(54) Title: ACCESS POINT LOCATION DISCOVERY IN UNMANAGED NETWORKS
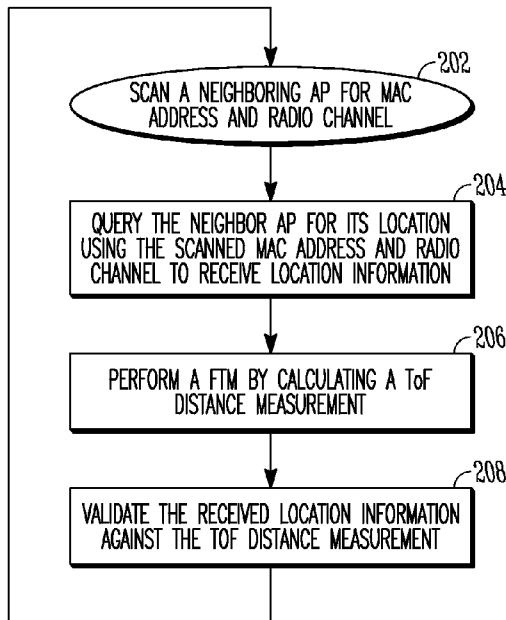
(57) Abstract: Embodiments of a system and method for
Access Point Location Discovery in Unmanaged Networks
are generally described herein. When a device attempts to
discern its location indoors, it must be aware of the exact
location of the network infrastructure that participates in the
measurement. Indoors, it is the location of the Access Points
(APs), which must be known to the device in order to trian-
gulate its position. A system and method are disclosed for
correctly discovering the exact location of network APs. An
AP populates a neighbor list with location information by
performing Wi-Fi scanning to receive a Media Access Con-
trol address and radio channel of a neighboring AP. The in-
terested AP then acquires the position of this AP neighbor
by querying its location and receiving its position informa-
tion. Lastly, the received neighbor location is validated for
correctness and reliability using Time of Flight measure-
ments.

FIG. 2

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).

Published:

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

ACCESS POINT LOCATION DISCOVERY IN UNMANAGED NETWORKS

5

[0001]   This application claims the benefit of priority to U.S. Patent Application Serial No. 14/197,570, filed on March 5, 2014, which is incorporated herein by reference in its entirety.

10   TECHNICAL FIELD

[0002]   Embodiments pertain to wireless networks. Some embodiments relate to wireless networks that operate in accordance with one of the IEEE 802.11 standards including the IEEE 802.11-2012 standards. Some embodiments

15   relate to time-of-flight (ToF) positioning. Some embodiments relate to location determination. Some embodiments relate to indoor navigation.

BACKGROUND

20   [0003]   Outdoor navigation and positioning has been widely deployed following the development of various global navigation-satellite-systems (GNSS) as well as various cellular systems. Indoor navigation and positioning differs from outdoor navigation and positioning because the indoor environment does not enable the reception of location signals from satellites or cellular base

25   stations as accurately as in the outdoor environment. As a result, accurate and real-time indoor navigation and positioning are difficult to achieve.

[0004]   Conventional indoor navigation and positioning methods, i.e. "fingerprinting", "site-mapping" etc., calculate location by measuring received signal strength from an Access Point (AP). A handheld device initiates a location

30   calculation by measuring the strength of a received signal and determines its position by figuring its distance from the location of a router or other access

point transmitting the received signal. Unfortunately, these methods are inaccurate due to large variances in received signal strength. Fluctuations in received signal strength produce an approximately 20 meter radius of error. Another drawback of conventional indoor location methods is the inability of the

5   network to initiate and significantly control the timing and management for location of a handheld device. When a device tries to query the location of APs in its vicinity, one query would preferably produce not only the location of a single AP, but also the location of that AP's neighbor APs as well. Receiving a complete tile, rather than the location of a single AP, reduces device power

10   consumption and unnecessary air interface. In a managed network this is a solved problem because there is a centric data base containing the positions of the entire infrastructure in the venue. An unmanaged network presents challenges because an AP is not aware of the location of its neighbor APs in an unmanaged network.

15   **[0005]**   In order for an unmanaged network to control the timing and management for location of handheld devices, the network must have the ability to discover the location of other access points belonging to the network that are in communication with the devices. Thus, there is a need for accurate indoor navigation and positioning methods that can be initiated and controlled by a

20   network having known access points.

BRIEF DESCRIPTION OF THE DRAWINGS

25   **[0006]**   FIG. 1 is a network diagram illustrating an exemplary network environment suitable for Access Point Location Discovery In Unmanaged Networks, according to some example embodiments;

[0007]   FIG. 2 shows a block diagram of a high level overview flow chart of Access Point Location Discovery In Unmanaged Networks, according to

30   some example embodiments;

[0008]   FIG. 3   illustrates a procedure for basic time-of-flight (ToF) calculation, in accordance with some exemplary embodiments; and

[0009]   FIG. 4 is a functional diagram of an exemplary communication station in accordance with some embodiments.

DETAILED DESCRIPTION

[0010]   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.

[0011]   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.

[0012]   The terms "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, smartphone, tablet, netbook, wireless terminal, laptop computer, a femtocell, High Data Rate (HDR) subscriber station, access point, access terminal, or other personal communication system (PCS) device. The device may be either mobile or stationary.

[0013]   The term "access point" as used herein may be a fixed station. An access point may also be referred to as an access node, a base station or some other similar terminology known in the art. An access terminal may also be called a mobile station, a user equipment (UE), a wireless communication device or some other similar terminology known in the art.

[0014]   A precise scalable Time-of-Flight (ToF) solution for indoor positioning and navigation is provided for environments where global-navigation-satellite-systems (GNSS, GPS, GLONASS and GALILEO) signals are not available. Time-of-Flight (ToF) is defined as the overall time a signal requires to propagate from the user to an Access Point (AP) and back to the user.

A measured ToF value is converted into distance by dividing the measured time by two and multiplying it by the speed of light.

[0015] In many instances and applications, a network requires the client location, preferably without client initiation, interruption, intervention, inconvenience, or responses. An accurate method for indoor location where the location of APs in an unmanaged network are known is disclosed. The present network initiated location methods do not require the client to perform any client initiated ToF procedures and/or reporting back to the AP. The AP, rather than the client, fully controls the timing and management of the overall indoor location procedure, making the procedure more convenient and power efficient for the client.

[0016] When a device attempts to discern its location, it must be aware of the exact location of the network infrastructure that participates in the measurement. In an outdoor environment using GNSS, it is the location of the satellites that are exactly known. In an indoor environment using Wi-Fi indoor positioning, it is the location of the APs, which must be known to the device in order to triangulate its position. A system and method are provided for correctly discovering the exact location of infrastructure elements necessary for positioning of devices indoors.

[0017] FIG. 1 illustrates various network elements of a wireless network in accordance with some embodiments. Wireless network 100 includes a plurality of communication stations (STAs) and one or more access points (APs) which may communicate in accordance with IEEE 802.11 communication techniques. The communication stations may be mobile devices that are non-stationary and do not have fixed locations. The one or more access points may be stationary and have fixed locations. The stations may include an interested AP STA-A 102 and one or more responding stations STA-B 104. The interested AP 102 may be a communication station that initiates ToF positioning with the neighboring AP STA-B 104 to determine its location. The ToF positioning procedure may include the exchange of messages including the exchange of messages, as described in more detail below in FIG.s 2-4.

[0018] In some embodiments, the interested AP STA-A 102 may be a positioning station and may determine its location relative to one or more

responding stations (e.g., cooperating stations and/or one or more access points). The cooperating stations may be either IEEE 802.11 configured communication stations (STAs) or APs. In other embodiments, the interested AP STA-A 102 may determine its location in geo-coordinates. In some embodiments, the neighboring AP may be able to determine its location either in relative or in geo-coordinates.

[0019]   FIG. 2 is a flowchart illustrating operations in performing a method 200 of Access Point Location Discovery in Unmanaged Networks, according to some example embodiments. Operations in the method 200 may be performed by the interested AP STA-A 102 and/or neighboring AP STA_B 104 described above with respect to FIG. 1.

[0020]   A device determines its position by first gaining knowledge of the exact location of the network infrastructure elements that participate in its triangulation measurements. Outdoor positioning devices first gain knowledge of the exact location of satellites and use the triangulation points to determine their locations. Rather than receiving satellite signals, indoor applications must use received Wi-Fi signals to learn the locations of network APs in their environments, which are then used as triangulation points. When a device tries to query the location of APs in its vicinity, one query would preferably produce not only the location of a single AP, but also the location of that AP's neighbor APs as well. Receiving a complete tile, rather than the location of a single AP, reduces device power consumption and unnecessary air interface. In a managed network this is a solved problem because there is a centric data base containing the positions of the entire infrastructure in the venue. An unmanaged network presents challenges because an AP is not aware of the location of its neighbor APs in an unmanaged network.

[0021]   A novel protocol for communicating location information between APs in an unmanaged network and a reliable method for discovering and independently validating the location information such that errors are not propagated through the network are disclosed. The 3-part method comprises neighbor discovery, negotiating with the neighbor to receive its location, and validating the received location information.

[0022]   In order for an AP to populate a neighbor list with location information, it must first become aware of its neighbor APs by performing a regular Wi-Fi scan for receiving a Media Access Control (MAC) address and radio channel of a neighboring AP. After becoming aware of a neighbor's MAC

5   address and radio channel, the interested AP must then acquire the position of this AP neighbor by querying its location and receiving its position information. Lastly, the neighbor location is validated for correctness and reliability.

[0023]   After discovery and communication, a validation process is performed according to one or more of the following operations. A Fine Timing

10   Measurement (FTM), or ToF distance measurement, is first performed as described in 802.11 and detailed below in FIG. 3. Performing the fine timing measurement provides a distance measurement (i.e. a single triangulation point). The distance measurement, or range, creates a circle of certainty, having a radius equal to the measured distance and within which, the neighbor AP is certainly

15   located. The circle of certainty is then used to initially validate the neighbor's communicated position. In other words, the actual ToF distance calculated from the fine timing measurement is compared to the position reported by the AP.

[0024]   As each AP can also provide his neighbor AP's position, the interested AP can compare positions that were received from different APs and

20   search for consistency, eliminating inconsistent locations such that any erroneous location is not propagated to other network entities. Each AP may also report its range from other APs and in some cases the position of the APs can be calculated independently, in a manner similar to finding a position from crowdsourcing, and can be used to compare with the reported location of a

25   queried AP.

[0025]   Each neighbor and the neighbor's neighbors are likewise queried in turn until the entirety of neighboring APs are located and validated. Upon completion of the query and validation process, the interested AP will have a list of its neighboring APs and their positions. Each AP in the now populated list

30   may be assigned a confidence/reliability "grade" according to one or more parameters that may include whether the reported position of the neighbor was confirmed by the measured the range, or distance, from the interested AP, and the number of times the same AP was reported with the same location by

different APs in the network. This validation process protects the user from receiving AP positions that were wrongly entered or delivered for any reason, including data corruption and transmission errors. A position wrongly entered in the list due to transmission errors or data corruption may be invalidated.

5   **[0026]**   As shown in FIG. 2, the method 200 includes operations 202, 204, 206, and 208. Beginning in operation 202, the interested AP scans a neighbor AP for its MAC address and radio channel. Control flow proceeds to operation 204.

[0027]   In operation 204, the interested AP queries the neighbor AP for

10 its location according to the scanned MAC address and radio channel and receives its location information. Control flow proceeds to operation 206.

[0028]   In operation 206, a FTM is performed by calculating a ToF distance measurement between the interested AP and the neighbor AP. The ToF measurement is performed using timers t1-t4 wherein, $ToF = ((t4-t1)-(t3-t2))/2$.

15 Messaging protocols for ToF measurements are detailed in FIG. 3 below. The distance is calculated by dividing the measured ToF by two and multiplying it by the speed of light. Control flow proceeds to operation 208.

[0029]   In operation 208, the received location is validated at least against the TOF distance measurement. Other validation including grading the reliability

20 of the reported location information may be performed. Other validation may comprise each AP in the now populated list having an assigned confidence/reliability "grade" according to one or more parameters that may include whether the reported position of the neighbor was confirmed by the measured the range, or distance, from the interested AP, and the number of times

25 the same AP was reported with the same location by different APs in the network. This validation process protects the user from receiving AP positions that were wrongly entered or delivered for any reason, including data corruption and transmission errors. A position wrongly entered in the list due to transmission errors or data corruption may be invalidated.

30 **[0030]**   Operations 202-208 are repeated until a current neighbor list is fully populated. Operations 202-208 are repeated querying each neighbor and the neighbor's neighbors in turn until the entirety of neighboring APs are located

and validated. Upon completion of the query and validation process, the interested AP will have a list of its neighboring APs and their positions.

[0031]   FIG. 3   illustrates a procedure for basic time-of-flight (ToF) distance calculation of Access Point Location Discovery in Unmanaged Networks, in accordance with some exemplary embodiments. As illustrated in FIG. 3, interested AP station STA-A 102 may be arranged to transmit a message M1 302 carrying a management frame to neighbor AP station STA-B 104, which may respond with an ACK 304. M1 302 may be a timing measurement action frame. The timing measurement action frame may be a unicast management frame. T1, the M1 time of departure (ToD) from the interested AP STA-A 102 and t2, the time of arrival (ToA) of M1 at the neighboring AP STA-B 104, are saved.

[0032]   The neighboring AP STA-B 104 may be arranged to transmit a message M2 306 at ToD, t3, carrying a management frame to interested AP STA-A 102, which may respond with an ACK 308. M2 306 may be a timing measurement action frame. The timing measurement action frame may be a unicast management frame. M2 306 may return saved time value t2 and a ToD of ACK 304, t3, time value to interested AP STA-A 102.

[0033]   All time of departures and time of arrivals, t1-t4, are saved at STA-A 102. Interested AP STA-A 102 computes the ToF by the following equation:

$$ToF = ((t4-t1)-(t3-t2))/2$$

(Equation 1)

[0034]   In some embodiments, the messages M1 302 and M2 306 may be a timing measurement action frame in accordance with 802.11. The message M1 302 may refer to an M1 frame and the message M2 306 may refer to an M2 frame. In some embodiments, the message M1 302 may be used to initiate ToF positioning with another AP.

[0035]   In some embodiments, the message M1 may be a first timing measurement action frame and the message M2 may be a second timing measurement action frame. In some embodiments, the timing measurement

action frames may be timing measurement frames. In some embodiments, a Media Access Control (MAC) Sublayer Management Entity (MLME) constructs the timing measurement frames.

[0036]   In some embodiments, the timing measurement information may be a t2 value and a t3 value (i.e., two values) or a t3-t2 value (i.e., a single difference value). In these embodiments, the interested AP may be arranged to parse the structure of the message M2 306. By parsing the structure of message M2 306, the interested AP STA-A 102 can determine whether the message M2 306 contains either a t2 and a t3 value (i.e., two values), or a t3-t2 value (i.e., a single difference value). In some of these embodiments, the message M2 306 may include different elements or employ sub-element coding to allow the initiation station to parse the structure of message M2 306.

[0037]   In some embodiments, t2 may be a time-stamp against a local clock associated with the arrival of message M1 302 at the neighboring AP STA-B 104, and t3 may be a time-stamp against the local clock associated with transmission of message M2 306 by the neighboring AP STA-B 104 (i.e., measured against the same clock as t2). In some embodiments, t1 may be a time-stamp against a local clock associated with the transmission of message M1 302 by the interested AP STA-A 102 and t4 may be a time-stamp against the local clock associated with receipt of the acknowledgement frame 304 that acknowledges receipt of the message M1 (i.e., measured against the same clock as t1).

[0038]   In some embodiments, the t2 value is the ToA of message M1 302 at the neighboring AP STA-B 104, and the t3 value is time that the ACK frame 304 is sent by the neighboring AP STA-B 104. The inclusion of both t2 and t3 values may be more optimal as it may allow a particular and more straightforward way to calibrate for difference in the clock rates at the two stations for increased ToF accuracy. Furthermore, inclusion of a single value (t3-t2) may allow the relative timing drift between the recipient and the responding stations to be tracked for increased ToF accuracy.

[0039]   FIG. 4 is a functional diagram of a communication station in accordance with some embodiments. In one embodiment, FIG. 4 illustrates a functional block diagram of an STA or UE 102 and 104 (FIG. 1) in accordance

with some embodiments. STA 400 may be suitable for use as UE 102 (FIG. 1). Communication station 400 may be suitable for use as either a neighbor, such as neighboring AP STA-B 104 (FIG. 1), or an interested AP, such as interested AP STA-A 102 (FIG. 1). The STA 400 may include physical layer circuitry 402 for

5   transmitting and receiving signals to and from eNBs 104 (FIG. 1) using one or more antennas 401. STA 400 may also include medium access control layer (MAC) circuitry 404 for controlling access to the wireless medium. UE 400 may also include processing circuitry 406 and memory 408 arranged to perform the operations described herein. In some embodiments, the physical layer circuitry

10   402 and the processing circuitry 404 may be configured to transmit and receive messages M1-M4 (FIG. 3) carrying time management frames as detailed above.

[0040]   In accordance with some embodiments, the MAC circuitry 404 may be arranged to contend for a wireless medium configure frames or packets for communicating over the wireless medium and the PHY circuitry 402 may be

15   arranged to transmit and receive signals. The PHY 402 may include circuitry for modulation/demodulation,   upconversion/downconversion,   filtering, amplification, etc. In some embodiments, the processing circuitry 404 of the STA device 400 may include one or more processors. In some embodiments, two or more antennas may be coupled to the physical layer circuitry arranged for

20   sending and receiving signals. The memory 408 may be store information for configuring the processing circuitry 406 to perform operations for configuring and transmitting message frames and performing the various operations described herein.

[0041]   In some embodiments, the communication station 400 may be

25   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,

30   etc.), or other device that may receive and/or transmit information wirelessly.

[0042]   In some embodiments, the communication station STA 400 may include one or more antennas. The antennas may comprise 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 to take advantage of spatial diversity and the different channel characteristics that may result between each of antennas and the antennas of a transmitting station.

[0043]   In some embodiments, the communication station STA 400 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.

[0044]   Although communication station STA 400 is illustrated as having several separate functional elements, one 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 comprise 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 STA 400 may refer to one or more processes operating on one or more processing elements.

[0045]   Embodiments may be implemented in one or a combination of hardware, firmware and software. 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 408 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 STA 400 may include one or more processors and may be configured with instructions stored on a computer-readable storage device memory 408.

5   **[0046]**   In one example, a method for Access Point location discovery in an unmanaged network comprises scanning, by an interested Access Point (AP), a neighboring AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP, querying, by the interested AP from the neighbor AP, a location of the neighboring AP using the scanned MAC address

10   and radio channel, receiving, at the interested AP from the neighboring AP, the location of the neighboring AP, performing, by the interested AP, a Fine Timing Measurement (FTM) by calculating a Time-of-Flight (TOF) distance measurement, and validating, at the interested AP, the received location of the neighboring IP against the ToF distance measurement.

15   **[0047]**   In another example, a communication station STA 400 is arranged to discover Access Point locations in an unmanaged network, the communication station comprising physical layer circuitry and processing elements to scan a neighboring AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP, query a location of the

20   neighboring AP using the scanned MAC address and radio channel, receive the location of the neighboring AP, perform a Fine Timing Measurement (FTM) by calculating a Time-of-Flight (TOF) distance measurement, and validate the received location of the neighboring IP against the ToF distance measurement.

[0048]   In another example, a non-transitory computer-readable storage

25   medium stores instructions for execution by one or more processors to perform operations for Access Point location discovery in an unmanaged network, the method comprising scanning, by an interested Access Point (AP), a neighboring AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP, querying, by the interested AP from the neighbor AP, a

30   location of the neighboring AP using the scanned MAC address and radio channel, receiving, at the interested AP from the neighboring AP, the location of the neighboring AP, performing, by the interested AP, a Fine Timing Measurement (FTM) by calculating a Time-of-Flight (TOF) distance

measurement, and validating, at the interested AP, the received location of the neighboring IP against the ToF distance measurement.

[0049]   In another example, a method for Access Point location discovery in an unmanaged network comprises determining, by an interested Access Point (AP), a list of locations for neighboring APs in a network and validating, at the interested AP, the list of locations for neighboring APs against a ToF distance measurement.

[0050]   In another example, a method for Access Point location discovery in an unmanaged network further comprises reporting, by the neighboring AP, its distance from its neighboring APs.

[0051]   In another example, a method for Access Point location discovery in an unmanaged network further comprises querying, by the interested AP, every neighbor and the neighbor's neighbors until the entirety of the interested AP's neighboring APs are located and validated.

[0052]   In another example, a method for Access Point location discovery in an unmanaged network further comprises assigning a reliability grade to a location according to whether the reported position of the neighboring AP was confirmed by the measured distance from the interested AP.

[0053]   In another example, a method for Access Point location discovery in an unmanaged network further comprises assigning a reliability grade to a location according to the number of times the same AP was reported with the same location by different APs in a network.

[0054]   In another example, a method for Access Point location discovery in an unmanaged network further comprises invalidating a position wrongly entered in a list due to transmission errors.

[0055]   In another example, a method for Access Point location discovery in an unmanaged network further comprises invalidating a position wrongly entered in the list due to data corruption.

[0056]   The Abstract is provided to comply with 37 C.F.R. Section 1.72(b) requiring an abstract that will allow the reader to ascertain the nature and gist of the technical disclosure. It is submitted with the understanding that it will not be used to limit or interpret the scope or meaning of the claims. The

following claims are hereby incorporated into the detailed description, with each claim standing on its own as a separate embodiment.

CLAIMS

What is claimed is:

5   1.   A method for Access Point location discovery in an unmanaged
network, the method comprising:

scanning, by an interested Access Point (AP), a neighboring AP
for a Media Access Control (MAC) address and radio channel belonging to the
neighboring AP;

10   querying, by the interested AP from the neighbor AP, a location
of the neighboring AP using the scanned MAC address and radio channel;

receiving, at the interested AP from the neighboring AP, the
location of the neighboring AP;

performing, by the interested AP, a Fine Timing Measurement

15   (FTM) by calculating a Time-of-Flight (TOF) distance measurement; and

validating, at the interested AP, the received location of the
neighboring IP against the ToF distance measurement.

2.   The method of claim 1 further comprising reporting, by the

20   neighboring AP, its distance from its neighboring APs.

3.   The method of claim 1 further comprising querying, by the
interested AP, every neighbor and the neighbor's neighbors until the entirety of
the interested AP's neighboring APs are located and validated .

25

4.   The method of claim 1 further comprising assigning a reliability
grade to a location according to whether the reported position of the neighboring
AP was confirmed by the measured distance from the interested AP.

30   5.   The method of claim 1 further comprising assigning a reliability
grade to a location according to the number of times the same AP was reported
with the same location by different APs in a network.

6.   A communication station arranged to discover Access Point locations in an unmanaged network, the communication station comprising physical layer circuitry and processing elements to:

scan a neighboring AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP;

query a location of the neighboring AP using the scanned MAC address and radio channel;

receive the location of the neighboring AP;

perform a Fine Timing Measurement (FTM) by calculating a Time-of-Flight (TOF) distance measurement; and

validate the received location of the neighboring IP against the ToF distance measurement.

7.   The communication station of claim 6 further arranged to report its distance from its neighboring APs.

8.   The communication station of claim 6 further arranged to query every neighbor and the neighbor's neighbors until the entirety of the interested AP's neighboring APs are located and validated .

9.   The communication station of claim 6 further arranged to assign a reliability grade to a location according to whether the reported position of the neighboring AP was confirmed by the measured distance from the interested AP.

10.   The communication station of claim 6 further arranged to assign a reliability grade to a location according to the number of times the same AP was reported with the same location by different APs in a network.

11.   A non-transitory computer-readable storage medium that stores instructions for execution by one or more processors to perform operations for Access Point location discovery in an unmanaged network, the method comprising:

scanning, by an interested Access Point (AP), a neighboring AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP;

querying, by the interested AP from the neighbor AP, a location

5   of the neighboring AP using the scanned MAC address and radio channel;

receiving, at the interested AP from the neighboring AP, the location of the neighboring AP;

performing, by the interested AP, a Fine Timing Measurement (FTM) by calculating a Time-of-Flight (TOF) distance measurement; and

10   validating, at the interested AP, the received location of the neighboring IP against the ToF distance measurement.

12.   The non-transitory computer-readable storage medium of claim 11 further comprising reporting, by the neighboring AP, its distance from its

15   neighboring APs.

13.   The non-transitory computer-readable storage medium of claim 11 further comprising querying, by the interested AP, every neighbor and the neighbor's neighbors until the entirety of the interested AP's neighboring APs

20   are located and validated .

14.   The non-transitory computer-readable storage medium of claim 11 further comprising assigning a reliability grade according to whether the reported position of the neighboring AP was confirmed by the measured distance

25   from the interested AP.

15.   The non-transitory computer-readable storage medium of claim 11 further comprising assigning a reliability grade according to the number of times the same AP was reported with the same location by different APs in a

30   network.

16.   A method for Access Point location discovery in an unmanaged network, the method comprising:

determining, by an interested Access Point (AP), a list of locations for neighboring APs in a network; and

validating, at the interested AP, the list of locations for neighboring APs against a ToF distance measurement.

17. The method of claim 16 further comprising assigning a reliability grade to the list according to whether the list of locations for neighboring APs was confirmed by the measured distance from the interested AP.

18. The method of claim 16 further comprising assigning a reliability grade to the list according to the number of times a same AP in the list of locations for neighboring IPs was reported with the same location by different APs in the network.

19. The method of claim 16 further comprising invalidating a position wrongly entered in the list due to transmission errors.

20. The method of claim 16 further comprising invalidating a position wrongly entered in the list due to data corruption.

21. The communication station of claim 6 further arranged to comprise physical layer circuitry and associated antenna(s) capable of scanning a neighboring (Access Point) AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP, querying a location of the neighboring AP using the scanned MAC address and radio channel, receiving, the location of the neighboring AP, and performing a Fine Timing Measurement (FTM) by calculating a Time-of-Flight (TOF) distance measurement.

22. The communication station of claim 6 further arranged to comprise processing circuitry for:

scanning a neighboring AP for a Media Access Control (MAC) address and radio channel belonging to the neighboring AP;

querying a location of the neighboring AP using the scanned
MAC address and radio channel;

receiving the location of the neighboring AP;

performing a Fine Timing Measurement (FTM) by calculating a
5   Time-of-Flight (TOF) distance measurement; and

validating the received location of the neighboring IP against
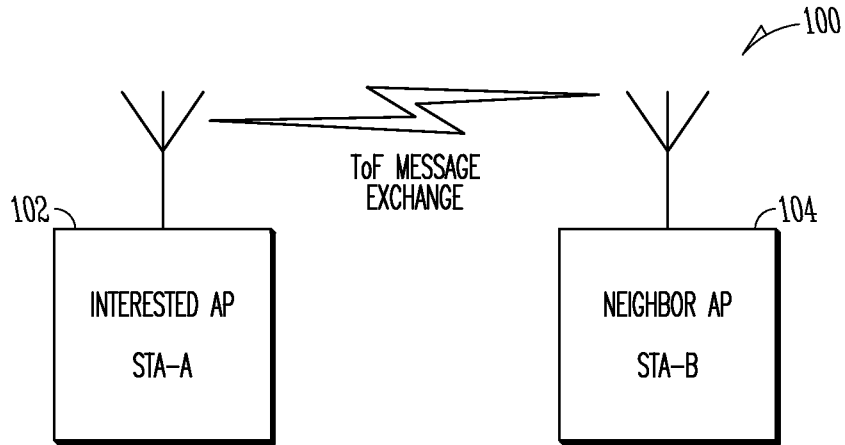the ToF distance measurement.

1/2
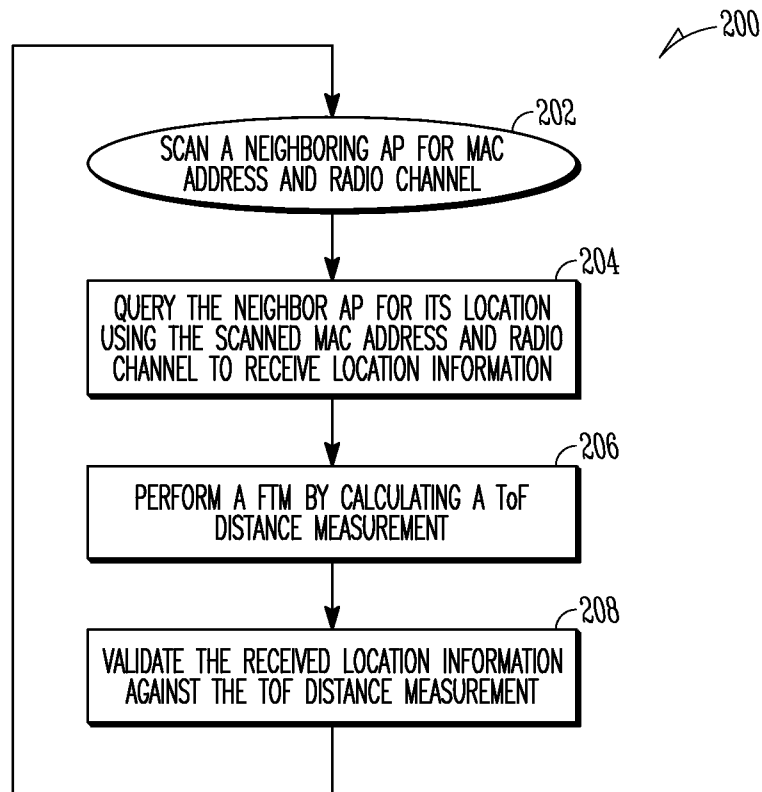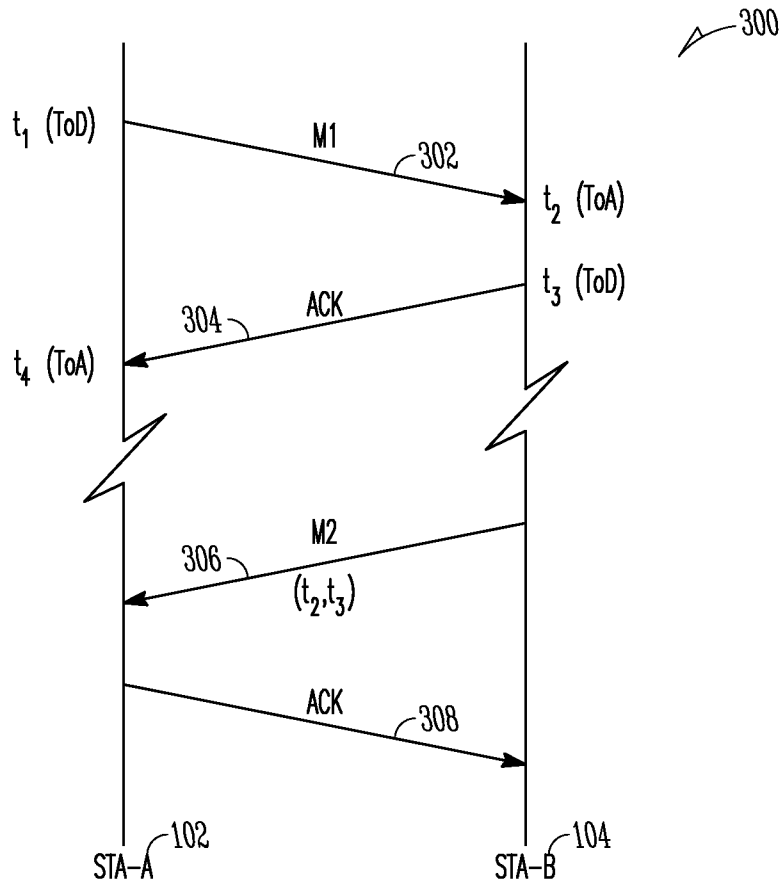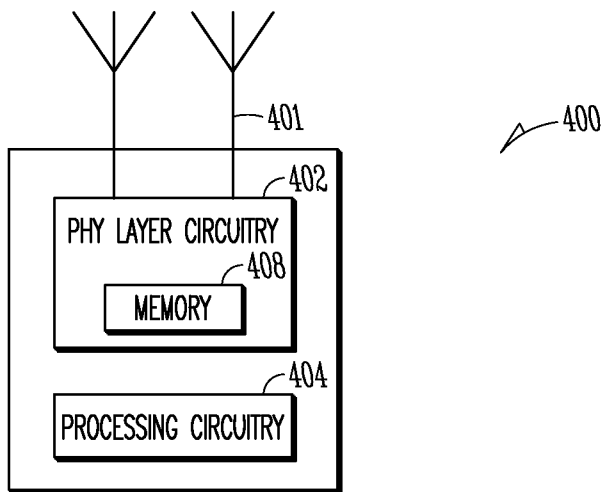

FIG. 1

FIG. 2

FIG. 3

FIG. 4

A. CLASSIFICATION OF SUBJECT MATTER

H04W 64/00(2009.01)i, H04W 48/16(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 64/00; H04W 88/08; H04L 12/26; G06F 17/30; H04W 8/08; H04Q 7/20; G01S 5/02; H04W 48/16

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: Access Point (AP), location discovery, Media Access Control address, radio channel, FTM (Fine Timing Measurement), TOF (Time-of-Flight)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2009-0122773 A1 (ALEKSANDAR M. GOGIC) 14 May 2009 See paragraphs [0051], [0055]; claims 1, 3; and figure 5.	16-20
A		1-15, 21-22
Y	US 2006-0009235 A1 (LEONID SHEYNBLAT et al.) 12 January 2006 See paragraphs [0101]-[0106]; claims 11, 16, 18, 20-21; and figure 5.	16-20
A	US 2010-0329123 A1 (HARISH VISWANATHAN et al.) 30 December 2010 See paragraphs [0042]-[0043]; claim 1; and figure 3.	1-22
A	KR 10-2011-0059077 A (SAMSUNG SDS CO., LTD.) 02 June 2011 See paragraphs [0089]-[0098]; and figure 2.	1-22
A	WO 2010-075369 A1 (QUALCOMM INCORPORATED) 01 July 2010 See paragraphs [0076]-[0079]; and figure 6.	1-22

☐ 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
23 June 2015 (23.06.2015)	**24 June 2015 (24.06.2015)**

Name and mailing address of the ISA/KR	Authorized officer
International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea	YU, Jae Chon
Facsimile No. +82-42-472-7140	Telephone No. +82-42-481-8647

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0122773 A1	14/05/2009	AU 2008-323930 A1	14/05/2009
		CA 2704127 A1	14/05/2009
		CA 2819536 A1	14/05/2009
		CN 101911798 A	08/12/2010
		CN 101911798 B	15/10/2014
		CN 103260177 A	21/08/2013
		EP 2220899 A2	25/08/2010
		EP 2220899 B1	15/05/2013
		IL 205377 D0	30/12/2010
		JP 05296089 B2	25/09/2013
		JP 05575943 B2	20/08/2014
		JP 2011-504328 A	03/02/2011
		JP 2013-153480 A	08/08/2013
		JP 2014-207704 A	30/10/2014
		KR 10-1170242 B1	01/08/2012
		KR 10-1283495 B1	15/07/2013
		KR 10-1287947 B1	22/07/2013
		KR 10-2010-0087368 A	04/08/2010
		KR 10-2012-0008548 A	30/01/2012
		KR 10-2012-0010284 A	02/02/2012
		MX 2010005143 A	01/06/2010
		RU 2010-123390 A	20/12/2011
		RU 2011-145014 A	20/05/2013
		RU 2474083 C2	27/01/2013
		RU 2499366 C2	20/11/2013
		TW 200939814 A	16/09/2009
		TW I393475 B	11/04/2013
		WO 2009-061901 A2	14/05/2009
		WO 2009-061901 A3	24/09/2009
US 2006-0009235 A1	12/01/2006	AU 2005-333140 A1	01/02/2007
		AU 2005-333140 A8	31/07/2008
		AU 2005-333140 B2	20/08/2009
		AU 2005-333140 B8	19/11/2009
		AU 2005-333140 C1	07/01/2010
		AU 2009-202647 A1	23/07/2009
		AU 2009-202647 B2	21/04/2011
		BR PI0512268 A	26/02/2008
		CA 2572610 A1	18/12/2005
		CA 2572610 C	09/11/2010
		CN 101032176 A	05/09/2007
		CN 101032176 B	02/01/2013
		CN 102547978 A	04/07/2012
		EP 1779683 A2	02/05/2007
		EP 1779683 A4	06/04/2011
		HK 1107490 A1	23/08/2013
		IL 180156 A	28/11/2013
		IL 180156 D0	20/03/2008
		JP 05080257 B2	21/11/2012

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		JP 2008-503758 A	07/02/2008
		JP 2011-019226 A	27/01/2011
		JP 2014-042247 A	06/03/2014
		KR 10-0938526 B1	25/01/2010
		KR 10-1003689 B1	23/12/2010
		KR 10-1119545 B1	13/03/2012
		KR 10-2007-0088455 A	29/08/2007
		KR 10-2009-0035749 A	10/04/2009
		KR 10-2010-0087393 A	04/08/2010
		US 7319878 B2	15/01/2008
		WO 2007-027166 A2	08/03/2007
		WO 2007-027166 A3	19/04/2007
US 2010-0329123 A1	30/12/2010	US 8743759 B2	03/06/2014
KR 10-2011-0059077 A	02/06/2011	EP 2327995 A3	06/07/2011
		JP 05258865 B2	07/08/2013
		JP 2011-099859 A	19/05/2011
		KR 10-1094616 B1	15/12/2011
		KR 10-1154732 B1	08/06/2012
		KR 10-1154749 B1	11/06/2012
		US 2011-0103360 A1	05/05/2011
WO 2010-075369 A1	01/07/2010	CN 102257402 A	23/11/2011
		CN 103675754 A	26/03/2014
		EP 2380035 A1	26/10/2011
		JP 05518894 B2	11/06/2014
		JP 2012-513032 A	07/06/2012
		JP 2014-131349 A	10/07/2014
		KR 10-1337760 B1	06/12/2013
		KR 10-2011-0097989 A	31/08/2011
		TW 201100846 A	01/01/2011
		US 2010-0159958 A1	24/06/2010
		US 2013-0072228 A1	21/03/2013
		US 2014-0018065 A1	16/01/2014
		US 8768344 B2	01/07/2014
		US 8831594 B2	09/09/2014