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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 September 2015 (11.09.2015) WIPO | PCT

(10) International Publication Number
WO 2015/132362 A1

[Continued on next page]

(54) Title: DETERMINATION METHOD AND CORRESPONDING TERMINAL, COMPUTER PROGRAM PRODUCT AND STORAGE MEDIUM
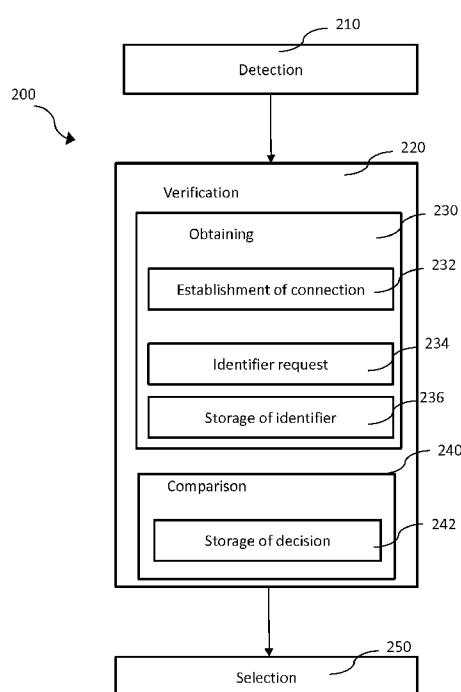
(57) Abstract: The present disclosure relates to a method for determining (200) an access point to be used by a communication terminal for accessing a wireless communication network. According to the present disclosure, the method comprises a detection of at least one access point by the terminal, a verification of the belonging to the local network of at least one of the detected access points and a selection of the access point to be used from among the detected access points verified as belonging to the communication network.

Figure 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

Determination method and corresponding terminal, computer program product and storage medium

1. Field of the present disclosure

The field of the present disclosure relates to communication networks, notably to local networks such as home networks, and to their access by wireless terminals.

A determination method for determining an access point to be used by a communication terminal for accessing a wireless communication network, and a corresponding communication terminal are described. In particular, the disclosed method and communication terminal can relate to a wireless communication network using a standard wireless communication protocol, such as the WIFI protocol.

2. Prior art

A communication network is often accessible, for a wireless terminal, from several access points. For example, in a local network, an access point to the home network can be present in a gateway device for interconnection with a remote network. Access points to the local network can also be present in several local devices, thus playing the role of repeaters (for example a device of "WIFI extender" type in the case of a network of WIFI type). It may for example involve local mobile devices such as a smartphone, or a tablet, or a decoder (or set-top box).

Moreover, in addition to giving access to the broadband network to the terminals which are members of a local network, a gateway device can often give access to the broadband network to which it is connected to devices external to the local network. It thus has two distinct identifiers: a private identifier (for example an identifier of private SSID type) reserved for the terminals which are members of the local network and a public identifier (for example an identifier of public SSID type), accessible to terminals which are members of the broadband network, even if they are not members of the local network. It can therefore be seen by other terminals of the local network as two different access points.

A terminal of a wireless network can detect the presence of several access points. It may involve access points in its neighborhood not belonging to its network or access points to its network.

As a result, when a terminal performs a search of the access points to a wireless network present in its neighborhood, it may detect several access points.

Moreover, the access points can vary over time (for example because some correspond to a mobile terminal) or according to the location of the terminal.

Currently, the user of a communication terminal is obliged to select himself, manually, the access point to be used for the connection of his terminal to the network. This selection is made especially difficult and tedious as the number of access points detected is large and the naming of the access points is unclear for the user. Finally, the association of a terminal with an access point can also be dependent on the prior entry of access keys (login and password for example).

3.   Summary.

The present disclosure makes it possible to improve the situation by proposing an easier and quicker method for a user of a terminal than the solutions of the prior art.

More specifically, the present disclosure relates to a method for determining an access point to be used by a communication terminal for accessing a wireless communication network.

According to the present disclosure, the determination method comprises:

- a detection of at least one access point by said terminal;
- a verification of the belonging to said network of at least one of the detected access points;
- a selection of said access point to be used from among the detected access points verified as belonging to said communication network.

In particular, in some embodiments, the selection can be done automatically by the terminal itself without interaction with the user of the terminal.

According to a particular embodiment, said verification comprises:

- an attempt to obtain an addressing identifier of said detected access point;
- when an addressing identifier is obtained, a comparison of said obtained identifier with at least one reference addressing identifier, associated with said communication network.

In particular, the present disclosure relates notably to a method for determining an access point to be used by a communication terminal for accessing a first communication network, said first network being a wireless communication network.

According to a particular embodiment, said method comprises the following steps, implemented by said terminal:

- detecting at least one access point;
- verifying a belonging to said first network of at least one of the detected access points, called access point to be verified, by taking account of a reference addressing identifier, associated with said first communication network, verifying

said belonging comprising requesting to obtain an addressing identifier, relating to a second network, of said access point to be verified;

- selecting said access point to be used from among the detected access points verified as belonging to said first communication network.

According to a particular characteristic, verifying said belonging takes account, when no addressing identifier is obtained for said access point to be verified, of a number of obtaining attempts already performed for said detected access point to be verified.

According to a particular embodiment, requesting to obtain an addressing identifier comprises:

- requesting an establishment of a connection of said terminal with said access point to be verified;

- when said connection is established, requesting a provision of said addressing identifier of said access point to be verified from a server external to said first network and accessible from said second network, by making use of said connection.

According to a particular characteristic, said obtained addressing identifier and said reference addressing identifier are public addresses on a broadband network.

According to a particular characteristic, requesting to obtain an addressing identifier further comprises storing, in said terminal, said obtained addressing identifier.

According to a particular characteristic, selecting said access point to be used takes into account a content reception performance criterion for at least one of said access points to be selected.

According to a particular embodiment, said performance criterion belongs to the group comprising:

- an average error rate;
- a maximum error rate;
- an average time without error;
- a maximum time without error;
- an average bitrate;
- a maximum bitrate.

According to a particular characteristic, selecting said access point to be used takes into account a duration of association with said terminal of at least one of said access points to be selected.

According to a particular characteristic, selecting said access point to be used takes into account a criterion of belonging to a subnetwork of said first network of at least one of said access points to be selected.

According to a particular characteristic, said belonging criterion comprises a comparison of an item of addressing information complementary to said addressing identifier of said at least one access point to be selected with a complementary reference item of addressing information.

According to a particular characteristic, said first network is a wireless communication network of Wifi type.

Although not explicitly described, the embodiments presented can be implemented using any combination or sub-combination. For example, an embodiment wherein the verification comprises, for an access point, an attempt to obtain an addressing identifier and a comparison of this addressing identifier, can be combined with an embodiment wherein the selection of the access point takes account of performance criteria and/or a duration of association with the terminal.

Other embodiments, easily conceivable by those skilled in the art on reading the present description, are also included within the scope of the present disclosure.

In particular, the present disclosure applies to any wireless network using a communication protocol known to the terminal and notably to a standard wireless communication protocol, such as the Bluetooth protocol for example or the WIFI protocol in the case of a local network.

According to another aspect, the present disclosure relates to a communication terminal, comprising at least one processor configured to determine an access point to be used to access a first communication network, said first network being a wireless communication network.

According to the present disclosure, said at least one processor is configured to:

- detect at least one access point accessible from said terminal ;
- verify the belonging to said first network of at least one of the detected access points, called access point to be verified, by taking account of a reference addressing identifier, associated with said first communication network, verifying the belonging to said first network of said access point to be verified comprising requesting to obtain (230) an addressing identifier, relating to a second network, of said access point to be verified;

- select an access point to be used by said terminal from among the detected access points verified as belonging to said first communication network.

According to another aspect, the present disclosure relates to a computer program product. According to the present disclosure, such a computer program product comprises program code instructions for executing the above determination method, in any one of the aforementioned embodiments, when said program is executed by a computer.

According to yet another aspect, the present disclosure relates to a computer-readable storage medium on which is saved a computer program comprising program code instructions for executing the determination method of the present disclosure, in any one of the aforementioned embodiments, when said program is executed by a computer.

Such a computer-readable storage medium can take the form of a computer program product loaded onto at least one computer-readable storage medium comprising computer-readable and computer-executable program code instructions.

Thus, in the present patent application, a computer-readable storage medium is considered as being a non-transitory storage medium having the intrinsic capacity to store information and the intrinsic capacity to enable a restitution of the information which it stores. A computer-readable storage medium can be for example, but not only, a system, a device or an item of equipment which is electronic, magnetic, optical, electromagnetic or infra-red, made of semiconductors or implements a combination of the techniques previously mentioned. It should be underlined that the following elements, which provide more specific examples of computer-readable storage media to which the principles of the present disclosure can be applied, are essentially mentioned for illustrative purposes and in no case constitute an exhaustive list, as will be easily interpreted by those skilled in the art: a portable computer diskette, a hardware disc, a memory of ROM (Read Only Memory) type, an erasable memory of EPROM (Erasable Programmable Read Only Memory) type or flash memory, a portable compact disc comprising a ROM memory (CD ROM), an item of optical storage equipment, an item of magnetic storage equipment, or any suitable combination of the preceding elements.

As would be easily understandable for those skilled in the art, the aspects of the present invention can be implemented by a terminal, a method, or a computer-readable storage medium. Thus, aspects of the present invention can be implemented in certain embodiments in the form of entirely hardware components (for example an electronic component or an electronic card equipped with components), or in the form of entirely software components (including for example firmware components, a "resident" software

program, microcode, etc.). Other embodiments can implement both hardware components and software components. In the present document, the term "module" will generally designate a component which can correspond either to a hardware component or to a software component. Moreover, aspects of the present invention can be implemented in the form of a computer-readable storage medium. Any combination of one or more computer-readable storage media can be used.

4. List of figures

The present disclosure will be better understood, and other specific features and advantages will emerge upon reading the following detailed description, relating to a particular embodiment, the description making reference to the annexed drawings wherein:

- **Figure 1** shows the environment of a mobile communication terminal seeking to connect to a local network, according to a particular embodiment.

- **Figure 2** is a functional diagram showing the determination method of the present disclosure, in a particular embodiment, compatible with an implementation in the communication terminal described in relation to figure 1;

- **Figure 3** shows the determination module of a communication terminal according to a particular embodiment.

A same element is designated in all the figures by the same reference symbol.

The figures shown are for illustrative purposes only and in no case limit the present disclosure to the embodiments shown.

5. Description of embodiments

The general principle of the present disclosure consists in performing a filtering of the access points which it is possible for a terminal to select according to whether or not they belong to a determined network.

Thus, the present disclosure can make it possible notably to avoid wasting time and to avoid unnecessary consumption of power testing the performance of access points which do not allow access to the network.

In particular, some embodiments adapted notably to a mobile device can enable the terminal to automatically scan all the access points which surround it, in order to select and/or connect to the access point to the network offering, for example, the best quality in terms of performance. This is especially useful in the case of a mobile terminal, caused to be in the neighborhood of different access points while being moved.

Thus, at least one embodiment can make it possible to limit the selection of the access point to be used by a terminal to only access points belonging to the network which it

wishes to access, instead of including in the selection all the access points visible by the communication terminal. In fact, testing a connection by an access point visible to the terminal but not belonging to the network constitutes a waste of time and unnecessary consumption of power. However, minimizing power consumption is a major constraint for a mobile terminal.

At least one embodiment can make it possible to compare the access points more efficiently, since only the access points belonging to the network will be evaluated. This is especially important when the selection is performed regularly, for example because the terminal to be connected is moved, or the access points to the network vary (for example because some access points are located on a mobile terminal).

Moreover, in some embodiments, for example embodiments wherein the encryption keys for connection to an access point are stored by the terminal, and wherein the selection criteria are predefined (for example a reception performance criterion), the choice of the access point to be used can be automated and not require interaction with a user of the terminal.

Moreover, due to this automation, it may be possible, without burdening the user, to regularly test certain access points to the network, for example all the access points within its range.

The user can thus benefit at any moment from the access point whose performance is best from among the access point available in the network.

In relation to figures 1 and 2, a particular embodiment is presented in the context of a local network of WIFI type which a mobile terminal 130 wishes to access, using the determination method of the present disclosure. In the embodiment shown, the local network implements the standard communication protocol IEE 802.11 – 2012 (of 29 March 2012).

Figure 1 shows the environment of the mobile communication terminal 130. Figure 1 shows a local network of WIFI type 100, connected to a broadband network 170, for example a network of an internet access provider, by a gateway device 110, equipped with a WIFI card, having on one hand a public access point 112 and on the other hand a private access point 114 reserved for members of the local network 100. A decoder 120 (or set-top box), also equipped with a WIFI card, comprises on one hand a WIFI client, which enables it to communicate with the private access point 114 of the gateway device 110, and on the other hand a private access point 122, which enables it to play a role of repeater between the gateway device 110 and a terminal wishing to connect to the local network 100. The gateway device 110 and the decoder 120 are visible to the terminal 130.

Figure 1 also shows another local network of WIFI type 150, located in the neighbourhood of the local network 100, and accessible from a gateway device 160 having on one hand a public access point 162 and on the other hand a private access point 164 reserved for members of the local network 150. The gateway device 160 is located in the

5   coverage area of the terminal 130.

Finally, another device 140, located in the coverage area of the terminal 130, comprises a private WIFI access point 142 to a GSM (global system monitoring) network.

In the embodiment shown, where the network is a local network of WIFI type, each access point is identified by a string of alphanumeric characters, such as a SSID (service

10   set identifier). It can also be identified for example by a MAC (media access control) address, which makes it possible to guarantee a unique identification of each access point.

Figure 2 shows the determination method of the present disclosure, in a particular embodiment, implemented in the terminal 130.

According to the present disclosure, the method for determining 200 the access

15   point to be used comprises a step 210 of detection by the terminal 130 of the access points in its neighborhood.

In the particular embodiment shown in figure 1, the terminal 130 thus sees six access points:

-    The public and private access point 162 and 164 of the device 160 (giving access to the

20   network 150);

-    The public and private access point 112 and 114 of the gateway device 110 (giving access to the network 100);

-     The private access point 122 of the decoder 120;

-    The private access point 142 of the mobile terminal 140.

25   In the embodiment shown in figure 2, the method then comprises a verification 220 of the belonging of at least one of the detected access points (called access point to be verified) to the local network. This verification can for example correspond to an allocation of a particular value to a belonging indicator stored at least temporarily by the terminal, as discussed in more detail below.

30   According to the embodiments, the verification 220 can be conducted for each of the detected access points 112, 114, 162, 164, 122 and 142 or only for certain detected access points, for example for the access points detected for the first time by the terminal 130. Such an embodiment is particularly suitable when the determination method is implemented periodically by the terminal 130.

In particular, the verification 220 can comprise an obtaining 230 of an addressing identifier of the access point to be verified on a broadband network.

In the particular embodiment shown, the addressing identifier is a public IP (internet protocol) address enabling the unique designation of an interface with a network using the internet protocol. Such an address can for example be assigned by a provider of access to a broadband communication network, for example via a DHCP (dynamic host configuration protocol) server.

The gateway device 110 has two interfaces to the broadband network (a so-called "private" interface reserved for the interconnections between the broadband network and the devices of the local network, via the intermediary of the private access point 114, and an interface of "hot spot" type, that is to say which can be used by all the terminals using the services of the access provider, via the intermediary of the public access point 112). Each of the interfaces of the gateway device 110 is identified by a different public address.

Each device which uses an interface of the gateway device 110 to interface with the broadband network will be seen as having as its public addressing identifier the addressing identifier of the interface of the gateway device which it uses.

The addressing information of an access point to be verified can for example be obtained from a server external to the network, for example a remote server in the particular embodiment shown. In the embodiment shown in figure 2, the obtaining 230 of the addressing information thus comprises an establishment of a connection 232 between the terminal 130 and the access point to be verified, on the initiative of the terminal 130. This step can possibly require the provision of an encryption key, such as a WEP (wired equivalent privacy) or WAP (Wi-Fi protected access) or WAP2 key.

Thus, in the embodiment shown in figure 1, the connection of the terminal 130 with the access point 142 can fail, due to the absence of provision of a particular encryption key. In some embodiments, the failure of a connection of the terminal with an access point to be verified (for example the access point 122 of figure 1) can result in the verified access point being considered as not belonging to the local network.

When a connection is established, the terminal 130 can then communicate, via the intermediary of an access point, with devices accessible on the broadband network. As shown in figure 2, the method can thus in particular comprise an access to a server external to the network, for a request to provide 234 the addressing identifier of the access point to be verified.

For example, it may involve the transmission of a request providing in return the public IP address of the device connected to the public internet network which transmitted the request, that is to say, in the embodiment shown in figure 1, the gateway 110.

In some embodiments, as shown in figure 2, the obtaining 230 of an addressing identifier can also comprise a storage 236 of the obtained addressing identifier.

For example, it may involve a storage, in a look-up table of the terminal, of the addressing identifier (for example a public IP address in the embodiment shown) in connection with an identifier of the access point (for example a SSID identifier in the embodiment shown or a MAC address).

Such an embodiment offers the advantage of enabling a subsequent obtaining of the addressing identifier associated with an access point without interrogation of a remote server, said obtaining therefore being quicker.

The embodiment shown then comprises a comparison 240 of the addressing identifier with at least one reference addressing identifier, associated with the local network. Such a reference addressing identifier can notably be the addressing identifier of the "private" interface for interconnection between the local network 101 and the broadband network of the gateway device 110. Such an identifier can for example be entered by a user of the terminal during a prior configuration, or be obtained beforehand or dynamically by interrogation of a remote server via the intermediary of a reference access point, known to the terminal as belonging to the local network, for example the private access point 114 of the gateway device 110. It can also be obtained from the terminal by near-field communication, when the terminal 130 is brought near to a gateway device 110.

In other embodiments, a comparison 240 with several reference identifiers can be performed. This can be the case for example in network configurations where several gateway devices enable an interconnection between the network of the terminal and another network, for example a broadband network.

The comparison 240 between the addressing identifier of the access point to be verified and a reference identifier results for example in an allocation of a particular value to a belonging indicator stored at least temporarily by the terminal, as discussed in more detail below.

Thus, with reference to figure 1, the addressing identifiers of the access points 162 and 164 (relating to the interfaces of the gateway device 160 with the network 150) will be different from the reference addressing identifier associated with the access point 114.

Likewise, the addressing identifier of the "public" access point 112 to the broadband network from the gateway device 110 will also be different from this reference addressing identifier.

As a result, the addressing identifiers being different from the reference addressing identifier, the access points 112, 162, 164 will be considered as not belonging to the local network.

In some embodiments, the verification 220 of the belonging to the local network can comprise a storage 242 of the belonging decision.

Thus, it may involve a storage, in a particular table, of all the identifiers of the access points considered as belonging to the local network (for example in the form of a list of SSIDs or MAC addresses). In such an embodiment, the indicator of belonging to the network of an access point will be the presence in the stored list of the identifier relating to the access point.

It may also involve a storage in a look-up table, for each detected access point, of an item of information, coded on at least one bit, representative of the result of the belonging verification. For example, in some embodiments, it may involve an item of information coded on two bits, a first bit indicating the allocation of a significant value, relative to at least one belonging verification, to the second bit, and the second bit, constituting a belonging indicator, being representative of the result of the belonging verification. For example, a value "1" allocated to the belonging indicator can indicate a belonging to the local network and a value "0" allocated to the belonging indicator can indicate a non-belonging to the network (or vice-versa). Such an embodiment makes it possible for example to attempt to obtain again the addressing identifier of an access point when a first connection to another network, for example a wide area network in the case of the embodiment shown in figure 2, by this access point has failed.

In other embodiments, it may also involve an item of information coded on more than two bits, being able to take several particular values, for example a first, initial value indicating the absence of verification relating to the access point, a second value, indicating a belonging of the access point to the network, a third value indicating a non-belonging of the access point to the network, other values indicating a failure of connection with the access point and/or the reason for the failure (in the case of absence a particular value can be allocated to the absence of provision of a required encryption key) and/or a current number of connection attempts.

In such an embodiment, when the verification is performed periodically, or when a same verification can comprises several connection attempts with an access point to be verified, it may for example be possible to attempt several times to obtain an addressing identifier of an access point, a determined number of failures to connect to an access point resulting for example in an access point considered as not belonging to the network.

In some embodiments, it may be possible, for example via a specific request of a user of the terminal 130, to force a verification of all the access points detected by a terminal.

In the embodiment shown in figure 2, the determination method 200 also comprises a selection 250 of the access point to be used by the terminal from among the access points considered as belonging to the local network. Thus, in the embodiment shown in figure 1, the selection is performed from among the access points 114 and 122.

The selection 250 can notably take account of a performance criterion for the access points belonging to the network of the terminal, and result in the selection of the access point whose performance is best (for example the one having the lowest average error rate, or the highest average bitrate).

It can also take account of a duration of association of the terminal with the access point with which it is associated at the time of the selection, for example so as not to change access point below a minimum duration of association.

In a variant, notably when the network 100 is a private network comprising several subnetworks, for example subnetworks of LAN type, the selection of an access point may take account not only of whether the access point belongs to the network 100 but also whether it belongs to a subnetwork of the network 100. This belonging can be determined for example by comparison of a complementary addressing identifier of the access point, such as a subnet mask (notably a DHCP *(Dynamic Host Configuration Protocol)* address) with a complementary addressing identifier determined (for example the DHCP address of a configuration server of the subnetwork, stored by the terminal), so as to select preferably for example an access point belonging to a particular subnetwork, having a complementary addressing identifier identical to a stored complementary addressing identifier.

The mobile communication terminal 130 shown in figure 1 is now presented in more detail in figure 3.

Figure 3 shows diagrammatically a hardware embodiment of the communication terminal 130 of figure 1, adapted to determine an access point to be used to access a wireless communication network.

The communication terminal 130 corresponds for example to a laptop, a tablet or a smartphone.

In the embodiment shown, the communication terminal 130 comprises the following elements, connected to each other by an address and data bus 300 which also transports a clock signal:

- a microprocessor 31 (or CPU);
- a graphics card 32;
- one or more I/O (input/output) devices 34, such as for example a keyboard, a mouse, a webcam, a microphone, etc.;
- a non-volatile memory of ROM (read only memory) type 35;
- a random access memory (RAM) 36;
- a communication interface RX 37 configured for the reception of data via a wireless (for example Wifi® or Bluetooth type) connection;
- a communication interface 38 configured for the transmission of data via a wireless (for example Wifi® or Bluetooth type) connection;
- a power supply 39.

The communication terminal 130 also comprises or is connected to a display device 33 of display screen type directly connected to the graphics card 32 by a dedicated bus 330. According to a variant, a display apparatus is external to the communication terminal 130 and is connected to the device 33 by a cable transmitting the display signals. The communication terminal 130, for example the graphics card 32, comprises a means for transmission or connector (not shown in figure 3) adapted to transmit a display signal to an external display means such as for example an LCD or plasma screen or a video projector.

It is noted that the word "register" used in the description of a memory designates in each of the memories mentioned a memory zone of low capacity (some binary data) as well as a memory zone of large capacity (enabling storage of a whole program or all or part of the data representative of data calculated or to be displayed).

When switched on, the microprocessor 31 loads and executes the instructions of the program contained in a register 360 of the RAM 36, and notably the algorithms implementing the steps of the method specific to the present disclosure and described hereafter.

According to a variant, the terminal comprises several microprocessors.

According to another variant, the power supply 39 is external to the device 6.

In particular the microprocessor is configured to determine an access point to be used to access a first communication network, said first network being a wireless communication network.

In the embodiment shown in figure 3, the microprocessor 31 can in particular be configured to:

- detect at least one access point accessible from said terminal ;
- verify the belonging to said first network of at least one of the detected access points, called access point to be verified, by taking account of a reference addressing identifier, associated with said first communication network, verifying the belonging to said first network of said access point to be verified comprising requesting to obtain (230) an addressing identifier, relating to a second network, of said access point to be verified;
- select an access point to be used by said terminal from among the detected access points verified as belonging to said first communication network.

CLAIMS

1.   Method for determining (200) an access point to be used by a communication terminal for accessing a first communication network, said first network being a wireless communication network, said method being characterized in that it comprises the following steps, implemented by said terminal:

   -    detecting (210) at least one access point;

   -    verifying (220) a belonging to said first network of at least one of the detected access points, called access point to be verified, by taking account of a reference addressing identifier, associated with said first communication network, verifying said belonging comprising requesting to obtain (230) an addressing identifier, relating to a second network, of said access point to be verified;

   -    selecting (250) said access point to be used from among the detected access points verified as belonging to said first communication network.

2.   Determination method according to claim 1, characterized in that verifying said belonging takes account, when no addressing identifier is obtained for said access point to be verified, of a number of obtaining attempts already performed for said access point to be verified.

3.   Determination method according to one of claims 1 or 2 characterized in that requesting to obtain an addressing identifier (230) comprises:

   -    requesting an establishment of a connection (232) of said terminal with said access point to be verified;

   -    when said connection is established, requesting a provision (234) of said addressing identifier of said access point to be verified from a server external to said first network and accessible from said second network, by making use of said connection.

4.   Determination method according to one of claims 1 to 3 characterized in that said obtained addressing identifier and said reference addressing identifier are public addresses on a broadband network.

5.   Determination method according to any one of claims 1 to 4 characterized in that requesting to obtain an addressing identifier (230) further comprises storing (236), in said terminal, said obtained addressing identifier.

6.   Determination method according to any one of claims 1 to 5 characterized in that selecting said access point to be used (250) takes into account a content reception performance criterion for at least one of said access points to be selected.

7.   Determination method according to any one of claims 1 to 6 characterized in that said performance criterion belongs to the group comprising:
-    an average error rate;
-    a maximum error rate;
-    an average time without error;
-    a maximum time without error;
-    an average bitrate;
-    a maximum bitrate.

8.   Determination method according to any one of claims 1 to 7 characterized in that selecting said access point to be used (250) takes into account a duration of association with said terminal of at least one of said access points to be selected.

9.   Determination method according to any one of claims 1 to 8 characterized in that selecting said access point to be used takes into account a criterion of belonging to a subnetwork of said first network of at least one of said access points to be selected.

10.   Determination method according to claim 9 characterized in that said belonging criterion comprises a comparison of an item of addressing information complementary to said addressing identifier of said at least one access point to be selected with a complementary reference item of addressing information.

11.   Determination method (200) according to any one of claims 1 to 10 characterized in that said first network is a wireless communication network of Wifi type.

12. Communication terminal, comprising at least one processor configured to determine an access point to be used to access a first communication network, said first network being a wireless communication network, said at least one processor being characterized in that it is configured to:

- detect at least one access point accessible from said terminal ;

- verify the belonging to said first network of at least one of the detected access points, called access point to be verified, by taking account of a reference addressing identifier, associated with said first communication network, verifying the belonging to said first network of said access point to be verified comprising requesting to obtain (230) an addressing identifier, relating to a second network, of said access point to be verified;

- select an access point to be used by said terminal from among the detected access points verified as belonging to said first communication network.

13. Computer program product, characterized in that it comprises program code instructions for executing the determination method according to any one of claims 1 to 11, when said program is executed by a computer.

14. A computer-readable storage medium on which is saved a computer program comprising program code instructions for executing the determination method, according to any one of claims 1 to 11, when said program is executed by a computer.

1/3
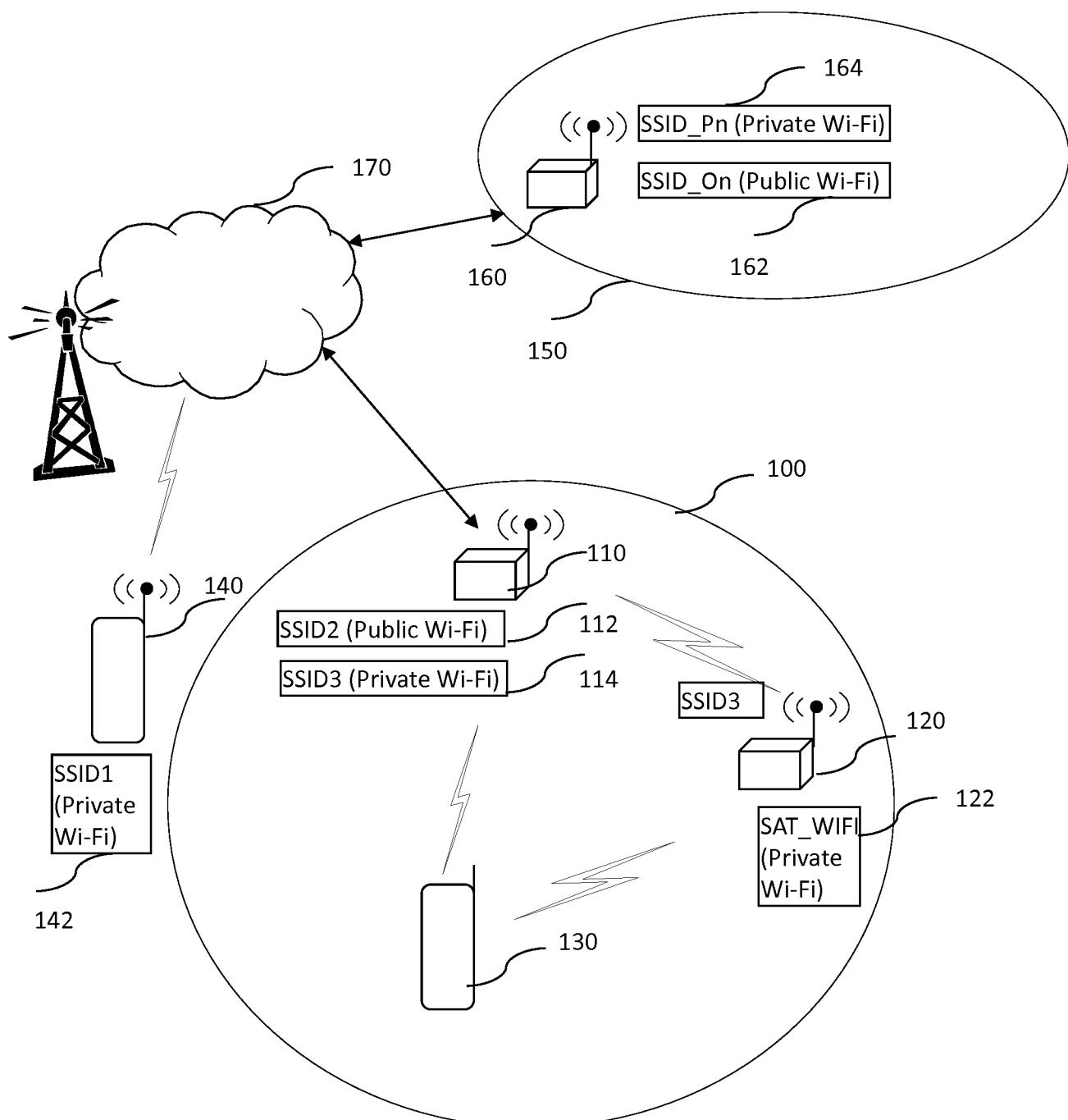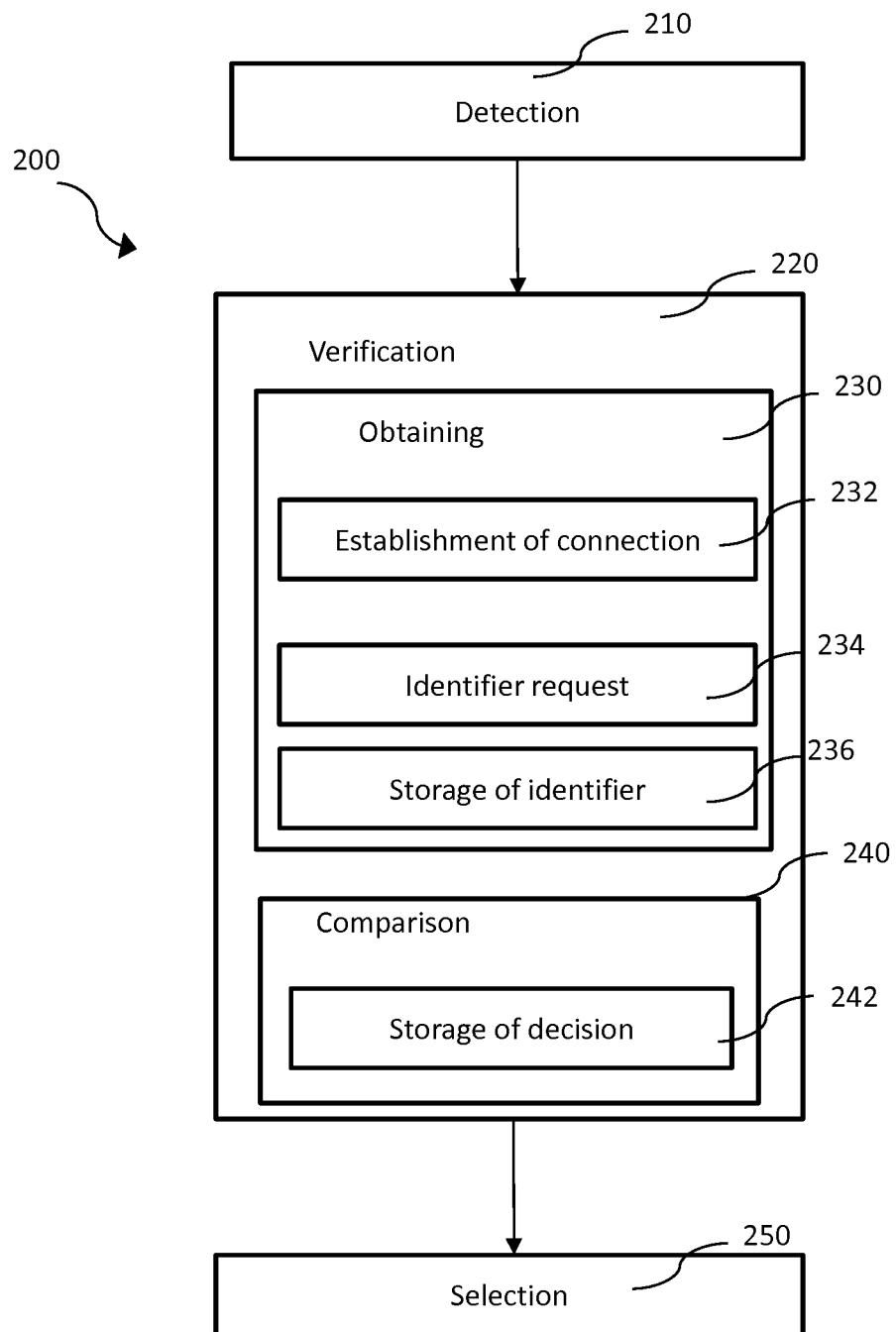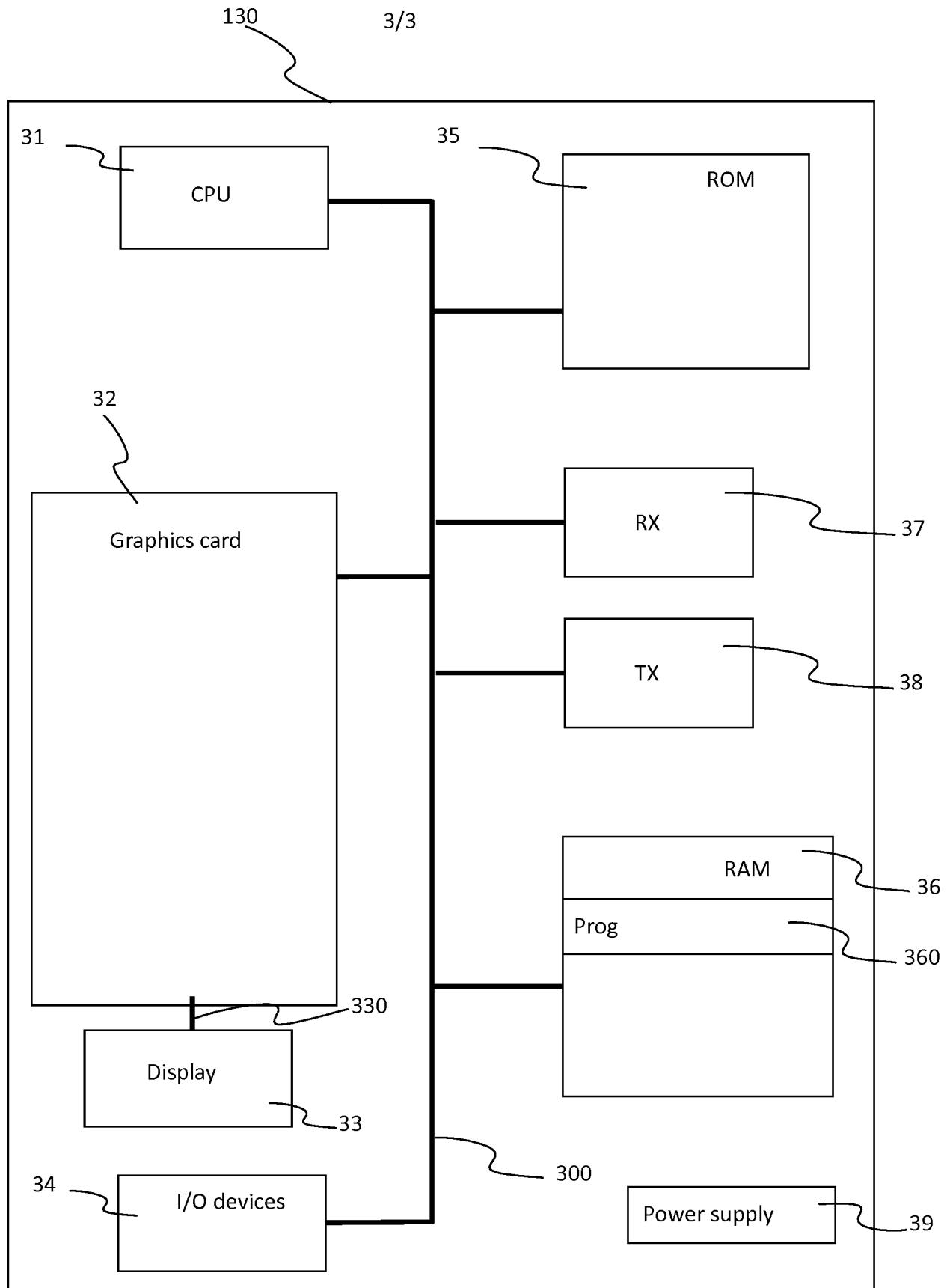
SSID_Pn (Private Wi-Fi)   164

SSID_On (Public Wi-Fi)

170

160   162

150

100

110

SSID2 (Public Wi-Fi)   112

SSID3 (Private Wi-Fi)   114

SSID3

120

140

SSID1
(Private
Wi-Fi)

142

SAT_WIFI
(Private
Wi-Fi)   122

130

Figure 1

Figure 2

Figure 3

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W48/16   H04W84/12
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W

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

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

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2008/008987 A2 (QUALCOMM INC [US]; BALASUBRAMANIAN SRINIVASAN [US]; KUZHIYIL ANUP [US]) 17 January 2008 (2008-01-17)	1-14
Y	abstract paragraphs [0006], [0022] - [0046], [0059] - [0060] -----	4
X	WO 2009/043048 A1 (DEVICESCAPE SOFTWARE INC [US]; WYNN SIMON [US]; FRASER DAVID [US]) 2 April 2009 (2009-04-02)	1,12-14
Y	paragraphs [0035] - [0072] -----	4
X	US 2005/148332 A1 (BUCKLEY ADRIAN [US] ET AL) 7 July 2005 (2005-07-07) abstract paragraphs [0039] - [0046] -----	1,12-14

☐ 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
21 May 2015	01/06/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Le Bras, Patrick

INTERNATIONAL SEARCH REPORT
Information on patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 2008008987	A2	17-01-2008	CN	101491144 A	22-07-2009
			EP	2044801 A2	08-04-2009
			JP	5209621 B2	12-06-2013
			JP	5242836 B2	24-07-2013
			JP	2009544245 A	10-12-2009
			JP	2013031193 A	07-02-2013
			KR	20090039776 A	22-04-2009
			TW	200822775 A	16-05-2008
			US	2008014934 A1	17-01-2008
			US	2013235861 A1	12-09-2013
			WO	2008008987 A2	17-01-2008
WO 2009043048	A1	02-04-2009	EP	2206278 A1	14-07-2010
			EP	2206400 A1	14-07-2010
			ES	2523323 T3	24-11-2014
			ES	2529679 T3	24-02-2015
			JP	5497646 B2	21-05-2014
			JP	2010541429 A	24-12-2010
			JP	2011503925 A	27-01-2011
			WO	2009043048 A1	02-04-2009
			WO	2009043053 A1	02-04-2009
US 2005148332	A1	07-07-2005	AU	2004312941 A1	21-07-2005
			CA	2552755 A1	21-07-2005
			CN	1926902 A	07-03-2007
			EP	1723816 A1	22-11-2006
			JP	4436930 B2	24-03-2010
			JP	2007518316 A	05-07-2007
			KR	20060129002 A	14-12-2006
			US	2005148332 A1	07-07-2005
			WO	2005067335 A1	21-07-2005