271] Example 11 includes the subject matter of Example 10, and optionally, wherein the NAN SDF from the second NAN device comprises a Service Descriptor Extension Attribute
30 (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

[00272] Example 12 includes the subject matter of any one of Examples 9-11, and optionally, wherein the NAN SDF from the second NAN device comprises a service name to indicate that the second NAN device supports the provisioning protocol.

[00273] Example 13 includes the subject matter of any one of Examples 9-12, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning information attribute comprising security-based provisioning information corresponding to the second NAN device.

[00274] Example 14 includes the subject matter of Example 13, and optionally, wherein the provisioning information attribute comprises a public key of the second NAN device.

[00275] Example 15 includes the subject matter of Example 14, and optionally, wherein at least one of the provisioning messages is based on the public key of the second NAN device.

[00276] Example 16 includes the subject matter of any one of Examples 1-15, and optionally, wherein the apparatus is configured to cause the first NAN device to setup the NAN schedule by exchanging with the second NAN device a NAN schedule request and a NAN schedule response, the NAN schedule request and the NAN schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

[00277] Example 17 includes the subject matter of Example 16, and optionally, wherein the NAN schedule request and the NAN schedule response comprise an NDL attribute, the NDL attribute comprising an NDL control field, the NDL control field comprising an NDL setup reason field having a predefined value to indicate that the NDL is to be set up for exchanging the provisioning messages.

[00278] Example 18 includes the subject matter of Example 16 or 17, and optionally, wherein the NAN schedule request comprises a provisioning information attribute comprising security-based provisioning information corresponding to a sender of the NAN schedule request.

[00279] Example 19 includes the subject matter of any one of Examples 1-18, and optionally, wherein the one or more provisioning messages comprise one or more messages of at least one of a provisioning authentication exchange, a provisioning configuration exchange, or a provisioning network introduction exchange.

[00280] Example 20 includes the subject matter of any one of Examples 1-19, and optionally, wherein the apparatus is configured to cause the first NAN device to cancel the NAN schedule after provisioning the security key according to the provisioning protocol.

[00281] Example 21 includes the subject matter of Example 20, and optionally, wherein the apparatus is configured to cause the first NAN device to implicitly cancel the NAN schedule upon completion of the provisioning of the security key according to the provisioning protocol.

5 [00282] Example 22 includes the subject matter of Example 20, and optionally, wherein the apparatus is configured to cause the first NAN device to explicitly cancel the NAN schedule by transmission of a schedule update notification, which does not include a NAN availability attribute.

[00283] Example 23 includes the subject matter of any one of Examples 1-22, and optionally, wherein the provisioning protocol comprises a security-based provisioning protocol.

10 [00284] Example 24 includes the subject matter of any one of Examples 1-23, and optionally, wherein the provisioning protocol comprises a Device Provisioning Protocol (DPP).

[00285] Example 25 includes the subject matter of any one of Examples 1-24, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

15 [00286] Example 26 includes the subject matter of any one of Examples 1-25, and optionally, wherein the apparatus is configured to cause the first NAN device to discover the second NAN device during a Discovery Window (DW) of a NAN cluster.

[00287] Example 27 includes the subject matter of any one of Examples 1-26, and optionally, comprising a radio.

20 [00288] Example 28 includes the subject matter of any one of Examples 1-27, and optionally, comprising one or more antennas, a processor, and a memory.

[00289] Example 29 includes a system of wireless communication comprising a first Neighbor Awareness Networking (NAN) device, the first NAN device comprising one or more antennas; a radio; a memory; a processor; and a controller configured to cause the first NAN device to setup a NAN schedule with a second NAN device; exchange with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and second NAN devices; and setup a secure NAN Data Path (NDP) with the second NAN device based on the security key.

25 [00290] Example 30 includes the subject matter of Example 29, and optionally, wherein the controller is configured to cause the first NAN device to transmit a NAN Service Discovery Frame (SDF) comprising an indication that the first NAN device supports the provisioning protocol.

30

[00291] Example 31 includes the subject matter of Example 30, and optionally, wherein the NAN SDF comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

5 [00292] Example 32 includes the subject matter of Example 31, and optionally, wherein the NAN SDF comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

[00293] Example 33 includes the subject matter of any one of Examples 30-32, and optionally, wherein the NAN SDF comprises a service name to indicate that the first NAN device supports the provisioning protocol.

10 [00294] Example 34 includes the subject matter of any one of Examples 30-33, and optionally, wherein the NAN SDF comprises a provisioning information attribute comprising security-based provisioning information corresponding to the first NAN device.

[00295] Example 35 includes the subject matter of Example 34, and optionally, wherein the provisioning information attribute comprises a public key of the first NAN device.

15 [00296] Example 36 includes the subject matter of Example 35, and optionally, wherein at least one of the provisioning messages is based on the public key of the first NAN device.

[00297] Example 37 includes the subject matter of any one of Examples 29-36, and optionally, wherein the controller is configured to cause the first NAN device to receive a NAN Service Discovery Frame (SDF) from the second NAN device, the NAN SDF from the second NAN
20 device comprising an indication that the second NAN device supports the provisioning protocol.

[00298] Example 38 includes the subject matter of Example 37, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

25 [00299] Example 39 includes the subject matter of Example 38, and optionally, wherein the NAN SDF from the second NAN device comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

[00300] Example 40 includes the subject matter of any one of Examples 37-39, and optionally, wherein the NAN SDF from the second NAN device comprises a service name to indicate that the second NAN device supports the provisioning protocol.

30 [00301] Example 41 includes the subject matter of any one of Examples 37-40, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning information

attribute comprising security-based provisioning information corresponding to the second NAN device.

[00302] Example 42 includes the subject matter of Example 41, and optionally, wherein the provisioning information attribute comprises a public key of the second NAN device.

5 [00303] Example 43 includes the subject matter of Example 42, and optionally, wherein at least one of the provisioning messages is based on the public key of the second NAN device.

[00304] Example 44 includes the subject matter of any one of Examples 29-43, and optionally, wherein the controller is configured to cause the first NAN device to setup the NAN schedule by exchanging with the second NAN device a NAN schedule request and a NAN schedule
10 response, the NAN schedule request and the NAN schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

[00305] Example 45 includes the subject matter of Example 44, and optionally, wherein the NAN schedule request and the NAN schedule response comprise an NDL attribute, the NDL attribute comprising an NDL control field, the NDL control field comprising an NDL setup
15 reason field having a predefined value to indicate that the NDL is to be set up for exchanging the provisioning messages.

[00306] Example 46 includes the subject matter of Example 44 or 45, and optionally, wherein the NAN schedule request comprises a provisioning information attribute comprising security-based provisioning information corresponding to a sender of the NAN schedule request.

20 [00307] Example 47 includes the subject matter of any one of Examples 29-46, and optionally, wherein the one or more provisioning messages comprise one or more messages of at least one of a provisioning authentication exchange, a provisioning configuration exchange, or a provisioning network introduction exchange.

[00308] Example 48 includes the subject matter of any one of Examples 29-47, and optionally,
25 wherein the controller is configured to cause the first NAN device to cancel the NAN schedule after provisioning the security key according to the provisioning protocol.

[00309] Example 49 includes the subject matter of Example 48, and optionally, wherein the controller is configured to cause the first NAN device to implicitly cancel the NAN schedule upon completion of the provisioning of the security key according to the provisioning protocol.

30 [00310] Example 50 includes the subject matter of Example 48, and optionally, wherein the controller is configured to cause the first NAN device to explicitly cancel the NAN schedule by

transmission of a schedule update notification, which does not include a NAN availability attribute.

[00311] Example 51 includes the subject matter of any one of Examples 29-50, and optionally, wherein the provisioning protocol comprises a security-based provisioning protocol.

5 [00312] Example 52 includes the subject matter of any one of Examples 29-51, and optionally, wherein the provisioning protocol comprises a Device Provisioning Protocol (DPP).

[00313] Example 53 includes the subject matter of any one of Examples 29-52, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

10 [00314] Example 54 includes the subject matter of any one of Examples 29-53, and optionally, wherein the controller is configured to cause the first NAN device to discover the second NAN device during a Discovery Window (DW) of a NAN cluster.

15 [00315] Example 55 includes a method to be performed at a first Neighbor Awareness Networking (NAN) device, the method comprising setting up a NAN schedule with a second NAN device; exchanging with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and second NAN devices; and setting up a secure NAN Data Path (NDP) with the second NAN device based on the security key.

20 [00316] Example 56 includes the subject matter of Example 55, and optionally, comprising transmitting a NAN Service Discovery Frame (SDF) comprising an indication that the first NAN device supports the provisioning protocol.

[00317] Example 57 includes the subject matter of Example 56, and optionally, wherein the NAN SDF comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

25 [00318] Example 58 includes the subject matter of Example 57, and optionally, wherein the NAN SDF comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

[00319] Example 59 includes the subject matter of any one of Examples 56-58, and optionally, wherein the NAN SDF comprises a service name to indicate that the first NAN device supports the provisioning protocol.

[00320] Example 60 includes the subject matter of any one of Examples 56-59, and optionally, wherein the NAN SDF comprises a provisioning information attribute comprising security-based provisioning information corresponding to the first NAN device.

5 [00321] Example 61 includes the subject matter of Example 60, and optionally, wherein the provisioning information attribute comprises a public key of the first NAN device.

[00322] Example 62 includes the subject matter of Example 61, and optionally, wherein at least one of the provisioning messages is based on the public key of the first NAN device.

10 [00323] Example 63 includes the subject matter of any one of Examples 55-62, and optionally, comprising receiving a NAN Service Discovery Frame (SDF) from the second NAN device, the NAN SDF from the second NAN device comprising an indication that the second NAN device supports the provisioning protocol.

[00324] Example 64 includes the subject matter of Example 63, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

15 [00325] Example 65 includes the subject matter of Example 64, and optionally, wherein the NAN SDF from the second NAN device comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

20 [00326] Example 66 includes the subject matter of any one of Examples 63-65, and optionally, wherein the NAN SDF from the second NAN device comprises a service name to indicate that the second NAN device supports the provisioning protocol.

[00327] Example 67 includes the subject matter of any one of Examples 63-66, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning information attribute comprising security-based provisioning information corresponding to the second NAN device.

25 [00328] Example 68 includes the subject matter of Example 67, and optionally, wherein the provisioning information attribute comprises a public key of the second NAN device.

[00329] Example 69 includes the subject matter of Example 68, and optionally, wherein at least one of the provisioning messages is based on the public key of the second NAN device.

30 [00330] Example 70 includes the subject matter of any one of Examples 55-69, and optionally, comprising setting up the NAN schedule by exchanging with the second NAN device a NAN schedule request and a NAN schedule response, the NAN schedule request and the NAN

schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

[00331] Example 71 includes the subject matter of Example 70, and optionally, wherein the NAN schedule request and the NAN schedule response comprise an NDL attribute, the NDL attribute comprising an NDL control field, the NDL control field comprising an NDL setup reason field having a predefined value to indicate that the NDL is to be set up for exchanging the provisioning messages.

[00332] Example 72 includes the subject matter of Example 70 or 71, and optionally, wherein the NAN schedule request comprises a provisioning information attribute comprising security-based provisioning information corresponding to a sender of the NAN schedule request.

[00333] Example 73 includes the subject matter of any one of Examples 55-72, and optionally, wherein the one or more provisioning messages comprise one or more messages of at least one of a provisioning authentication exchange, a provisioning configuration exchange, or a provisioning network introduction exchange.

[00334] Example 74 includes the subject matter of any one of Examples 55-73, and optionally, comprising cancelling the NAN schedule after provisioning the security key according to the provisioning protocol.

[00335] Example 75 includes the subject matter of Example 74, and optionally, comprising cancelling the NAN schedule upon completion of the provisioning of the security key according to the provisioning protocol.

[00336] Example 76 includes the subject matter of Example 74, and optionally, comprising cancelling the NAN schedule by transmission of a schedule update notification, which does not include a NAN availability attribute.

[00337] Example 77 includes the subject matter of any one of Examples 55-76, and optionally, wherein the provisioning protocol comprises a security-based provisioning protocol.

[00338] Example 78 includes the subject matter of any one of Examples 55-77, and optionally, wherein the provisioning protocol comprises a Device Provisioning Protocol (DPP).

[00339] Example 79 includes the subject matter of any one of Examples 55-78, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

[00340] Example 80 includes the subject matter of any one of Examples 55-79, and optionally, comprising discovering the second NAN device during a Discovery Window (DW) of a NAN cluster.

5 [00341] Example 81 includes a product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one processor, enable the at least one processor to cause a first Neighbor Awareness Networking (NAN) device to setup a NAN schedule with a second NAN device; exchange with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and
10 second NAN devices; and setup a secure NAN Data Path (NDP) with the second NAN device based on the security key.

[00342] Example 82 includes the subject matter of Example 81, and optionally, wherein the instructions, when executed, cause the first NAN device to transmit a NAN Service Discovery Frame (SDF) comprising an indication that the first NAN device supports the provisioning
15 protocol.

[00343] Example 83 includes the subject matter of Example 82, and optionally, wherein the NAN SDF comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

20 [00344] Example 84 includes the subject matter of Example 83, and optionally, wherein the NAN SDF comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

[00345] Example 85 includes the subject matter of any one of Examples 82-84, and optionally, wherein the NAN SDF comprises a service name to indicate that the first NAN device supports the provisioning protocol.

25 [00346] Example 86 includes the subject matter of any one of Examples 82-85, and optionally, wherein the NAN SDF comprises a provisioning information attribute comprising security-based provisioning information corresponding to the first NAN device.

[00347] Example 87 includes the subject matter of Example 86, and optionally, wherein the provisioning information attribute comprises a public key of the first NAN device.

30 [00348] Example 88 includes the subject matter of Example 87, and optionally, wherein at least one of the provisioning messages is based on the public key of the first NAN device.

[00349] Example 89 includes the subject matter of any one of Examples 81-88, and optionally, wherein the instructions, when executed, cause the first NAN device to receive a NAN Service Discovery Frame (SDF) from the second NAN device, the NAN SDF from the second NAN device comprising an indication that the second NAN device supports the provisioning protocol.

5 [00350] Example 90 includes the subject matter of Example 89, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

[00351] Example 91 includes the subject matter of Example 90, and optionally, wherein the NAN SDF from the second NAN device comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

10

[00352] Example 92 includes the subject matter of any one of Examples 89-91, and optionally, wherein the NAN SDF from the second NAN device comprises a service name to indicate that the second NAN device supports the provisioning protocol.

[00353] Example 93 includes the subject matter of any one of Examples 89-92, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning information attribute comprising security-based provisioning information corresponding to the second NAN device.

15

[00354] Example 94 includes the subject matter of Example 93, and optionally, wherein the provisioning information attribute comprises a public key of the second NAN device.

20 [00355] Example 95 includes the subject matter of Example 94, and optionally, wherein at least one of the provisioning messages is based on the public key of the second NAN device.

[00356] Example 96 includes the subject matter of any one of Examples 81-95, and optionally, wherein the instructions, when executed, cause the first NAN device to setup the NAN schedule by exchanging with the second NAN device a NAN schedule request and a NAN schedule response, the NAN schedule request and the NAN schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

25

[00357] Example 97 includes the subject matter of Example 96, and optionally, wherein the NAN schedule request and the NAN schedule response comprise an NDL attribute, the NDL attribute comprising an NDL control field, the NDL control field comprising an NDL setup reason field having a predefined value to indicate that the NDL is to be set up for exchanging the provisioning messages.

30

[00358] Example 98 includes the subject matter of Example 96 or 97, and optionally, wherein the NAN schedule request comprises a provisioning information attribute comprising security-based provisioning information corresponding to a sender of the NAN schedule request.

5 [00359] Example 99 includes the subject matter of any one of Examples 81-98, and optionally, wherein the one or more provisioning messages comprise one or more messages of at least one of a provisioning authentication exchange, a provisioning configuration exchange, or a provisioning network introduction exchange.

10 [00360] Example 100 includes the subject matter of any one of Examples 81-99, and optionally, wherein the instructions, when executed, cause the first NAN device to cancel the NAN schedule after provisioning the security key according to the provisioning protocol.

[00361] Example 101 includes the subject matter of Example 100, and optionally, wherein the instructions, when executed, cause the first NAN device to implicitly cancel the NAN schedule upon completion of the provisioning of the security key according to the provisioning protocol.

15 [00362] Example 102 includes the subject matter of Example 100, and optionally, wherein the instructions, when executed, cause the first NAN device to explicitly cancel the NAN schedule by transmission of a schedule update notification, which does not include a NAN availability attribute.

[00363] Example 103 includes the subject matter of any one of Examples 81-102, and optionally, wherein the provisioning protocol comprises a security-based provisioning protocol.

20 [00364] Example 104 includes the subject matter of any one of Examples 81-103, and optionally, wherein the provisioning protocol comprises a Device Provisioning Protocol (DPP).

[00365] Example 105 includes the subject matter of any one of Examples 81-104, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

25 [00366] Example 106 includes the subject matter of any one of Examples 81-105, and optionally, wherein the instructions, when executed, cause the first NAN device to discover the second NAN device during a Discovery Window (DW) of a NAN cluster.

30 [00367] Example 107 includes an apparatus of wireless communication by a first Neighbor Awareness Networking (NAN) device, the apparatus comprising means for setting up a NAN schedule with a second NAN device; means for exchanging with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and second NAN devices; and means for setting up a secure NAN Data Path (NDP) with the second NAN device based on the security key.

[00368] Example 108 includes the subject matter of Example 107, and optionally, comprising means for transmitting a NAN Service Discovery Frame (SDF) comprising an indication that the first NAN device supports the provisioning protocol.

5 [00369] Example 109 includes the subject matter of Example 108, and optionally, wherein the NAN SDF comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

[00370] Example 110 includes the subject matter of Example 109, and optionally, wherein the NAN SDF comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

10 [00371] Example 111 includes the subject matter of any one of Examples 108-110, and optionally, wherein the NAN SDF comprises a service name to indicate that the first NAN device supports the provisioning protocol.

[00372] Example 112 includes the subject matter of any one of Examples 108-111, and optionally, wherein the NAN SDF comprises a provisioning information attribute comprising
15 security-based provisioning information corresponding to the first NAN device.

[00373] Example 113 includes the subject matter of Example 112, and optionally, wherein the provisioning information attribute comprises a public key of the first NAN device.

[00374] Example 114 includes the subject matter of Example 113, and optionally, wherein at least one of the provisioning messages is based on the public key of the first NAN device.

20 [00375] Example 115 includes the subject matter of any one of Examples 107-114, and optionally, comprising means for receiving a NAN Service Discovery Frame (SDF) from the second NAN device, the NAN SDF from the second NAN device comprising an indication that the second NAN device supports the provisioning protocol.

[00376] Example 116 includes the subject matter of Example 115, and optionally, wherein the
25 NAN SDF from the second NAN device comprises a provisioning-supported field having a predefined value to indicate that the provisioning protocol is supported.

[00377] Example 117 includes the subject matter of Example 116, and optionally, wherein the NAN SDF from the second NAN device comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.

[00378] Example 118 includes the subject matter of any one of Examples 115-117, and optionally, wherein the NAN SDF from the second NAN device comprises a service name to indicate that the second NAN device supports the provisioning protocol.

5 [00379] Example 119 includes the subject matter of any one of Examples 115-118, and optionally, wherein the NAN SDF from the second NAN device comprises a provisioning information attribute comprising security-based provisioning information corresponding to the second NAN device.

[00380] Example 120 includes the subject matter of Example 119, and optionally, wherein the provisioning information attribute comprises a public key of the second NAN device.

10 [00381] Example 121 includes the subject matter of Example 120, and optionally, wherein at least one of the provisioning messages is based on the public key of the second NAN device.

[00382] Example 122 includes the subject matter of any one of Examples 107-121, and optionally, comprising means for setting up the NAN schedule by exchanging with the second NAN device a NAN schedule request and a NAN schedule response, the NAN schedule request and the NAN schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

15 [00383] Example 123 includes the subject matter of Example 122, and optionally, wherein the NAN schedule request and the NAN schedule response comprise an NDL attribute, the NDL attribute comprising an NDL control field, the NDL control field comprising an NDL setup reason field having a predefined value to indicate that the NDL is to be set up for exchanging the provisioning messages.

[00384] Example 124 includes the subject matter of Example 122 or 123, and optionally, wherein the NAN schedule request comprises a provisioning information attribute comprising security-based provisioning information corresponding to a sender of the NAN schedule request.

25 [00385] Example 125 includes the subject matter of any one of Examples 107-124, and optionally, wherein the one or more provisioning messages comprise one or more messages of at least one of a provisioning authentication exchange, a provisioning configuration exchange, or a provisioning network introduction exchange.

30 [00386] Example 126 includes the subject matter of any one of Examples 107-125, and optionally, comprising means for cancelling the NAN schedule after provisioning the security key according to the provisioning protocol.

[00387] Example 127 includes the subject matter of Example 126, and optionally, comprising means for cancelling the NAN schedule upon completion of the provisioning of the security key according to the provisioning protocol.

5 [00388] Example 128 includes the subject matter of Example 126, and optionally, comprising means for cancelling the NAN schedule by transmission of a schedule update notification, which does not include a NAN availability attribute.

[00389] Example 129 includes the subject matter of any one of Examples 107-128, and optionally, wherein the provisioning protocol comprises a security-based provisioning protocol.

10 [00390] Example 130 includes the subject matter of any one of Examples 107-129, and optionally, wherein the provisioning protocol comprises a Device Provisioning Protocol (DPP).

[00391] Example 131 includes the subject matter of any one of Examples 107-130, and optionally, wherein the security key comprises a Pairwise Master Key (PMK).

15 [00392] Example 132 includes the subject matter of any one of Examples 107-131, and optionally, comprising means for discovering the second NAN device during a Discovery Window (DW) of a NAN cluster.

[00393] Functions, operations, components and/or features described herein with reference to one or more embodiments, may be combined with, or may be utilized in combination with, one or more other functions, operations, components and/or features described herein with reference to one or more other embodiments, or vice versa.

20 [00394] While certain features have been illustrated and described herein, many modifications, substitutions, changes, and equivalents may occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall within the true spirit of the disclosure.

CLAIMS

What is claimed is:

1. An apparatus comprising logic and circuitry configured to cause a first Neighbor Awareness Networking (NAN) device to:
 - 5 setup a NAN schedule with a second NAN device;
 exchange with the second NAN device, according to the NAN schedule, one or more provisioning messages of a provisioning protocol to provision a security key for the first and second NAN devices; and
 setup a secure NAN Data Path (NDP) with the second NAN device based on the
10 security key.
2. The apparatus of claim 1 configured to cause the first NAN device to transmit a NAN Service Discovery Frame (SDF) comprising an indication that the first NAN device supports the provisioning protocol.
3. The apparatus of claim 2, wherein the NAN SDF comprises a provisioning-supported
15 field having a predefined value to indicate that the provisioning protocol is supported.
4. The apparatus of claim 3, wherein the NAN SDF comprises a Service Descriptor Extension Attribute (SDEA), the SDEA comprising a control field comprising the provisioning-supported field.
5. The apparatus of claim 2, wherein the NAN SDF comprises a service name to indicate
20 that the first NAN device supports the provisioning protocol.
6. The apparatus of claim 2, wherein the NAN SDF comprises a provisioning information attribute comprising security-based provisioning information corresponding to the first NAN device.
7. The apparatus of claim 6, wherein the provisioning information attribute comprises a
25 public key of the first NAN device.
8. The apparatus of claim 7, wherein at least one of the provisioning messages is based on the public key of the first NAN device.
9. The apparatus of claim 1 configured to cause the first NAN device to receive a NAN Service Discovery Frame (SDF) from the second NAN device, the NAN SDF from the second

NAN device comprising an indication that the second NAN device supports the provisioning protocol.

10. The apparatus of any one of claims 1-9 configured to cause the first NAN device to setup the NAN schedule by exchanging with the second NAN device a NAN schedule request and a NAN schedule response, the NAN schedule request and the NAN schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

11. The apparatus of claim 10, wherein the NAN schedule request and the NAN schedule response comprise an NDL attribute, the NDL attribute comprising an NDL control field, the NDL control field comprising an NDL setup reason field having a predefined value to indicate that the NDL is to be set up for exchanging the provisioning messages.

12. The apparatus of claim 10, wherein the NAN schedule request comprises a provisioning information attribute comprising security-based provisioning information corresponding to a sender of the NAN schedule request.

13. The apparatus of any one of claims 1-9, wherein the one or more provisioning messages comprise one or more messages of at least one of a provisioning authentication exchange, a provisioning configuration exchange, or a provisioning network introduction exchange.

14. The apparatus of any one of claims 1-9 configured to cause the first NAN device to cancel the NAN schedule after provisioning the security key according to the provisioning protocol.

15. The apparatus of any one of claims 1-9, wherein the provisioning protocol comprises a Device Provisioning Protocol (DPP).

16. The apparatus of any one of claims 1-9, wherein the security key comprises a Pairwise Master Key (PMK).

17. The apparatus of any one of claims 1-9 configured to cause the first NAN device to discover the second NAN device during a Discovery Window (DW) of a NAN cluster.

18. The apparatus of any one of claims 1-9 comprising a radio.

19. A system of wireless communication comprising a first Neighbor Awareness Networking (NAN) device, the first NAN device comprising:

one or more antennas;
a radio;
a memory;
a processor; and

- 5 a controller configured to cause the first NAN device to:
 setup a NAN schedule with a second NAN device;
 exchange with the second NAN device, according to the NAN schedule, one or
more provisioning messages of a provisioning protocol to provision a security key for
the first and second NAN devices; and
10 setup a secure NAN Data Path (NDP) with the second NAN device based on the
security key.

20. The system of claim 19, wherein the controller is configured to cause the first NAN
device to setup the NAN schedule by exchanging with the second NAN device a NAN schedule
request and a NAN schedule response, the NAN schedule request and the NAN schedule
15 response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging
the provisioning messages.

21. The system of claim 20, wherein the NAN schedule request comprises a provisioning
information attribute comprising security-based provisioning information corresponding to a
sender of the NAN schedule request.

- 20 22. A method to be performed at a first Neighbor Awareness Networking (NAN) device,
the method comprising:
 setting up a NAN schedule with a second NAN device;
 exchanging with the second NAN device, according to the NAN schedule, one or more
provisioning messages of a provisioning protocol to provision a security key for the first and
25 second NAN devices; and
 setting up a secure NAN Data Path (NDP) with the second NAN device based on the
security key.

23. The method of claim 22 comprising transmitting a NAN Service Discovery Frame
(SDF) comprising an indication that the first NAN device supports the provisioning protocol.

- 30 24. The method of claim 22 comprising setting up the NAN schedule by exchanging with
the second NAN device a NAN schedule request and a NAN schedule response, the NAN

schedule request and the NAN schedule response comprising an indication that a NAN Device Link (NDL) is to be set up for exchanging the provisioning messages.

25. A product comprising one or more tangible computer-readable non-transitory storage media comprising computer-executable instructions operable to, when executed by at least one processor, enable the at least one processor to cause a first Neighbor Awareness Networking (NAN) device to perform the method of any one of claims 22-24.

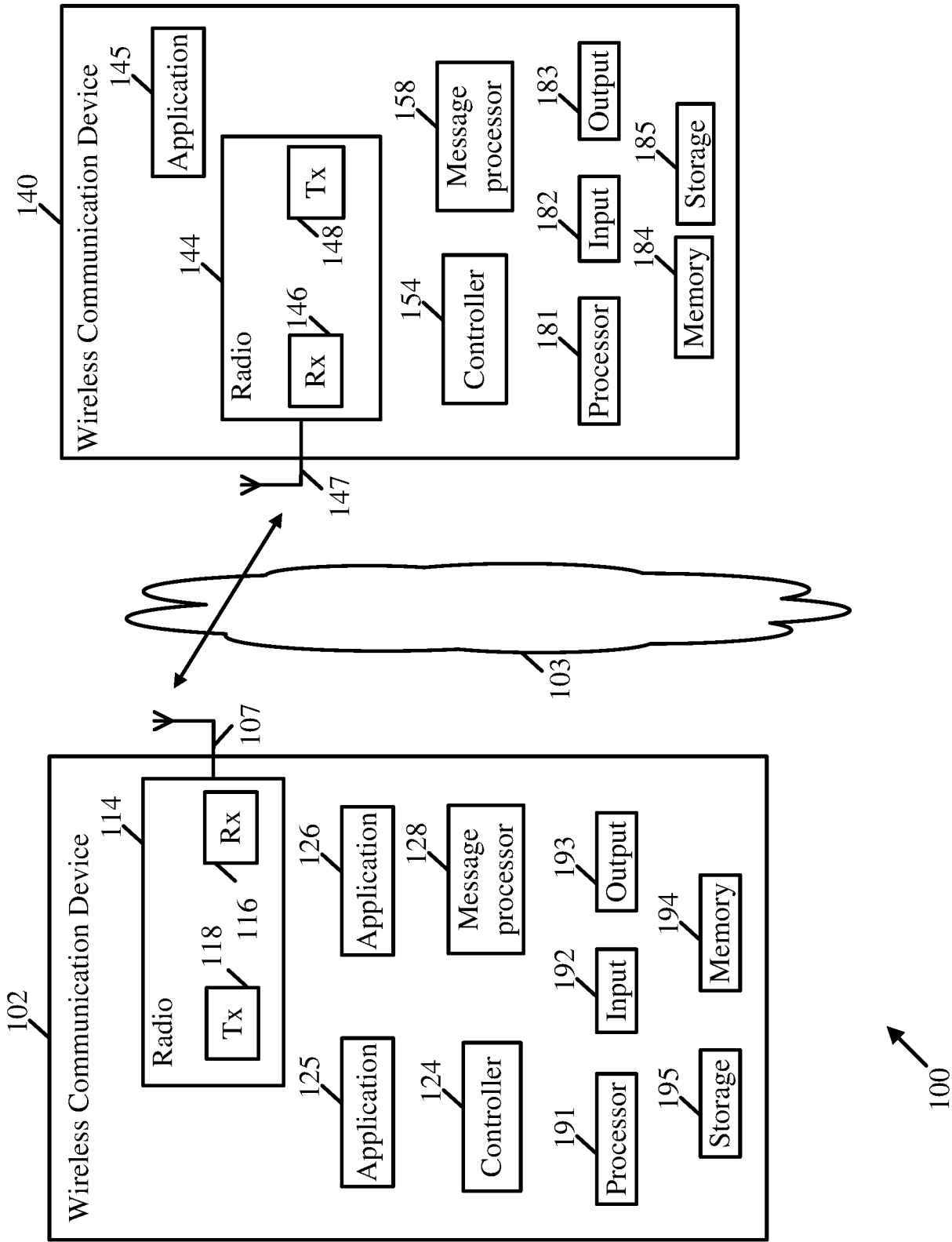


Fig. 1

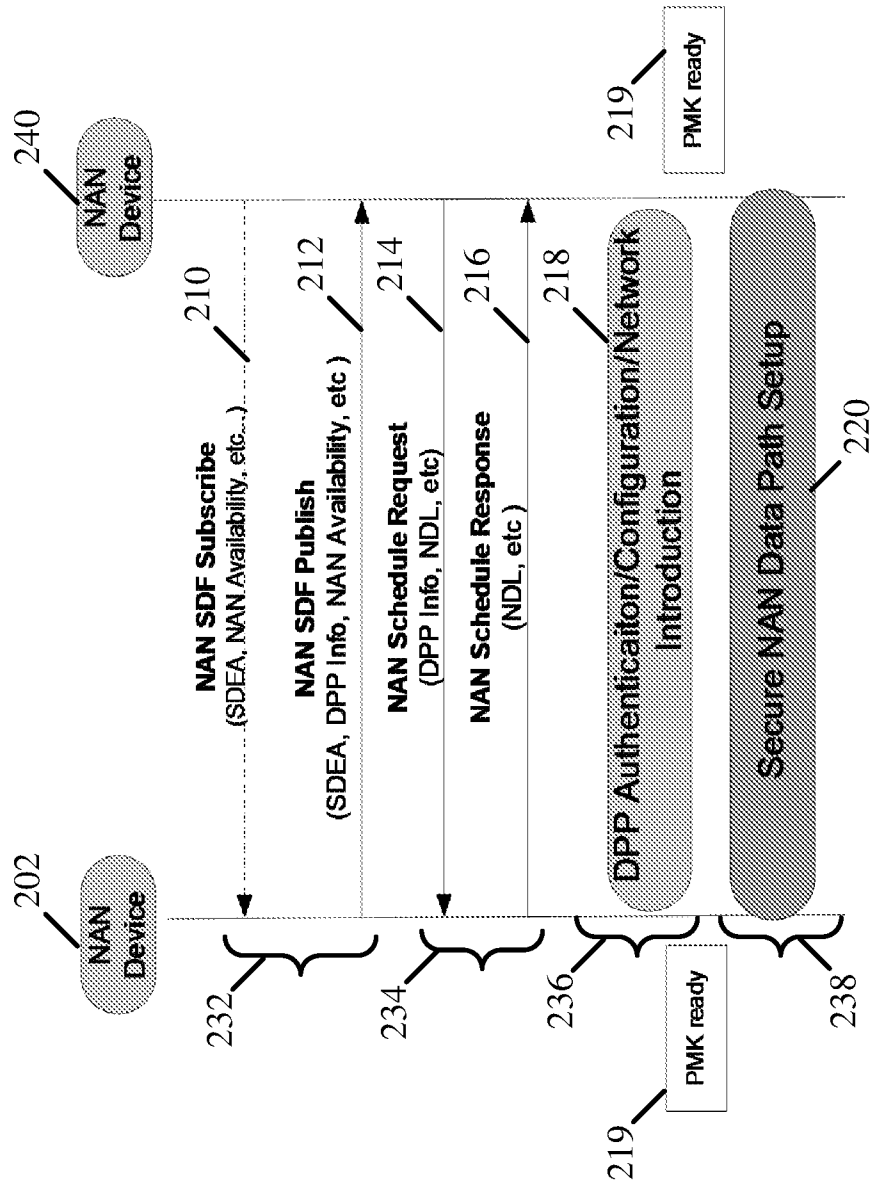


Fig. 2

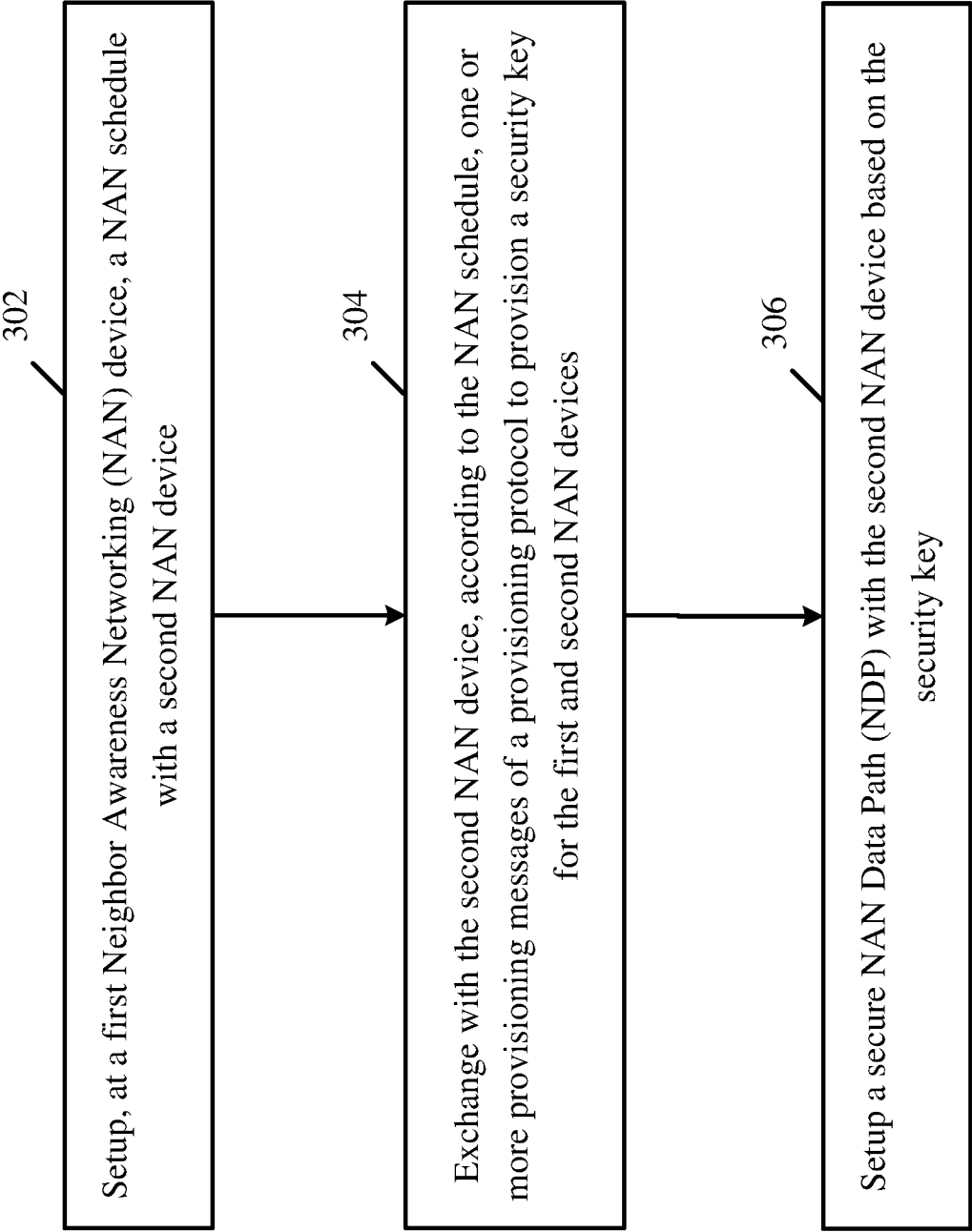


Fig. 3

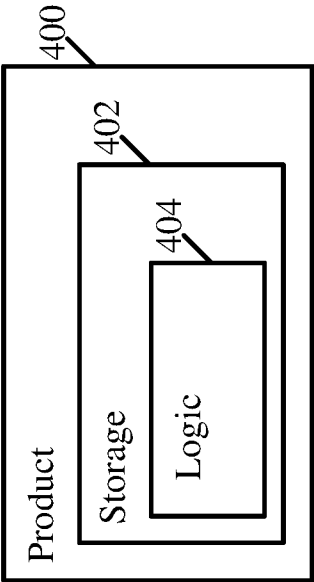


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/068482**A. CLASSIFICATION OF SUBJECT MATTER****H04W 4/50(2018.01)i, H04W 12/04(2009.01)i, H04W 72/12(2009.01)i, H04W 8/00(2009.01)i, H04W 84/18(2009.01)i**

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)

H04W 4/50; H04W 24/02; H04W 76/02; H04W 48/08; H04W 48/16; H04L 29/06; H04W 8/00; H04W 12/06; H04W 12/04; H04W 72/12; H04W 84/18

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: NAN, security, key, NDP, SDF, protocol

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2016-0286398 A1 (QUALCOMM INCORPORATED) 29 September 2016 See paragraphs [0006], [0010], [0015], [0086], [0093], [0105], [0125], [0134], [0224], [0226], [0337], [0365], [0388], [0392]-[0396], [0403], [0416]; and figure 1.	1-25
Y	US 2016-0277370 A1 (SAMSUNG ELECTRONICS CO., LTD.) 22 September 2016 See paragraphs [0003], [0023], [0052], [0058], [0091]; and figure 2.	1-25
A	US 2017-0055305 A1 (APPLE INC.) 23 February 2017 See paragraphs [0008], [0091]-[0097]; and figure 4.	1-25
A	KR 10-2017-0008769 A (LG ELECTRONICS INC.) 24 January 2017 See paragraphs [0046], [0049], [0084]; and figures 2-3.	1-25
A	US 2015-0365835 A1 (JONATHAN SEGEV et al.) 17 December 2015 See paragraphs [0026]-[0029]; and figure 3.	1-25



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

30 May 2018 (30.05.2018)

Date of mailing of the international search report

30 May 2018 (30.05.2018)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

NHO, Ji Myong

Telephone No. +82-42-481-8528



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2017/068482

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2016-0286398 A1	29/09/2016	CA 2976149 A1	29/09/2016
		CA 2976151 A1	29/09/2016
		CA 2976271 A1	29/09/2016
		CA 2977583 A1	29/09/2016
		CN 107409034 A	28/11/2017
		CN 107409415 A	28/11/2017
		CN 107431913 A	01/12/2017
		CN 107455012 A	08/12/2017
		EP 3275112 A1	31/01/2018
		EP 3275225 A1	31/01/2018
		EP 3275231 A1	31/01/2018
		EP 3275265 A1	31/01/2018
		KR 10-2017-0129771 A	27/11/2017
		KR 10-2017-0129772 A	27/11/2017
		KR 10-2017-0130425 A	28/11/2017
		KR 10-2017-0132166 A	01/12/2017
		TW 201639400 A	01/11/2016
		TW 201639401 A	01/11/2016
		TW 201639402 A	01/11/2016
		TW 201639408 A	01/11/2016
		US 2016-0286572 A1	29/09/2016
		US 2016-0286573 A1	29/09/2016
		US 2016-0286574 A1	29/09/2016
		WO 2016-154199 A1	29/09/2016
		WO 2016-154202 A1	29/09/2016
		WO 2016-154207 A1	29/09/2016
		WO 2016-154213 A1	29/09/2016
US 2016-0277370 A1	22/09/2016	CN 107431923 A	01/12/2017
		EP 3272179 A1	24/01/2018
		EP 3272179 A4	28/03/2018
		KR 10-2016-0112560 A	28/09/2016
		WO 2016-148534 A1	22/09/2016
US 2017-0055305 A1	23/02/2017	US 2017-055261 A1	23/02/2017
KR 10-2017-0008769 A	24/01/2017	CN 106465239 A	22/02/2017
		JP 2017-520957 A	27/07/2017
		US 2017-0111849 A1	20/04/2017
		US 9924446 B2	20/03/2018
		WO 2015-170818 A1	12/11/2015
US 2015-0365835 A1	17/12/2015	US 9763073 B2	12/09/2017