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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 November 2018 (01.11.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/200128 A1

(51) International Patent Classification:
H04W 24/10 (2009.01) *H04W 64/00* (2009.01)

(21) International Application Number:
PCT/US2018/025561

(22) International Filing Date:
30 March 2018 (30.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/489,964 25 April 2017 (25.04.2017) US

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

(72) Inventors: **LI, Qinghua**; 5117 Chiltern Lane, San Ramon, California 94582 (US). **JIANG, Feng**; Pole number C2, 4th floor, Building SC-123600, Juliette Lane, Santa Clara, California 95054 (US). **SEGEV, Jonathan**; 47 Hamataim, 40600 Tel Mond (IL). **ABRAMOVSKY, Benny**; Yigal Mosinzon St. 4, 4971024 Petah Tikva (IL). **CHEN, Xiaogang**; 7808 NW Blue Pointe Ln, Portland, Oregon 97229 (US). **STACEY, Robert**; 2871 NW Cumberland Rd., Portland, Oregon 97210 (US).

(74) Agent: **GRIFFIN III, Malvern U.** et al.; 999 Peachtree Street NE, Suite 2300, Atlanta, Georgia 30309 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, 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))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:
— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: ENHANCED DETECTION OF ADVERSARY ATTACKS FOR WIRELESS COMMUNICATIONS

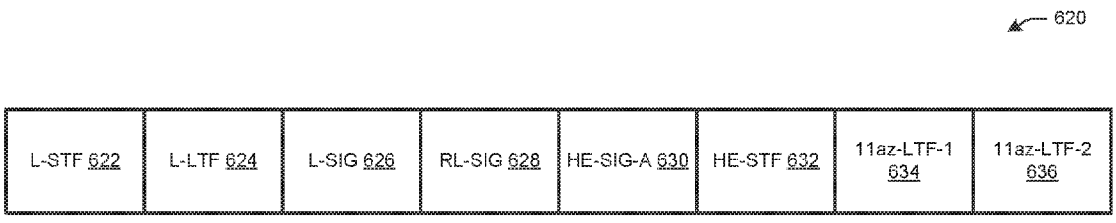

FIG. 6B

(57) Abstract: This disclosure describes systems, methods, and devices related to attack signal detection. A device may send a frame to one or more initiating devices. The device may identify a first sounding signal of a sounding signal sequence received from a first initiating device. The device may identify a second sounding signal of the sounding signal sequence received from the first initiating device. The device may send one or more null data packet frames to the first initiating device. The device may send a location measurement report to the first initiating device.

WO 2018/200128 A1

ENHANCED DETECTION OF ADVERSARY ATTACKS FOR WIRELESS COMMUNICATIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 62/489,964, filed April 25, 2017, entitled "Detecting Adversary Attack," the disclosure of which is incorporated by reference as if set forth in full.

TECHNICAL FIELD

[0002] This disclosure generally relates to systems and methods for wireless communications and, more particularly, to detecting adversary attacks in wireless communications.

BACKGROUND

[0003] Wireless devices are becoming widely prevalent and are increasingly requesting access to wireless channels. The growing density of wireless deployments require increased network and spectrum availability. Wireless devices may communicate over a next generation 60 GHz (NG60) network, an enhanced directional multi-gigabit (EDMG) network, and/or any other network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 depicts a network diagram illustrating an example network, in accordance with one or more example embodiments of the present disclosure.

[0005] FIG. 2 illustrative adversary attack process.

[0006] FIG. 3A depicts an illustrative sequence of sounding signals, in accordance with one or more example embodiments of the present disclosure.

[0007] FIG. 3B depicts an illustrative sequence of sounding signals, in accordance with one or more example embodiments of the present disclosure.

[0008] FIG. 3C depicts an illustrative sequence of sounding signals, in accordance with one or more example embodiments of the present disclosure.

[0009] FIG. 4A depicts an illustrative sequence, in accordance with one or more example embodiments of the present disclosure.

[0010] FIG. 4B depicts an illustrative sequence, in accordance with one or more example embodiments of the present disclosure.

[0011] FIG. 5A illustrates an illustrative sequence, in accordance with one or more

example embodiments of the present disclosure.

[0012] FIG. 5B illustrates an illustrative sequence, in accordance with one or more example embodiments of the present disclosure.

[0013] FIG. 6A illustrates a portion of a null data packet, in accordance with one or more example embodiments of the present disclosure.

[0014] FIG. 6B illustrates a portion of a null data packet, in accordance with one or more example embodiments of the present disclosure.

[0015] FIG. 7A illustrates a flow diagram of an illustrative process for enhanced attack detection, in accordance with one or more example embodiments of the present disclosure.

[0016] FIG. 7B illustrates a flow diagram of an illustrative process for enhanced attack detection, in accordance with one or more example embodiments of the present disclosure.

[0017] FIG. 8 illustrates a functional diagram of an example communication station that may be suitable for use as a user device, in accordance with one or more example embodiments of the present disclosure.

[0018] FIG. 9 is a block diagram of an example machine upon which any of one or more techniques (e.g., methods) may be performed, in accordance with one or more example embodiments of the present disclosure.

DETAILED DESCRIPTION

[0019] Example embodiments described herein provide certain systems, methods, and devices for enhanced attack detection. The following description and the drawings sufficiently illustrate specific embodiments to enable those skilled in the art to practice them. Other embodiments may incorporate structural, logical, electrical, process, and other changes. Portions and features of some embodiments may be included in, or substituted for, those of other embodiments. Embodiments set forth in the claims encompass all available equivalents of those claims.

[0020] Devices may communicate over a next generation 60 GHz (NG60) network, an enhanced directional multi-gigabit (EDMG) network, and/or any other network. Devices operating in EDMG may be referred to herein as EDMG devices. This may include user devices, and/or APs or other devices capable of communicating in accordance to a communication standard.

[0021] In wireless communications, security may be important for a variety of reasons. For example, ranging and positioning operations may benefit from enhanced security. Ranging and positioning operations (e.g., as in the IEEE 802.11az and 802.11mc Wi-Fi communication

standards) may allow devices to determine the distance and position of a user or other devices by sending signals to and receiving signals from those devices, and measuring signal times of arrival, for example. Based on determined location or distance of another device, a measuring device may determine whether to unlock. Therefore, the determined distance or location using ranging and positioning operations may be important to device security, and may allow for adversarial attacks.

[0022] Multiple threat modes may threaten security in IEEE 802.11az communications. For example, an adversary may generate a fake channel tap signal to trick a device. One way to trick a device is to make the device determine that a user is close enough to unlock the device when the user is actually further away. To execute an adversarial attack, a device may use a variety of signals. For example, if a ranging or positioning signal waveform and/or timing is known, an attacker can mimic the waveform and send the a signal according to the waveform to a device just before a non-adversarial signal (e.g., a channel sounding signal). This way, a receiving device may interpret the adversarial signal as a proper ranging or positioning signal for measurement purposes, and may improperly measure a location or distance of another device. An adversarial signal may be a jam signal which may include symbols similar to the symbols of a proper ranging or positioning signal.

[0023] Therefore, it may be desirable for a device to be able to detect an adversarial attack, and if the attack is detected, a device may discard a location or position measurement determined using the attack signal, and may request a new measurement.

[0024] Example embodiments of the present disclosure relate to systems, methods, and devices for enhanced detection of adversary attacks for wireless communications.

[0025] In one or more embodiments, an adversarial attack may be detected by using repetitive signals (e.g., channel sounding signals). For example, multiple ranging or positioning signals may be sent from one device to another. If the receiving device is aware of the pattern of multiple signals, then the receiving device may determine whether each received signal is proper, and can identify adversarial signals which do not match expected signal waveforms and/or timing. With repetitive signals, a channel response may not change significantly within a channel coherence time (e.g., 10 milliseconds). Two or more channel sounding signals may be sent within a channel coherence time so that, for example, a receiving device may determine whether a proper sequence of repetitive signals is received during that channel coherence time. For example, without multiple sounding signals, an attacker may send a random jam signal, which may be interpreted as a sounding signal. When a sequence of

sounding signals is used for enhanced attack detection, an attacker using multiple random jam signals may not know the changes between sounding signals and make corresponding changes in the jam signals, and a receiving device which is aware of what the sounding signal changes may be able to differentiate between proper sounding signals and attack attempts.

[0026] In one or more embodiments, a channel sounding signal may vary in each sounding time and part of the sounding signal. For example, even though the legacy training field sequence is known to an adversary, a cyclic shift of the legacy training field sequence may be unknown to the adversary and the shift amount may be varied between a first sounding signal and a second sounding signal. Without knowing the difference between the sounding signals, an adversary device may be unlikely to replicate the variation, and therefore a receiving device may recognize an adversary attack when a sequence of signals does not match the required variation. For example, interference may vary from one sounding signal to another. A receiving device may evaluate consistency among channel responses estimated within a channel coherence time. If channel responses are the same or similar enough within an expected variance, then the receiving device may determine that no attack exists. Otherwise, the receiving device may determine that an attack or interference exists, and therefore measured results of the signals may be unreliable.

[0027] In one or more embodiments, ranging and positioning operations may also use multiple channel soundings within a short time (e.g., 1-10 milliseconds), or may avoid using multiple channel soundings within such a time period. A station (STA) device may request that an access point (AP) indicate an attack detection mode to be used for communications between the AP and STA. The AP may announce an attack detection mode capability using a beacon or fine timing measurement (FTM) frame (e.g., an FTM response frame) sent to the STA, for example. The STA may receive the beacon, FTM response frame, or any other frame sent by the AP indicating the attack detection mode, and may identify the attack detection mode (e.g., secure mode) for subsequent communications. When an attack detection mode is applied by the AP and/or STA in a burst of sounding signals, the indication of an attack detection mode may be in a trigger frame or in a null data packet announcement (NDP-A) frame, in a beacon, or in another frame during a negotiation phase between the AP and STA. In some manner, the AP and STA may communicate the attack detection mode before ranging and positioning operations occur.

[0028] In one or more embodiments, to detect an attack, an AP and/or STA may need to sound a channel multiple times by sending sounding signals. One example attack detection

mode may implement a change between two consecutive sounding signals. The change between consecutive sounding signals may be unknown to an attacker so that, for example, the attacker is unlikely to replicate the sequence of sounding signals.

[0029] Sounding signals may use one or more sounding frames. A sounding frame may include a legacy portion and a non-legacy portion, and may be in the form of a null data packet (NDP) frame as defined by IEEE 802.11ax, IEEE 802.11ac, or IEEE 802.11mc standards, for example (e.g., a packet whose data field is null, but the packet may still carry other information such as training symbols which may be used for channel estimation or other channel evaluations/characteristics). An IEEE 802.11a device may read a legacy portion of a sounding frame, but may not be able to read a non-legacy portion of a sounding frame.

[0030] Both the legacy and non-legacy portions of a sounding frame may include sounding signals. A channel sounding signal may include a sequence of modulated signals (e.g., in a frequency domain) whose modulation may be binary phase shift keying (BPSK) or a higher quadrature amplitude modulation.

[0031] In one or more embodiments, an AP or STA sending a non-legacy portion of a channel sounding signal may change consecutive channel sounding signals (e.g., a second channel sounding signal may be different from a first channel sounding signal) within a short time period (e.g., 1-10 milliseconds). For example, a sending device may send different sequences of channel sounding symbols (e.g., orthogonal frequency division multiplex symbols) within the different channel sounding signals. In another example, a sending device may apply shifts to different channel sounding signals. A shift may be a linear or cyclic shift in a time domain, or a linear phase shift in a frequency domain. Similarly, in one or more embodiments, an AP or STA sending a legacy portion of a channel sounding signal may change consecutive channel sounding signals (e.g., a second channel sounding signal may be different from a first channel sounding signal) within a short time period (e.g., 1-10 milliseconds). For example, a sending device may apply shifts to different channel sounding signals. A shift may be a linear or cyclic shift in a time domain, or a linear phase shift in a frequency domain. For example, a sounding signal may be included in a legacy portion of a frame (e.g., with a legacy long training field). Because a legacy device may use the sounding signal in a legacy portion of a frame, the sequence of modulated signals in a non-legacy portion of a frame may be the same as the sequence used in the legacy portion of the frame, but one or more shifts may be applied (e.g., the non-legacy sounding signal sequence may be shifted in some manner from the legacy sounding sequence).

[0032] In one or more embodiments, a receiving device may need to be aware of the change between sounding signals in order to be able to determine if the received sounding signals are valid or include a part of an attempted attack. This way, a receiving device may estimate a channel based on valid sounding signals rather than on attack signals. For example, if a sequence of channel sounding signals includes a change between sounding signals, a receiving device may need to be aware of the specific sequence and the differences in the sounding signals within a sequence. In another example, a shift of a channel sounding signal may change from one sounding signal to another, and a receiving device may report measurements to a sending device based on the sounding signals, so the receiver may need to be aware of the shift change. A shift change of sounding signals may be encrypted to make it more difficult for an attacker to be aware of the shift. For example, an encrypted random seed for generating a shift change may be communicated between devices during a negotiation phase or during a measurement feedback phase.

[0033] In one or more embodiments, although a change may be applied to both legacy and non-legacy portions of a sounding frame, a change to a non-legacy portion of a sounding frame may be sufficient to significantly reduce the likelihood of a successful attack. An adversary may use a legacy portion of a sounding frame to estimate a channel, correct clock offsets, and set orthogonal frequency division multiplexing (OFDM) symbol boundaries, and then generate an attack on the non-legacy portion of the sounding frame. An attacker may generate a fake first channel tap ahead of the actual first channel arrival of a sounding signal. Therefore, the ranging and position operations, which may rely on a non-legacy portion of a sounding frame, may be vulnerable to an attack without proper mitigation techniques. If a change is applied to a non-legacy portion of a sounding frame, the change (e.g., a cyclic shift diversity shift) applied to a legacy portion of the sounding frame may be different than the change applied to the non-legacy portion of the sounding frame for enhanced protection.

[0034] A channel sounding signal may be bidirectional, meaning two ranging devices may sound a channel with each other. Attack detection may be applied in only one direction, however. To enhance security protection, attack detection may be applied in both directions of a channel sounding sequence between devices.

[0035] In one or more embodiments, in a bidirectional channel sounding, a channel sounding sequence may be completed in one direction (e.g., AP to STA or STA to AP) and repeated in the other direction between devices. Between bidirectional sounding sequences, a time interval may be short (e.g., a short interframe space, or less than 10 milliseconds). The

time range between bidirectional sounding sequences may be specified by an IEEE 802.11 standard and programmed into a device, or may be specified in a device negotiation phase, by a trigger frame, and/or by an NDP-A frame. One or more new types of trigger frames and/or NDP-A frames may need to be defined for triggering and announcing multiple NDP frames. In some other embodiments, in a bidirectional channel sounding, a channel sounding sequence may be completed in one direction (e.g., AP to STA or STA to AP) and repeated in the other direction between devices. In one or each direction, there may be multiple sounding signals with changes such that multiple different sounding signals are sent within a short time (e.g., right next to each other).

[0036] In one or more embodiments, there may be differences between attack detection for multiuser and single user modes. For backward compatibility with legacy devices without enhanced attack security, indications of attack detection capabilities may be included in a beacon, during a device negotiation phase, a trigger frame, or an NDP-A frame. An indication of attack detection capabilities may indicate to a receiving device of a sounding signal that the sounding signal may be sent multiple times with some change between respective sounding signals of a sequence of sounding signals. A receiving device may receive the sounding signals and compare channel estimates based on those sounding signals to determine whether the channel estimates are valid or represent an attack. If no attack is detected, a receiver device may combine channel estimates from repeated sounding signals to enhance ranging and positioning accuracy.

[0037] The above descriptions are for purposes of illustration and are not meant to be limiting. Numerous other examples, configurations, processes, etc., may exist, some of which are described in greater detail below. Example embodiments will now be described with reference to the accompanying figures.

[0038] FIG. 1 is a network diagram illustrating an example network environment, in accordance with one or more example embodiments of the present disclosure. Wireless network 100 may include one or more user device(s) 120 and one or more access point(s) (AP) 102, which may communicate in accordance with IEEE 802.11 communication standards, such as the IEEE 802.11ax and/or IEEE 802.11ac and/or IEEE 802.11ad and/or IEEE 802.11ay specifications. The user device(s) 120 may be referred to as stations (STAs). The user device(s) 120 may be mobile devices that are non-stationary and do not have fixed locations. Although the AP 102 is shown to be communicating on multiple antennas with user devices

120, it should be understood that this is only for illustrative purposes and that any user device 120 may also communicate using multiple antennas with other user devices 120 and/or AP 102.

[0039] In some embodiments, the user device(s) 120 and the AP 102 may include one or more computer systems similar to that of the functional diagram of FIG. 8 and/or the example machine/system of FIG. 9.

[0040] One or more illustrative user device(s) 120 and/or AP 102 may be operable by one or more user(s) 110. The user device(s) 120 (e.g., 124, 126, or 128) and/or AP 102 may include any suitable processor-driven device including, but not limited to, a mobile device or a non-mobile, e.g., a static, device. For example, user device(s) 120 and/or AP 102 may include, a user equipment (UE), a station (STA), an access point (AP), a personal computer (PC), a wearable wireless device (e.g., bracelet, watch, glasses, ring, etc.), a desktop computer, a mobile computer, a laptop computer, an ultrabook™ 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 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. It is understood that the above is a list of devices. However, other devices, including smart devices, Internet of Things (IoT), such as lamps, climate control, car components, household components, appliances, etc. may also be included in this list.

[0041] Any of the user device(s) 120 (e.g., user devices 124, 126, 128), and AP 102 may be configured to communicate with each other via one or more communications networks 130 and/or 135 wirelessly or wired. Any of the communications networks 130 and/or 135 may include, but not limited to, any one of a combination of different types of suitable communications networks such as, for example, broadcasting networks, cable networks, public networks (e.g., the Internet), private networks, wireless networks, cellular networks, or any other suitable private and/or public networks. Further, any of the communications networks 130 and/or 135 may have any suitable communication range associated therewith and may include, for example, global networks (e.g., the Internet), metropolitan area networks (MANs), wide area networks (WANs), local area networks (LANs), or personal area networks (PANs). In addition, any of the communications networks 130 and/or 135 may include any type of medium over which network traffic may be carried including, but not limited to, coaxial cable, twisted-pair wire, optical fiber, a hybrid fiber coaxial (HFC) medium, microwave terrestrial transceivers, radio frequency communication mediums, white space communication mediums, ultra-high frequency communication mediums, satellite communication mediums, or any combination thereof.

[0042] Any of the user device(s) 120 (e.g., user devices 124, 126, 128), and AP 102 may include one or more communications antennas. The one or more communications antennas may be any suitable type of antennas corresponding to the communications protocols used by the user device(s) 120 (e.g., user devices 124, 126 and 128), and AP 102. Some non-limiting examples of suitable communications antennas include Wi-Fi antennas, Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of standards compatible antennas, directional antennas, non-directional antennas, dipole antennas, folded dipole antennas, patch antennas, multiple-input multiple-output (MIMO) antennas, or the like. The one or more communications antennas may be communicatively coupled to a radio component to transmit and/or receive signals, such as communications signals to and/or from the user devices 120 and/or AP 102.

[0043] Any of the user devices 120 (e.g., user devices 124, 126, 128), and AP 102 may include multiple antennas that may include one or more directional antennas. The one or more directional antennas may be steered to a plurality of beam directions. For example, at least one antenna of a user device 120 (or an AP 102) may be steered to a plurality of beam directions. For example, a user device 120 (or an AP 102) may transmit a directional transmission to another user device 120 (or another AP 102).

[0044] Any of the user device(s) 120 (e.g., user devices 124, 126, 128), and AP 102 may be configured to perform directional transmission and/or directional reception in conjunction with wirelessly communicating in a wireless network. Any of the user device(s) 120 (e.g., user devices 124, 126, 128), and AP 102 may be configured to perform such directional transmission and/or reception using a set of multiple antenna arrays (e.g., DMG antenna arrays or the like). Each of the multiple antenna arrays may be used for transmission and/or reception in a particular respective direction or range of directions. Any of the user device(s) 120 (e.g., user devices 124, 126, 128), and AP 102 may be configured to perform any given directional transmission towards one or more defined transmit sectors. Any of the user device(s) 120 (e.g., user devices 124, 126, 128), and AP 102 may be configured to perform any given directional reception from one or more defined receive sectors.

[0045] MIMO beamforming in a wireless network may be accomplished using RF beamforming and/or digital beamforming. In some embodiments, in performing a given MIMO transmission, user devices 120 and/or AP 102 may be configured to use all or a subset of its one or more communications antennas to perform MIMO beamforming.

[0046] Any of the user devices 120 (e.g., user devices 124, 126, 128), and AP 102 may include any suitable radio and/or transceiver for transmitting and/or receiving radio frequency (RF) signals in the bandwidth and/or channels corresponding to the communications protocols utilized by any of the user device(s) 120 and AP 102 to communicate with each other. The radio components may include hardware and/or software to modulate and/or demodulate communications signals according to pre-established transmission protocols. The radio components may further have hardware and/or software instructions to communicate via one or more Wi-Fi and/or Wi-Fi direct protocols, as standardized by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standards. In certain example embodiments, the radio component, in cooperation with the communications antennas, may be configured to communicate via 2.4 GHz channels (e.g. 802.11b, 802.11g, 802.11n, 802.11ax), 5 GHz channels (e.g. 802.11n, 802.11ac, 802.11ax), or 60 GHZ channels (e.g. 802.11ad, 802.11ay). In some embodiments, non-Wi-Fi protocols may be used for communications between devices, such as Bluetooth, dedicated short-range communication (DSRC), Ultra-High Frequency (UHF) (e.g. IEEE 802.11af, IEEE 802.22), white band frequency (e.g., white spaces), or other packetized radio communications. The radio component may include any known receiver and baseband suitable for communicating via the communications protocols. The radio component

may further include a low noise amplifier (LNA), additional signal amplifiers, an analog-to-digital (A/D) converter, one or more buffers, and digital baseband.

[0047] Some demonstrative embodiments may be used in conjunction with a wireless communication network communicating over a frequency band of 60 GHz. However, other embodiments may be implemented utilizing any other suitable wireless communication frequency bands, for example, an extremely high frequency (EHF) band (the millimeter wave (mmWave) frequency band), a frequency band within the frequency band of between 20 GHz and 300 GHz, a WLAN frequency band, a WPAN frequency band, a frequency band according to the WGA specification, and the like.

[0048] The phrases "directional multi-gigabit (DMG)" and "directional band (DBand)", as used herein, may relate to a frequency band wherein the channel starting frequency is above 45 GHz. In one example, DMG communications may involve one or more directional links to communicate at a rate of multiple gigabits per second, for example, at least 1 gigabit per second, 7 gigabits per second, or any other rate.

[0049] In some demonstrative embodiments, the user device(s) 120 and/or the AP 102 may be configured to operate in accordance with one or more specifications, including one or more IEEE 802.11 specifications, (e.g., an IEEE 802.11az specification, an IEEE 802.11mc specification, and/or any other specification and/or protocol). For example, an amendment to a DMG operation in the 60 GHz band, according to an IEEE 802.11az standard, may be defined, for example, by an IEEE 802.11ay project.

[0050] It is understood that a basic service set (BSS) provides the basic building block of an 802.11 wireless LAN. For example, in infrastructure mode, a single access point (AP) together with all associated stations (STAs) is called a BSS.

[0051] In one or more embodiments, an AP may be referred to as a responding device, and an STA may be referred to as an initiating device.

[0052] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0053] FIG. 2 depicts an illustrative adversary attack process 200.

[0054] An AP 202 and STA 204 may be attempting to perform a channel sounding sequence with each other. STA 206 may be a device attempting to attack AP 202 and/or STA 204. AP 202 may send sounding signal 208, sounding signal 210, and sounding signal 212 to STA 204, which may receive each of the sounding signals. However, STA 206 may send an attack signal 214, attack signal 216, and attack signal 218 to STA 204.

[0055] STA 206 may send attack signal 214 to arrive at STA 204 before sounding signal 208. STA 206 may send attack signal 216 to arrive at STA 204 before sounding signal 210. STA 206 may send attack signal 218 to arrive at STA 204 before sounding signal 212. If STA 204 receives attack signal 214 before receiving sounding signal 208, for example, STA 204 may estimate a range or position based on attack signal 214 and based on sounding signal 208, and STA 204 may be tricked by STA 206. For example, if attack signal 214 causes STA 204 to determine that a device (e.g., AP 202) is close enough to unlock a display when STA 204 would otherwise not unlock the display, then STA 204 may become vulnerable from a security perspective. Because a device may use a time of arrival of a sounding signal, the device may use the sounding signal in a ranging or positioning operation. Therefore, if STA 204 receives attack signal 214 before sounding signal 208, for example, STA 204 may be tricked into thinking that a device is at a different range/position than the device really is. For example, STA 204 may rely on the time of arrival of the attack signal 214, which may suggest that a device is closer to STA 204 than the device really is. If STA 204 unlocks services based on a determined distance, then STA 204 may be tricked into unlocking for an attacker.

[0056] Therefore, enhanced attack signal detection may reduce device security vulnerabilities. By determining that an attack signal is improper, then ranging and position measurements based on the time of arrive of an attack signal may be discarded so that a receiving device may not become vulnerable to attacks.

[0057] Enhanced attack signal detection may include single direction sounding sequences or bidirectional sounding sequences. For example, in a bidirectional sounding sequence, AP 202 and STA 204 may sound a channel with each other. While AP 202 may send sounding signal 208, sounding signal 210, and/or sounding signal 212, STA 204 may also send one or more sounding signals to AP 202 in a similar manner.

[0058] Ranging and position measurements may be performed after sounding signals are received and evaluated. For example, after a receipt of sounding signal 208, sounding signal 210, and/or sounding signal 212, STA 204 may generate a location measurement report (e.g., LMR 220) and provide the location measurement report to AP 202 or AP 202 may generate and send LMR 220 to STA 204. AP 202 or STA 204 may evaluate the location measurement report. A location measurement report may be sent by one or more devices after the sounding sequences described below in FIGs. 4A, 4B, 5A, and 5B to provide position and ranging estimates to a device which transmitted one or more sounding signals.

[0059] FIG. 3A depicts an illustrative sequence 300 of sounding signals, in accordance

with one or more example embodiments of the present disclosure.

[0060] Referring to FIG. 3A, STA 302 may receive sequence 300, which may include sounding signal 304 and sounding signal 306 during a time interval 308. Sounding signal 304 and sounding signal 306 may consist of the same waveform. The channel responses estimated from sounding signal 304 and sounding signal 306 may be channel estimate 310 and channel estimate 312, respectively. Because sounding signal 304 and sounding signal 306 may be the same, and the channel response may remain the same for the time interval 308, channel estimate 310 and channel estimate 312 should be the same in the absence of attack signals. If the attacker knows that sounding signal 304 and sounding signal 306 are sent and they are the same before or during the soundings, the attacker can attack both sounding signal 304 and sounding signal 306 in the same way such that the channel estimates from both soundings are still the same. In this case, STA 302 may not determine whether the channel estimates are corrupted by the attack or not.

[0061] In one or more embodiments, the sequence 300 of sounding signal 304 and sounding signal 306 may reduce the likelihood of an attacker (e.g., STA 206 of FIG 2) exploiting a vulnerability of STA 302. For example, an attacker may not be aware of the sequence 300, and may only send one attack signal (e.g., attack signal 214 of FIG. 2), but may not send a second attack signal to replicate sequence 300. In addition, sounding signal 306 may differ from sounding signal 304 in one or more ways.

[0062] In one or more embodiments, STA 302 may send sequence 300, which may include sounding signal 304 and sounding signal 306 during time interval 308.

[0063] In one or more embodiments, STA 302 may execute a bidirectional sounding process. For example, STA 302 may receive sequence 300, which may include sounding signal 304 and sounding signal 306 from an AP (e.g., AP 202 FIG. 2), and may similarly send sounding signals to the AP for bidirectional communications.

[0064] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0065] FIG. 3B depicts an illustrative sequence 320 of sounding signals, in accordance with one or more example embodiments of the present disclosure.

[0066] Referring to FIG. 3B, STA 322 may receive sequence 320, which may include sounding signal 324 and sounding signal 326 during a time interval 328. Sounding signal 324 and sounding signal 326 may consist of a different waveform. The channel responses estimated from sounding signal 324 and sounding signal 326 may be channel estimate 330 and channel

estimate 332, respectively. Although sounding signal 324 and sounding signal 326 may be different, channel responses may remain the same for the time interval 328. Therefore, channel estimate 330 and channel estimate 332 should be the same in the absence of attack signals. Even if the attacker knows that sounding signal 324 and sounding signal 326 are sent and are different before or during the soundings, as long as the attacker does not know the difference between the two sounding signals, the attacker may not attack both sounding signal 324 and sounding signal 326 adaptively such that the resultant channel estimates from both soundings are the same. Checking for consistency among the channel estimates, STA 322 may determine whether the channel estimates are corrupted by an attack or not. For example, STA 322 may detect or declare an attack if channel estimate 330 and channel estimate 332 in FIG. 3B look different.

[0067] In one or more embodiments, the repetition of sounding signal 324 and sounding signal 326 in sequence 320 may allow STA 322 to detect an attack. For example, STA 322 may be aware of the application of different sounding signals 324 and 326. STA 322 may be informed of sequence 320 before the sounding. STA 322 may know that sequence 320 with different sounding signals 324 and 326 may be used in secure mode to detect attacks. If channel estimate 332 is significantly different from channel estimate 330 such that the difference is greater than those normally caused by noise, STA 322 may detect an attempted attack and/or channel interference and/or abnormal noise. Because STA 322 may determine a channel response based on sounding signal 324 and on sounding signal 326, a determined channel response may not change significantly within time interval 328 (e.g., a channel coherence time), allowing STA 322 to determine whether sequence 320 is valid or represents an attack. For example, if channel estimate 330 and channel estimate 332 changed too significantly during time interval 328, STA 322 may determine that an attack and/or interference have occurred, and STA 322 may seek additional sounding signals for further channel estimation or may declare the channel estimates or the conducted soundings are not secure. If interference/noise varies from sounding signal 324 to sounding signal 326, STA 322 may determine a consistency among estimated channel responses based on sounding signal 324 and sounding signal 326. If estimated channel responses (e.g., channel estimate 330 and channel estimate 332) are the same or similar enough (e.g., within a threshold tolerance level), then STA 322 may determine that no attack has been attempted. Similarly, if interference/noise varies from sounding signal 324 to sounding signal 326, STA 322 may determine a consistency among estimated channel responses based on sounding signal 324 and sounding signal 326. If

estimated channel responses (e.g., channel estimate 330 and channel estimate 332) are the same or similar enough (e.g., within a threshold tolerance level), then STA 322 may determine that no attack has been attempted.

[0068] In one or more embodiments, STA 322 may send sequence 320, which may include sounding signal 324 and sounding signal 326 during time interval 328.

[0069] In one or more embodiments, STA 322 may execute a bidirectional sounding process. For example, STA 322 may receive sequence 320, which may include sounding signal 324 and sounding signal 326 from an AP (e.g., AP 202 FIG. 2), and may similarly send sounding signals to the AP for bidirectional communications.

[0070] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0071] FIG. 3C depicts an illustrative sequence 340 of sounding signals, in accordance with one or more example embodiments of the present disclosure.

[0072] Referring to FIG. 3C, STA 342 may send or receive sounding signals, including sounding symbol sequence 344 and sounding symbol sequence 346 during a time interval (e.g., time interval 308 of FIG. 3A). Sounding symbol sequence 344 and sounding symbol sequence 346 may be modulated symbols (e.g., in a frequency domain) with a modulation of binary phase shift keying (BPSK) or a higher quadrative amplitude modulation (QAM).

[0073] In one or more embodiments, sounding symbol sequence 344 and sounding symbol sequence 346 may both include symbols S1-S4, but with a shift.

[0074] In one or more embodiments, sounding signals may be a part of a sounding frame, which may include legacy and non-legacy portions. For example, sounding symbol sequence 344 may be part of a legacy portion 354 and/or a non-legacy portion 356. Sounding symbol sequence 346 may be part of a legacy portion 358 and/or a non-legacy portion 360.

[0075] In one or more embodiments, in a cyclic shift, symbols S1, S2, S3, and S4 in sounding symbol sequence 344 of a sounding signal (e.g., sounding signal 304 of FIG. 3A) may be cyclically shifted to the order of S4, S1, S2, S3 in sounding sequence 346 of a second sounding signal (e.g., sounding signal 306 of FIG. 3A). This way, if a sounding signal with sounding symbol sequence 344 is cyclically shifted from a sounding signal with sounding symbol sequence 346, STA 342 may be able to determine whether an attack has been attempted. For example, one or more symbols S1-S4 may include a cyclic prefix repeated at the beginning and/or end of a symbol sequence (e.g., sounding symbol sequence 344, sounding symbol sequence 346).

[0076] In one or more embodiments, shifts between two soundings (e.g., a first sounding signal including a time-domain sample sequence and a second sounding signal including the cyclically shifted time-domain sample sequence) may be linear or cyclic in time.

[0077] In one or more embodiments, shifts between two soundings (e.g., a sounding signal including sounding symbol sequence 344 and a sounding signal including sounding symbol sequence 346) may be in a frequency domain. For example, a phase used to send a sounding signal including sounding symbol sequence 344 may be different than a phase used to send a sounding signal including sounding symbol sequence 346.

[0078] If STA 342, as a receiving device, is aware of an expected shift based on a communicated secure mode/capability, STA 342 may determine whether the shift matches (e.g., is the same as or within a threshold tolerance) a shift corresponding to a secure mode/capability. If a match occurs, STA 342 may determine than no attack has occurred, but otherwise may determine that an attack and/or interference may have occurred. For example, to estimate a channel, STA 342 may need to be aware of the shift applied. Alternatively, if STA 342 is unaware of the shift, STA 342 may send measurement results back to the device which sent the sounding signals (e.g., AP 202 of FIG. 2), and that device may determine for STA 342 whether an attack has been attempted. In order for STA 342 to be aware of the applied shift, the shift may be provided by an encrypted indication so that an attacker may not be aware of the shift. For example, an encrypted random seed for generating the change between sounding symbol sequence 344 and sounding symbol sequence 346 may be provided to STA 342 in an exchange during a negotiation phase or during a measurement feedback phase (e.g., a phase during which ranging and positioning measurements are exchanged between devices).

[0079] In one or more embodiments, legacy portion 354 and non-legacy portion 356 may be in a sounding signal (e.g., sounding signal 304 of FIG. 3A, sounding signal 324 of FIG. 3B), and legacy portion 358 and non-legacy portion 360 may be in another sounding signal (e.g., sounding signal 306 of FIG. 3A, sounding signal 326 of FIG. 3B) in a sounding sequence (e.g., sequence 300 of FIG. 3A, sequence 320 of FIG. 3B).

[0080] In one or more embodiments, a change (e.g., a waveform change as in FIG. 3B or a shift as in FIG. 3C) may be applied to both legacy portions (e.g., legacy portion 354 and legacy portion 358 of FIG. 3C) and to non-legacy portions (e.g., non-legacy portion 356 and non-legacy portion 360 of FIG. 3C). However, applying a change to a non-legacy portion (e.g., applying a change between non-legacy portion 356 and non-legacy portion 360 of FIG. 3C) may be sufficient for enhanced attack detection. This may be because an attacker may use a

legacy portion (e.g., legacy portion 354 of FIG. 3C) to estimate a channel, correct clock offsets, and set OFDM symbol boundaries, and then generate an attack on a non-legacy portion (e.g., non-legacy portion 356 of FIG. 3C). The effect of an attack (e.g., attack signal 214 of FIG. 2) may be a fake channel tap which arrives before the first arrival of actual sounding signal (e.g., as shown in FIG. 2). Thus, a ranging or positioning measurement may be based significantly on a non-legacy portion, which may be more susceptible to an attack. If a change is also applied to a non-legacy portion, the change may be different than the one applied to a legacy portion (e.g., a change between legacy portion 354 and legacy portion 358 may be different than a change between non-legacy portion 356 and non-legacy portion 360 of FIG. 3C) within a sequence of sounding signals (e.g., sequence 320 of FIG. 3B, sequence 340 of FIC. 3C).

[0081] In one or more embodiments, sequence 340 may be part of a single direction exchange, or may be part of a bidirectional exchange. For example, STA 342 may receive sounding symbol sequence 344 and sounding symbol sequence 346 from another device (e.g., AP 202 of FIG. 2), or may send sounding symbol sequence 344 and sounding symbol sequence 346 to another device. In a bidirectional exchange, STA 342 may send sounding symbol sequence 344 and sounding symbol sequence 346 while also receiving similar sequences from another device.

[0082] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0083] FIG. 4A depicts an illustrative sequence 400, in accordance with one or more example embodiments of the present disclosure.

[0084] Referring to FIG. 4A, AP 402 may be in communication with one or more devices (e.g., STA 404 and STA 418) in a channel, and may send a trigger frame 406 to those devices. One or more devices (e.g., STA 404) may respond by sending an NDP frame (e.g., NDP frame 408) to AP 402. AP 402 may send an NDP-A frame 410 and an NDP frame 412 to one or more devices in a channel. This sequence 400 may represent a sounding sequence according to the IEEE 802.11az standard. Without repetition, however, one sequence 400 may not support enhanced attack detection. Thus, sequence 400 may be adapted for enhanced attack detection.

[0085] In one or more embodiments, sequence 400 may be repeated after a time period (e.g., after a short inter frame space, less than 10 milliseconds) to implement enhanced attack detection (e.g., according to FIG. 3B or FIG. 3C). The time period may be specified in an IEEE 802.11 standard, agreed upon by AP 402 and one or more devices during a negotiation, and/or indicated in a trigger frame (e.g., trigger frame 406), and/or in an NDP-A frame (e.g., NDP-A

frame 410).

[0086] In one or more embodiments, sequence 400 may use existing NDP frames (e.g., NDP frame 408, NDP frame 412, NDP frame 420) to carry channel sounding signals. For example, trigger frame 406 may trigger the STA 404, STA 418 to send one or more sounding signals in a respective NDP frame (e.g., NDP frame 408, NDP frame 420). The AP 402 may send one or more sounding signals in NDP frame 412. The AP 402 may generate and send an LMR (e.g., LMR 414) to the STA 404 and STA 418, which may receive the LMR and determine whether ranging and positioning operations were valid and not subject to an attack, for example. Based on the LMR, the STAs may determine their respective locations.

[0087] In one or more embodiments, multi-user MIMO and/or orthogonal frequency division multiple access (OFDMA) may be used in a channel shared by one or more devices. For example, STA 418 may share a channel with AP 402 and STA 404. STA 418 may receive trigger frame 406, NDP-A frame 410, NDP frame 412, and/or beacon 416 from AP 402. STA 418 may send NDP frame 420 to AP 402, which may send frames to any devices in a channel, and may receive frames from any devices in a channel.

[0088] In one or more embodiments, by repeating sequence 400, implementation may be simplified. For example, using repetition of sounding signals by repeating sequence 400 may require only minor changes to existing processes. An attack detection mode/capability may be indicated in a trigger frame (e.g., trigger frame 406), an NDP-A frame (e.g., NDP-A frame 410), in a beacon 416, or during a negotiation phase which may include at least a portion of sequence 400. The indication of a secure mode/capability may indicate a number of sounding signals in a sounding sequence (e.g., how many NDP frames may be sent within one TXOP or how many repeated sounding signals may be sent in one NDP frame).

[0089] In one or more embodiments, bidirectional sounding is completed and is repeated. For example, AP 402 may receive one or more sounding signals (e.g., NDP frame 408) from STA 404, and may send one or more sounding signals (e.g., NDP frame 412) to STA 404 before STA 404 sends one or more subsequent sounding signals to AP 402 as part of a repetitive sounding sequence.

[0090] In one or more embodiments, LMR 414 may include time of arrival data associated with one or more NDP frames (e.g., NDP frame 408, NDP frame 420), and time of departure data associated with NDP frame 412. The time of departure and time of arrival data may be used to determine a range between AP 402 and STA 404, STA 418.

[0091] In one or more embodiments, NDP frame 412 may use an existing NDP frame

format, or may be adapted as shown in FIG. 6B, for example.

[0092] In one or more embodiments, trigger frame 406 and NDP-A frame 410 may be replaced with frames of a different format than existing trigger frames and NDP-A frames.

[0093] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0094] FIG. 4B depicts an illustrative sequence 450, in accordance with one or more example embodiments of the present disclosure.

[0095] In one or more embodiments, AP 452 may be in communication with one or more devices in a channel (e.g., STA 454, STA 476), and may send a trigger frame 456 to the devices in the channel. The one or more devices may respond by each sending an NDP frame (e.g., NDP frame 458, NDP frame 477) to AP 452. AP 452 may send trigger frame 460 to the one or more devices. The one or more devices may respond by each sending an NDP frame (e.g., NDP frame 462, NDP frame 478) to AP 452. AP 452 may send an NDP-A frame 464, an NDP frame 466, and NDP-A frame 468, and an NDP frame 470 to the one or more devices. The AP 452 may generate and send an LMR (e.g., LMR 472) to one or more other devices (e.g., STA 454, STA 476), which may receive the LMR. The LMR may include time of arrival information of one or more NDP frames (e.g., NDP 458, NDP frame 462, NDP frame 477, NDP frame 478), and a time of departure of an NDP frame (e.g., NDP frame 466, NDP frame 470). The time of departure and time of arrival data may be used to determine a range between AP 452 and STA 454, STA 476, for example. The one or more devices may use multiuser MIMO and/or OFDMA to share a channel.

[0096] In one or more embodiments, sequence 450 may use existing NDP frames (e.g., NDP frame 458, NDP frame 462, NDP frame 466, NDP frame 470, NDP frame 477, NDP frame 478) to carry channel sounding signals. For example, trigger frame 456 may trigger STA 454 and STA 476 to each send one or more sounding signals in their respective NDP frames (e.g., NDP frame 458, NDP frame 462, NDP frame 477, NDP frame 478). AP 452 may send one or more sounding signals in NDP frame 466, and one or more sounding signals in NDP frame 470.

[0097] In one or more embodiments, the secure mode/capability may be indicated in a trigger frame (e.g., trigger frame 456, trigger frame 460), an NDP-A frame (e.g., NDP-A frame 464, NDP-A frame 468), in a beacon 474, or during a negotiation phase which may include at least a portion of sequence 450. The indication of a secure mode/capability may indicate a number of repeated sounding signals in a sounding sequence.

[0098] In one or more embodiments, sequence 450 may be a variation of sequence 400 of FIG. 4A. Instead of a device sending a sounding signal sequence to another device and receiving a sounding signal sequence from the other device before sending another sounding signal sequence to the other device, sequence 450 may include multiple sounding signals sent in one direction (e.g., from AP 452 to STA 454 and to STA 476) before multiple sounding signals are sent in the opposite direction (e.g., from STA 454 and STA 476 to AP 452). For example, referring to FIG. 4A, STA 404 and STA 418 may send one or more sounding signals in a set of NDP frames (e.g., NDP frame 408, NDP frame 420), and AP 402 may send one or more sounding signals in NDP frame 412. Then, sequence 400 of FIG. 4A may repeat, so STA 404 and/or STA 418 may send another NDP frame (not shown) before AP 402 sends another NDP-A frame and another NDP frame (not shown). In FIG. 4B, STA 454 and STA 476 may complete their sounding signal sequences by sending one or more sounding signals in the set of NDP frames (e.g., NDP frame 458, NDP frame 477) and one or more sounding signals in another set of NDP frames (e.g., NDP frame 462, NDP frame 478) before AP 452 sends a sequence of sounding signals in NDP frame 466 and NDP frame 470.

[0099] In one or more embodiments, trigger frame 460 and NDP-A frame 468 may be replaced with frames of a different format than existing trigger frames and NDP-A frames.

[0100] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0101] Referring to FIG. 4A and 4B, a receiver device (e.g., STA 404 and/or STA 418 of FIG. 4A, STA 454 and/or STA 476 of FIG. 4B) may determine channel estimates based on received sounding signals (e.g., using training symbols in one or more NDP frames), and may compare the channel estimates to determine whether an attack has been attempted. If the receiver device has determined that no attack has been attempted, the receiver device may combine the channel estimates to enhance ranging and positioning accuracy. Also, FIG. 4A and FIG. 4B may refer to a multiuser mode.

[0102] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0103] FIG. 5A illustrates an illustrative sequence 500, in accordance with one or more example embodiments of the present disclosure.

[0104] Referring to FIG. 5A, STA 502 may be in communication with STA 504. Either of STA 502 or STA 504 may be an AP. STA 502 and STA 504 may be non-AP STAs (e.g., in a peer-to-peer operation). STA 502 may send an NDP-A frame 506 and an NDP frame 508 to

STA 504. STA 504 may respond by sending an NDP frame 510 to STA 502. NDP-A frame 506 may announce that one or more sounding signals may be sent in NDP frame 508. The STA 502 may generate and send an LMR 512 to STA 504, which may receive LMR 512 and determine whether ranging and positioning operations were valid and not subject to an attack, for example.

[0105] In one or more embodiments, all or a portion of sequence 500 may be repeated. For example, after a time period (e.g., a short inter frame space, less than 10 milliseconds), sequence 500 may be repeated for enhanced security. STA 502 may send another NDP-A frame and another NDP frame (not shown), and STA 504 may send another NDP frame (not shown) in repetition of sequence 500.

[0106] Sequence 500 may be according to the IEEE 802.11az standard, and may be adapted to support enhanced attack detection by repeating sequence 500 to allow for multiple channel sounding signals. Sequence 500 may refer to a single user mode.

[0107] In one or more embodiments, sequence 500 may use existing NDP frames (e.g., NDP frame 508, NDP frame 510) to carry channel sounding signals. For example, NDP-A frame 506 may announce to STA 504 that STA 502 may send one or more sounding signals in NDP frame 508. STA 504 may send one or more sounding signals in NDP frame 510.

[0108] In one or more embodiments, at least a portion of sequence 500 may be repeated to allow for enhanced attack detection. NDP frame 508 may include one or more sounding signals. For example, NDP frame 508 may include two sounding signals for repeated channel sounding signals with a variation between them. NDP frame 510 may include two sounding signals for repeated channel sounding signals with a variation between them. After STA 502 receives NDP frame 510, STA 502 may send another NDP frame (not shown), and STA 504 may send another NDP frame (not shown) in repetition of sequence 500 to allow for each device to send a sequence of sounding signals via the NDP frames. This way, each STA may allow the other STA to send one or more sounding signals before sending the next one or more sounding signals in a sequence.

[0109] In one or more embodiments, the secure mode/capability may be indicated in an NDP-A frame (e.g., NDP-A frame 506), in a beacon 514, or during a negotiation phase which may include at least a portion of an FTM sequence (e.g., an FTM request and/or FTM response frame). The indication of a secure mode/capability may indicate a number of sounding signals in a sounding sequence (e.g., how many NDP frames may be sent or how many repetitive sounding signals may be sent in one NDP frame).

[0110] In one or more embodiments, NDP-A frame 506 may be replaced with a frame of a different format than existing NDP-A frames.

[0111] In one or more embodiments, NDP frame 508 and/or NDP frame 510 may use existing NDP frame formats, or may use a new NDP frame format (e.g. ,as shown in FIG. 6B). For example, a new NDP frame format may allow for multiple sounding signals in an NDP frame.

[0112] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0113] FIG. 5B illustrates an illustrative sequence 500, in accordance with one or more example embodiments of the present disclosure.

[0114] Referring to FIG. 5B, STA 542 may be in communication with STA 544. Either of STA 542 or STA 544 may be an AP. STA 542 and STA 544 may be non-AP STAs (e.g., in a peer-to-peer application). STA 542 may send an NDP-A frame 546, an NDP frame 548, and an NDP frame 550 to STA 544. STA 544 may respond by sending an NDP frame 552 and another NDP frame 554 to STA 542. NDP-A frame 546 may announce that sounding signals may be sent in NDP frame 548 and in NDP frame 550. The STA 542 may generate and send an LMR 556 to STA 544, which may receive LMR 556 and derive range information based on information included in LMR for example. Sequence 540 may refer to a single user mode.

[0115] In one or more embodiments, each STA may finish sending its respective sounding signal sequence before the other STA sends its sounding signal sequence. For example, STA 542 may send one or more sounding signals in NDP frame 548 and in NDP frame 550 before STA 544 sends a one or more sounding signals in NDP frame 552 and NDP frame 554.

[0116] In one or more embodiments, the secure mode may be indicated in an NDP-A frame (e.g., NDP-A frame 546), in a beacon 558, or during a negotiation phase. The indication of a secure mode may indicate a number of sounding signals in a sounding sequence (e.g., how many NDP frames may be sent).

[0117] In one or more embodiments, NDP-A frame 546 may be replaced with a frame of a different format than existing NDP-A frames.

[0118] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0119] FIG. 6A illustrates a portion 600 of an NDP frame, in accordance with one or more example embodiments of the present disclosure.

[0120] Referring to FIG. 6A, the portion 600 of an NDP frame may be formatted according

to the IEEE 802.11ax standard, and may be similar to NDP frame formats defined in the IEEE 802.11mc, 802.11ac, and 802.11n standards. The portion 600 of an NDP frame may include a legacy short training field (L-STF) 602, a legacy long training field (L-LTF 604), a legacy signal field (L-SIG) 606, a repeat legacy signal field (RL-SIG) 608, a high efficiency signal-A field (HE-SIG-A) 610, a high efficiency short training field (HE-STF) 612, and a high efficiency long training field (HE-LTF) 614. A legacy portion may include the L-STF field 602, L-LTF field 604, and L-SIG field 606, and may correspond to legacy fields in the IEEE 802.11a, 802.11ac, and 802.11n standards. For example, L-STF field 602 may correspond to the IEEE 802.11a standard, L-LTF field 604 may correspond to the IEEE 802.11ac standard, and L-SIG field 606 may correspond to the IEEE 802.11n standard.

[0121] In one or more embodiments, the portion 600 of an NDP frame may be included in the NDP frames in FIGs. 4A, 4B, 5A, and 5B. When using repetition of sounding signals in FIGs. 4A, 4B, 5A, and 5B, the legacy fields and/or the non-legacy fields of portion 600 may be repeated.

[0122] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0123] FIG. 6B illustrates a portion 620 of an NDP frame, in accordance with one or more example embodiments of the present disclosure.

[0124] Referring to FIG. 6B, the portion 620 of an NDP frame may be formatted according to the IEEE 802.11ax standard, and may be similar to NDP frame formats defined in the IEEE 802.11mc, 802.11ac, and 802.11n standards. The portion 620 of an NDP frame may include a legacy short training field (L-STF) 622, a legacy long training field (L-LTF 624), a legacy signal field (L-SIG) 626, a repeat legacy signal field (RL-SIG) 628, a high efficiency signal-A field (HE-SIG-A) 630, a high efficiency short training field (HE-STF) 632, and one or more 11az secure long training fields (e.g., 11az-LTF-1 field 634, 11az-LTF-2 field 636). A legacy portion may include the L-STF field 602, L-LTF field 604, and L-SIG field 606, and may correspond to legacy fields in the IEEE 802.11a, 802.11ac, and 802.11n standards. For example, L-STF field 622 may correspond to the IEEE 802.11a standard, L-LTF field 624 may correspond to the IEEE 802.11ac standard, and L-SIG field 626 may correspond to the IEEE 802.11n standard. The 11az secure long training fields may correspond to the IEEE 802.11az standard.

[0125] In one or more embodiments, to reduce overhead among multiple NDP frames, however, the non-legacy parts (e.g., 11az-LTF-1 field 634, 11az-LTF-2 field 636) may be

repeated. The repeated 11az-LTF fields may be different from one another to allow for a receiving device to detect an attack. As explained above with regard to FIGs. 3A, 3B, and 3C, a change between 11az-LTF-1 field 634 and 11az-LTF-2 field 636 may be represented by a shift or by different sounding symbols or different waveforms. Using the compact format of portion 620, sounding exchanges using NDP frames for both single user and multiuser may be simplified. In one or more embodiments, 11az-LTF-1 field 634 may be associated with different antennas and/or different users and 11az-LTF-2 field 636 may be the repeated version of 11az-LTF-1 field 634 with a variation. Repetition of 11az-LFT fields may include two or more 11az-LTF fields. 11az-LTF-1 field 634 may be associated with a spatial stream used for transmission of an NDP frame, and 11az-LTF-2 field 636 may be associated with another spatial stream used for transmission of the NDP frame.

[0126] In one or more embodiments, the IEEE 802.11ax NDP frame may be modified for the IEEE 802.11az standard. For example, the portion 600 of FIG. 6A may be modified according to the portion 620 of FIG. 6B. Similarly, the NDP frame from the IEEE 802.11ac standard may be modified for the IEEE 802.11az standard. The IEEE 802.11ac NDP frame may be used for a single user environment, and the IEEE 802.11ax NDP frame with portion 600 of FIG. 6A may be used for a multiuser environment. The different NDP frame formats may be used interchangeably in different environments.

[0127] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0128] FIG. 7A illustrates a flow diagram of an illustrative process 700 for enhanced attack detection, in accordance with one or more example embodiments of the present disclosure.

[0129] At block 702, one or more processors of a device (e.g., AP 102 of FIG. 1) may cause the device to send a frame to an STA (e.g., user device(s) 120 of FIG. 1). The frame may include an indication of a secure mode/capability associated with a sounding signal sequence. The frame may be a beacon or an FTM response frame. The frame/secure mode may indicate a number of sounding signals to be sent during the sounding signal sequence and/or may indicate a shift among respective sounding signals of a sounding signal sequence. The frame may be sent to additional STAs. For example, the device may identify a request frame received from the STA, and the request frame may propose a number of sounding signals to use in the sounding signal sequence. The frame sent by the device may be in response to the request frame and may set the actual number of sounding signals to be used in the sounding signal sequence. The device may be a responding device.

[0130] At block 704, one or more processors of the device may identify a first sounding signal of a sounding signal sequence received from an initiating device (e.g., user device(s) 120 of FIG. 1). The sounding signal may be determined based at least in part on the secure mode. For example, the first sounding signal may be associated with a difference in symbols or a shift when compared with a second sounding signal in a sounding signal sequence.

[0131] At block 706, one or more processors of the device may identify a second sounding signal of the sounding signal sequence received from the initiating device, based at least in part on the secure mode. The first sounding signal may be different than the second sounding signal. For example, the second sounding signal may include a different sequence of symbols than the first sounding signal. The second sounding signal may be shifted in time and/or frequency from the first sounding signal. A shift may be linear or cyclical. A cyclic shift may be used on any combination of sounding signals, and respective sounding signals may include a common or different cyclic shift. In the time domain, a cyclic shift may be linear or cyclical. In the frequency domain, a shift may be linear. Other sounding signals may also be identified from the initiating device or from other sounding signals received from other initiating devices. For example, if the secure mode/capability supports more than two sounding signals in a sequence, the secure mode/capability will indicate such, and additional sounding signals may be determined.

[0132] At block 708, one or more processors of the device may cause the device to send one or more null data packet frames to the initiating device and/or other initiating devices. The one or more null data packet frames may include a sequence of multiple sounding signals which may be different from one another.

[0133] At block 710, one or more processors of the device may cause the device to send a location measurement report to the initiating device and/or other initiating devices. The device may determine the location measurement report using the one or more received sounding signals of the sounding signal sequence. The location measurement report may indicate a time of arrival of the one or more sounding signals of the sounding signal sequence (e.g., in an NDP frame), and also may indicate a time of departure of an NDP frame sent from the responding device to one or more of the initiating devices.

[0134] In one or more embodiments, after sending the sounding signal sequence of sounding signals, the device may also send measurement reports (e.g., an FTM measurement report) to initiating STA. An initiating device may determine range information based on the measurement report. If an STA provides sounding signals to the device, the sounding signals

between devices may alternate, or the device may complete its sounding signal sequence before an STA provides sounding signals.

[0135] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0136] FIG. 7B illustrates a flow diagram of an illustrative process 750 for enhanced attack detection, in accordance with one or more example embodiments of the present disclosure.

[0137] At block 752, one or more processors of a device (e.g., the user device(s) 120 of FIG. 1) may identify a frame received from another device (e.g., AP 102 of FIG. 1). The frame may include an indication of a secure mode/capability associated with a sounding signal sequence. The frame may be a beacon, an NDP-A frame, a trigger frame, or an FTM response frame. The identified frame/secure mode/capability may indicate how many sounding signals may be sent in a sounding signal sequence, and a difference between sounding signals in a sounding signal sequence. For example, the identified frame may be a frame sent in response to a request frame, which the device may send, and which may include a proposed number of sounding signals to use in the sounding signal sequence. The identified frame may be in response to the request frame sent by the device, and may indicate the set number of sounding signals to use in the sounding signal sequence. The device may be an initiating device.

[0138] At block 754, one or more processors of the device may cause the device to send a first sounding signal of a sounding signal sequence and a second sounding signal of the sounding signal sequence to the responding device. The second sounding signal may be according to the secure mode/capability as indicated in the frame received from the other device. The second sounding signal may be different from the first sounding signal of the sounding signal sequence. Each sounding signal may be sent in an NDP frame.

[0139] At block 756, one or more processors of the device may identify an NDP frame received from a responding device. The NDP frame may include one or more sounding signals, and if there are multiple sounding signals, the sounding signals may be different from one another. The device may identify the third sounding signal and the fourth sounding signal from the NDP frame received from the responding device.

[0140] At block 758, one or more processors of the device may determine a difference between a third channel estimation associated with the third sounding signal and a fourth channel estimation associated with the fourth sounding signal. The difference may be intentional as indicated by the secure mode/capability. The difference may be determined based on channel estimations associated with the sounding signals. The channel estimations

may be transmitted in an LMR. If the difference between channel estimations associated with the first and second sounding signals are within a threshold value measuring the allowable difference between the channel estimations, then the device may measure a time of arrival using the sounding signals of the sounding signal sequence, and may determine a range of the other device based on the time of arrival and/or time of departure determinations. If the measurements do not meet a threshold difference value measuring the allowable difference between the channel estimations, then the device may determine that an attack may have been attempted, and may not rely on the measurement. The device may discard time of arrival measurements if the device determines that the difference in sounding signals and/or measurements made based on the sounding signals is not within a difference threshold value. Channel estimation differences may be determined using channel estimations in a time and/or frequency domain, and may include determining a difference between respective channel estimations, determining an amplitude ratio between respective channel estimations, and/or determining a power ratio between respective channel estimations. If the calculations do not meet one or more difference thresholds, it may be determined that some measurements may be discarded. To improve a signal-to-noise ratio of a channel estimation, the device may average multiple channel estimations associated with sounding signals, resulting in improved accuracy of time of arrival estimation. The device also may request additional sounding signals. The device may also send sounding signals to the other device, either alternating with sounding signals from the other device, or one of the devices waiting until the other has completed a sounding signal sequence. The differences between the sounding signals may include a shift in the time and/or frequency domains. A shift may be linear or cyclical in the time domain, and may be linear in the frequency domain.

[0141] It is understood that the above descriptions are for purposes of illustration and are not meant to be limiting.

[0142] FIG. 8 shows a functional diagram of an exemplary communication station 800 in accordance with some embodiments. In one embodiment, FIG. 8 illustrates a functional block diagram of a communication station that may be suitable for use as an AP 102 (FIG. 1) or a user device 120 (FIG. 1) in accordance with some embodiments. The communication station 800 may also be suitable for use as a handheld device, a mobile device, a cellular telephone, a smartphone, a tablet, a netbook, a wireless terminal, a laptop computer, a wearable computer device, a femtocell, a high data rate (HDR) subscriber station, an access point, an access terminal, or other personal communication system (PCS) device.

[0143] The communication station 800 may include communications circuitry 802 and a transceiver 810 for transmitting and receiving signals to and from other communication stations using one or more antennas 801. The communications circuitry 802 may include circuitry that can operate the physical layer (PHY) communications and/or medium access control (MAC) communications for controlling access to the wireless medium, and/or any other communications layers for transmitting and receiving signals. The communication station 800 may also include processing circuitry 806 and memory 808 arranged to perform the operations described herein. In some embodiments, the communications circuitry 802 and the processing circuitry 806 may be configured to perform operations detailed in FIGs. 2, 3A, 3B, 3C, 4A, 4B, 5A, 5B, 6A, 6B, 7A, and 7C.

[0144] In accordance with some embodiments, the communications circuitry 802 may be arranged to contend for a wireless medium and configure frames or packets for communicating over the wireless medium. The communications circuitry 802 may be arranged to transmit and receive signals. The communications circuitry 802 may also include circuitry for modulation/demodulation, upconversion/downconversion, filtering, amplification, etc. In some embodiments, the processing circuitry 806 of the communication station 800 may include one or more processors. In other embodiments, two or more antennas 801 may be coupled to the communications circuitry 802 arranged for sending and receiving signals. The memory 808 may store information for configuring the processing circuitry 806 to perform operations for configuring and transmitting message frames and performing the various operations described herein. The memory 808 may include any type of memory, including non-transitory memory, for storing information in a form readable by a machine (e.g., a computer). For example, the memory 808 may include a computer-readable storage device, read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices and other storage devices and media.

[0145] In some embodiments, the communication station 800 may be part of a portable wireless communication device, such as a personal digital assistant (PDA), a laptop or portable computer with wireless communication capability, a web tablet, a wireless telephone, a smartphone, a wireless headset, a pager, an instant messaging device, a digital camera, an access point, a television, a medical device (e.g., a heart rate monitor, a blood pressure monitor, etc.), a wearable computer device, or another device that may receive and/or transmit information wirelessly.

[0146] In some embodiments, the communication station 800 may include one or more antennas 801. The antennas 801 may include one or more directional or omnidirectional antennas, including, for example, dipole antennas, monopole antennas, patch antennas, loop antennas, microstrip antennas, or other types of antennas suitable for transmission of RF signals. In some embodiments, instead of two or more antennas, a single antenna with multiple apertures may be used. In these embodiments, each aperture may be considered a separate antenna. In some multiple-input multiple-output (MIMO) embodiments, the antennas may be effectively separated for spatial diversity and the different channel characteristics that may result between each of the antennas and the antennas of a transmitting station.

[0147] In some embodiments, the communication station 800 may include one or more of a keyboard, a display, a non-volatile memory port, multiple antennas, a graphics processor, an application processor, speakers, and other mobile device elements. The display may be an LCD screen including a touch screen.

[0148] Although the communication station 800 is illustrated as having several separate functional elements, two or more of the functional elements may be combined and may be implemented by combinations of software-configured elements, such as processing elements including digital signal processors (DSPs), and/or other hardware elements. For example, some elements may include one or more microprocessors, DSPs, field- programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), radio- frequency integrated circuits (RFICs) and combinations of various hardware and logic circuitry for performing at least the functions described herein. In some embodiments, the functional elements of the communication station 800 may refer to one or more processes operating on one or more processing elements.

[0149] Certain embodiments may be implemented in one or a combination of hardware, firmware, and software. Other embodiments may also be implemented as instructions stored on a computer-readable storage device, which may be read and executed by at least one processor to perform the operations described herein. A computer-readable storage device may include any non-transitory memory mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a computer-readable storage device may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media. In some embodiments, the communication station 800 may include one or more processors and may be configured with instructions stored on a computer-readable storage device memory.

[0150] FIG. 9 illustrates a block diagram of an example of a machine 900 or system upon which any one or more of the techniques (e.g., methodologies) discussed herein may be performed. In other embodiments, the machine 900 may operate as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the machine 900 may operate in the capacity of a server machine, a client machine, or both in server-client network environments. In an example, the machine 900 may act as a peer machine in peer-to-peer (P2P) (or other distributed) network environments. The machine 900 may be a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a mobile telephone, a wearable computer device, a web appliance, a network router, a switch or bridge, or any machine capable of executing instructions (sequential or otherwise) that specify actions to be taken by that machine, such as a base station. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein, such as cloud computing, software as a service (SaaS), or other computer cluster configurations.

[0151] Examples, as described herein, may include or may operate on logic or a number of components, modules, or mechanisms. Modules are tangible entities (e.g., hardware) capable of performing specified operations when operating. A module includes hardware. In an example, the hardware may be specifically configured to carry out a specific operation (e.g., hardwired). In another example, the hardware may include configurable execution units (e.g., transistors, circuits, etc.) and a computer readable medium containing instructions where the instructions configure the execution units to carry out a specific operation when in operation. The configuring may occur under the direction of the executions units or a loading mechanism. Accordingly, the execution units are communicatively coupled to the computer-readable medium when the device is operating. In this example, the execution units may be a member of more than one module. For example, under operation, the execution units may be configured by a first set of instructions to implement a first module at one point in time and reconfigured by a second set of instructions to implement a second module at a second point in time.

[0152] The machine (e.g., computer system) 900 may include a hardware processor 902 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), a hardware processor core, or any combination thereof), a main memory 904 and a static memory 906, some or all of which may communicate with each other via an interlink (e.g., bus) 908. The machine 900 may further include a power management device 932, a graphics display device 910, an

alphanumeric input device 912 (e.g., a keyboard), and a user interface (UI) navigation device 914 (e.g., a mouse). In an example, the graphics display device 910, alphanumeric input device 912, and UI navigation device 914 may be a touch screen display. The machine 900 may additionally include a storage device (i.e., drive unit) 916, a signal generation device 918 (e.g., a speaker), an enhanced attack detection device 919, a network interface device/transceiver 920 coupled to antenna(s) 930, and one or more sensors 928, such as a global positioning system (GPS) sensor, a compass, an accelerometer, or other sensor. The machine 900 may include an output controller 934, such as a serial (e.g., universal serial bus (USB), parallel, or other wired or wireless (e.g., infrared (IR), near field communication (NFC), etc.) connection to communicate with or control one or more peripheral devices (e.g., a printer, a card reader, etc.)).

[0153] The storage device 916 may include a machine readable medium 922 on which is stored one or more sets of data structures or instructions 924 (e.g., software) embodying or utilized by any one or more of the techniques or functions described herein. The instructions 924 may also reside, completely or at least partially, within the main memory 904, within the static memory 906, or within the hardware processor 902 during execution thereof by the machine 900. In an example, one or any combination of the hardware processor 902, the main memory 904, the static memory 906, or the storage device 916 may constitute machine-readable media.

[0154] The enhanced attack detection device 919 may carry out or perform any of the operations and processes (e.g., process 700 of FIG. 7A, process 750 of FIG. 7B described and shown above.

[0155] In one or more embodiments, enhanced attack detection device 919 may cause to send a frame to one or more initiating devices; identify a first sounding signal of a sounding signal sequence received from a first initiating device; identify a second sounding signal of the sounding signal sequence received from the first initiating device, wherein the first sounding signal is different than the second sounding signal; cause to send one or more null data packet frames to the first initiating device; and cause to send a location measurement report to the first initiating device, wherein the location measurement report is based at least in part on the first sounding signal and the second sounding signal.

[0156] In one or more embodiments, enhanced attack detection device 919 may identify an announcement frame received from a responding device; cause to send a first sounding signal of a sounding signal sequence and a second sounding signal of the sounding signal sequence

to the responding device; identify a third sounding signal received from the responding device; identify a fourth sounding signal received from the responding device, wherein the fourth sounding signal may be different than the third sounding signal; and determine a difference between a first channel estimation associated with the third sounding signal and a second channel estimation associated with the fourth sounding signal.

[0157] It is understood that the above are only a subset of what the enhanced attack detection device 919 may be configured to perform and that other functions included throughout this disclosure may also be performed by the enhanced attack detection device 919.

[0158] While the machine-readable medium 922 is illustrated as a single medium, the term "machine-readable medium" may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) configured to store the one or more instructions 924.

[0159] Various embodiments may be implemented fully or partially in software and/or firmware. This software and/or firmware may take the form of instructions contained in or on a non-transitory computer-readable storage medium. Those instructions may then be read and executed by one or more processors to enable performance of the operations described herein. The instructions may be in any suitable form, such as but not limited to source code, compiled code, interpreted code, executable code, static code, dynamic code, and the like. Such a computer-readable medium may include any tangible non-transitory medium for storing information in a form readable by one or more computers, such as but not limited to read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; a flash memory, etc.

[0160] The term “machine-readable medium” may include any medium that is capable of storing, encoding, or carrying instructions for execution by the machine 900 and that cause the machine 900 to perform any one or more of the techniques of the present disclosure, or that is capable of storing, encoding, or carrying data structures used by or associated with such instructions. Non-limiting machine-readable medium examples may include solid-state memories and optical and magnetic media. In an example, a massed machine-readable medium includes a machine-readable medium with a plurality of particles having resting mass. Specific examples of massed machine-readable media may include non-volatile memory, such as semiconductor memory devices (e.g., electrically programmable read-only memory (EPROM), or electrically erasable programmable read-only memory (EEPROM)) and flash memory

devices; magnetic disks, such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM and DVD- ROM disks.

[0161] The instructions 924 may further be transmitted or received over a communications network 926 using a transmission medium via the network interface device/transceiver 920 utilizing any one of a number of transfer protocols (e.g., frame relay, internet protocol (IP), transmission control protocol (TCP), user datagram protocol (UDP), hypertext transfer protocol (HTTP), etc.). Example communications networks may include a local area network (LAN), a wide area network (WAN), a packet data network (e.g., the Internet), mobile telephone networks (e.g., cellular networks), plain old telephone (POTS) networks, wireless data networks (e.g., Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of standards known as Wi-Fi®, IEEE 802.16 family of standards known as WiMax®), IEEE 802.15.4 family of standards, and peer-to-peer (P2P) networks, among others. In an example, the network interface device/transceiver 1120 may include one or more physical jacks (e.g., Ethernet, coaxial, or phone jacks) or one or more antennas to connect to the communications network 926. In an example, the network interface device/transceiver 920 may include a plurality of antennas to wirelessly communicate using at least one of single-input multiple-output (SIMO), multiple-input multiple-output (MIMO), or multiple-input single-output (MISO) techniques. The term "transmission medium" shall be taken to include any intangible medium that is capable of storing, encoding, or carrying instructions for execution by the machine 900 and includes digital or analog communications signals or other intangible media to facilitate communication of such software. The operations and processes described and shown above may be carried out or performed in any suitable order as desired in various implementations. Additionally, in certain implementations, at least a portion of the operations may be carried out in parallel. Furthermore, in certain implementations, less than or more than the operations described may be performed.

[0162] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments. The terms "computing device," "user device," "communication station," "station," "handheld device," "mobile device," "wireless device" and "user equipment" (UE) as used herein refers to a wireless communication device such as a cellular telephone, a smartphone, a tablet, a netbook, a wireless terminal, a laptop computer, a femtocell, a high data rate (HDR) subscriber station, an

access point, a printer, a point of sale device, an access terminal, or other personal communication system (PCS) device. The device may be either mobile or stationary.

[0163] As used within this document, the term "communicate" is intended to include transmitting, or receiving, or both transmitting and receiving. This may be particularly useful in claims when describing the organization of data that is being transmitted by one device and received by another, but only the functionality of one of those devices is required to infringe the claim. Similarly, the bidirectional exchange of data between two devices (both devices transmit and receive during the exchange) may be described as "communicating," when only the functionality of one of those devices is being claimed. The term "communicating" as used herein with respect to a wireless communication signal includes transmitting the wireless communication signal and/or receiving the wireless communication signal. For example, a wireless communication unit, which is capable of communicating a wireless communication signal, may include a wireless transmitter to transmit the wireless communication signal to at least one other wireless communication unit, and/or a wireless communication receiver to receive the wireless communication signal from at least one other wireless communication unit.

[0164] As used herein, unless otherwise specified, the use of the ordinal adjectives "first," "second," "third," etc., to describe a common object, merely indicates 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.

[0165] The term "access point" (AP) as used herein may be a fixed station. An access point may also be referred to as an access node, a base station, an evolved node B (eNodeB), or some other similar terminology known in the art. An access terminal may also be called a mobile station, user equipment (UE), a wireless communication device, or some other similar terminology known in the art. Embodiments disclosed herein generally pertain to wireless networks. Some embodiments may relate to wireless networks that operate in accordance with one of the IEEE 802.11 standards.

[0166] Some embodiments may be used in conjunction with various devices and systems, for example, a personal computer (PC), a desktop computer, a mobile computer, a laptop computer, a notebook computer, a tablet computer, a server computer, a handheld computer, a handheld device, a personal digital assistant (PDA) device, a handheld PDA device, an on-board device, an off-board device, a hybrid device, a vehicular device, a non-vehicular device, a mobile or portable device, a consumer device, a non-mobile or non-portable device, a wireless communication station, a wireless communication device, a wireless access point (AP), a wired

or wireless router, a wired or wireless modem, a video device, an audio device, an audio-video (A/V) device, a wired or wireless network, a wireless area network, a wireless video area network (WVAN), a local area network (LAN), a wireless LAN (WLAN), a personal area network (PAN), a wireless PAN (WPAN), and the like.

[0167] 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 system (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 single input single output (SISO) 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.

[0168] Some embodiments may be used in conjunction with one or more types of wireless communication signals and/or systems following one or more wireless communication protocols, for example, radio frequency (RF), infrared (IR), frequency-division multiplexing (FDM), orthogonal FDM (OFDM), time-division multiplexing (TDM), time-division multiple access (TDMA), 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 communications (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.

[0169] Example 1 may include a device, the device comprising memory and processing circuitry configured to: cause to send a frame to one or more initiating devices; identify a first sounding signal of a sounding signal sequence received from a first initiating device; identify a second sounding signal of the sounding signal sequence received from the first initiating device, wherein the first sounding signal is different than the second sounding signal; cause to

send one or more null data packet frames to the first initiating device; and cause to send a location measurement report to the first initiating device, wherein the location measurement report is based at least in part on the first sounding signal and the second sounding signal.

[0170] Example 2 may include the device of example 1 and/or some other example herein, wherein the first sounding signal comprises a first sequence of channel sounding symbols and the second sounding signal comprises a second sequence of channel sounding signals, and wherein the first sequence is different than the second sequence.

[0171] Example 3 may include the device of example 1 and/or some other example herein, wherein the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

[0172] Example42 may include the device of example 3 and/or some other example herein, wherein the second sounding signal is shifted linearly or cyclically in the time domain from the first sounding signal.

[0173] Example 5 may include the device of example 3 and/or some other example herein, wherein the second sounding signal is shifted linearly in the frequency domain from first sounding signal.

[0174] Example 6 may include the device of example 1 and/or some other example herein, wherein the frame is a trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement frame.

[0175] Example 7 may include the device of example 1 and/or some other example herein, wherein the attack detection mode indicates a number of sounding signals to be sent during the sounding signal sequence.

[0176] Example 8 may include the device of example 1 and/or some other example herein, further comprising a transceiver configured to transmit and receive wireless signals.

[0177] Example 9 may include the device of example 8 and/or some other example herein, further comprising one or more antennas coupled to the transceiver.

[0178] Example 10 may include a non-transitory computer-readable medium storing computer-executable instructions which when executed by one or more processors result in performing operations comprising: identifying, by an initiating device, an announcement frame received from a responding device; causing to send a first sounding signal of a sounding signal sequence and a second sounding signal of the sounding signal sequence to the responding device; identifying, by the initiating device, a third sounding signal received from the responding device; identifying, by the initiating device, a fourth sounding signal received from

the responding device, wherein the fourth sounding signal is different than the third sounding signal; and determining a difference between a first channel estimation associated with the third sounding signal and a second channel estimation associated with the fourth sounding signal.

[0179] Example 11 may include the non-transitory computer-readable medium of example 10 and/or some other example herein, the operations further comprising: determining that the difference is consistent with the attack detection mode; and measuring a position of the access point device based at least in part the first sounding signal and the second sounding signal. Identifying the third sounding signal and identifying the fourth sounding signal comprise identifying a null data packet frame, wherein the null data packet frame comprises a first training field associated with the third sounding signal and a second training field associated with the fourth sounding signal. The operations may further include determining that the difference is within a threshold value; measuring a time of arrival based at least in part the first sounding signal and the second sounding signal; and determining a range between the initiating device and the responding device based at least in part on the time of arrival.

[0180] Example 12 may include the non-transitory computer-readable medium of example 10 and/or some other example herein, the operations further comprising: determining that the difference is not consistent with the attack detection mode; and discarding a position measurement associated with the first sounding signal and the second sounding signal.

[0181] Example 13 may include the non-transitory computer-readable medium of example 10 and/or some other example herein, wherein determining the difference comprises determining that the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

[0182] Example 14 may include the non-transitory computer-readable medium of example 13 and/or some other example herein, wherein determining the difference comprises determining that the second sounding signal is shifted linearly or cyclically in the time domain from the first sounding signal.

[0183] Example 15 may include the non-transitory computer-readable medium of example 13 and/or some other example herein, wherein determining the difference further comprises determining that the second sounding signal is shifted linearly in the frequency domain from first sounding signal.

[0184] Example 16 may include the non-transitory computer-readable medium of example 10 and/or some other example herein, wherein the frame is a trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement frame.

[0185] Example 17 may include the non-transitory computer-readable medium of example 10 and/or some other example herein, wherein the attack detection mode indicates a number of sounding signals to be sent during the sounding signal sequence.

[0186] Example 18 may include a method, comprising: causing to send, by one or more processors of a responding device, a frame to one or more initiating devices; identifying a first sounding signal of a sounding signal sequence received from a first initiating device; identifying a second sounding signal of the sounding signal sequence received from the first initiating device, wherein the first sounding signal is different than the second sounding signal; causing to send one or more null data packet frames to the first initiating device; and causing to send a location measurement report to the first initiating device, wherein the location measurement report is based at least in part on the first sounding signal and the second sounding signal.

[0187] Example 19 may include the method of example 18 and/or some other example herein, wherein the first sounding signal comprises a first sequence of channel sounding symbols and the second sounding signal comprises a second sequence of channel sounding signals, and wherein the first sequence is different than the second sequence.

[0188] Example 20 may include the method of example 18 and/or some other example herein, wherein the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

[0189] Example 21 may include the method of example 18 and/or some other example herein, wherein the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

[0190] Example 22 may include the method of example 21 and/or some other example herein, wherein the second sounding signal is shifted linearly or cyclically in the time domain from the first sounding signal.

[0191] Example 23 may include the method of example 21 and/or some other example herein, wherein the second sounding signal is shifted linearly in the frequency domain from first sounding signal.

[0192] Example 24 may include the method of example 18 and/or some other example herein, wherein the frame is a trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement frame.

[0193] Example 25 may include the method of example 18 and/or some other example herein, wherein the attack detection mode indicates a number of sounding signals to be sent

during the sounding signal sequence.

[0194] Example 26 may comprise an apparatus comprising: means for identifying, by an initiating device, an announcement frame received from a responding device; means for causing to send a first sounding signal of a sounding signal sequence and a second sounding signal of the sounding signal sequence to the responding device; means for identifying, by the initiating device, a third sounding signal received from the responding device; means for identifying, by the initiating device, a fourth sounding signal received from the responding device, wherein the fourth sounding signal is different than the third sounding signal; and means for determining a difference between a first channel estimation associated with the third sounding signal and a second channel estimation associated with the fourth sounding signal.

[0195] Example 27 may include the apparatus of example 26 and/or some other example herein, further comprising means for determining that the difference is consistent with the attack detection mode; and measuring a position of the access point device based at least in part the first sounding signal and the second sounding signal.

[0196] Example 28 may include the apparatus of example 26 and/or some other example herein, further comprising means for determining that the difference is not consistent with the attack detection mode; and discarding a position measurement associated with the first sounding signal and the second sounding signal.

[0197] Example 29 may include the apparatus of example 26 and/or some other example herein, wherein means for determining the difference comprises means for determining that the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

[0198] Example 30 may include the apparatus of example 29 and/or some other example herein, wherein means for determining the difference comprises means for determining that the second sounding signal is shifted linearly or cyclically in the time domain from the first sounding signal.

[0199] Example 31 may include the apparatus of example 29 and/or some other example herein, wherein means for determining the difference further comprises means for determining that the second sounding signal is shifted linearly in the frequency domain from first sounding signal.

[0200] Example 32 may include the apparatus of example 26 and/or some other example herein, wherein the frame is a trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement frame.

[0201] Example 33 may include the apparatus of example 26 and/or some other example herein, wherein the attack detection mode indicates a number of sounding signals to be sent during the sounding signal sequence.

[0202] Embodiments according to the disclosure are in particular disclosed in the attached claims directed to a method, a storage medium, a device and a computer program product, wherein any feature mentioned in one claim category, e.g., method, can be claimed in another claim category, e.g., system, as well. The dependencies or references back in the attached claims are chosen for formal reasons only. However, any subject matter resulting from a deliberate reference back to any previous claims (in particular multiple dependencies) can be claimed as well, so that any combination of claims and the features thereof are disclosed and can be claimed regardless of the dependencies chosen in the attached claims. The subject-matter which can be claimed comprises not only the combinations of features as set out in the attached claims but also any other combination of features in the claims, wherein each feature mentioned in the claims can be combined with any other feature or combination of other features in the claims. Furthermore, any of the embodiments and features described or depicted herein can be claimed in a separate claim and/or in any combination with any embodiment or feature described or depicted herein or with any of the features of the attached claims.

[0203] The foregoing description of one or more implementations provides illustration and description, but is not intended to be exhaustive or to limit the scope of embodiments to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of various embodiments.

[0204] Certain aspects of the disclosure are described above with reference to block and flow diagrams of systems, methods, apparatuses, and/or computer program products according to various implementations. It will be understood that one or more blocks of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and the flow diagrams, respectively, may be implemented by computer-executable program instructions. Likewise, some blocks of the block diagrams and flow diagrams may not necessarily need to be performed in the order presented, or may not necessarily need to be performed at all, according to some implementations.

[0205] These computer-executable program instructions may be loaded onto a special-purpose computer or other particular machine, a processor, or other programmable data processing apparatus to produce a particular machine, such that the instructions that execute on the computer, processor, or other programmable data processing apparatus create means for

implementing one or more functions specified in the flow diagram block or blocks. These computer program instructions may also be stored in a computer-readable storage media or memory that may direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable storage media produce an article of manufacture including instruction means that implement one or more functions specified in the flow diagram block or blocks. As an example, certain implementations may provide for a computer program product, comprising a computer-readable storage medium having a computer-readable program code or program instructions implemented therein, said computer-readable program code adapted to be executed to implement one or more functions specified in the flow diagram block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational elements or steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions that execute on the computer or other programmable apparatus provide elements or steps for implementing the functions specified in the flow diagram block or blocks.

[0206] Accordingly, blocks of the block diagrams and flow diagrams support combinations of means for performing the specified functions, combinations of elements or steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that each block of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and flow diagrams, may be implemented by special-purpose, hardware-based computer systems that perform the specified functions, elements or steps, or combinations of special-purpose hardware and computer instructions.

[0207] Conditional language, such as, among others, "can," "could," "might," or "may," unless specifically stated otherwise, or otherwise understood within the context as used, is generally intended to convey that certain implementations could include, while other implementations do not include, certain features, elements, and/or operations. Thus, such conditional language is not generally intended to imply that features, elements, and/or operations are in any way required for one or more implementations or that one or more implementations necessarily include logic for deciding, with or without user input or prompting, whether these features, elements, and/or operations are included or are to be performed in any particular implementation.

[0208] Many modifications and other implementations of the disclosure set forth herein will be apparent having the benefit of the teachings presented in the foregoing descriptions and

the associated drawings. Therefore, it is to be understood that the disclosure is not to be limited to the specific implementations disclosed and that modifications and other implementations are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

CLAIMS

What is claimed is:

1. A responding device, the responding device comprising memory and processing circuitry configured to:

cause to send a frame to one or more initiating devices;

identify a first sounding signal of a sounding signal sequence received from a first initiating device;

identify a second sounding signal of the sounding signal sequence received from the first initiating device, wherein the first sounding signal is different than the second sounding signal;

cause to send one or more null data packet frames to the first initiating device; and

cause to send a location measurement report to the first initiating device, wherein the location measurement report is based at least in part on the first sounding signal and the second sounding signal.

2. The responding device of claim 1, wherein to identify the first sounding signal and to identify the second sounding signal comprise the memory and processing circuitry being further configured to identify a null data packet frame received from the first initiating device, wherein the null data packet frame comprises a first training field associated with the first sounding signal and a second training field associated with the second sounding signal.

3. The responding device of claim 1, wherein the first sounding signal comprises a first sequence of channel sounding signals and the second sounding signal comprises a second sequence of channel sounding signals, and wherein the first sequence is different than the second sequence.

4. The responding device of claim 1, wherein the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

5. The responding device of claim 4, wherein the second sounding signal is shifted linearly or cyclically in the time domain from the first sounding signal.

6. The responding device of claim 4, wherein the second sounding signal is shifted linearly in the frequency domain from first sounding signal.

7. The responding device of claim 1, wherein the frame is a trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement response frame, and wherein the frame comprises an indication of a number of sounding signals of the sounding signal sequence.

8. The responding device of claim 1, further comprising a transceiver configured to transmit and receive wireless signals.

9. The responding device of claim 8, further comprising one or more antennas coupled to the transceiver.

10. A non-transitory computer-readable medium storing computer-executable instructions which when executed by one or more processors result in performing operations comprising:

identifying, by an initiating device, an announcement frame received from a responding device;

causing to send a first sounding signal of a sounding signal sequence and a second sounding signal of the sounding signal sequence to the responding device;

identifying, by the initiating device, a third sounding signal received from the responding device;

identifying, by the initiating device, a fourth sounding signal received from the responding device, wherein the fourth sounding signal is different than the third sounding signal; and

determining a difference between a first channel estimation associated with the third sounding signal and a second channel estimation associated with the fourth sounding signal.

11. The non-transitory computer-readable medium of claim 10, wherein identifying the third sounding signal and identifying the fourth sounding signal comprise identifying a null data packet frame, wherein the null data packet frame comprises a first training field associated with the third sounding signal and a second training field associated with the fourth sounding signal.

12. The non-transitory computer-readable medium of claim 10, the operations further comprising:

determining that the difference is within a threshold value;

measuring a time of arrival based at least in part the first sounding signal and the second sounding signal; and

determining a range between the initiating device and the responding device based at least in part on the time of arrival.

13. The non-transitory computer-readable medium of claim 10, the operations further comprising:

determining that the difference is not within a threshold value; and

discarding a time of arrival measurement associated with at least one of the first sounding signal or the second sounding signal.

14. The non-transitory computer-readable medium of claim 10, wherein determining the difference comprises determining the difference between the first channel estimation and the second channel estimation in a frequency domain.

15. The non-transitory computer-readable medium of claim 14, wherein determining the difference comprises determining the difference between the first channel estimation and the second channel estimation in a time domain.

16. The non-transitory computer-readable medium of claim 14, wherein determining the difference comprises at least one of subtracting the one channel estimation from the other channel estimation and determining a ratio between a power of the subtraction difference and a power of the first or second channel estimation, determining a ratio between a first amplitude of the first channel estimation and a second amplitude of the second channel estimation, or determining a ratio between a first power of the first channel estimation and a second power of the second channel estimation.

17. The non-transitory computer-readable medium of claim 10, the operations further comprising identifying a frame received from the responding device, wherein the frame is a

trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement response frame, and wherein the frame comprises an indication of a number of sounding signals of the sounding signal sequence.

18. A method, comprising:

causing to send, by one or more processors of a responding device, a frame to one or more initiating devices;

identifying a first sounding signal of a sounding signal sequence received from a first initiating device;

identifying a second sounding signal of the sounding signal sequence received from the first initiating device, wherein the first sounding signal is different than the second sounding signal;

causing to send one or more null data packet frames to the first initiating device; and

causing to send a location measurement report to the first initiating device, wherein the location measurement report is based at least in part on the first sounding signal and the second sounding signal.

19. The method of claim 18, wherein identifying the first sounding signal and identifying the second sounding signal comprise identifying a null data packet frame received from the first initiating device, wherein the null data packet frame comprises a first training field associated with the first sounding signal and a second training field associated with the second sounding signal.

20. The method of claim 18, wherein the first sounding signal comprises a first sequence of channel sounding signals and the second sounding signal comprises a second sequence of channel sounding signals, and wherein the first sequence is different than the second sequence.

21. The method of claim 18, wherein the second sounding signal is shifted in at least one of a time domain or a frequency domain from the first sounding signal.

22. The method of claim 21, wherein the second sounding signal is shifted linearly or cyclically in the time domain from the first sounding signal.

23. The method of claim 21, wherein the second sounding signal is shifted linearly in the frequency domain from first sounding signal.

24. The method of claim 18, wherein the frame is a trigger frame, a null data packet announcement frame, a beacon, or a fine timing measurement response frame, and wherein the frame comprises an indication of a number of sounding signals of the sounding signal sequence.

25. The method of claim 18, further comprising determining a difference between a first channel estimation associated with the first sounding signal and a second channel estimation associated with the second sounding signal.

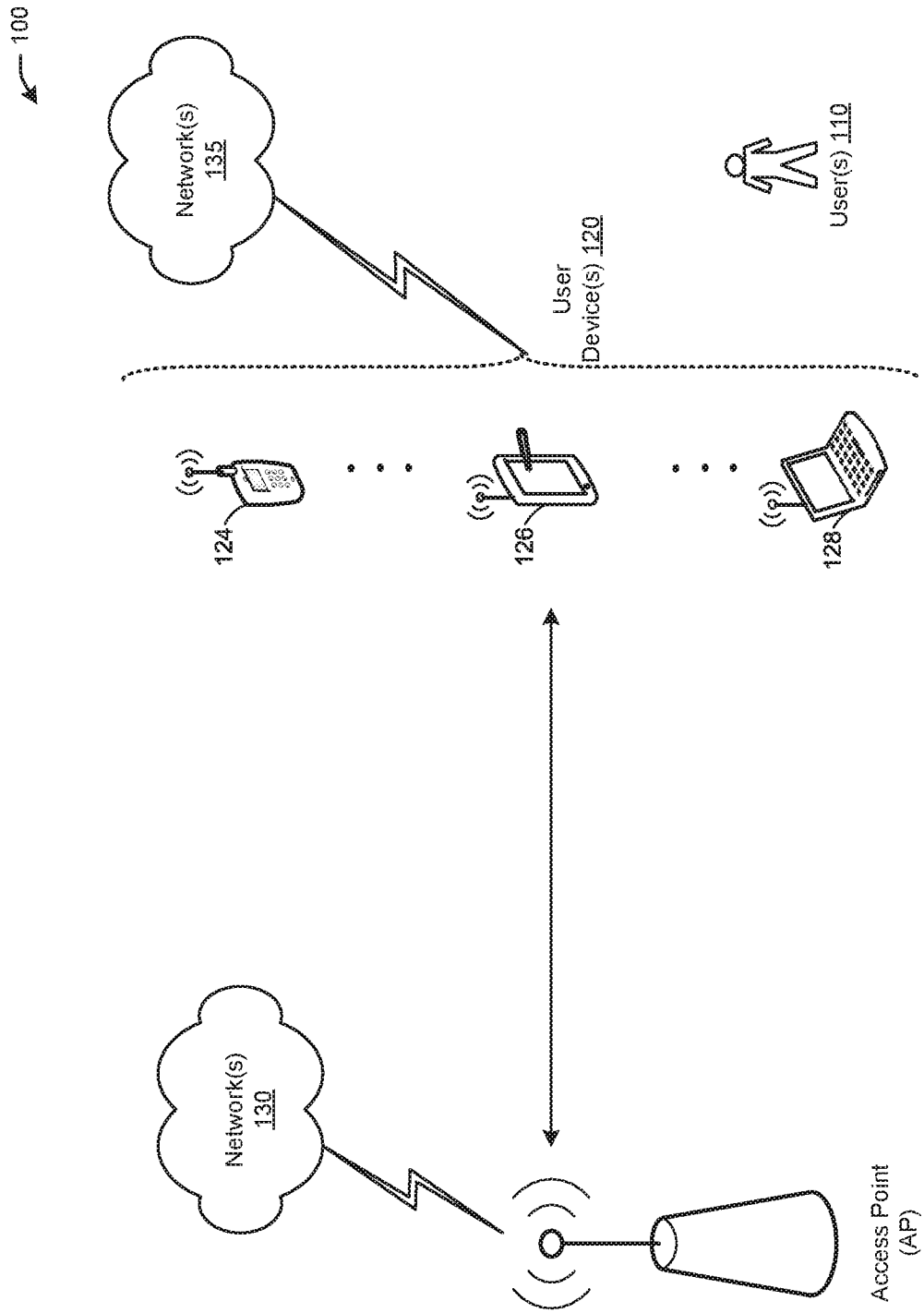
100
Network(s)
135
User(s) 110
User
Device(s) 120
124
126
128
Network(s)
130
Access Point
(AP)
102

FIG. 1

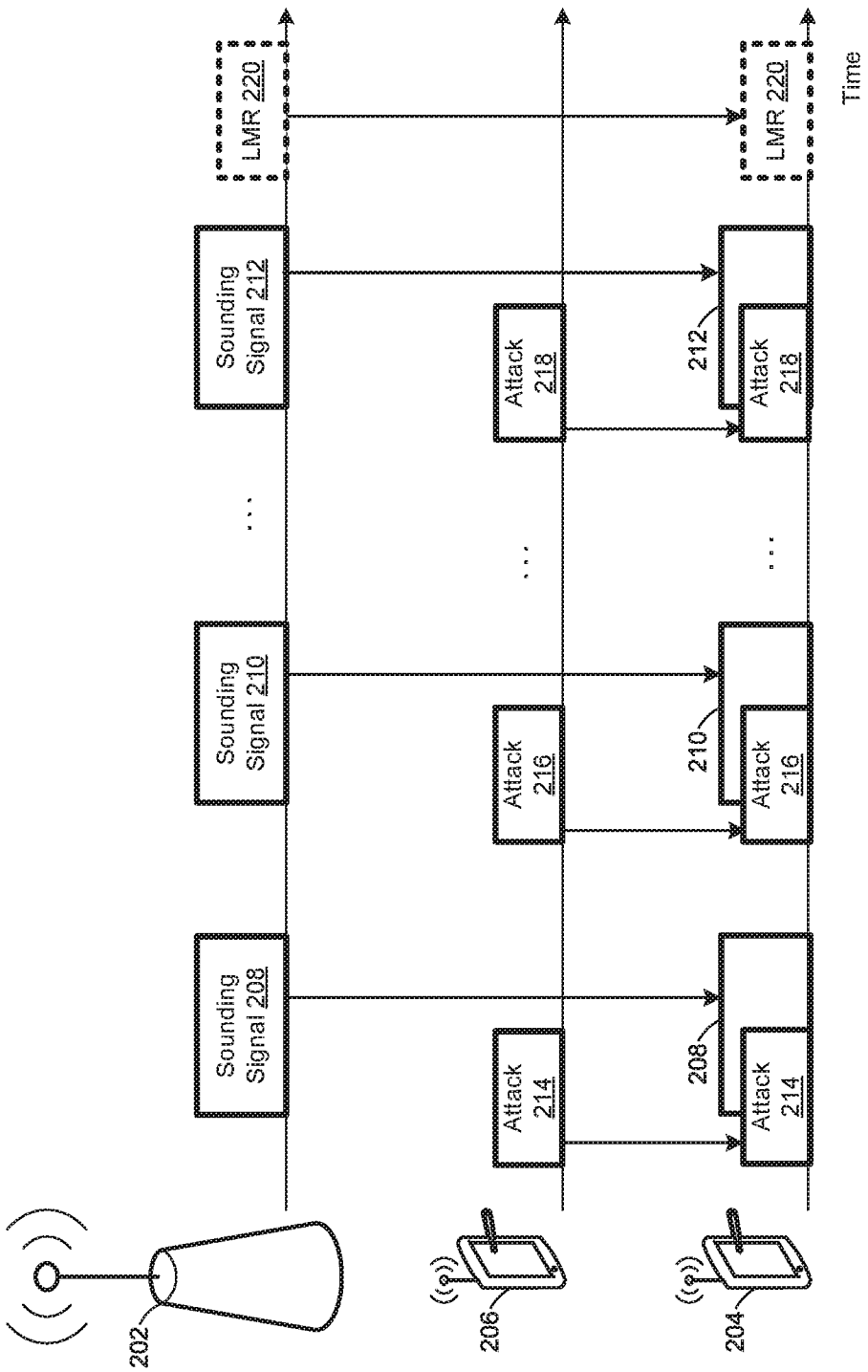
200
Sounding Signal 208
Sounding Signal 210
Sounding Signal 212
LMR 220
Attack 214
Attack 216
Attack 218
208
210
212
202
206
204
Time

FIG. 2

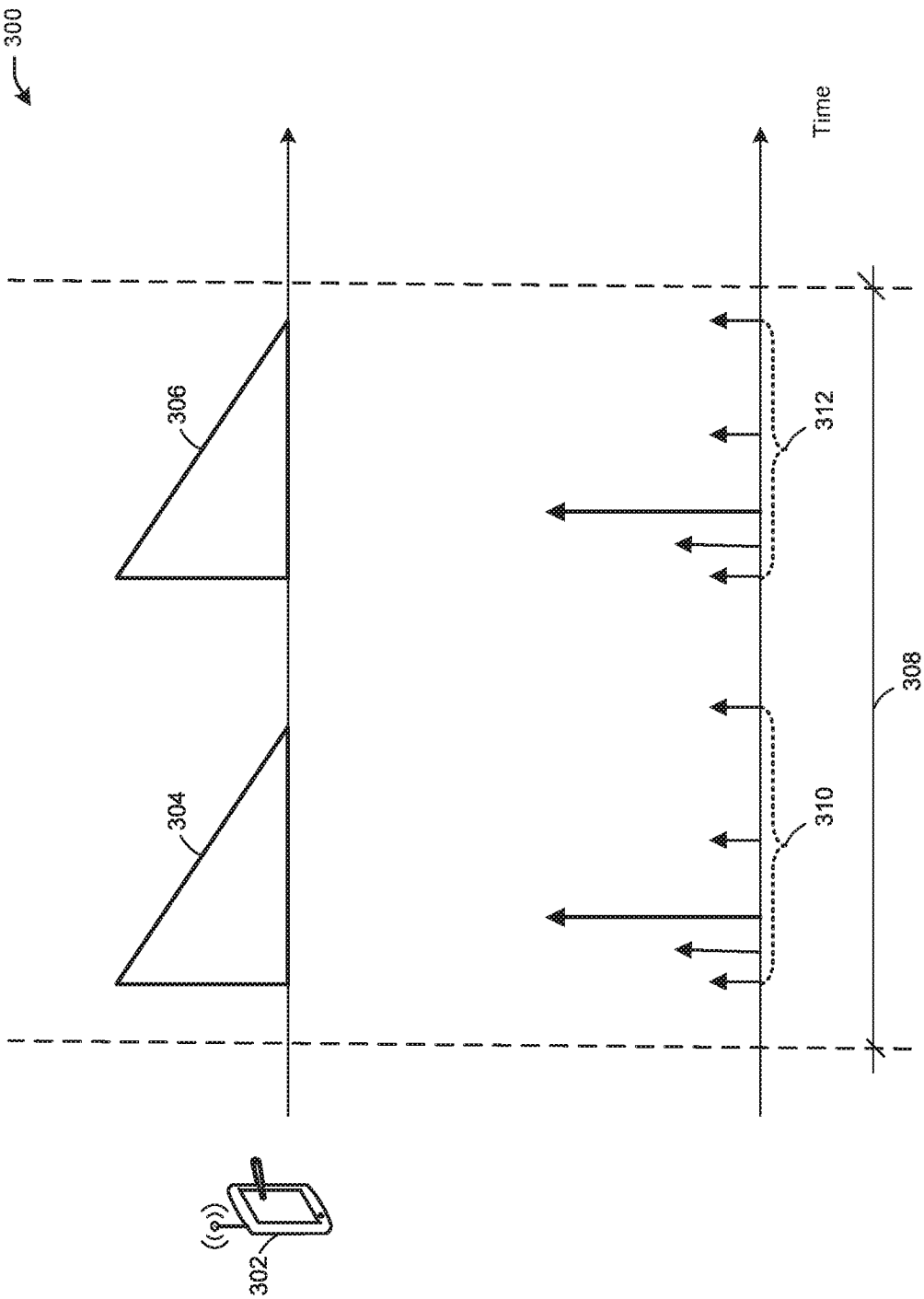

FIG. 3A

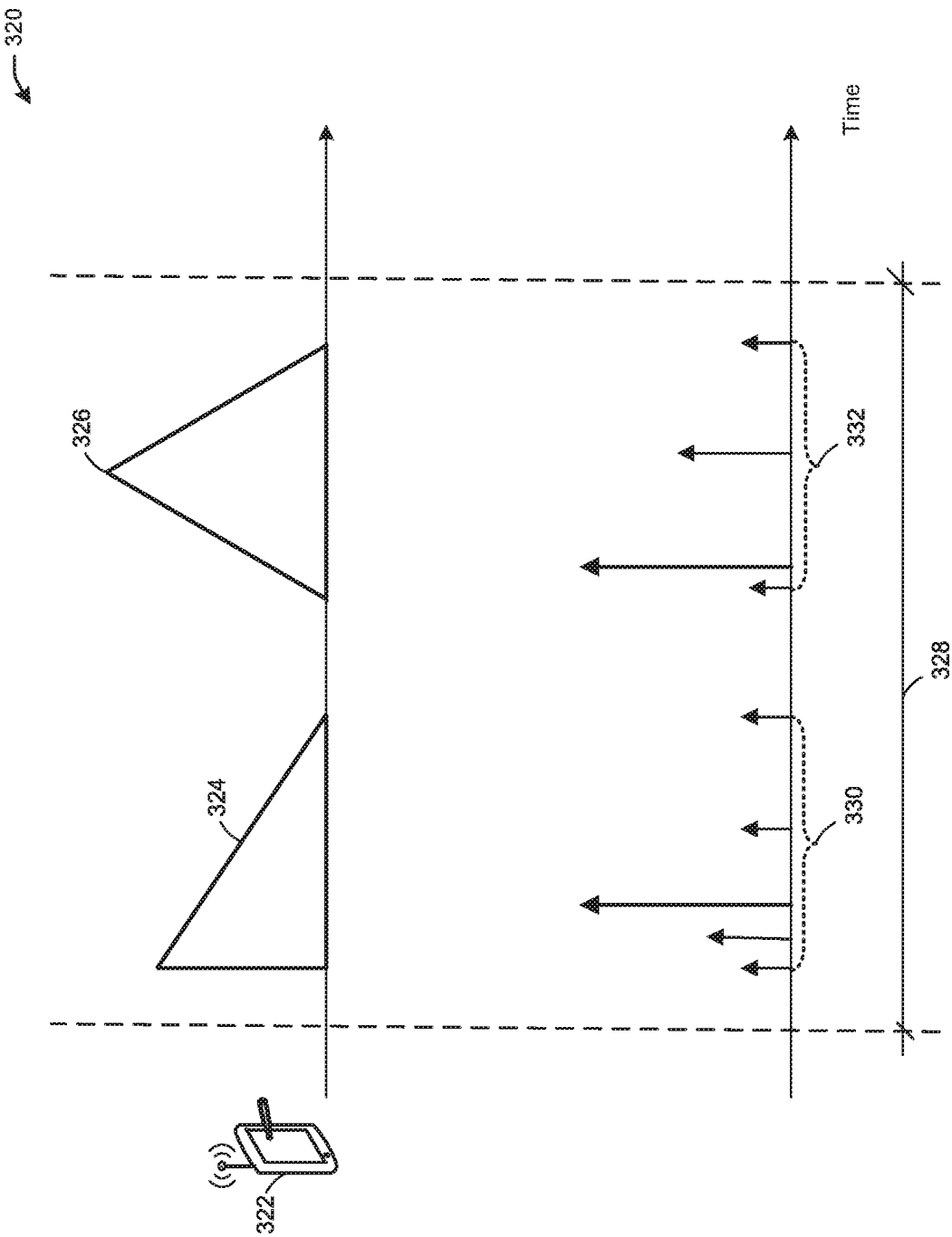

FIG. 3B

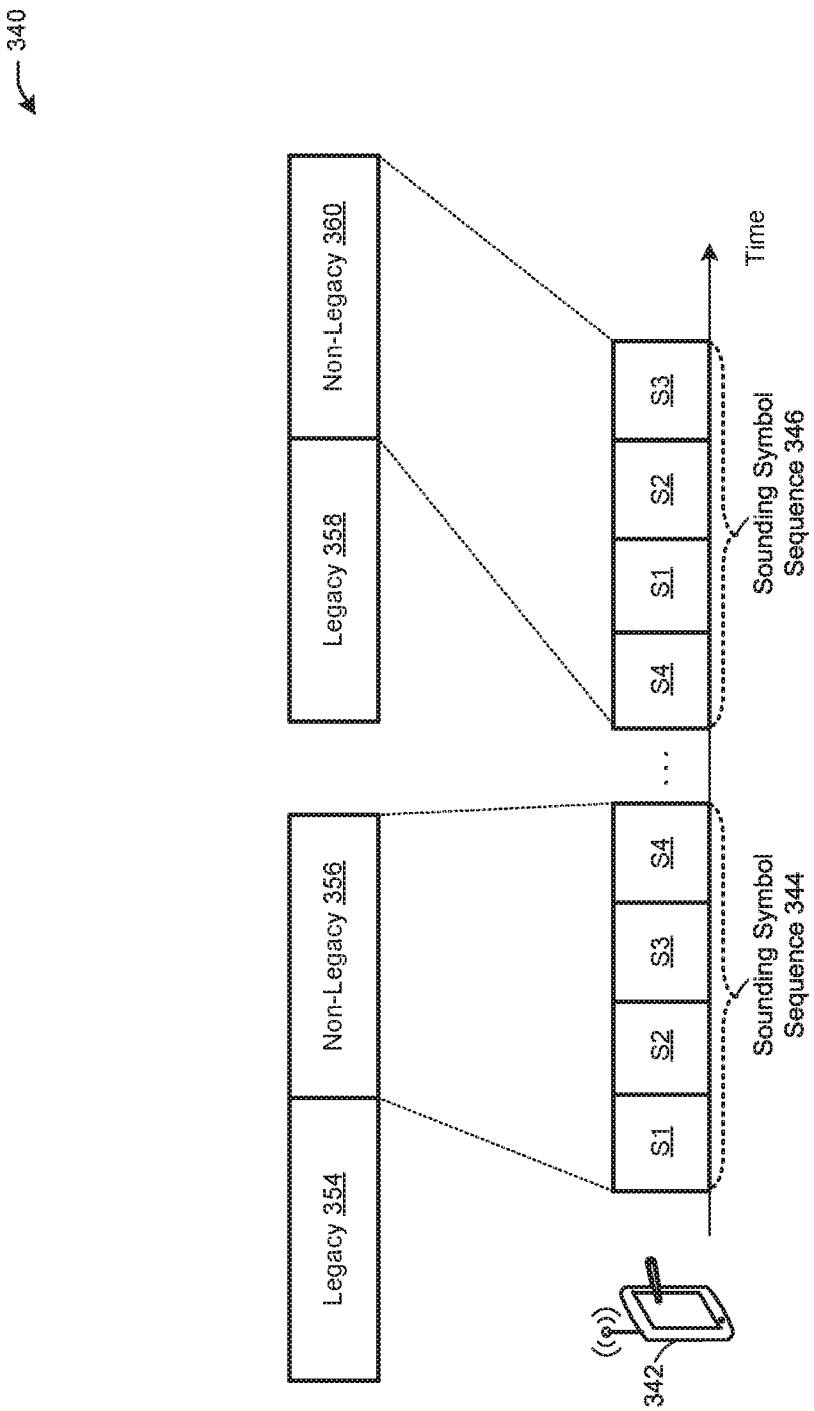
340
Legacy 354
Non-Legacy 356
Legacy 358
Non-Legacy 360
S1
S2
S3
S4
S1
S2
S3
S4
Sounding Symbol Sequence 344
Sounding Symbol Sequence 346
Time
342

FIG. 3C

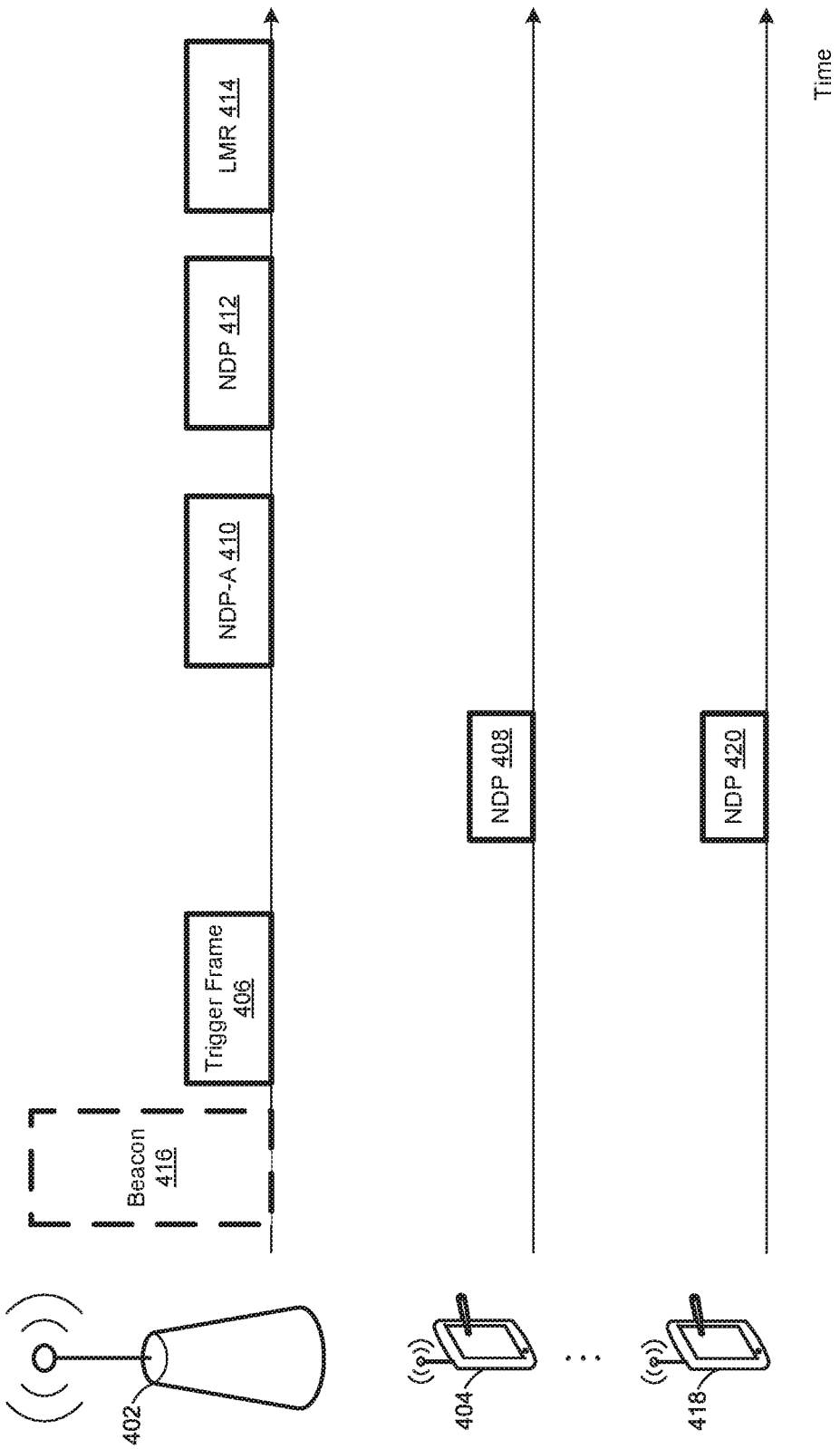
400
LMR 414
NDP 412
NDP-A 410
Trigger Frame 406
Beacon 416
NDP 408
NDP 420
Time
402
404
418

FIG. 4A

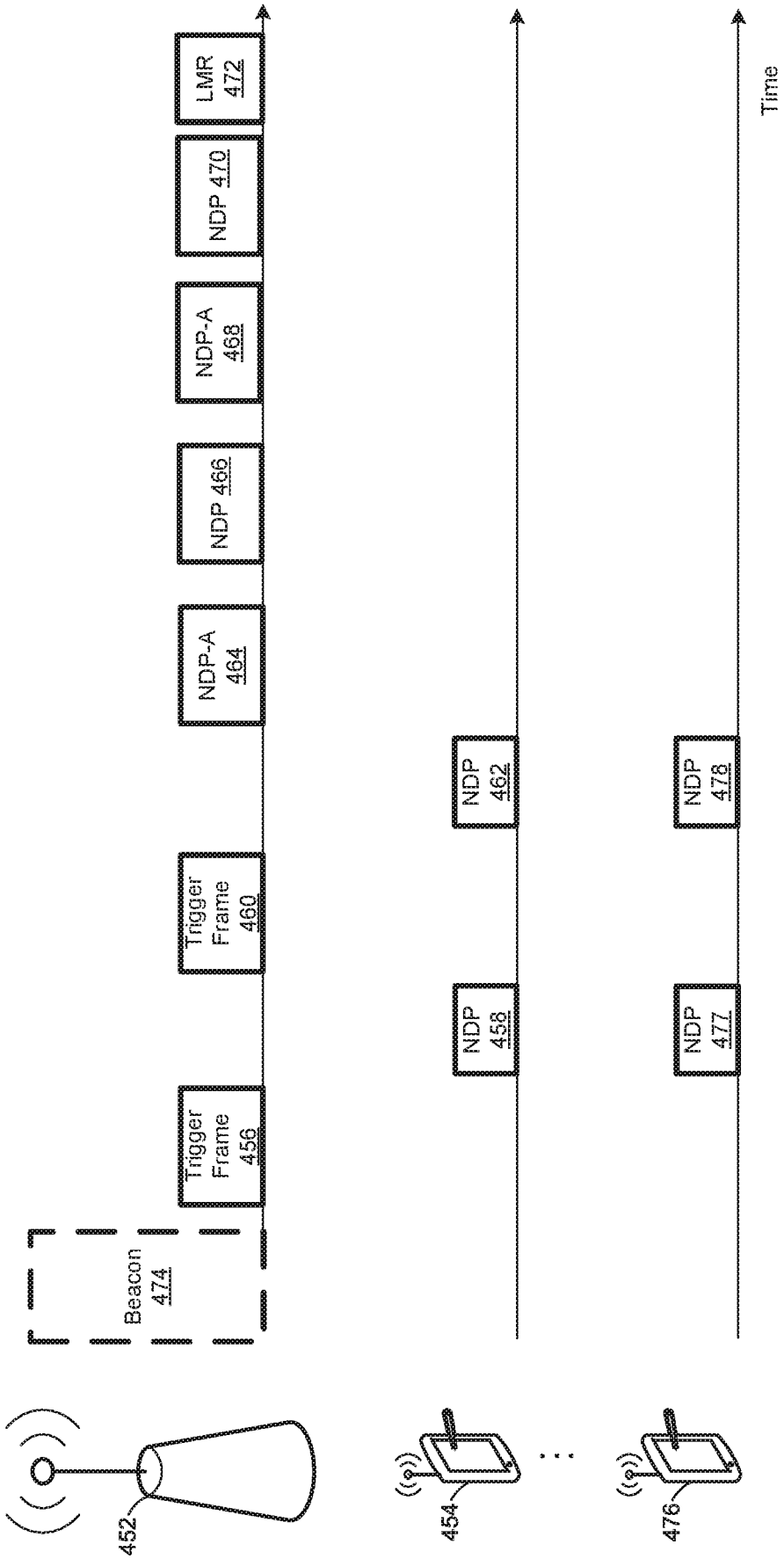
450
Beacon 474
Trigger Frame 456
Trigger Frame 460
NDP-A 464
NDP 466
NDP-A 468
NDP 470
LMR 472
NDP 458
NDP 462
NDP 477
NDP 478
Time
452
454
476

FIG. 4B

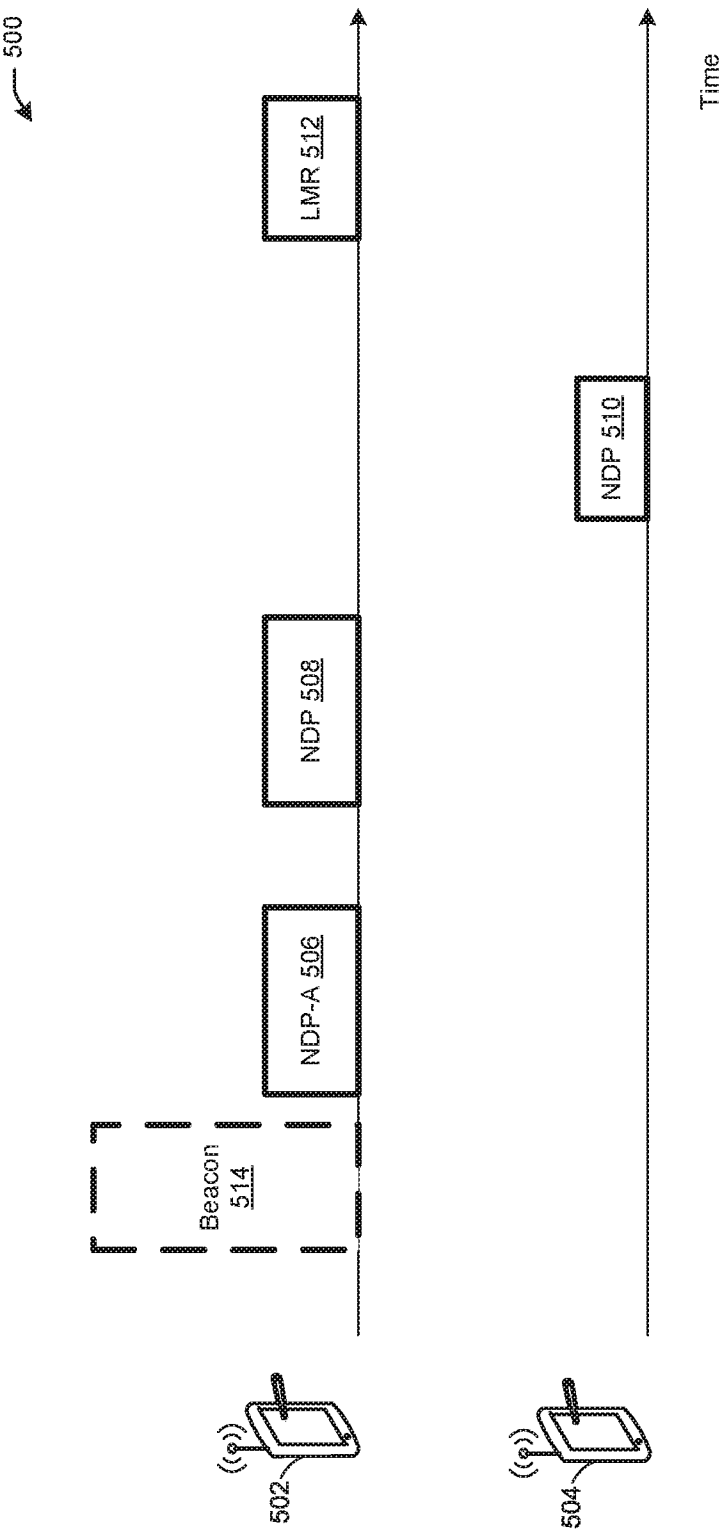

FIG. 5A

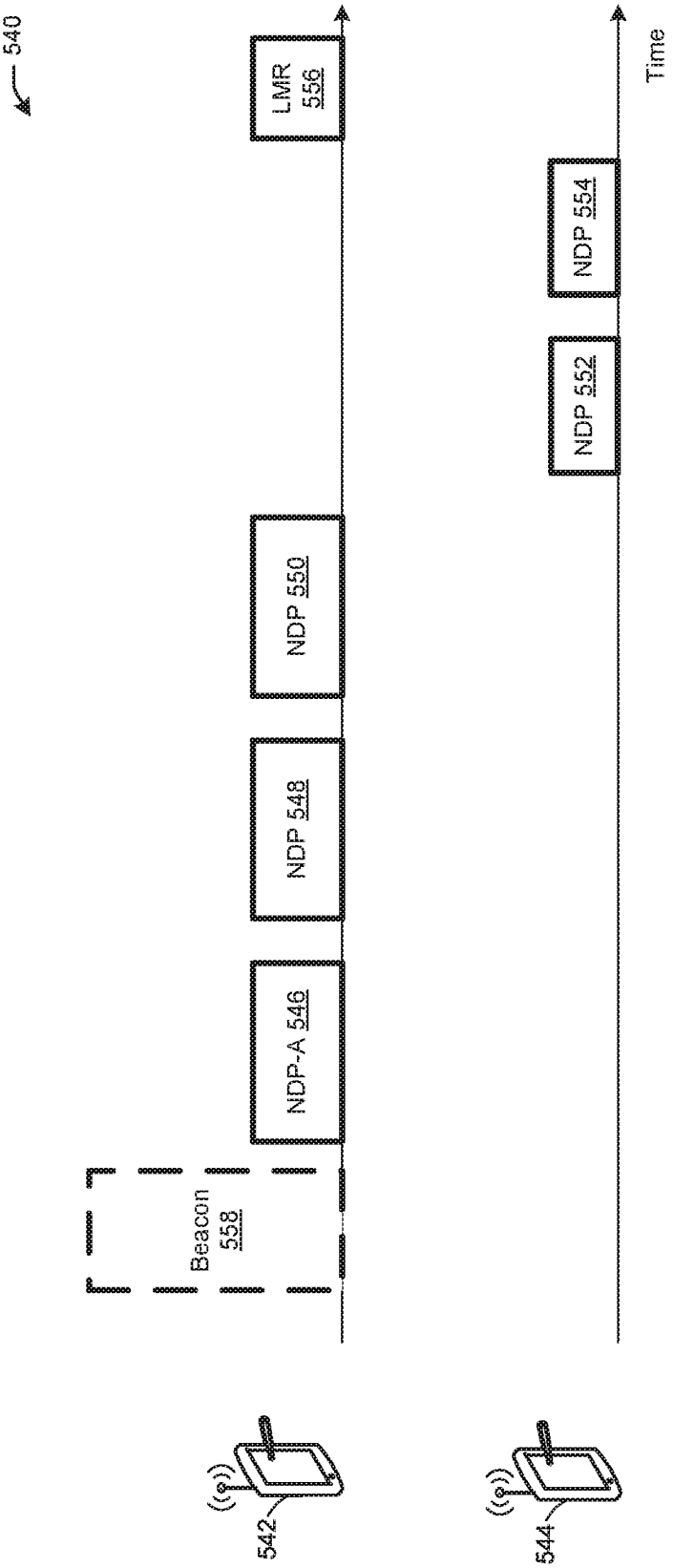
540
LMR 556
NDP 550
NDP 548
NDP-A 546
Beacon 558
NDP 552
NDP 554
Time
542
544

FIG. 5B

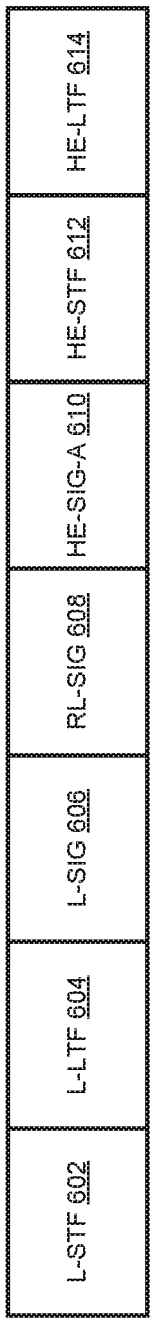

FIG. 6A

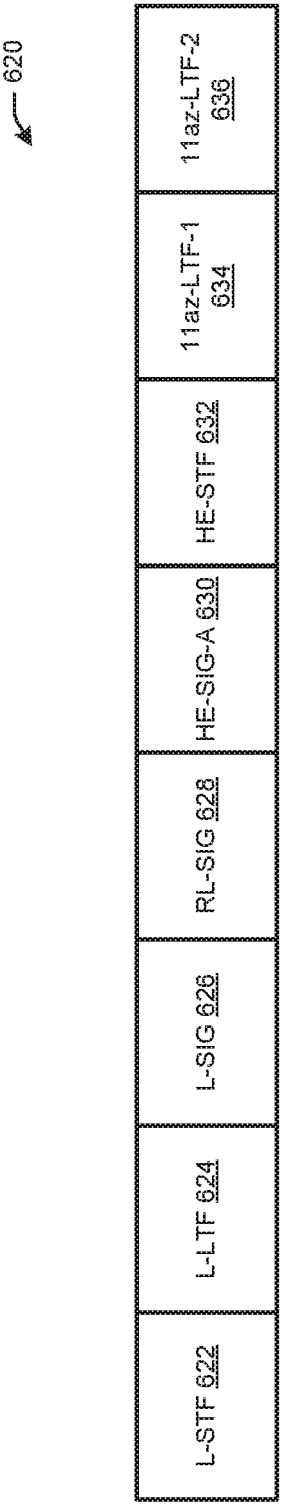

FIG. 6B

FIGs. 6A and 6B

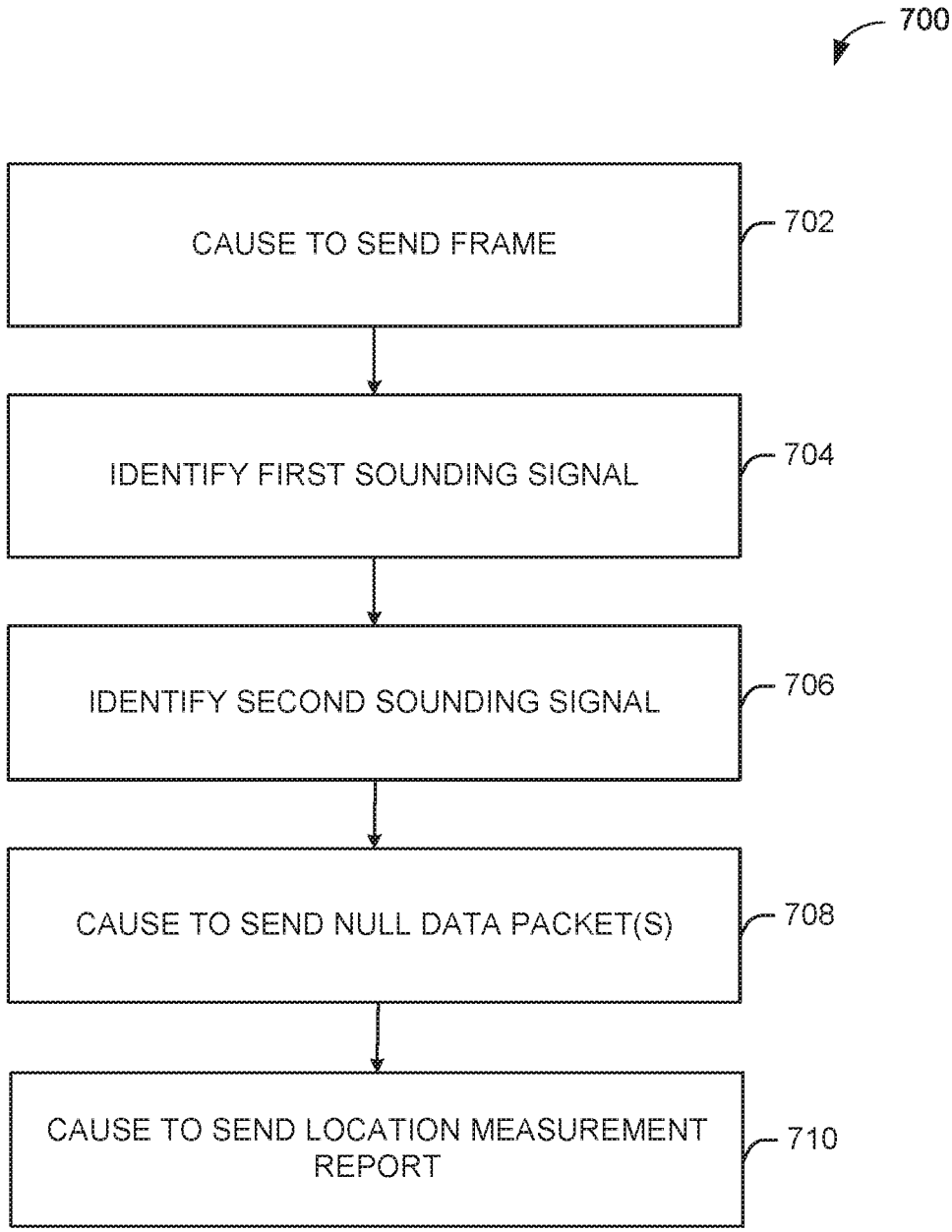
700
CAUSE TO SEND FRAME
702
IDENTIFY FIRST SOUNDING SIGNAL
704
IDENTIFY SECOND SOUNDING SIGNAL
706
CAUSE TO SEND NULL DATA PACKET(S)
708
CAUSE TO SEND LOCATION MEASUREMENT REPORT
710

FIG. 7A

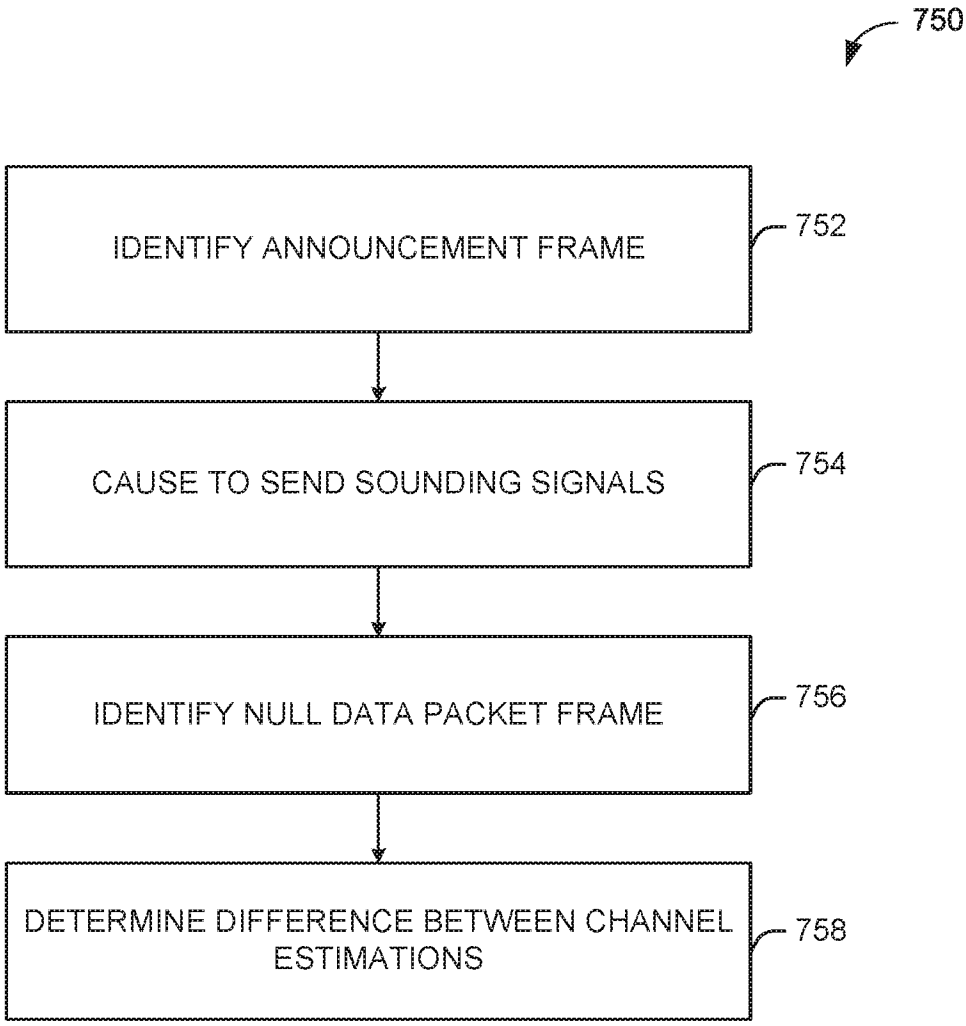
750
IDENTIFY ANNOUNCEMENT FRAME
752
CAUSE TO SEND SOUNDING SIGNALS
754
IDENTIFY NULL DATA PACKET FRAME
756
DETERMINE DIFFERENCE BETWEEN CHANNEL ESTIMATIONS
758

FIG. 7B

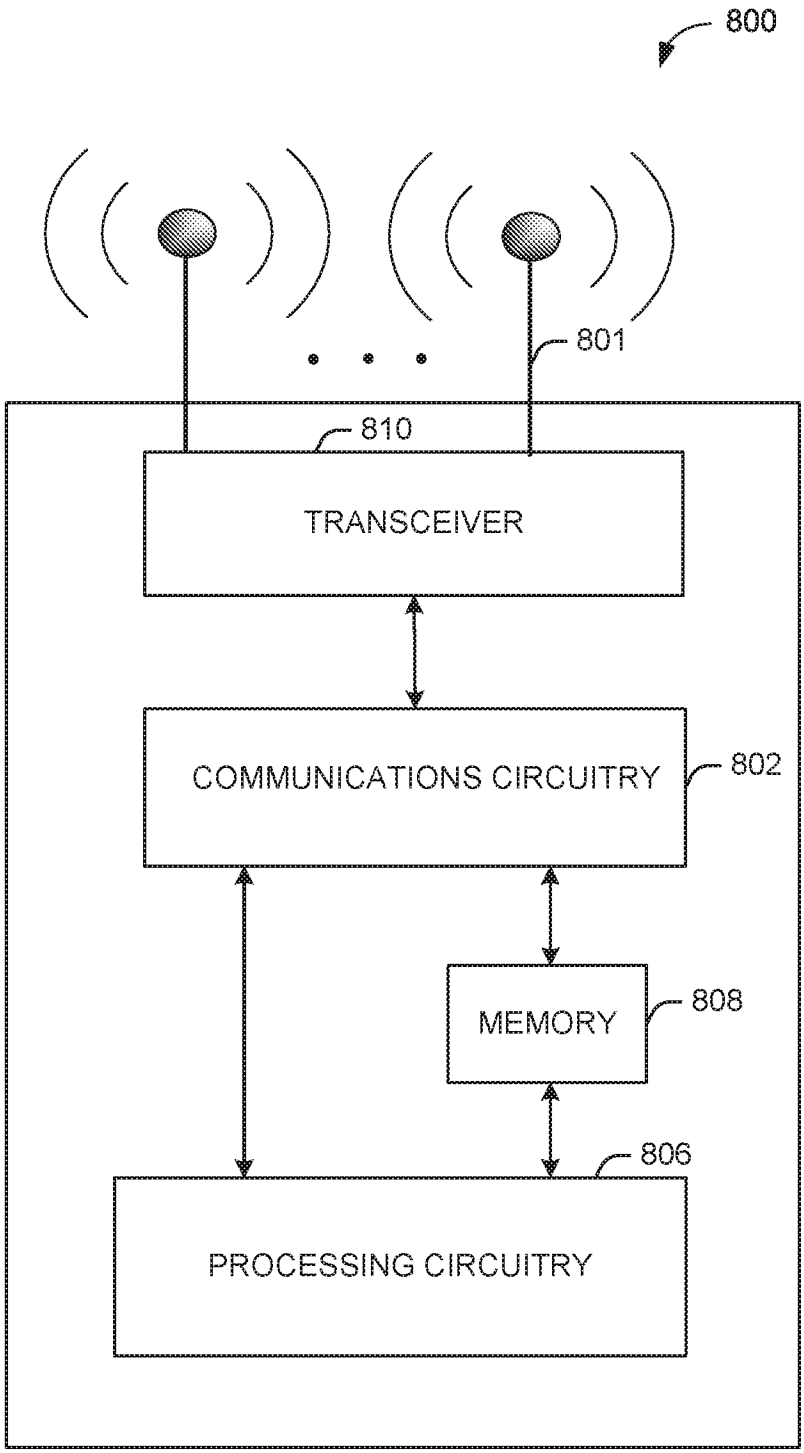
800
801
810
TRANSCEIVER
COMMUNICATIONS CIRCUITRY
802
MEMORY
808
806
PROCESSING CIRCUITRY

FIG. 8

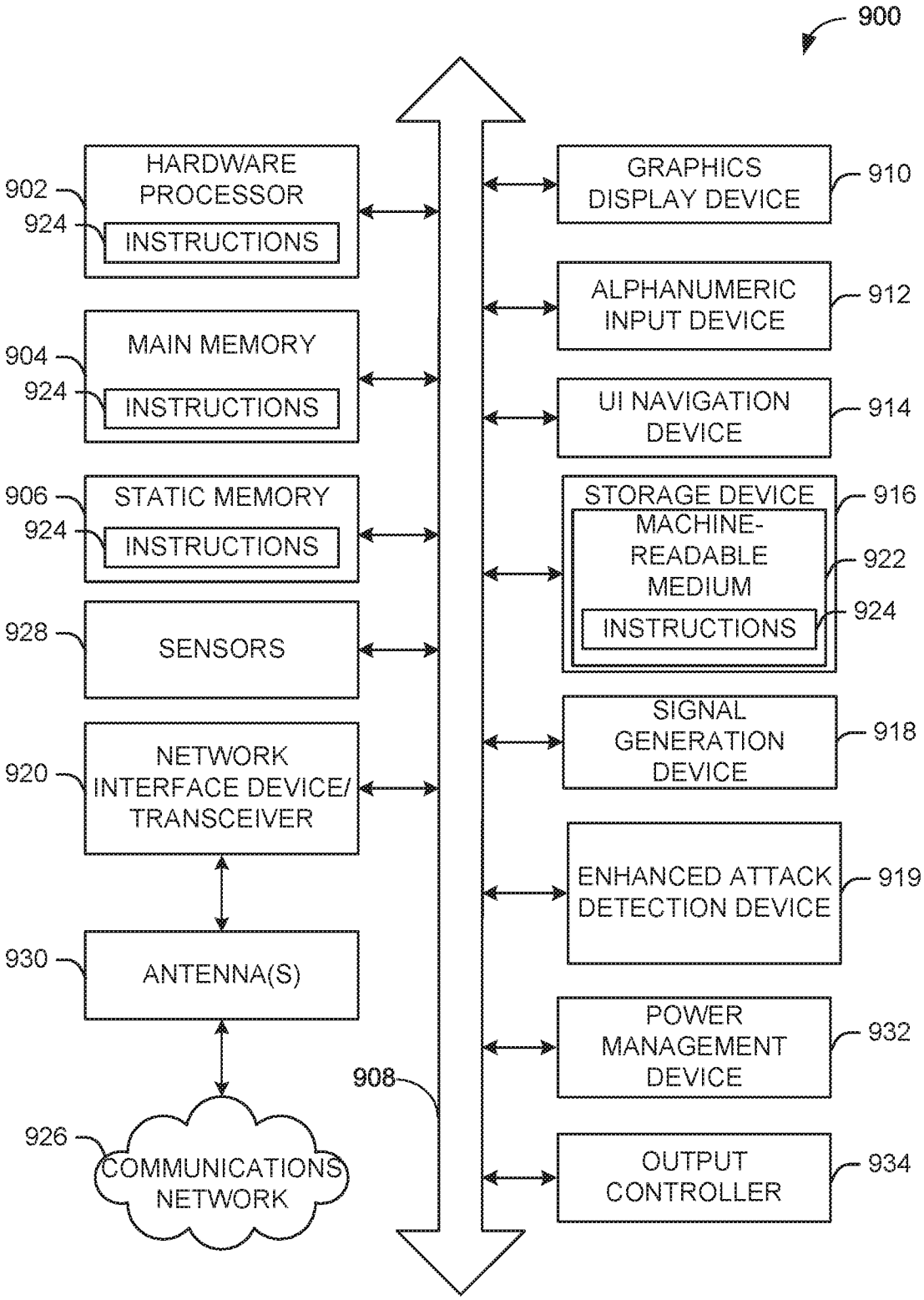
900
HARDWARE PROCESSOR
902
924
INSTRUCTIONS
MAIN MEMORY
904
924
INSTRUCTIONS
STATIC MEMORY
906
924
INSTRUCTIONS
928
SENSORS
NETWORK INTERFACE DEVICE/ TRANSCEIVER
920
930
ANTENNA(S)
926
COMMUNICATIONS NETWORK
908
GRAPHICS DISPLAY DEVICE
910
ALPHANUMERIC INPUT DEVICE
912
UI NAVIGATION DEVICE
914
STORAGE DEVICE
916
MACHINE-READABLE MEDIUM
922
INSTRUCTIONS
924
SIGNAL GENERATION DEVICE
918
ENHANCED ATTACK DETECTION DEVICE
919
POWER MANAGEMENT DEVICE
932
OUTPUT CONTROLLER
934

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2018/025561

A. CLASSIFICATION OF SUBJECT MATTER

H04W 24/10(2009.01)i, H04W 64/00(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 24/10; H04W 24/02; H04L 12/26; H04W 4/02; H04L 27/04; G01S 5/02; H04W 64/00

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: sounding signal, shift, NDP(null data packet), TOA(time of arrival), location measurement report

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014-0301219 A1 (SHANI BEN-HAIM et al.) 09 October 2014 See paragraphs [0054]-[0062]; and figure 5C.	1,3,8,9,18,20
A		2,4-7,10-17,19,21-25
Y	US 2012-0300874 A1 (HONGYUAN ZHANG) 29 November 2012 See paragraphs [0109]-[0110]; and figure 14.	1,3,8,9,18,20
A	US 2016-0366548 A1 (JAMES JUNE-MING WANG et al.) 15 December 2016 See paragraphs [0044]-[0045]; and figure 4.	1-25
A	LIWEN CHU, '11az NDP Announcement', IEEE 802.11-17/0474r1, 16 March 2017 (https://mentor.ieee.org/802.11/dcn/17/11-17-0474-01-00az-11az-ndp-announcement.pptx) See slides 2-7.	1-25
A	YUVAL AMIZUE et al., 'NDP-Based Measurement Protocol', IEEE 802.11-17-0481-01-00az, 15 March 2017 (https://mentor.ieee.org/802.11/dcn/17/11-17-0481-01-00az-ndp-based-su-11az-measurement-protocol.pptx) See slides 5-7.	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	Date of mailing of the international search report
31 August 2018 (31.08.2018)	**31 August 2018 (31.08.2018)**

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
YANG, Jeong Rok
Telephone No. +82-42-481-5709

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2018/025561

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0301219 A1	09/10/2014	CN 105051566 A	11/11/2015
		EP 2959309 A1	30/12/2015
		EP 2959309 A4	19/10/2016
		TW 201436623 A	16/09/2014
		US 2017-0208484 A1	20/07/2017
		US 9532239 B2	27/12/2016
		WO 2014-130070 A1	28/08/2014
US 2012-0300874 A1	29/11/2012	EP 2715965 A2	09/04/2014
		EP 2715965 B1	18/10/2017
		JP 2014-519754 A	14/08/2014
		KR 10-2014-0037128 A	26/03/2014
		US 2015-0172026 A1	18/06/2015
		US 2017-0215104 A1	27/07/2017
		US 8948283 B2	03/02/2015
		WO 2012-162309 A2	29/11/2012
		WO 2012-162309 A3	04/07/2013
US 2016-0366548 A1	15/12/2016	EP 3100543 A1	07/12/2016
		EP 3100543 A4	02/08/2017
		EP 3111566 A2	04/01/2017
		EP 3111566 A4	01/11/2017
		US 2017-0070893 A1	09/03/2017
		WO 2015-130618 A2	03/09/2015
		WO 2015-130618 A3	19/11/2015
		WO 2015-130712 A1	03/09/2015