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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2015 (29.01.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/012767 A1

(51) International Patent Classification:
H04W 64/00 (2009.01) *H04W 24/00* (2009.01) *H04W 4/02* (2009.01) *H04L 29/08* (2006.01)

(21) International Application Number:
PCT/SG2014/000353

(22) International Filing Date:
25 July 2014 (25.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201305733-6 26 July 2013 (26.07.2013) SG

(71) Applicant: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way, #20-10, Connexis, Singapore 138632 (SG).

(72) Inventors: **SHANKAR S/O PATHMASUNTHARAM, Jaya**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **SHARMA, Pankaj**; c/o PKM, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG).

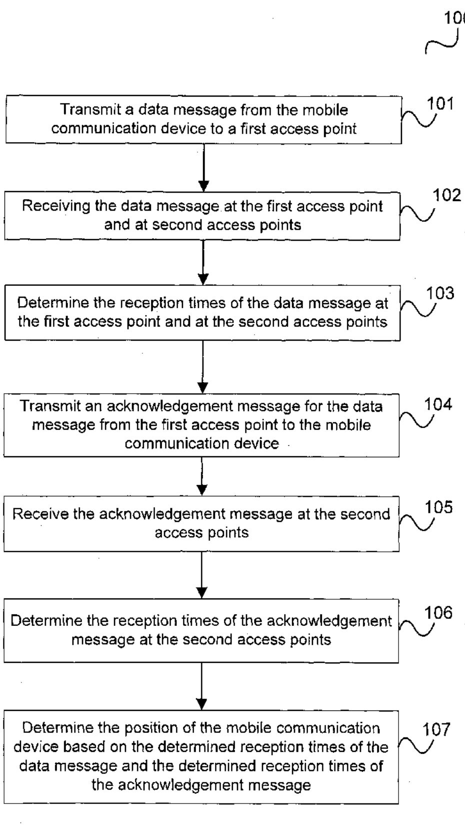
(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**; P. O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

[Continued on next page]

(54) Title: METHOD AND POSITIONING DEVICE FOR LOCALIZATION OF A MOBILE COMMUNICATION DEVICE



(57) Abstract: According to one embodiment, a method for localization of a mobile communication device is described comprising transmitting a data message from the mobile communication device to a first access point, determining the reception times of the data message at the first access point and at second access points, transmitting an acknowledgement message for the data message from the first access point to the mobile communication device, determining the reception times of the acknowledgement message at the second access points and determining the position of the mobile communication device based on the reception times of the data message and the reception times of the acknowledgement message.

WO 2015/012767 A1

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).

Published:

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

Method and positioning device for localization of a mobile communication device

Field of the invention

Embodiments of the invention generally relate to methods and positioning devices for localization of a mobile communication device.

Background of the invention

Indoor localization is a key component that is central to enabling the concept of "Internet of Things". There have been many recent demands for better indoor localization coming from different industry sectors. In the aerospace industry, it is essential to track items and users in large hangers. In the port terminal areas, there are requirements to track cars that are unloaded from large ships and parked in multi-storey car parks. Due to the sheer number of cars, it is impractical for the port operators to identify a specific car's location. In the healthcare environment, indoor localization is important to aid in way-finding for patients with cognitive impairments. Currently, some position-based indoor tracking systems have been used in hospitals, warehouses, offices, etc. where expensive equipment needs to be tracked to optimize their usage. Indoor navigation systems are also needed in a large public area to provide position indications for the users. For example, tourists could use indoor navigation services in large museums to view the artefacts more efficiently according to user preference. Shoppers could benefit if items and shops can be easily identified in large shopping malls. Accordingly, efficient methods for localization, e.g. indoor localization, are desirable.

Summary of the invention

In one embodiment, a method for localization of a mobile communication device is provided including transmitting a data message from the mobile communication device to a first access point, receiving the data message at the first access point and at second access points; determining the reception times of the data message at the first access point and at the second access points, transmitting an acknowledgement message for the data message from the first access point to the mobile communication device, receiving the acknowledgement message at the second access points, determining the reception times of the acknowledgement message at the second access points and determining the position of the mobile communication device based on the determined reception times of the data message and the determined reception times of the acknowledgement message.

According to a further embodiment, a positioning device according to the method described above is provided.

Short description of the figures

Illustrative embodiments of the invention are explained below with reference to the drawings.

Figure 1 shows a flow diagram illustrating a method for localization of a mobile communication device.

Figure 2 shows a positioning device for localization of a mobile communication device.

Figure 3 shows a message flow diagram illustrating a 4-way handshake process according to IEEE 802.11.

Figure 4 shows a signal diagram.

Figure 5 shows a communication arrangement according to an embodiment.

Figure 6 shows the architecture of an access point according to an embodiment.

Figure 7 shows the 4-way handshake message exchange used for triangulation according to one embodiment in the communication arrangement of figure 5.

Figure 8 shows a message flow diagram illustrating a 4-way handshake message exchange used for a localization process according to one embodiment.

Figure 9 shows a message flow diagram illustrating measuring of times at a master localization access point.

Figure 10 shows a message flow diagram illustrating measuring of times at a localization access point.

Figure 11 shows a message flow diagram illustrating the triggering of an analog-to-digital circuit for time measuring.

Detailed description

Localization is touted as the key component to enable new applications for mobile devices. App stores for mobile devices offer thousands of location based applications. While outdoor localization is typically easier to implement, indoor localization has been a major challenge to implement. For example, GPS (Global Positioning System) does not work well indoors. As a result of this, many different techniques have been provided for indoor localization. Some of the techniques include finger printing of WiFi base stations signals, mapping of base stations, UWB positioning, etc. However, typically, none of these techniques offer a practical or cost effective way to locate a mobile device like a hand phone with about two meters accuracy.

In general the location of a mobile device can be derived from radio frequency, photonic, sound waves, mechanical, video analysis and magnetic field systems. Such systems may use different localization techniques to derive the location including methods such as triangulation (lateration, angulation, time of arrival, received signal strength, etc), proximity and dead reckoning.

Indoor localization may for example be based on a WiFi system. The use of WiFi is typically not selected based on its superiority but more on the popularity of the WiFi technology. In fact, a UWB localization scheme may allow a higher accuracy but it is not easily applicable since the corresponding infrastructure has not yet been provided and UWB is usually not yet adopted at end user devices. Similarly, indoor localization schemes based on ZigBee, Bluetooth or cellular network are not as popular as WiFi. A localization system based on a cellular network typically does not allow a sufficient accuracy in an indoor environment.

The Global positioning system (GPS) is the most widely used satellite-based positioning system which offers maximum coverage. GPS capability can be added to various devices by adding GPS cards and accessories in these devices, which enable location-based services. However, GPS cannot be deployed for indoor use, because line-of-sight transmission between receivers and satellites is not possible in an indoor environment.

Typically, indoor positioning poses several challenges:

- Propagation model: Indoor environments are more complex because of various obstacles. For example walls, equipment and human beings influence the propagation of electromagnetic waves. This leads to multi-path effects.

- Interference: Some interference and noise sources from other wired and wireless networks degrade the accuracy of positioning when RF (radio frequency) based positioning is used.

- Mainly NLOS (no line of sight) situations: Building and spaces are normally complex with walls, pillars and other objects. Therefore there are many NLOS situations and localization techniques such as RF based, video based, light based positioning techniques etc. that depend on an LOS (line of sight) situation typically do not work well.

- Time synchronization: Techniques that depend on time of arrival may need complex synchronization schemes. This introduces more infrastructure devices that require proper planning for placement of nodes.

- Cost: This includes the cost of the infrastructure components, the cost of a positioning device for each user, space cost and the cost of system installation and maintenance.

- Performance: Different techniques offer different accuracy and precision. Accuracy is for example defined as the average error distance, and precision is for example defined as the success probability of position estimations with respect to a predefined accuracy. Delay is another performance aspect which includes the delay of measuring, calculating positions of estimated target and forwarding the results to the component requesting the localization.

In the following, embodiments are described which allow providing an accurate (2 meters or better) localization scheme for indoor tracking, e.g. based on WiFi. The scheme may for example work with existing mobile devices that are equipped with WiFi transceivers. There are many WiFi devices today and the cost of WiFi chipset is low because of mass production of these devices. Due to the popularity of WiFi, it is easier to capitalize on the WiFi radio communication rather than to introduce a location device based on an additional technology that can be specifically used for indoor localization.

It should be noted that introducing a system requiring a technology which is not usually implemented such as UWB can be expected to be prohibitive because handset manufacturers for example would have to adopt this technology. Further, the cost of the UWB system, for example, is also high. In contrast, according to one embodiment a technique is used that introduces some infrastructure nodes which could operate with a handset (e.g. a mobile phone) without requiring any changes to the software and hardware on the handset.

Figure 1 shows a flow diagram 100 illustrating a method for localization of a mobile communication device.

In 101, the mobile communication device transmits a data message to a first access point.

In 102, the first access point and second access points receive the data message.

In 103, the reception times of the data message at the first access point and at the second access points are determined.

In 104, the first access point transmits an acknowledgement message for the data message to the mobile communication device.

In 105, the second access points receive the acknowledgement message.

In 106, the reception times of the acknowledgement message at the second access points are determined.

In 107, the (geographical) position of the mobile communication device is determined based on the determined reception times of the data message and the determined reception times of the acknowledgement message.

In other words, localization is performed based on the messages exchanged in course of a handshake process including, in this example, a data message and an acknowledgement message. The handshake process may include further messages. For example, it may be a 4-way handshake process as used for data transmission, e.g. according to IEEE 802.11. A data message may be understood as a message carrying useful data (or user data), e.g. data including content transmitted by the user of the mobile communication device such as speech, video, image or text data from the user.

Localization of a device may be understood as determining the geographical position of the device, e.g. in terms of longitude and latitude.

Determining the position of the mobile communication device may for example include compensating timer offsets between the first access point and the second access points in the determined reception times of the data message based on the determined reception times of the acknowledgement message.

For example, the method may further include the first access point determining a sending time of the acknowledgement message and compensating timer offsets based on the determined reception times of the acknowledgement message and the determined sending time.

According to one embodiment, determining the position of the mobile communication device includes determining the position of the mobile communication device by a triangulation based on the determined reception times of the data message.

The first access point and the second access points are for example access points of a wireless local area network.

The method may further include assigning the same data link layer address (e.g. MAC address) to the first access point and the second access points and addressing the data message to the address.

The method may further include suppressing acknowledgement messages generated by the second access points in response to the data message.

According to one embodiment, the data message and the acknowledgement message are part of a handshake process for data transmission from the mobile communication device to the first access point.

The handshake process is for example a 2-way handshake process or a 4-way handshake process.

The method may for example be a 4-way handshake process and include, as part of the 4-way handshake process, sending a request to send message from the mobile communication device to the first access point and sending a clear to send message from the first access point to the mobile communication device.

The method may further include assigning the same data link layer address to the first access point and the second access points and addressing the request to send message to the address and further comprising suppressing clear to send messages generated by the second access points in response to the request to send message.

The handshake process is for example a 4-way handshake process according to IEEE 802.11.

The mobile communication device is for example a mobile terminal, e.g. a mobile phone, for example supporting IEEE 802.11.

According to one embodiment, the access points are access points operating according to a wireless local area network standard such as IEEE 802.11, e.g. WiFi access points, and the client device is a client device according to the wireless local area network standard, e.g. a WiFi client device.

The second access points include for example two or more access points.

The method illustrated in figure 1 is for example performed by a positioning device as illustrated in figure 2.

Figure 2 shows a positioning device 200 for localization of a mobile communication device.

The positioning device 200 includes a determiner 201 configured to determine the reception times of a data message, sent by a mobile communication device to a first access point, at the first access point and at second access points and to determine the reception times of an acknowledgement message, sent by the first access point to the mobile communication device, at the second access points.

The positioning device 200 further includes a processor 202 configured to determine the position of the mobile communication device based on the determined reception times of the data message and the determined reception times of the acknowledgement message.

The positioning device may for example be one of the first access point and the second access points and the mobile communication device. Accordingly, the determiner may determine the reception time of a message by measuring the reception time of the message as received by itself or based on information received from another device which has received the message and has measured its reception time.

The components of the positioning device (e.g. the determiner and the processor) may for example be implemented by one or more circuits. A "circuit" may be understood as any kind of a logic implementing entity, which may be special purpose circuitry or a processor executing software stored in a memory, firmware, or any combination thereof. Thus a "circuit" may be a hard-wired logic circuit or a programmable logic circuit such as a programmable processor, e.g. a microprocessor. A "circuit" may also be a processor executing software, e.g. any kind of computer program. Any other kind of implementation of the respective functions which will be described in more detail below may also be understood as a "circuit".

It should be noted that embodiments described in context with the method illustrated in figure 1 are analogously valid for the positioning device 200 and vice versa.

In the following, embodiments are described in more detail.

According to IEEE 802.11, data frames are sent using either 2-way handshake or a 4-way handshake process. The 4-way handshake is illustrated in figure 3.

Figure 3 shows a message flow diagram 300.

The message flow illustrates a data transmission from a first device, in this example an access point (AP) 301, to a second device, in this example a mobile terminal 302, which operate according to IEEE 802.11, e.g. WiFi devices.

Each message (or frame) transmitted is subjected to a propagation delay when it is transmitted from one device to the other. This is illustrated by the messages being drawn with a slope indicating that a message arrives later at one device than it is transmitted at the other (assuming time increases along axes 303, 304 from top to bottom).

The inter-frame times are normally set to a fixed value which is known as SIFS 305 in IEEE 802.11.

First, the device transmitting data, in this example AP 301, transmits an RTS (Request to Send) message 306.

The device receiving the data, in this example mobile terminal 302, responds with a CTS (Clear to Send) message 307.

After having received the CTS message 307, the AP 301 transmits data 308 which arrives at the mobile terminal 302 (like also the other messages) with a propagation delay 309. According to one embodiment, the propagation delay 309 of a data message 308 is used for localization as will be described in more detail below.

The mobile terminal 302 acknowledges the data reception with an acknowledgement 310.

According to one embodiment, the $T/\overline{R}$ signal or TX pin on the WiFi interface hardware of a communication device is used. The $T/\overline{R}$ signal indicates the state of the WiFi baseband circuit, namely whether it is going to transmit or receive a frame over the air interface. The signal is normally triggered at a certain interval before a frame is sent out over the air interface. From observation in the oscilloscope, it can be seen that the time between $T/\overline{R}$ signal activation and transmission of a frame is normally consistent (i.e. constant). Typically, the $T/\overline{R}$ signal is used to activate the RF transmission circuitry. In a typical WiFi reference design, the $T/\overline{R}$ signal is pulled low when the frame is ready to be sent out as it is illustrated in figure 4.

Figure 4 shows a signal diagram 400.

Time increases from left to right. A first graph 401 illustrates the $T/\overline{R}$ signal and a second graph 402 illustrates a frame transmission. As illustrated, the $T/\overline{R}$ is low during the frame transmission.

The $T/\overline{R}$ signal and many other pins/leads on a WiFi Interface card of a WiFi device are normally clock synchronized e.g. to the Medium Access Control (MAC) clock of the device.

The period in which the $T/\overline{R}$ signal goes down during the transmission typically correlates with an internal counter in the WiFi chipset of the device. The SIFS interval as shown in Figure 3 above is also subjected to another internal counter and the SIFS interval is consistent (i.e. constant).

According to one embodiment, a localization approach for locating a mobile device (e.g. a mobile handset) with WiFi interface is provided that uses a localization system architecture as illustrated in figure 5.

Figure 5 shows a communication arrangement 500.

A mobile device 501 (or mobile client) which has a WiFi interface is localized by a set of WiFi Localization APs (LAPs) 502 and one or more Master Localization APs (MAP) 503. The operation of the MAP 503 and LAPs 502 can be interchangeable between the APs 502, 503. The dotted lines in the figure 5 show the possible connectivity graph of the nodes in the arrangement.

As will be described in the following, according to one embodiment, a localization approach is used that is based on time difference of arrival, which depends on a time synchronization between LAPs 502 and MAP 503.

The LAPs 502 and the MAP 503 have for example an architecture as illustrated in the hardware block diagram of figure 6.

Figure 6 shows the architecture of an access point 600 according to an embodiment.

The access point 600 includes a WiFi device 601, e.g. in form of a WiFi card including a WIFI baseband chipset, providing WiFi communication via a first antenna 602.

The access point 600 further includes a micro controller 603 (or processor, e.g. in form of a CPU) to interface with the WiFi device 601 and to control the WiFi device 601. In addition to this, the micro controller 603 interfaces with an ADC (analog-to-digital conversion) and FPGA block 604. The ADC and FPGA block 604 interfaces with a RF front end 605 (e.g. implementing a 2 Stage LNA) to receive an incoming RF carrier signal related to WiFi (i.e. according to the IEEE 802.11 standard) via a second antenna 606.

Alternatively, the ADC and FPGA block 604 could also tap the RF carrier signal from the WiFi device 601 instead of using a separate input block (i.e. the RF front end 605) and a separate antenna. In such a configuration, a single antenna can be shared between the WiFi device 601 and the RF front end 605.

The WiFi device 601 (in other words the WiFi interface) is used for transmission and reception of messages according to IEEE 802.11 (also referred to as WiFi messages). The RF front end 605 is used for reception of WiFi messages and is used to process the time of arrival (TOA) of the RF carrier signal used for the transmission of the WiFi messages. The ADC and FPGA block 604 is used for the purpose of finding the time of arrival of the RF carrier signal, i.e. the time of arrival of the WiFi messages.

The RF front end 605 is also used to achieve proper gain control of the incoming RF carrier signal. The ADC and FPGA block 604 interfaces with the WiFi device 601 to tap some signals such as the $T/\overline{R}$ Pin (TX signal), control the power amplifier, derive the message (or frame) type, etc. The micro-controller 603 interfaces with the ADC and FPGA block 604 to control the localization operation and also receive the sampled TOA signal information.

According to one embodiment, a time difference of arrival procedure is used that makes use of the 4-way handshake protocol as explained with reference to figure 3.

Figure 7 shows the 4-way handshake message exchange used for triangulation according to one embodiment in the communication arrangement 500 of figure 5.

The message (or frame) exchange is carried out between a mobile terminal 701, LAPs 702 and a MAP 703 corresponding to the mobile terminal 501, the LAP 502 and the MAP 503 of the communication arrangement 500.

As mentioned in context of figure 5, at least one MAP 703 helps to provide triangulation for the mobile terminal 701 (or mobile station (MS)). The MAP 703 plays the role of the Master Localization AP. However, other APs 702 can also take turns to act as MAP.

The embodiment described in the following can be implemented without changes to the WiFi hardware and software residing in the mobile terminal 701 (assuming a typical WiFi support by the mobile terminal 701). The mobile terminal 701 just needs to use a standard 4-way handshake with the LAPs 702 and the MAP 703 to achieve the localization.

The LAPs 702 and the MAP 703 are configured with the same MAC (Medium Access Control) address when the localization process (triangulation process) is carried out. Although for the purpose of localization process the MAC address is set to be the same, the LAPs 702 and the MAP 703 can also change their MAC address to a unique address to communicate normally with other devices.

Figure 8 shows a message flow diagram 800 illustrating a 4-way handshake message exchange used for a localization process according to one embodiment.

The message exchange takes place between a mobile station 801, a MAP 802 and, in this example, two LAPs 803, 804 corresponding to the mobile terminal 701, the MAP 703 and two of the LAPs 702.

The 4-way handshake message exchange includes the mobile station 801 sending an RTS message 805, the MAP 802 responding with a CTS message 806, the mobile station 801 sending a data message 807 and the MAP 802 responding with an ACK message 808 as explained with reference to figure 3.

Thus, the 4-way handshake process can actually be seen to take place between the mobile station 801 and the MAP 802 but the LAPs 803, 804 also react to the 4-way handshake since they have the same MAC address as the MAP 802.

The transmission of the RTS message and the data message to the LAPs is illustrated in figure 7 by means of first solid arrows 704. The transmission of the CTS message and the ACK message from the MAP 703 to the mobile station 701 is illustrated by means of second solid arrows 705. Dashed arrows 706 indicate the overhearing of the CTS message and the ACK message by the LAPs 702.

The localization process starts when the mobile station 801 sends the RTS message (or frame) 805 to the MAP 802 and the LAPs 803, 804 (due to the same MAC address). The MAP 802 and the LAPs 803, 804 receive and process the frame because these devices share the same MAC address. The WiFi baseband chipsets in the LAPs 803, 804 and the MAP 802 then process the RTS message and reply with a CTS message. However, the transmitters of the LAPs 803, 804 are muted such that the CTS frame from the LAPs 803, 804 are suppressed from being sent out and only the CTS message 806 of the MAP 802 is transmitted to the mobile station 801. This can be achieved by, for example, switching off the power amplifier of the LAPs 803, 804 during transmission or by other software/firmware or hardware means.

When the mobile station 801 receives the CTS message 806 from the mobile station 802, it processes it and sends out the data message (data frame) 807. The data frame 807 is received by the LAPs 803, 804 and the MAP 802 because their MAC address matches the destination MAC address in the data frame. The WiFi baseband chipset in the LAPs 803, 804 and the MAP 802 then processes the data frame and replies with an ACK frame.

However, the transmitters of the LAPs 803, 804 are again muted such that the ACK frames from LAPs 803, 804 are suppressed from being sent out. This can be achieved by, for example, switching off the power amplifier during transmission or by other software/firmware or hardware suppression means. The ACK frame 808 from the MAP 802 is allowed to be transmitted through the RF interface of its Wifi device 601 to the mobile station 801 to complete the 4-way handshake process. When the MAP 801 sends out the ACK frame 808 with the mobile station's destination MAC address, it is also overheard and processed by the neighbouring LAPs 803, 804. This processing is not carried out by the WiFi device 601 but by the ADC and FPGA block 604. This processing includes measuring the time of arrival of the ACK frame 808 at the respective LAP 803, 804 and is used by the LAP 803, 804 for MAP/LAPs time synchronizing purposes in the Time Difference of Arrival (TDOA) calculation.

The timestamp measuring at the MAP 801 is illustrated in figure 9.

Figure 9 shows a message flow diagram 900.

The message flow diagram 900 corresponds to the message flow of figure 8 and thus includes the exchange of an RTS message 905, a CTS message 906, a data message 907 and an ACK message 908 between a mobile station 901, a MAP 902 and LAPs 903, 904.

The ADC and FPGA block 604 of the MAP 901 measures and records two timestamps. The first timestamp 909 is the arrival of the data message 907 at the MAP 901. The second timestamp 910 is the TX pin activation of the WIFI baseband chipset of the MAP 901. Alternative to the TX pin activation, the second timestamp 910 can be recorded based on the beginning of the transmission of the ACK frame 908 by the

MAP. To help the ADC and FPGA block 604 of the MAP 901 to sample the incoming signal at the right time, the TX pin activation during the CTS frame preparation 911 may be used. Due to the fixed CTS frame size, the ADC and FPGA block 604 can use a rough offset to start sampling the incoming data message 907 at the correct time.

The timestamp measurement of an incoming signal (i.e. the data message 907 in this case) can be done by the ADC and FPGA block 604 using a high speed counter (for example a 1 GHz counter). This counter is free running the MAP 902. The counter is first started when the data frame 907 arrives. The counter can then be stopped at the start of the TX pin activation 910 due to ACK frame preparation or at the start of the ACK frame reception measured by the ADC/FPGA block 604.

The timestamp measuring at the LAPs 803, 804 is illustrated for the first LAP 803 as an example in figure 10.

Figure 10 shows a message flow diagram 1000.

The message flow diagram 1000 corresponds to the message flow of figure 8 and thus includes the exchange of an RTS message 1005, a CTS message 1006, a data message 1007 and an ACK message 1008 between a mobile station 1001, a MAP 1002 and LAPs 1003, 1004.

The ADC/FPGA block 604 of the LAP 803 measures the time of arrival of the data frame 1007 as a first time stamp. Similar to the MAP 1002, the measurement can be done using a high speed counter (for example a 1 GHz counter). These counters are free running in all LAPs 1003, 1004 and are unsynchronized to each other and to the one of the MAP 1002. The counter is first started when the data frame 1006 arrives. Once the data frame 1007 is read by the LAP's WIFI device 601, the LAP's WIFI device 601 prepares an ACK frame to send to the mobile station 1001. However, the ACK frame is suppressed from being transmitted. This operation is for example controlled by the ADC and FGPA block 604 or the WIFI interface driver. The time of arrival of the ACK frame 1008 that is transmitted from the MAP 1002 is measured by the LAP's ADC and FPGA block 604 as a second timestamp 1010. The time of arrival of this ACK frame is used to stop the counter and is used to back calculate the estimated synchronized time with the MAP 1002.

To allow distance of arrival localization a time synchronization between the APs 502, 503 is used. For this, it is assumed that the distance between the LAPs 502 and the MAP 503 are known prior to the localization process. Further, it is assumed that the LAPs 502 and the MAP 503 are static (i.e. do not change their position).

Since the TX pin trigger time (second MAP time stamp 910) at the MAP 503 and the time of arrival of the ACK frame 1006 at the LAPs 502, 503 (second LAP time stamp 1010) are consistent (i.e. it's the same up to a difference which can be determined from the known distance between the MAP and the LAPs) these time measurements can be used to synchronize the counters of the LAPs 502 and the MAP 503. (It should be noted that the MAP 503 can also measure the arrival time of its own ACK message instead of observing its TX pin time.)

Basically, by subtracting the known propagation delay between a LAP 502 and the MAP 503 the counters (clocks) of the LAP

502 and the MAP 503 can be synchronized. Thus, synchronized times of arrival of the data frame 1106 at the MAP 1102 and the LAPs 1103, 1104 can be obtained from which the mobile station's position can be determined by means of triangulation. For example, the LAPs 1103, 1104 report the times of arrival of the data frame 1106 which they have measured to the MAP 1102 which performs the triangulation and reports the localization result to the mobile station 1101.

Alternatively, the MAP 1102 and the LAPs 1103, 1104 report the times of arrival of the data frame 1106 which they have measured to the mobile station 1101 and the mobile station 1102 performs the triangulation itself.

The triggering for the ADC sampling at the LAPs 502 and the MAP 503 is illustrated in figure 11.

Figure 11 shows a message flow diagram 1100.

The message flow diagram 1100 corresponds to the message flow of figure 8 and thus includes the exchange of an RTS message 1105, a CTS message 1106, a data message 1107 and an ACK message 1108 between a mobile station 1101, a MAP 1102 and LAPs 1103, 1104.

The TX pin at the MAP 1102 and at the LAPs 1103, 1104 is triggered when the RTS frame arrives at the MAP 1102 and the LAPs 1103, 1104 and when the respective CTS message is prepared to be sent back to the mobile station 1101. This TX pin activation is then used by the FPGA and ADC block 604 of the respective MAP 1102 or LAP 1103, 1104. Based on the 4-way handshake protocol, the data frame 1107 from the mobile station 1101 can be estimated to arrive at the MAP 1102 and the LAPs 1103, 1104 after some period. The time can also be estimated based on prior 4-way handshake operations between the mobile station 1101 and the MAP 1102 and the LAPs 1103, 1104. ADC sampling at a MAP 1102 or LAP 1103, 1104 is performed just before the data frame 1107 arrives at the respective MAP 1102 or LAP 1103, 1104. Once the samples are obtained, the samples are passed to the FPGA for processing. If the DATA frame size is kept constant, the ADC and FPGA block 604 of a LAP 502, 503 can also estimate the arrival time of the ACK frame 1106 from the MAP 902.

Claims

1. A method for localization of a mobile communication device comprising:
transmitting a data message from the mobile communication device to a first access point;
receiving the data message at the first access point and at second access points;
determining the reception times of the data message at the first access point and at the second access points;
transmitting an acknowledgement message for the data message from the first access point to the mobile communication device;
receiving the acknowledgement message at the second access points;
determining the reception times of the acknowledgement message at the second access points; and
determining the position of the mobile communication device based on the determined reception times of the data message and the determined reception times of the acknowledgement message.

2. The method according to claim 1, wherein determining the position of the mobile communication device includes compensating timer offsets between the first access point and the second access points in the determined reception times of the data message based on the determined reception times of the acknowledgement message.

3. The method according to claim 2, further including the first access point determining a sending time of the acknowledgement message and compensating timer offsets

based on the determined reception times of the acknowledgement message and the determined sending time.

4. The method according to any one of claims 1 to 3, wherein determining the position of the mobile communication device includes determining the position of the mobile communication device by a triangulation based on the determined reception times of the data message.

5. The method according to any one of claims 1 to 4, wherein the first access point and the second access points are access points of a wireless local area network.

6. The method according to any one of claims 1 to 5, further comprising assigning the same data link layer address to the first access point and the second access points and addressing the data message to the address.

7. The method according to claim 6, further comprising suppressing acknowledgement messages generated by the second access points in response to the data message.

8. The method according to any one of claims 1 to 7, wherein the data message and the acknowledgement message are part of a handshake process for data transmission from the mobile communication device to the first access point.

9. The method according to claim 8, wherein the handshake process is a 2-way handshake process or a 4-way handshake process.

10. The method according to claim 1, wherein the handshake process is a 4-way handshake process and further includes, as part of the 4-way handshake process, sending a request to send message from the mobile communication device to the first access point and sending a clear to send message from the first access point to the mobile communication device.

11. The method according to claim 10, further comprising assigning the same data link layer address to the first access point and the second access points and addressing the request to send message to the address and further comprising suppressing clear to send messages generated by the second access points in response to the request to send message.

12. The method according to any one of claims 9 or 11, wherein the handshake process is a 4-way handshake process according to IEEE 802.11.

13. The method according to any one of claims 1 to 12, wherein the mobile communication device is a mobile terminal.

14. The method according to any one of claims 1 to 13, wherein the access points are WiFi access points and the mobile terminal is a WiFi client device.

15. The method according to any one of claims 1 to 14, wherein the second access points are two or more access points.

16. A positioning device for localization of a mobile communication device comprising:

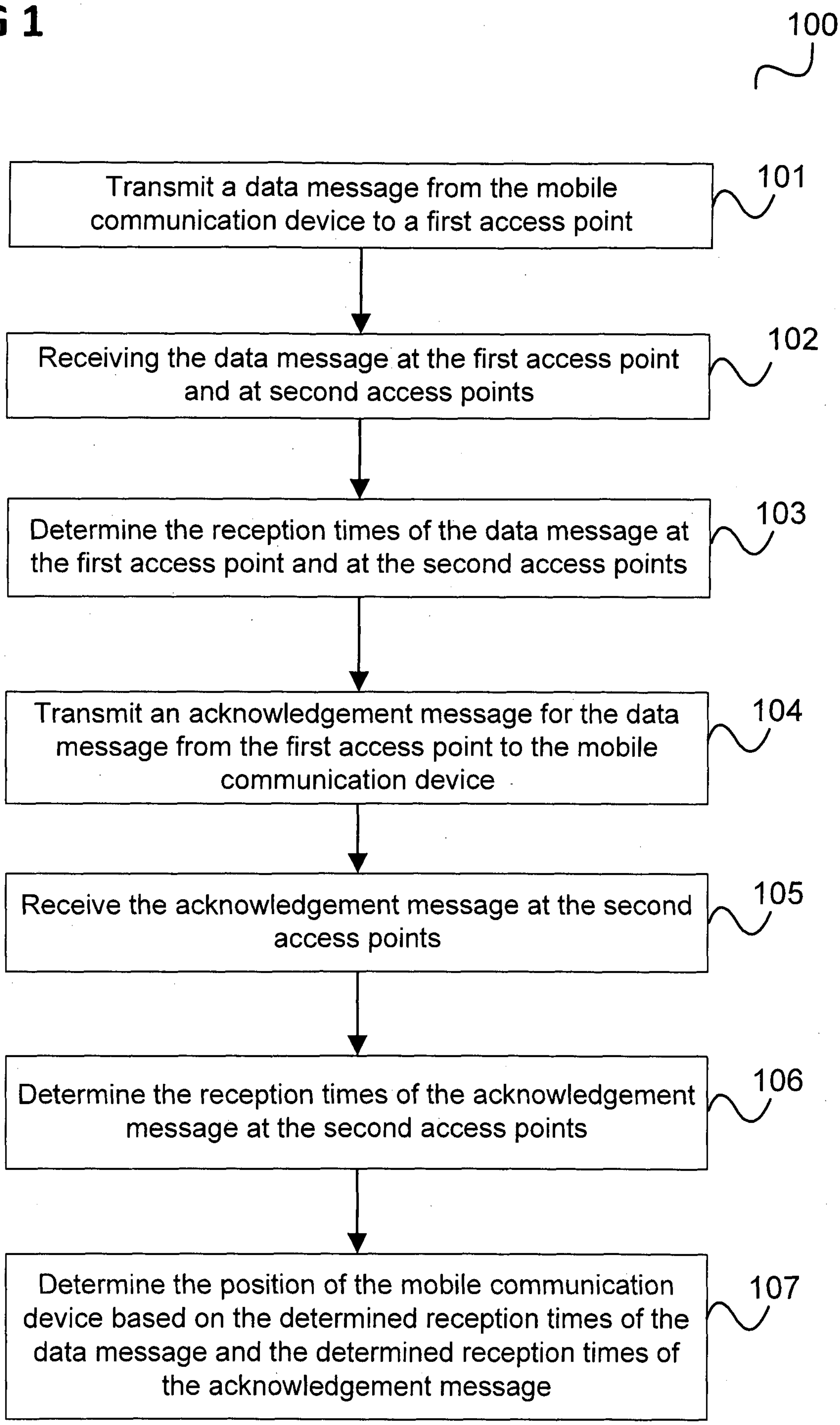
a determiner configured to

determine the reception times of a data message, sent by a mobile communication device to a first access point, at the first access point and at second access points; and

determine the reception times of an acknowledgement message, sent by the first access point to the mobile communication device, at the second access points; and

a processor configured to determine the position of the mobile communication device based on the determined reception times of the data message and the determined reception times of the acknowledgement message.

FIG 1


100
Transmit a data message from the mobile communication device to a first access point
101
Receiving the data message at the first access point and at second access points
102
Determine the reception times of the data message at the first access point and at the second access points
103
Transmit an acknowledgement message for the data message from the first access point to the mobile communication device
104
Receive the acknowledgement message at the second access points
105
Determine the reception times of the acknowledgement message at the second access points
106
Determine the position of the mobile communication device based on the determined reception times of the data message and the determined reception times of the acknowledgement message
107

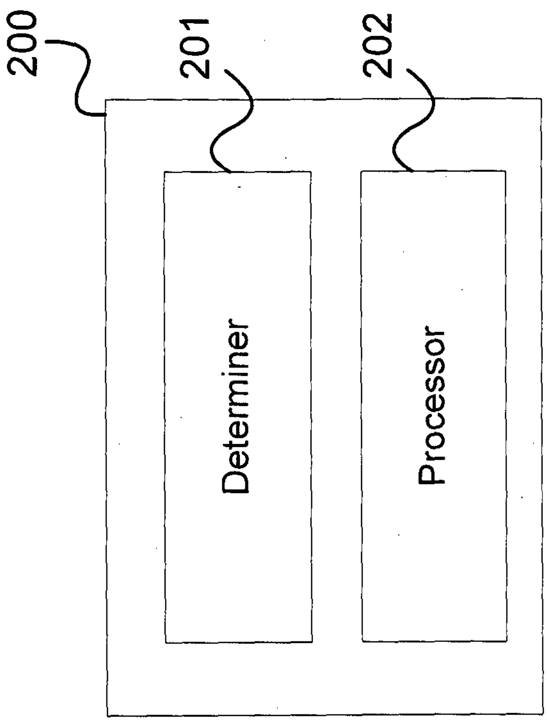
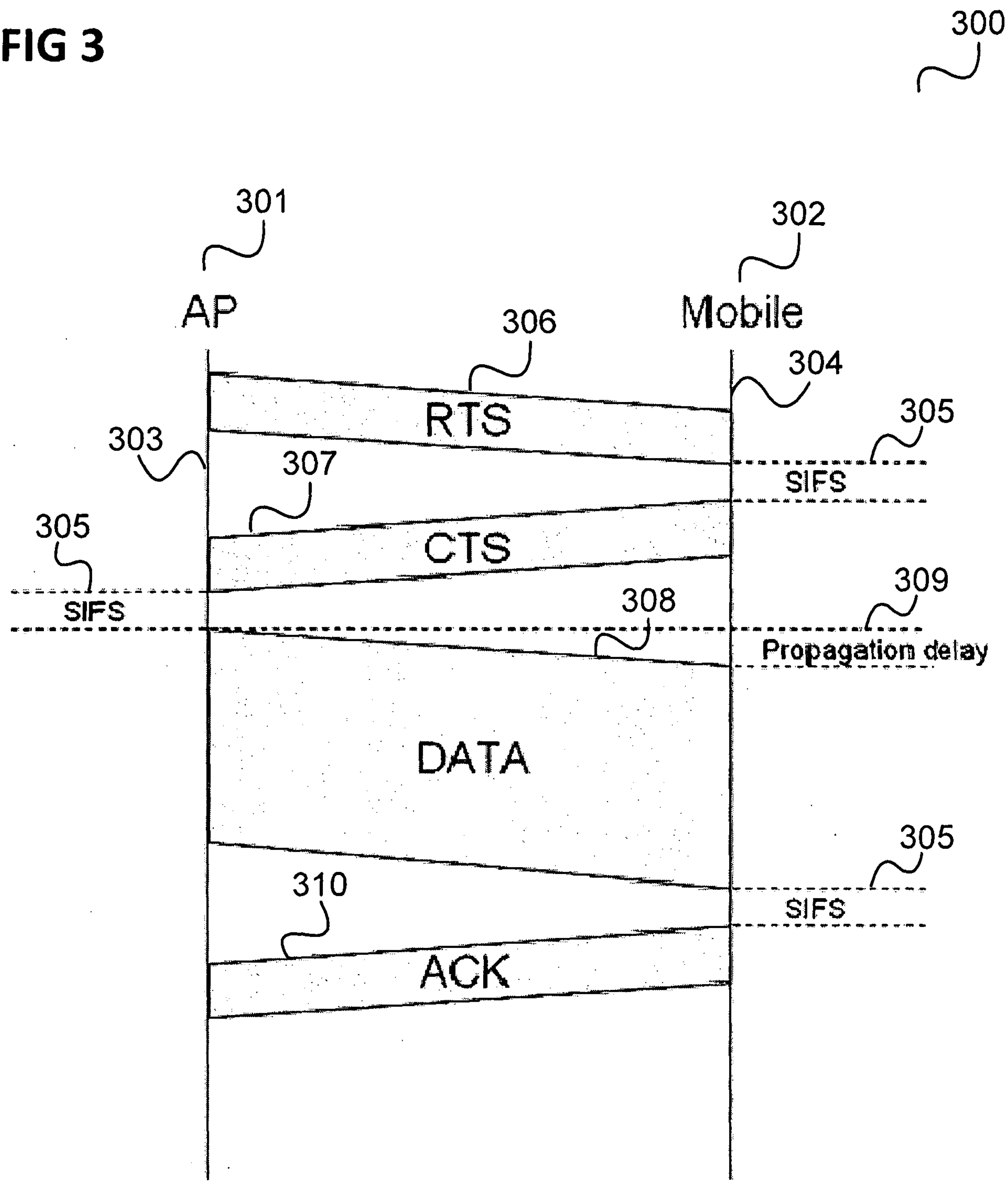


FIG 2

FIG 3


300
301
AP
302
Mobile
306
304
RTS
303
305
307
SIFS
305
CTS
SIFS
308
309
Propagation delay
DATA
305
310
SIFS
ACK

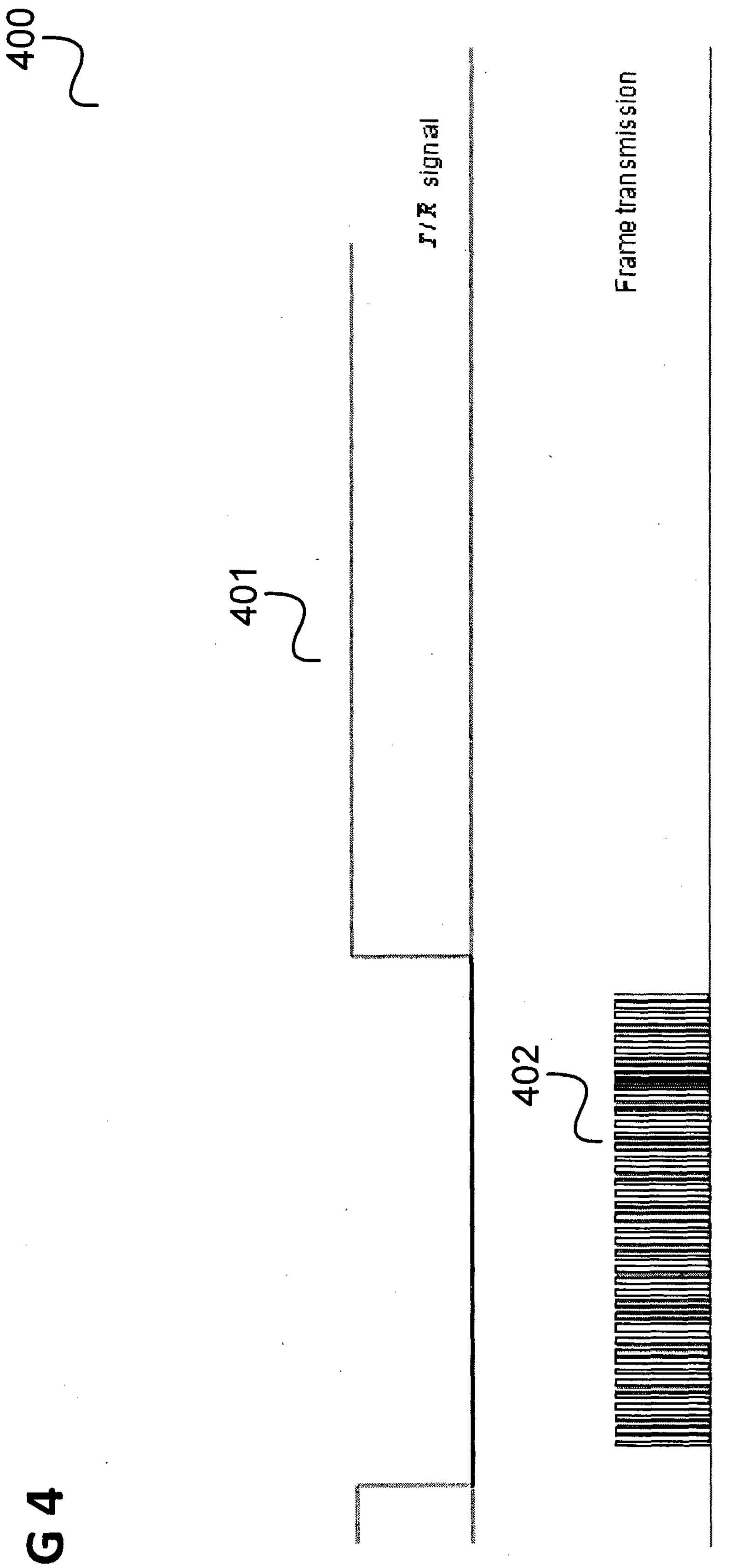


FIG 4

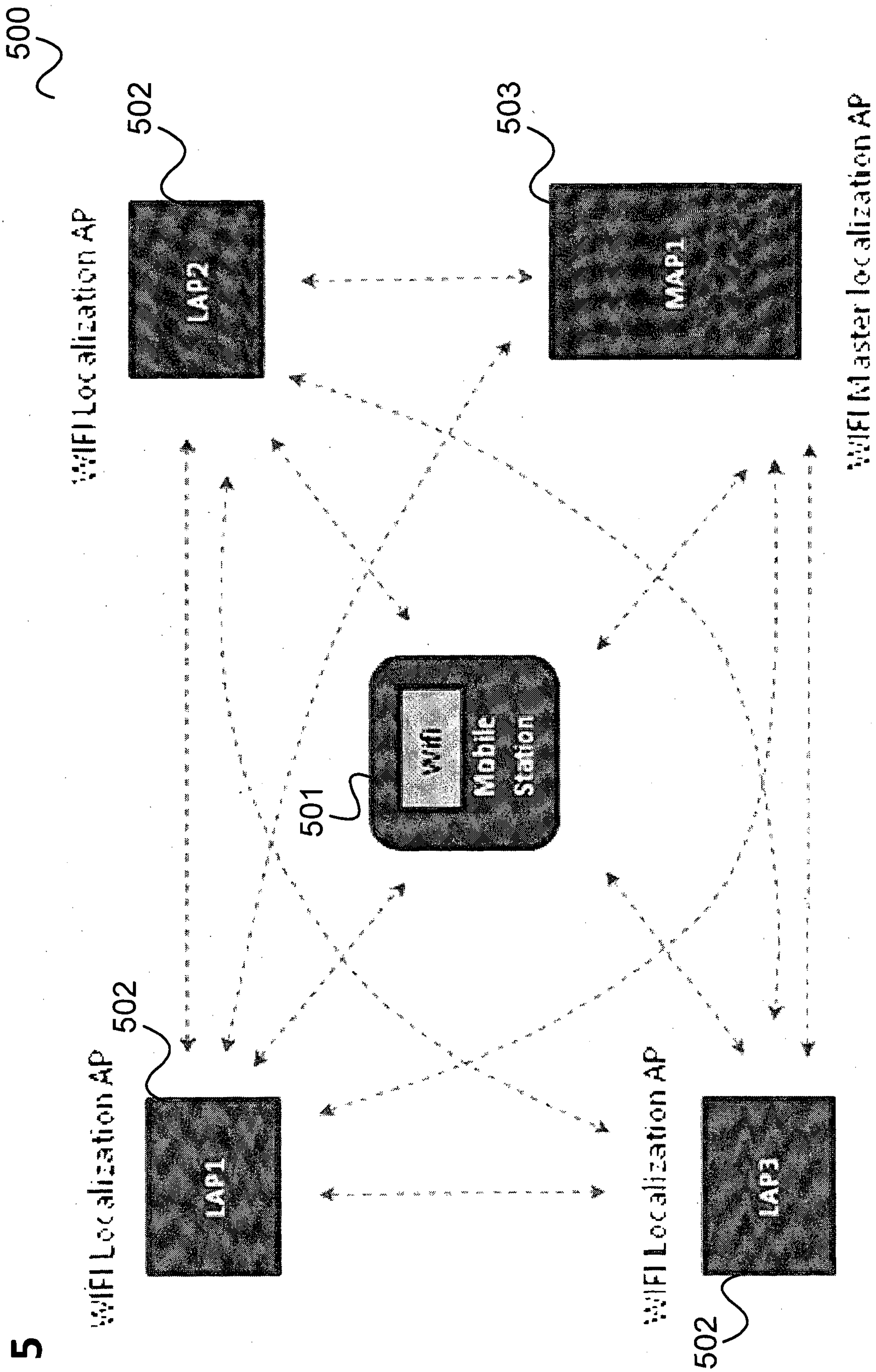
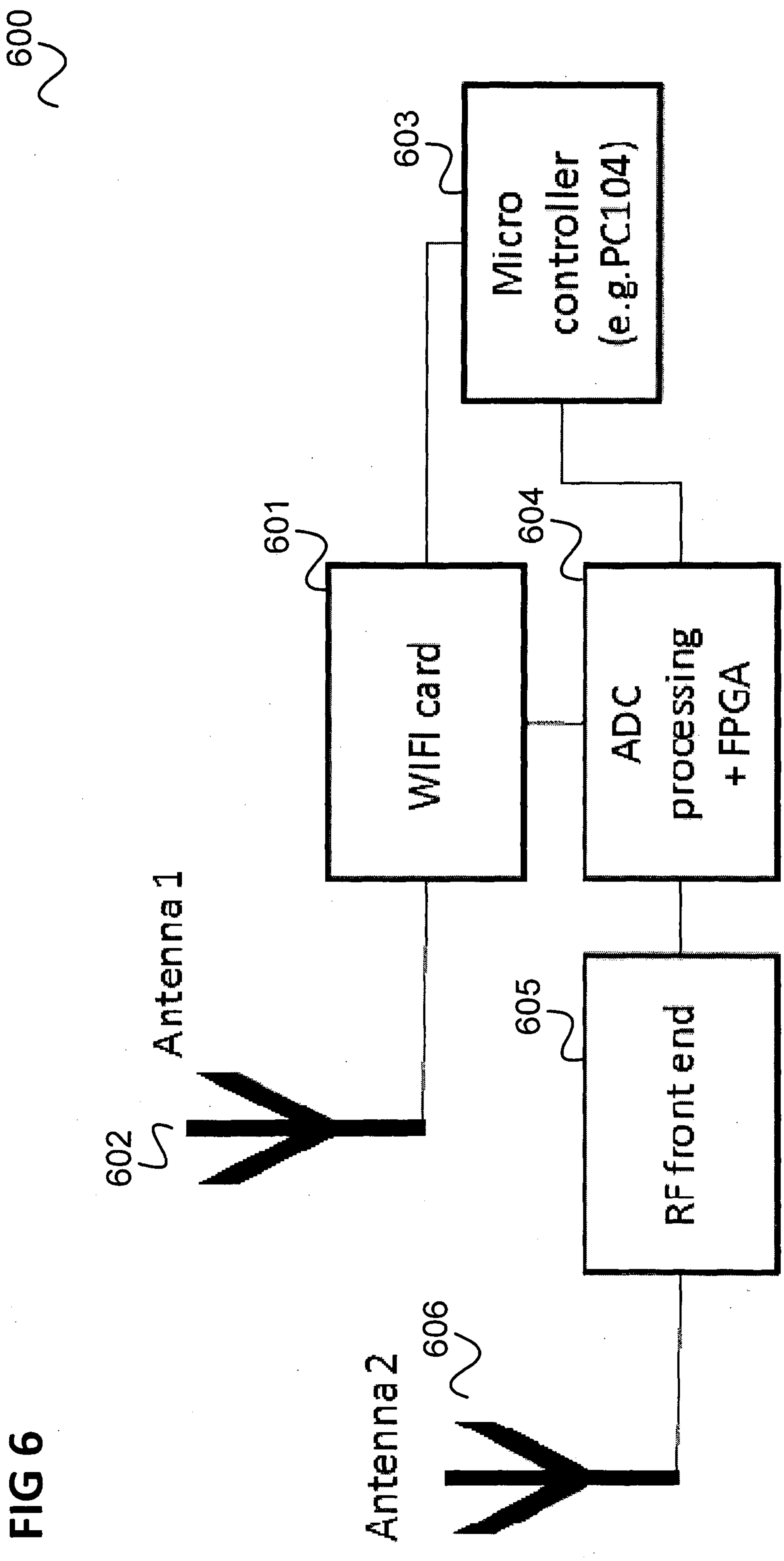

500
502
WIFI Localization AP
LAP2
503
MAP1
WIFI Master localization AP
Wifi
Mobile
Station
501
502
WIFI Localization AP
LAP1
WIFI Localization AP
LAP3
502

FIG 5

FIG 6


600
603
Micro controller (e.g.PC104)
601
WIFI card
604
ADC processing + FPGA
605
RF front end
Antenna 1
602
Antenna 2
606

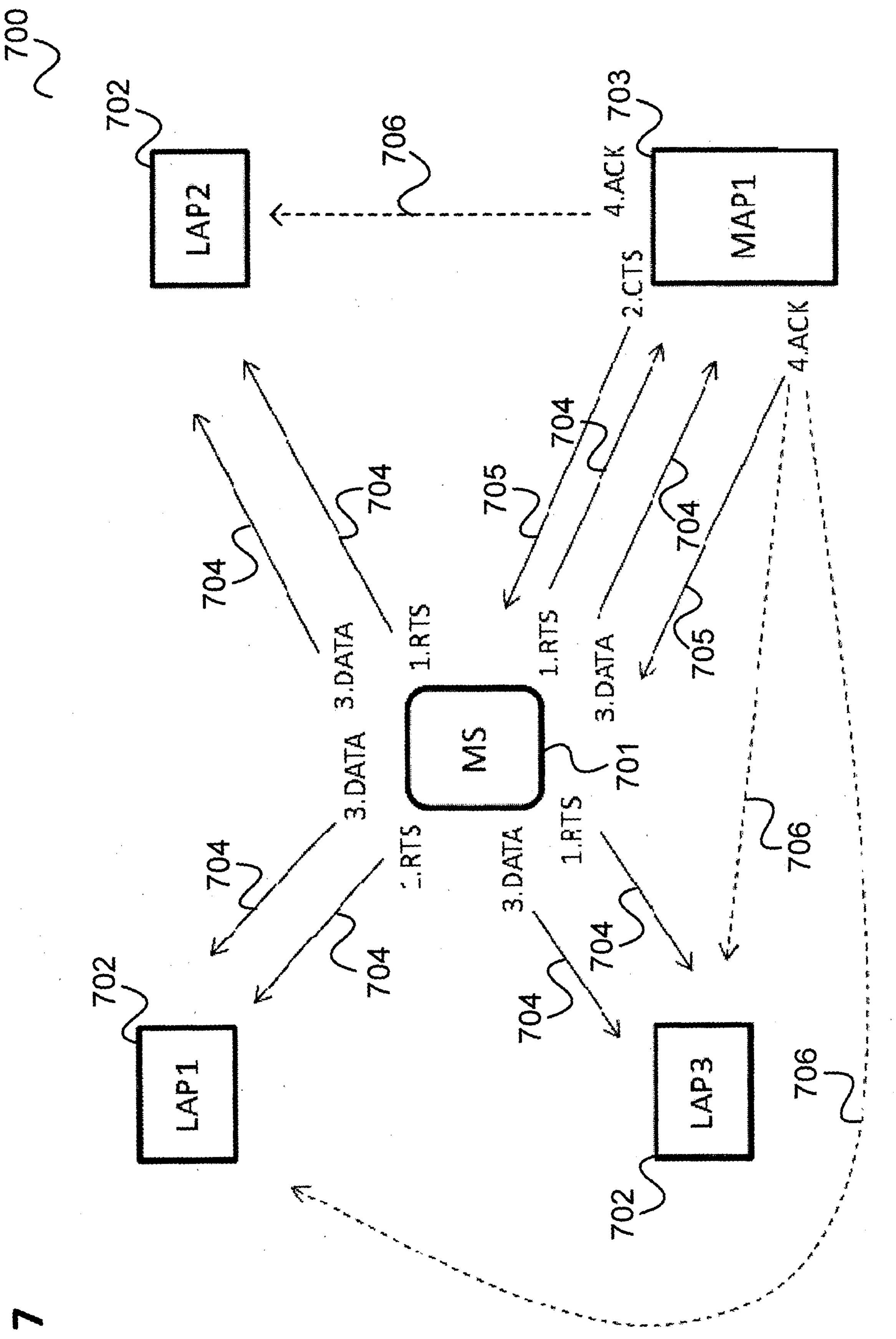
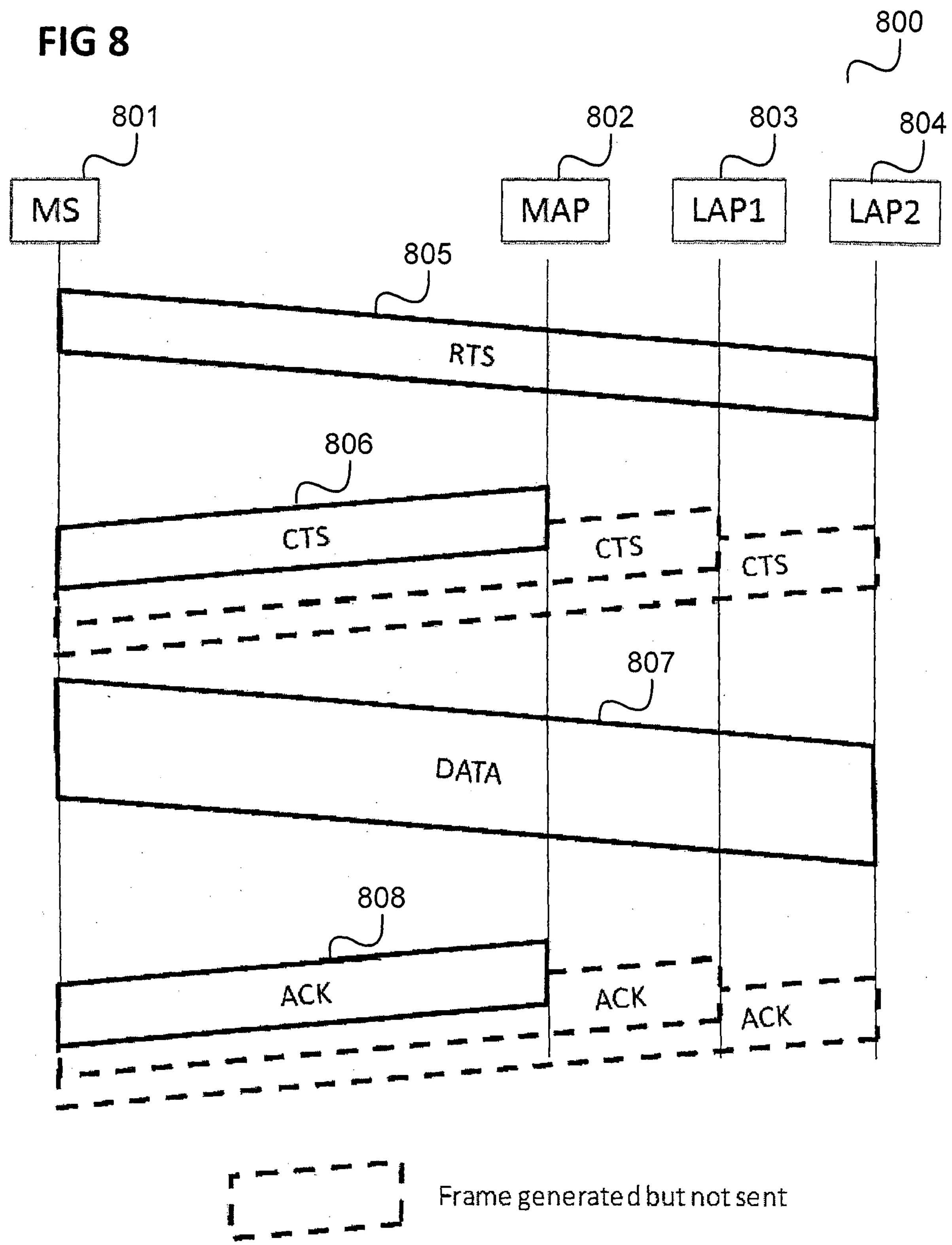

700
702
LAP2
706
4.ACK
703
MAP1
2.CTS
4.ACK
704
705
704
704
704
705
1.RTS
3.DATA
1.RTS
3.DATA
MS
701
3.DATA
3.DATA
1.RTS
706
704
704
704
704
702
LAP1
LAP3
702
706

FIG 7

FIG 8


800
801
802
803
804
MS
MAP
LAP1
LAP2
805
RTS
806
CTS
CTS
CTS
807
DATA
808
ACK
ACK
ACK
Frame generated but not sent

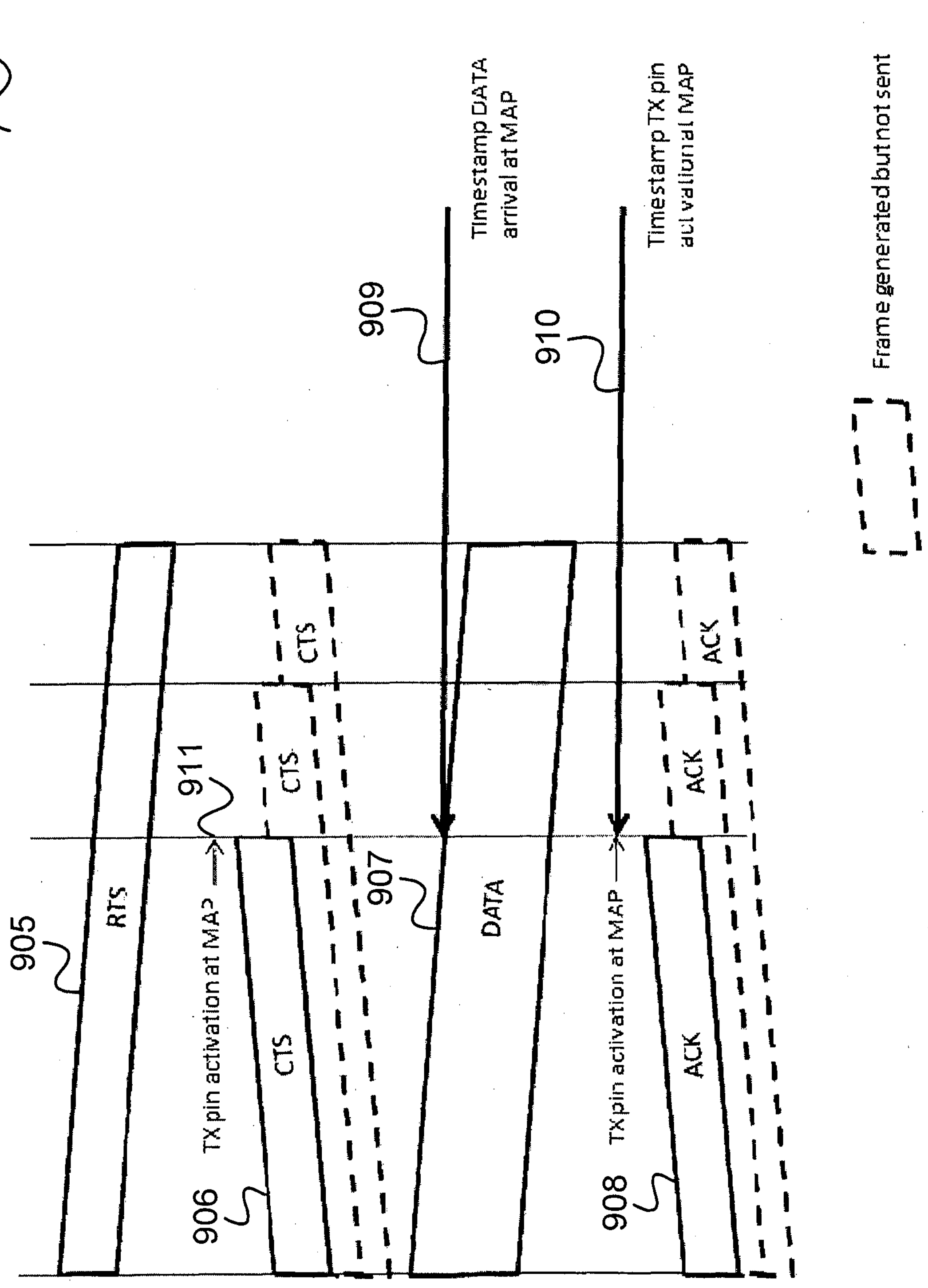

900
901
MS
902
MAP
903
LAP1
904
LAP2
905
RTS
906
CTS
CTS
CTS
907
DATA
908
ACK
ACK
ACK
909
910
911
TX pin activation at MAP
TX pin activation at MAP
Timestamp DATA arrival at MAP
Timestamp TX pin activation at MAP
Frame generated but not sent

FIG 9

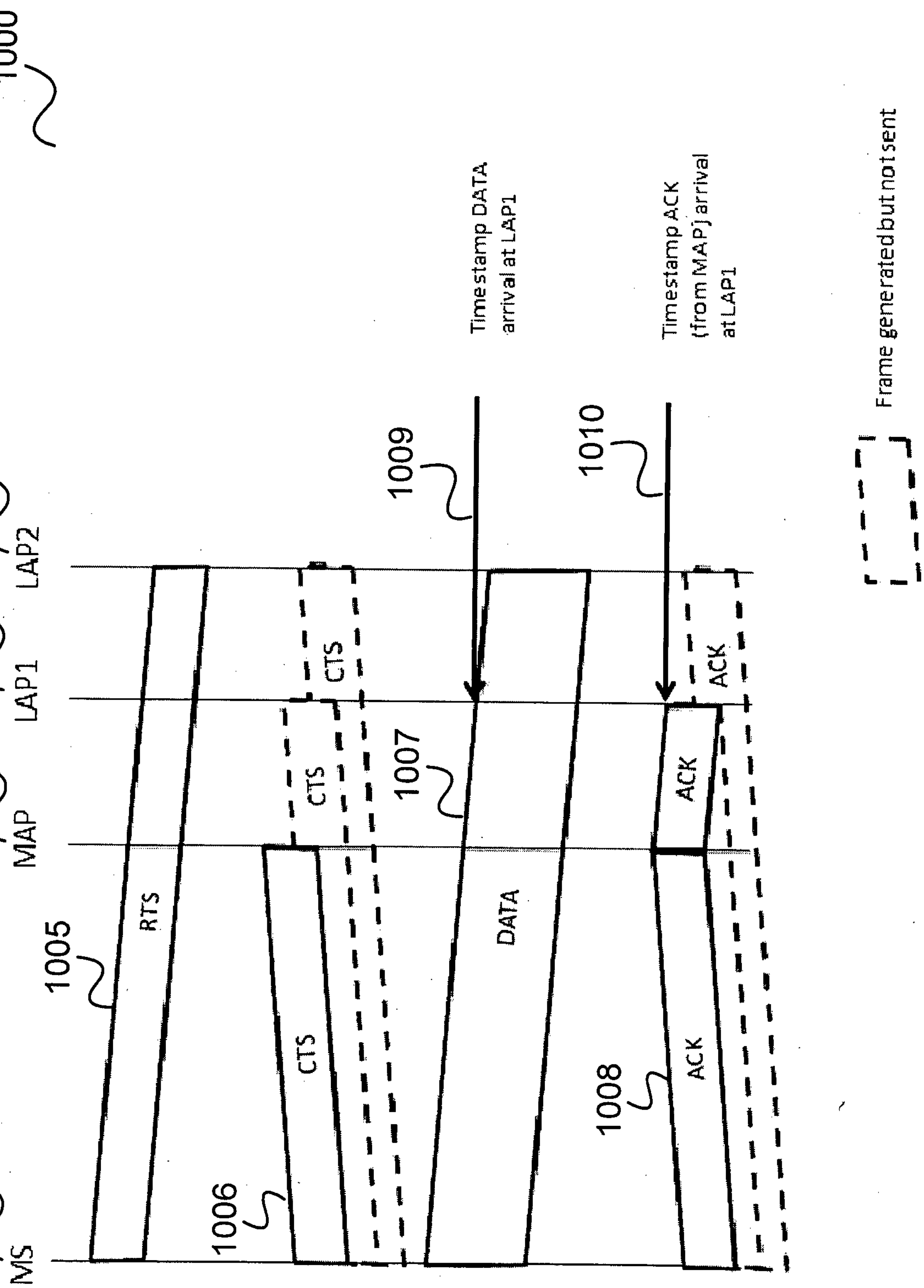
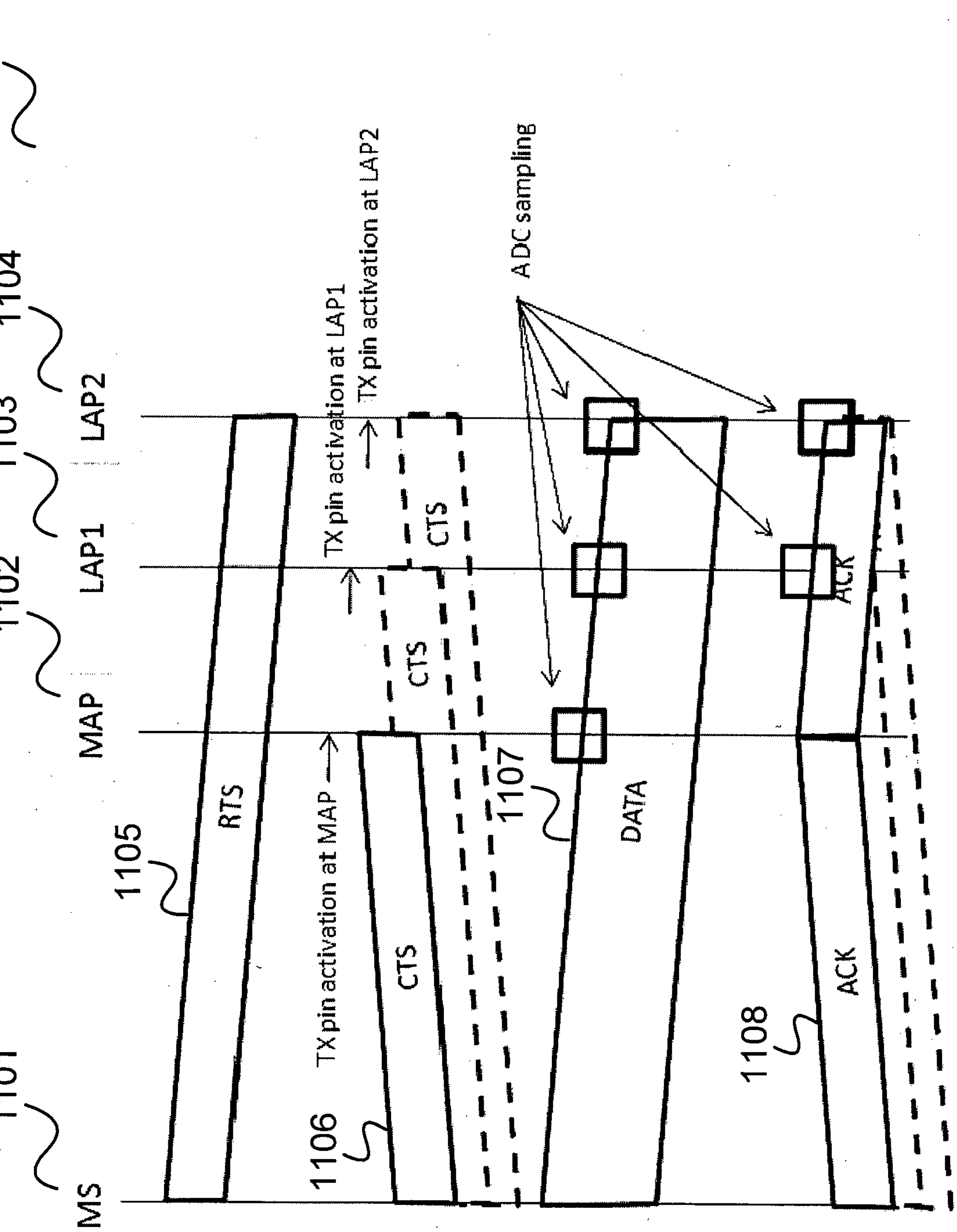

1000
MS
1001
MAP
1002
LAP1
1003
LAP2
1004
RTS
1005
CTS
1006
CTS
CTS
DATA
1007
ACK
1008
ACK
ACK
1009
Timestamp DATA arrival at LAP1
1010
Timestamp ACK (from MAPj arrival at LAP1
Frame generated but not sent

FIG 10

FIG 11


1100
1101
1102
1103
1104
MS
MAP
LAP1
LAP2
TX pin activation at MAP
TX pin activation at LAP1
TX pin activation at LAP2
ADC sampling
1105
RTS
1106
CTS
CTS
CTS
1107
DATA
1108
ACK
ACK

INTERNATIONAL SEARCH REPORT	International application No. **PCT/SG2014/000353**

A. CLASSIFICATION OF SUBJECT MATTER

H04W 64/00 (2009.01) H04W 4/02 (2009.01) H04W 24/00 (2009.01) H04L 29/08 (2006.01)

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)

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

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

EPODOC, WPI, INSPEC, GOOGLE and GOOGLE PATENTS: Keywords (mobile device, localization, transmit, message, plurality, access point, receive, time of arrival, acknowledgement, triangulation, hand_shake) and like terms.

The LENS: Invention title (Method and positioning device for localization of a mobile communication device), Inventor's name (SHANKAR, Jaya; SHARMA, Pankaj) and applicant's name (Agency for science, technology and research) searched.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C   [X] 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	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
8 September 2014	08 September 2014
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	**Authorised officer** Nidhal Odeh AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0262832498

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2011/0183683 A1 (DAS et al.) 28 July 2011 See whole document, in particular: Title; Abstract; Paras. 5, 12-25, 28, 30-33, 39-49, 57; Figs. 1-5.	1-16

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/SG2014/000353**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2011/0183683 A1	28 July 2011	US 8457657 B2	04 Jun 2013
		TW 201208430 A	16 Feb 2012
		WO 2011091297 A1	28 Jul 2011

End of Annex