US 20070249365A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2007/0249365 A1**

Jendbro (43) **Pub. Date: Oct. 25, 2007**

(54) **DEVICE, METHOD AND COMPUTER PROGRAM FOR CONNECTING A MOBILE DEVICE TO A WIRELESS NETWORK**

(75) Inventor: **Magnus Jendbro**, Staffanstorp (SE)

Correspondence Address:
ALBIHNS STOCKHOLM AB
BOX 5581, LINNEGATAN 2
SE-114 85 STOCKHOLM; SWEDENn
STOCKHOLM (SE)

(73) Assignee: **Sony Ericsson Mobile Communications AB**, Lund (SE)

(21) Appl. No.: **11/381,152**

(22) Filed: **May 2, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/745,192, filed on Apr. 20, 2006.

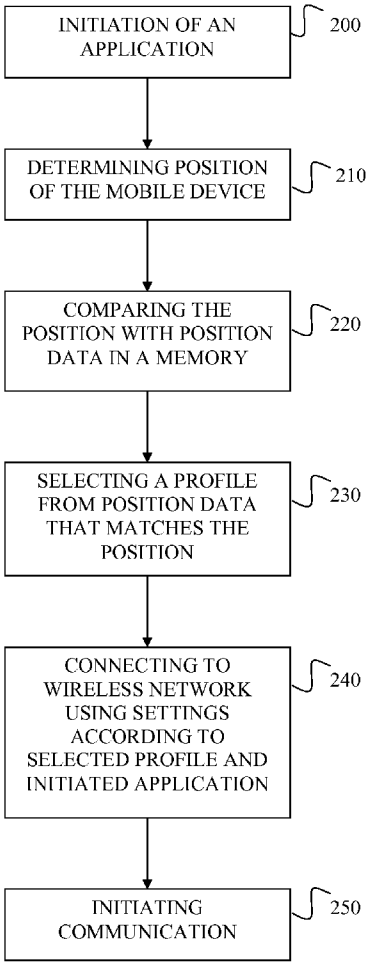
Publication Classification

(51) **Int. Cl.**
H04Q 7/20 (2006.01)

(52) **U.S. Cl.** **455/456.1**

(57) **ABSTRACT**

A solution for a mobile communications device, for controlling connection to a communications network. The invention involves positioning of the mobile device based on received positioning information signals, and comparison of a determined current position for the device with stored position data. If the determined position matches stored position data, a profile related to that position data is selected. The profile comprises settings usable for connection to a communications network. The determined position identifies the profile to use, and when an application involving connection to a network is initiated by a user, the appropriate client and related settings are automatically used.



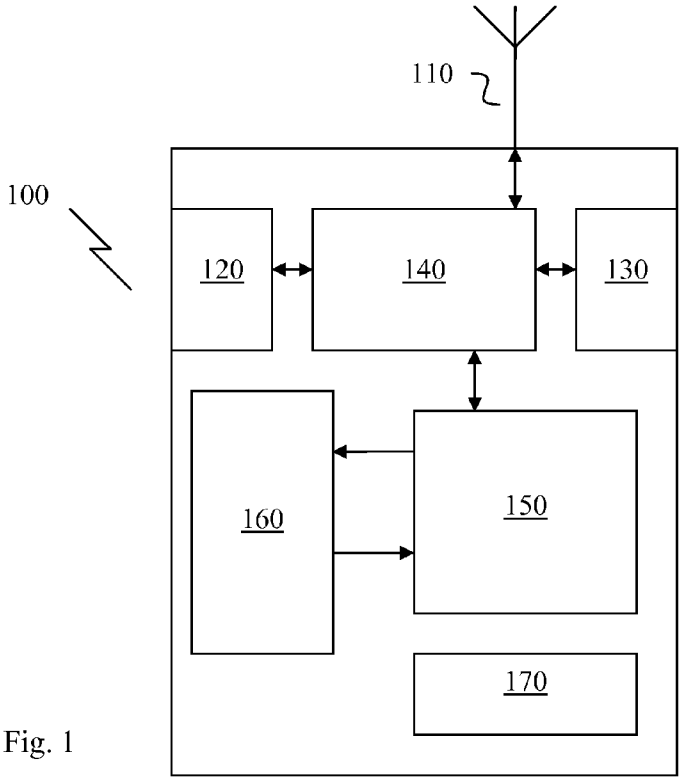


Fig. 1

POSITION [CELL ID]	PROFILE	WLAN ACCESS	VoIP	EMAIL
15433 OPERATOR I	HOME	WEP	FREE VoIP CLIENT	EUDORA CLIENT
32541 OPERATOR II	OFFICE	VPN CLIENT SETTINGS	HIGH SECURITTY VoIP CLIENT	MICROSOFT OUTLOOK
DEFAULT	PUBLIC	VPN CLIENT SETTINGS	FREE VoIP CLIENT	MICROSOFT OUTLOOK EXPRESS

Fig. 4

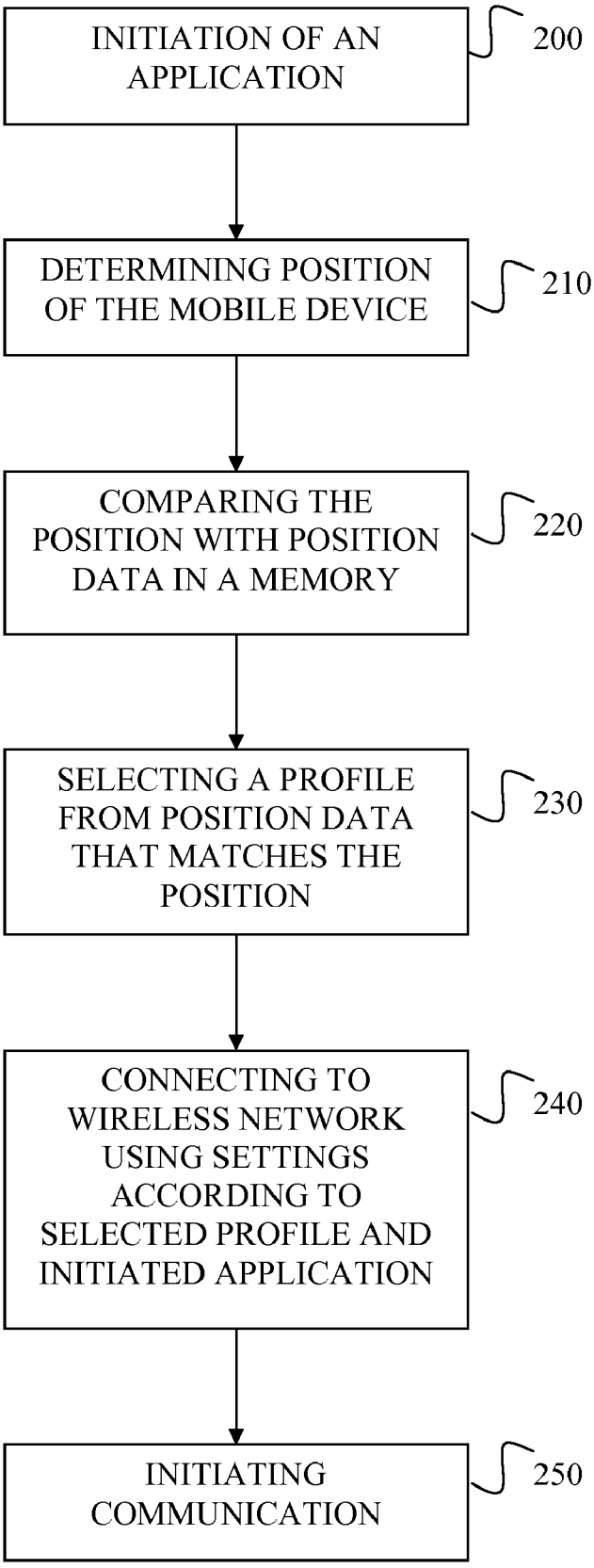


Fig. 2

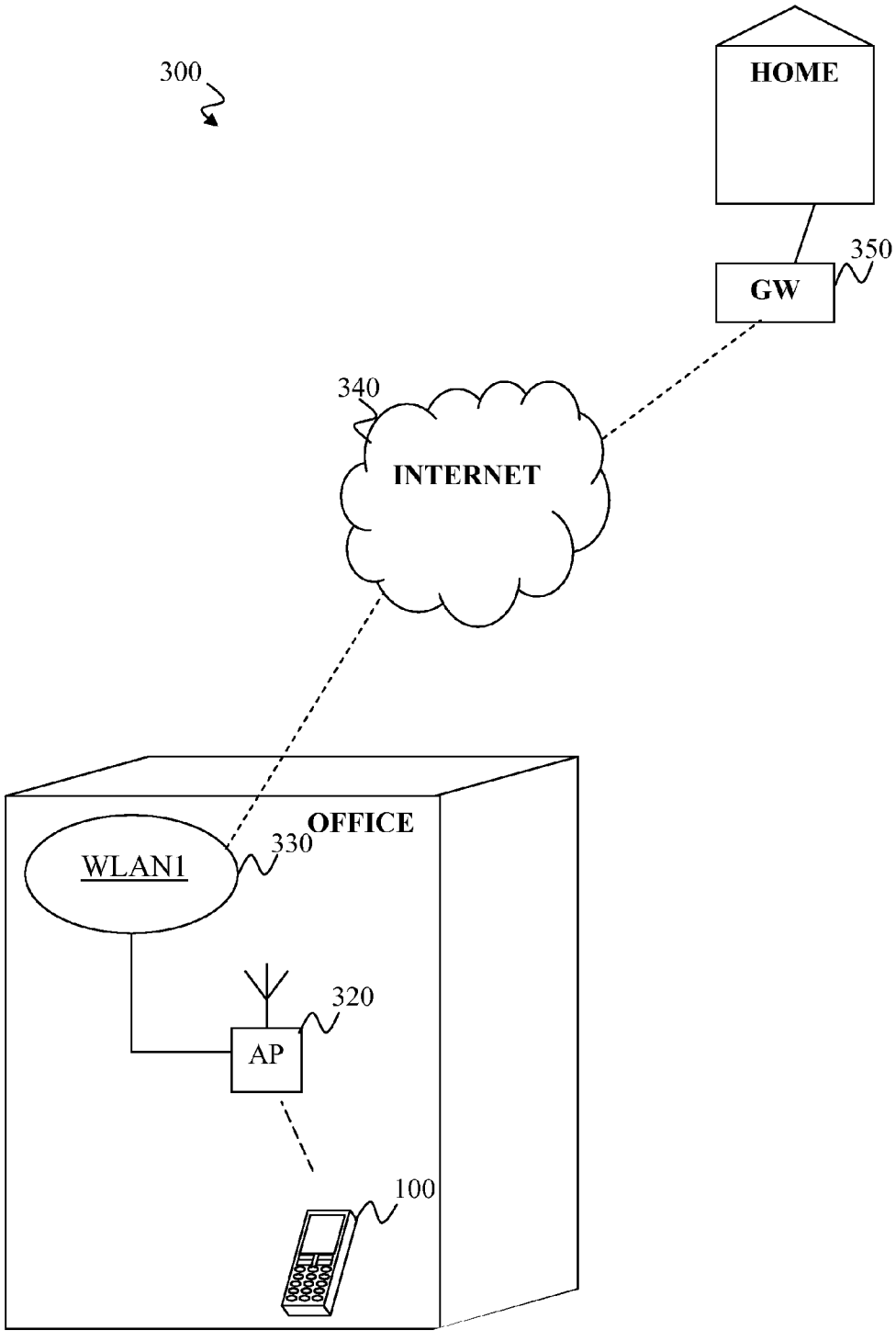


Fig. 3

DEVICE, METHOD AND COMPUTER PROGRAM FOR CONNECTING A MOBILE DEVICE TO A WIRELESS NETWORK

FIELD OF THE INVENTION

[0001] The present invention relates to the field of mobile communications, and in particular to the procedure of setting up a wireless communication connection between a mobile device and a communications network. More specifically, the invention relates to matching of position data for automatic selection of a profile for setting up such a connection.

BACKGROUND OF THE INVENTION

[0002] Today, a significant penetration of WLANs and VoIP systems has occurred both in homes and offices. VoIP enables the convergence of data and voice networks, allowing network administrators of major corporations or home users to cut costs. At the same time residential gateways provide a mechanism for data WLAN connectivity. Most WLAN usage is for data applications in devices, such as mobile phones, printers, cameras and WLAN IP phones. In general, security issues surrounding WLAN apply to all devices that connect to it, in order to guarantee that trusted relationships are achieved between communicating devices and to prevent eavesdropping of radio signals.

[0003] The 802.11i standard enables support for both packet and authentication security. Previous generations of 802.11 security methods revolved around the WEP protocol. The authentication provided by WEP does not provide two-way authentication, i.e. the user does not authenticate the network. The 802.11i standard addresses security deficiencies of WEP using wireless protected access (WPA) and the ratified 802.11i specification has been adopted as WPA2, WPA2 enhances WPA by using the Advanced Encryption Standard, AES, instead of the cipher method RC4 as the encryption engine, 802.11i also discloses a new robust security network (RSN) that may require hardware changes.

[0004] Referring to the WLAN security setup, WLAN IP phones provide the ability for a user to pick up their "home" phone and use the same phone anywhere were access to a broadband network is available. Thus, security measures need to encompass these use cases in addition to the traditional security setup. The type of security offered is typically limited to setting up an access point and a device connected to a computer or multiple computers.

[0005] 802.11i provides for two different types of authentication mechanisms, pre-shared key (PSK) mode and 802.1x-based authentication mode. PSK is essentially a user setup that replaces the pairwise master key (PMK) that would have been exchanged via the 802.1x mechanism. Most ease-of-use implementations for home networks use the PSK mode as the core of their framework.

[0006] WLAN IP phones are network devices that normally use network-based authentication[24]. The type of messaging passed between elements is governed by the extensible authentication protocol (EAP). This messaging describes an authentication method using request and response sequences. There are different types of content formats that can be implemented, such as TLS, TTLS and SIM. The purpose of 802.1x in an 802.11i context is to

[0007] In the present and near future a WLAN user will need to access different WLAN networks and these different networks will need both different applications as well as different security measures in order to work in a secure and proper manner, as it is disclosed above. A user may e.g. need to use one kind of VoIP client in the home or in a public hotspot environment and a completely different VoIP client at work. Different application may require the user to authenticate the usage by using a VPN client at the office that is not required in home or in the hot spot environment or vice versa.

[0008] WO-A1-2005/109934, discloses a method to facilitate the selection of a WLAN, wherein the selection is based on an order of preference. The order of preference is based on the positioning of the mobile node. The position of the mobile node is determined based on e.g. the country code received from a cellular network. The main object of the method is to select a WLAN out of a plurality of available WLAN's based on the country wherein the mobile is used.

[0009] US, A1, 20050190747 discloses a mobile phone that is capable of acting differently depending on the place where the mobile phone is used. When the mobile phone is at home the phone receives calls via the home number and when the mobile phone is at work it receives calls to the office. When the mobile phone detects a public hot spot the wireless VoIP is used. From the WLAN detected a profile associated with the detected WLAN, and stored in the mobile phone, is used. The place where the mobile device is used is based on the identity of the WLAN. However, this method requires the mobile device to always scan and search for available wireless networks to set up a connection for communication over said wireless network and, this continuously scanning result in an excessive drainage of the battery of the mobile device.

[0010] A general objective of the invention is to provide a solution for mobile devices which provides easy and quick selection of settings to use when connecting to a network with a certain application.

[0011] An aspect of this object is to provide a solution which ensures that proper security procedures for different applications are used in the connection process.

[0012] Yet another aspect of this object is to provide a solution which does not entail excessive drainage of a battery of the wireless communications device.

SUMMARY OF THE INVENTION

[0013] The present invention relates to a device, as well as a method and a computer program product for use in a mobile device, for controlling connection to a communications network. More specifically, the invention involves positioning of the mobile device, and comparison of a determined current position with stored position data. If the determined position matches stored position data, a profile related to that position data is selected, which profile comprises settings for connection to the network Preferably, selection of a certain profile and launching of a related client works automatically when an application is initiated by a user. This means less user interaction, while appropriate settings may still be employed for different scenarios, typically for different applications and at different positions. Furthermore, the mobile device does not have to scan for wireless networks to connect to, since the network and

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.