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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001665 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/021037

(22) International Filing Date: 28 June 2004 (28.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/483,552 27 June 2003 (27.06.2003) US

(71) Applicant: **BITFONE CORPORATION** [US/US]; 32451 Golden Lantern, Suite 301, Laguna Niguel, CA 92677 (US).

(72) Inventors: **MAROLIA, Sunil**; 32 Terra Vista, Dana Point, CA 92629 (US). **RAO, Bindu, Rama**; 21 Henley Drive, Laguna Niguel, California 92677 (US).

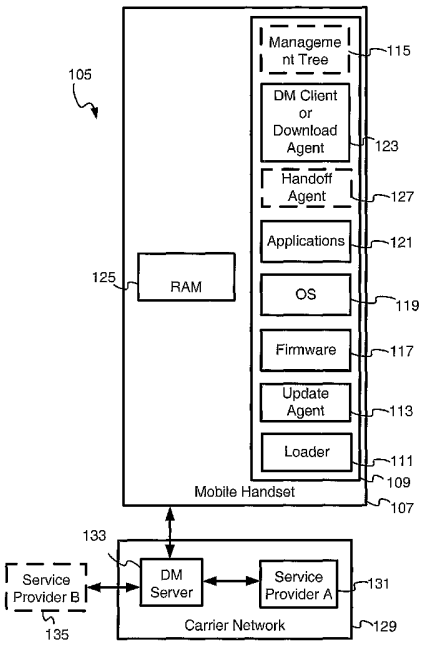
(74) Agent: **BORG, Kevin, E.**; McAndrews, Held & Malloy, Ltd., 500 W. Madison Street, Suite 3400, Chicago, IL 60661 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR DOWNLOADING UPDATE PACKAGES INTO A MOBILE HANDSET IN A CARRIER NETWORK



(57) Abstract: Aspects of the present invention may be seen in a system and method for downloading update packages into an electronic device communicatively coupled to a carrier network. The system may facilitate the update of firmware/software in the electronic device. Different protocols may be utilized for discovery and download of update packages. Also, different protocols may be utilized for provisioning and for subsequent downloading of update packages.

WO 2005/001665 A2

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Attorney Docket No. 15642WO01

SYSTEM AND METHOD FOR DOWNLOADING UPDATE PACKAGES INTO A MOBILE HANDSET IN A CARRIER NETWORK

BACKGROUND OF THE INVENTION

[0001] Electronic devices, such as mobile phones and personal digital assistants (PDA's), often contain firmware and application software that are either provided by the manufacturers of the electronic devices, by telecommunication carriers, or by third parties. These firmware and application software often contain software bugs. New versions of the firmware and software are periodically released to fix the bugs or to introduce new features, or both.

[0002] Electronic devices may use update packages containing information necessary to update firmware/software in electronic devices. Update packages may be downloaded into handsets such that their software or firmware could be updated. It is desirable that the download be efficient and be conducted when convenient to the user. If updating the mobile handset involves interaction with various servers in a carrier network, it may not be appropriate to employ the same protocol for all such interactions. As a result, there is a need to use appropriate protocols for the different types of interactions between a mobile handset and one or more server in the carrier network.

[0003] Further limitations and disadvantages of conventional and traditional approaches will become apparent to one of ordinary skill in the art through comparison of such systems with the present invention.

BRIEF SUMMARY OF THE INVENTION

[0004] Aspects of the present invention may be seen in a system that facilitates the updating of firmware in an electronic device, using updating information received through a network. The system may comprise at least one electronic device having firmware, and being able to be communicatively coupled to a server to download firmware updating information. The system may determine when the at least one electronic device is to be communicatively coupled to the server to download the updating information.

[0005] The system may also comprise device information used in identifying the updating information for the at least one electronic device, wherein the

system may utilize the device information to determine when the at least one electronic device is to be communicatively coupled to the server to download the updating information. In an embodiment of the present invention, the server may be one of a management server and a delivery server.

[0006] The system may further comprise a first protocol utilized by the at least one electronic device to communicate with the management server, and a second protocol utilized by the at least one electronic device to communicate with the delivery server. The system may be capable of causing the at least one electronic device to be communicatively coupled to the management server first, and then to the delivery server to download the updating information. In an embodiment of the present invention, the first protocol may comprise the SyncML DM protocol, and the second protocol may comprise the Open Mobile Alliance Download OTA protocol.

[0007] In an embodiment of the present invention, the at least one electronic device may employ the first protocol to communicate the device information to the management server, and the second protocol to download the updating information from the delivery server based on the device information.

[0008] In an embodiment of the present invention, the device information may comprise manufacturer identification, model identification, and a firmware version. In another embodiment of the present invention, the device information may comprise manufacturer identification, model identification, a first firmware version, and a second firmware version. In yet another embodiment of the present invention, the device information may comprise manufacturer identification, model identification, a first firmware version, and a firmware version of an application.

[0009] Another aspect of the present invention may be seen in an electronic device that employs a first protocol to interact with a first server to determine the existence of updating information for updating the electronic device, and employs a second protocol to retrieve the updating information from a second server if the first server indicates the existence of the updating information in

the second server. In an embodiment of the present invention, the first server may comprise a management server.

[0010] In an embodiment of the present invention, the electronic device may communicate device information to the first server, and may receive from the first server information identifying a second protocol and a remote reference to employ for the download of updating information. The electronic device may communicate to the first server the device information and an indication of a download protocol supported by the electronic device as the second protocol.

[0011] In an embodiment of the present invention, the electronic device may employ a first protocol to communicate the device information to the first server and in response, may download the updating information from the first server employing the first protocol

[0012] The method of operating a management server interacting with an electronic device employing a management protocol, may comprise receiving device information from the electronic device; processing the device information to determine whether updating information exists for updating firmware or software in the electronic device; and communicating location and protocol information to the electronic device to enable the electronic device to download the updating information employing the location information and the protocol information.

[0013] In an embodiment of the present invention, the management server may communicate a universal resource locator (URL) comprising the location and the protocol information to the electronic device.

[0014] In an embodiment of the present invention, the method may also comprise instructing the electronic device to employ one of a first protocol and a second protocol to download the updating information based on the device information.

[0015] These and other features and advantages of the present invention may be appreciated from a review of the following detailed description of the present

invention, along with the accompanying figures in which like reference numerals refer to like parts throughout.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[0016] Fig. 1 illustrates a block diagram of an exemplary update system for downloading firmware/software updates in a mobile handset, in accordance with an embodiment of the present invention.

[0017] Fig. 2 illustrates a flow diagram of an exemplary operation of an update system for downloading firmware/software updates in a mobile handset, in accordance with an embodiment of the present invention.

[0018] Fig. 3 illustrates a flow diagram of an exemplary process for OTA firmware update, in accordance with an embodiment of the present invention.

[0019] Fig. 4 illustrates a flow diagram of the OMA Download process for downloading generic content to mobile handsets, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0020] The present invention relates generally to downloading updates of firmware/software components in electronic devices such as, for example, mobile handsets from a server, and specifically to the use of protocols that make such downloads possible. Although the following discusses aspects of the invention in terms of a mobile handset, it should be clear that the following also applies to other mobile electronic devices such as, for example, personal digital assistants (PDAs), pagers, personal computers (PCs), and similar handheld electronic devices.

[0021] **Fig. 1** illustrates a block diagram of an exemplary update system 105 for downloading firmware/software updates in a mobile handset 107, in accordance with an embodiment of the present invention. An update package for an electronic device such as, for example, mobile handset 107 may comprise executable instructions used to convert firmware/software in the mobile handset 107 from one version to another. In an embodiment of the present invention,

the update system 105 may comprise the mobile handset 107 communicatively coupled to a carrier network 129.

[0022] The carrier network 129 may comprises a device management (DM) server 133 and a service provider A 131. In an embodiment of the present invention, the carrier network 129 may also comprise an external service provider B 135, which may be external to the carrier network 129.

[0023] In an embodiment of the present invention, the mobile handset 107 may comprise a random access memory (RAM) unit 125 and a non-volatile memory 109. The non-volatile memory 109 may have a plurality of components such as, for example, a loader 111, an update agent 113, firmware 117, an operating system (OS) 119, applications 121, and a DM client/download agent 123. In an embodiment of the present invention, the non-volatile memory 109 may also comprise a management tree 115 and a handoff agent 127.

[0024] In an embodiment of the present invention, the system 105 may provide access to the mobile handset 107 from service providers that are either internal to the carrier network 129 such as, for example, the service provider A 131, or external to the carrier network 129 such as, for example, the service provider B 135.

[0025] In an embodiment of the present invention, the DM server 133 may facilitate access to the mobile handset 107 by service provider A 131 and service provider B 135 for provisioning software/firmware downloads and managing the components in the mobile handset 107. In an embodiment of the present invention, the DM server 133 may facilitate the creation and management of managed objects in the mobile handset 107. The managed objects may be arranged in a data structure such as, for example, the management tree 115. In an embodiment of the present invention, the DM client/download agent 123 in the mobile handset 107 may facilitate access to managed objects in the management tree 115.

[0026] The applications 121, the OS 119 and the firmware 117 may access managed objects by interacting with the DM client 123. In another embodiment of the present invention, the applications 121, the OS 119 and the firmware 117 may access managed objects without using the DM client 123. The DM client/download agent 123 may be capable of storing information in the management tree 115, as well as in other locations in the non-volatile memory 109, or RAM 125, of the mobile handset 107. The stored information may be subsequently retrieved by an update agent 113 or by other components in the mobile handset 107.

[0027] In an embodiment of the present invention, the managed objects in the management tree 115 may represent hardware or software components including, for example, provisioning parameters and configuration parameters, that may be set remotely from the DM server 133, or that may be created and manipulated remotely from the DM server 133. In an embodiment of the present invention, the DM server 133 and the mobile handset 107 may employ protocols such as, for example, a SyncML DM protocol to manage the management tree and the other components in the mobile handset 107. In another embodiment of the present invention, the DM client 123 and the DM server 133 may communicate using transport protocols such as, for example, the SyncML DM protocol to facilitate device management of the mobile handset 107. Further details of the SyncML DM protocol, management tree, and managed objects may be found in the documents "SyncML Device Management Tree and Description, Version 1.1.1", October 2, 2002, and "SyncML Device Management Standardized Objects, Version 1.1.1", October 1, 2002, by the SyncML Initiative, Ltd., the entire subject matter of each of which is hereby incorporated herein by reference, in its entirety.

[0028] In an embodiment of the present invention, the service provider A 131 may employ SyncML DM protocols to provision configuration parameters and other parameters into the mobile handset 107 such as, for example, during configuration or provisioning of a new handset by the carrier network 129. The

service provider A 131 may employ a different protocol such as, for example, the OMA (Open Mobile Alliance) download protocol for downloading large content such as, for example, large update packages into the mobile handset 107. Further details of the OMA download protocol may be found in the document.

[0029] In an embodiment of the present invention, the service provider A 131 may be associated with a unique service subscribed to by the mobile handset 107. The service provider A 131 may be associated with specific management parameters, configuration information, subscriber information and/or an application 121 in the mobile handset 107. The service provider A 131 may employ one or more appropriate managed objects to represent such information, and each of these may be uniquely addressable as managed objects that are part of the management tree 115. For example, the service provider A 131 may provision the universal resource identifier (URI) or universal resource locator (URL) of the service provider B 135, during provisioning of the mobile handset 107 when a user newly acquires the handset. Such provisioning information may end up as a managed object in the management tree 115. The mobile handset 107 may subsequently initiate the download of an update package directly from the service provider B 135 (with or without employing the services of the DM server 133), and may employ the DM client/download agent 123 to download an associated update package. The mobile handset 107 may then store the downloaded update package in non-volatile memory 109. In an embodiment of the present invention, the mobile handset 107 may elect not to employ the management tree 115 as a destination for the downloaded update package.

[0030] In an embodiment of the present invention, provisioning of a newly acquired mobile handset 107 by an end-user, by the DM server 133, or by a service provider such as, for example, service provider A 131, may be accompanied by communicating mobile handset 107-related information to service provider B 135. Service provider B 135 may include end-user,

subscription-related information, where service provider B 135 may be capable of scheduling or initiating the subsequent transfer of firmware/software update packages to the mobile handset 107. The service provider B 135 may send a notification to the newly provisioned mobile handset 107 that may notify the mobile handset 107, or the user of the mobile handset 107, to initiate the download of one or more update packages so as to conduct an update of available firmware/software, incorporation of new software, or reconfiguration of specific parameters in the mobile handset 107.

[0031] **Fig. 2** illustrates a flow diagram of an exemplary operation of an update system for downloading firmware/software updates in a mobile handset, in accordance with an embodiment of the present invention. The update system may be such as, for example, the update system 105 of **Fig. 1**. Processing may begin at a start block 205, when the mobile handset 107 is powered up or comes into the vicinity of the carrier network 129. At a next block 207, the carrier network 129 may determine the status of the mobile handset 107. For example, the subscription of the user of the mobile handset 107 may be verified. At a next decision block 209, it may be determined whether the mobile handset 107 is a new one, i.e. being used for the first time. In an embodiment of the present invention, the determination may be made by the mobile handset 107. In another embodiment of the present invention, the carrier network 129 may make such determination by employing data available in customer care databases, in service providers, or in other systems.

[0032] If, at the decision block 209, it is determined that the mobile handset 107 is a new one, i.e. being used for the first time within the carrier network 129, then, at a next block 211, the mobile handset 107 may be provisioned with configuration parameters, network parameters, security codes, etc., as necessary. Then, at a next decision block 213, it may be determined whether the mobile handset 107 requires additional software, bug fixes, updates to firmware/software, etc.

[0033] If, at the decision block 209, it is determined that the mobile handset 107 is not a new one, but a known one, then at a next decision block 213, it may be determined whether the mobile handset 107 requires additional software, bug fixes, updates to firmware/software, etc.

[0034] If, at the decision block 213 it is determined that no updates, additional software, bug fixes, updates to firmware/software, etc., are necessary, then at a next block 223, the normal operation of the mobile handset 107 may be started before finally terminating at an end block 225.

[0035] If, at the at the decision block 213, it is determined that the mobile handset 107 may require updates, additional software, bug fixes, updates to firmware/software, etc., then, at a next block 215, such updates may be scheduled. In an embodiment of the present invention, service provider B 135 may be capable of providing such update packages to the mobile handset 107. Service provider B 135 may be also capable of scheduling the download of update packages and of sending notification to the mobile handset 107 to initiate such downloads. Then, at a next block 217, the user of the mobile handset 107 may be notified of the need to update the firmware/software in the mobile handset 107. In an embodiment of the present invention, the DM server 133 may schedule download of update packages by the mobile handset 107 from service provider B 135.

[0036] At a next block 219, the mobile handset 107 may initiate the download of one or more update packages. In an embodiment of the present invention, the mobile handset 107 may initiate the download based on a schedule of downloads communicated to the mobile handset 107 by the carrier network 129. In another embodiment of the present invention, the mobile handset 107 may receive a notification for download at a scheduled time in response to which the mobile handset 107, or the associated user, may initiate the download of one or more update packages. In an embodiment of the present invention, the update package(s) may be pushed to the mobile handset 107 by the DM server 133 or

service provider B 135, based on a schedule or a queue of download commands maintained for download by the mobile handset 107.

[0037] Then, at a next block 221, the update agent 113 may update the firmware/software in the mobile handset 107 using the downloaded update package(s). At a next block 223, the normal operation of the mobile handset 107 may be started before finally terminating at an end block 225.

[0038] In an embodiment of the present invention, a firmware update protocol may be utilized for over-the-air (OTA) firmware updates. The protocol may specify a set of standard commands and associated parameters, where the standard may be based on the command set of both the SyncML DM protocol and the OMA Generic Content Download OTA Specification. SyncML DM is the leading standards initiative that focuses on remote device management for wireless devices. The OMA Generic Content Download OTA Specification provides a flexible protocol for enabling the download of generic content. In an embodiment of the present invention, by combining elements of these protocols, a protocol may be constructed that provides the ability to use SyncML DM for controlling the main device management functions, and to use the OMA Download protocol to download larger binary objects such as, for example, firmware updates.

[0039] **Fig. 3** illustrates a flow diagram of an exemplary process for OTA firmware update, in accordance with an embodiment of the present invention. The firmware update may begin with push initiation 301, where a mobile handset such as, for example, mobile handset 107 of **Fig. 1** may open a data connection to a server. In an embodiment of the present invention, users may not be expected to proactively check for the existence of firmware updates. Therefore, an electronic device such as, for example, the mobile handset 107 may support a mechanism for remotely initiating a data session. In an embodiment of the present invention, the SyncML DM protocol may provide a framework by which clients (i.e., mobile handsets such as mobile handset 107)

may receive a "Notification Initiation Alert" that may trigger the client to start a data session.

[0040] For example, the OTA Flash Forum protocol may use General Package#0 as specified in the SyncML DM Notification Initiation Session document. Further details of this aspect of SyncML DM may be found in the document "SyncML Notification Initiated Session, Version 1.1.1", October 2, 2002, by the SyncML Initiative, Ltd., the entire subject matter of which is hereby incorporated herein by reference, in its entirety. SyncML DM may specify that WAP Push may be used for this purpose, and may also specify a format acceptable for the purpose of firmware upgrade initiation. In an embodiment of the present invention, a SyncML DM client or a compatible client may be used for the initiation of the update process to allow use of the SyncML DM Notification specification.

[0041] The firmware update process of Fig. 3 may then perform device a capabilities exchange 303, where a minimum set of selection criteria may be sent by the mobile handset to the server, to permit the server to provide the mobile handset with the appropriate firmware update. In an embodiment of the present invention, the minimum set of selection criteria to adequately determine the required update for a mobile handset may, for example, be the model name, the manufacturer name, and the current installed firmware version.

[0042] In an embodiment of the present invention, SyncML DM may provide a standardized framework to exchange the selection criteria listed hereinabove. The SyncML DM Standardized Objects document defines a set of mandatory objects that are to be supported by the client and the server. SyncML DM does not mandate that this information be exchanged at the beginning of a management session. However, SyncML DM may require support by both client and server. In an embodiment of the present invention, the SyncML DM specification may be used as the primary means for exchanging device capabilities for the purpose of identifying available firmware updates.

[0043] In an embodiment of the present invention, additional parameters may be used to provide more granular selection of firmware updates. For example, the firmware update service may only be provided based on a subscription and therefore a specific device ID may be required. SyncML DM specifies a host of other required objects for the device identifier. These other required objects may be used to provide additional selection criteria.

[0044] Referring again to the illustration of **Fig. 3**, the firmware update may then perform firmware download 305. In an embodiment of the present invention, when dealing with high-volume distribution with large file sizes such as, for example, firmware update packages, it may be best for carriers to reduce the amount of OTA traffic. To provide a more efficient, standardized download mechanism, the Flash Forum protocol may leverage portions of the Open Mobile Alliance Generic Content Download Over The Air Specification.

[0045] **Fig. 4** illustrates a flow diagram of the OMA Download process for downloading generic content to mobile handsets, in accordance with an embodiment of the present invention. The OMA Download process may begin with object discovery 401. The OMA Download specification suggests several methods for discovery such as, for example, a reference on a Web page, or inside an email or a multimedia messaging service (MMS) message, or storing in memory or in an accessory attached to the phone. The OTA Flash Forum may not assume that end-users will proactively update their phones, without appropriate notification and a seamless user-experience. In an embodiment of the present invention, the SyncML DM protocol may be used for the object discovery 401 as described herein. Based on the push initiation 301 and capabilities exchange 303 performed by SyncML DM as shown in **Fig. 3**, the appropriate URL may be provided to the OMA Download Agent for the object discovery 401 of **Fig. 4**.

[0046] In an embodiment of the present invention, the firmware update URL may be an object within the SyncML DM management tree. The SyncML DM specification may allow for the EXEC command to be sent using the firmware

update URL as the target. This EXEC command may trigger a method to launch the OMA OTA download client.

[0047] The OMA download may then perform download descriptor retrieval 403. The device hosting the download agent may support either W-HTTP or WSP, and may support WAPTLS or WTLS, as well as other protocols. The download descriptor may be sent using other mechanisms such as MMS, email, or an instant messaging protocol. Based on the URL received from the SyncML DM session, the OMA-compliant download agent may download the download descriptor with the necessary parameters. In an embodiment of the present invention, the necessary parameters may be sent as part of the HTTP GET request URL, or as part of HTTP header.

[0048] The OMA download may then perform download descriptor processing 405. The download descriptor may provide information about the firmware update, device requirements, and may also contain a URI to the delivery server for the actual download of update packages.

[0049] The OMA download may then perform the capabilities check 407. The download agent may use the information in the descriptor such as, for example, size and type, to check whether the mobile handset may be capable of using the firmware update object. This may prevent downloading of firmware update objects that will not work properly. The download agent may use the size attribute of the download descriptor to check whether the device may be capable of using or installing the update package. If the update package cannot be installed due to lack of memory, an "insufficient memory" status may be posted to the server and the end-user may be notified.

[0050] The OMA download may then provide user confirmation 409. Information from the download descriptor may be made available to the user, if available, to accept or reject the download. The download descriptor may include such information as, for example, the name, vendor, size, type, and description. In an embodiment of the present invention, if the user does not

approve the downloading, the OMA Download Agent may post a "User Cancelled" status report to the server. The user confirmation may be utilized for enabling the download. In an embodiment of the present invention, additional confirmation may also be employed to conduct subsequent operations such as, for example, firmware updates.

[0051] The retrieval of the firmware update object 411 may be performed using HTTP (or HTTPS), and may be performed according to the scheme indicated by the ObjectURI attribute of the download descriptor. The OMA Download Agent may invoke the URL in the objectURI element of the download descriptor to request the update package. This URL may point to the delivery server and may contain mandatory parameters and optional parameters.

[0052] In an embodiment of the present invention, the download agent may request a chunk of the update package binary by specifying a byte range in the request header to allow devices with limited available RAM to handle larger update downloads. The server may then respond back with the update package binary chunk of the requested range, and the response HTTP header may contain the information of the bytes being sent. In an embodiment of the present invention, there may be a content-range header indicating the byte range being sent, and a content-length header indicating the actual number of bytes being sent. If the last byte position is not greater than or equal to the first byte position, the requested header may be considered syntactically incorrect and the server may ignore it and the entire update package may be sent. If the last byte position is greater than the length of the update package binary it may be set to the one less than the length of the update package binary.

[0053] The OMA download process may then perform installation 413 of the update. The OMA Download Specification indicates that installation is complete when the downloaded object has been prepared for execution/rendering on the device, or an unrecoverable failure has occurred. This model may be followed for firmware updates. In an embodiment of the present invention, a successful download may imply installation, for the purpose

of notifying the OMA compliant download server. A successful download may not necessarily mean that the firmware has been updated successfully, only that the update was successfully downloaded.

[0054] Installation notification 415 may then follow. If the installNotifyURI attribute in the download descriptor has been explicitly used, the OMA Download Agent may relay the status of the installation back to the OMA Download Server via the installNotifyURI. For firmware upgrades, this may only imply that the firmware update has been successfully downloaded. It may not necessarily mean that the firmware update has been processed.

[0055] Referring back to the process for OTA firmware update of **Fig. 3**, following firmware download 305, firmware installation 307 may be performed. In an embodiment of the present invention, for firmware update installation, a mechanism may exist in the mobile handset that may provide the location of the downloaded firmware update. This mechanism may be, for example, a device management tree object on which an EXEC command will trigger the update mechanism. The firmware update location may be in a location accessible by a non-SyncML DM client. In an embodiment of the present invention, the mobile handset may provide the end-user with a prompt as to whether or not to proceed with the firmware update installation. If the user accepts the installation, the firmware update may be processed. If the user rejects the installation, the process may terminate without updating the firmware.

[0056] In an embodiment of the present invention, updating the firmware may involve the mobile handset becoming inoperable during the time of the firmware update. In an embodiment of the present invention, if an interruption of the firmware update occurs, the update process may not be capable of immediately returning the device to a normal operating condition. In the case that the device cannot immediately return to normal operating condition, the end-user may be presented with a warning that the phone will be offline and the approximate time of the update, prior to beginning the firmware installation.

[0057] Upon completion of the firmware update process, the mobile handset may send to the server a notification of the resulting status of the firmware update 309. In an embodiment of the present invention, for non-fatal update failures, the end-user may be provided with an indication of the failure and return the mobile handset to an operational mode. The mobile handset may send a notification to the SyncML DM compliant server that the update failed to install. Some non-fatal reasons for failure of a firmware update may be, for example, user rejection, corrupted update package, wrong update package, or failed signature authentication.

[0058] Upon completion of a successful firmware update, the end-user may be provided with an indication that the firmware was successfully updated. The mobile handset may send a notification to the SyncML DM compliant server that the update was successful.

[0059] In an embodiment of the present invention, the notification may use either a data channel or out-of-band channel such as, for example, short message service (SMS). In the case of SyncML DM, the device may provide the new firmware version to the SyncML DM compliant server using the objects DevInfo and DevDetail as required management objects supported by the client and server. DevInfo may, for example, include the following SyncML DM objects: Man (manufacturer identifier) and Mod (Model identifier). These objects may be sent at the beginning of every management session. SyncML DM may also require support for the FwV (Firmware version) object under DevDetail. In an embodiment of the present invention, for SMS notification, the device may support mobile originated SMS. Using SMS may provide reduced network congestion.

[0060] The present invention may be realized in hardware, software, firmware and/or a combination thereof. The present invention may be realized in a centralized fashion in at least one computer system, or in a distributed fashion where different elements are spread across several interconnected computer systems. Any kind of computer system or other apparatus adapted for carrying

out the methods described herein may be suitable. A typical combination of hardware and software may be a general-purpose computer system with a computer program that, when being loaded and executed, controls the computer system to carry out the methods described herein.

[0061] The present invention may also be embedded in a computer program product comprising all of the features enabling implementation of the methods described herein which when loaded in a computer system is adapted to carry out these methods. Computer program in the present context means any expression, in any language, code or notation, of a set of instructions intended to cause a system having information processing capability to perform a particular function either directly or after either or both of the following: a) conversion to another language, code or notation; and b) reproduction in a different material form.

[0062] While the present invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the present invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the present invention without departing from its scope. Therefore, it is intended that the present invention not be limited to the particular embodiment disclosed, but that the present invention will include all embodiments falling within the scope of the appended claims.

CLAIMS

What is claimed is:

1. A system that facilitates the updating of firmware in an electronic device, using updating information received through a network, the system comprising:

at least one electronic device having firmware, and being able to be communicatively coupled to a server to download firmware updating information; and

wherein the system determines when the at least one electronic device is to be communicatively coupled to the server to download the updating information.

2. The system according to claim 1 further comprising:

device information used in identifying the updating information for the at least one electronic device; and

wherein the system utilizes the device information to determine when the at least one electronic device is to be communicatively coupled to the server to download the updating information.

3. The system according to claim 1 wherein the server is one of a management server and a delivery server.

4. The system according to claim 3 further comprising:

a first protocol utilized by the at least one electronic device to communicate with the management server; and

a second protocol utilized by the at least one electronic device to communicate with the delivery server.

5. The system according to claim 4 wherein the system is capable of causing the at least one electronic device to be communicatively coupled to the management server first, and then to the delivery server to download the updating information.

6. The system according to claim 5 wherein the at least one electronic device employs the first protocol to communicate the device information to the management server, and the second protocol to download the updating information from the delivery server based on the device information.

7. The system according to claim 2 wherein the device information comprises manufacturer identification, model identification, and a firmware version.

8. The system according to claim 2 wherein the device information comprises manufacturer identification, model identification, a first firmware version, and a second firmware version.

9. The system according to claim 2 wherein the device information comprises manufacturer identification, model identification, a first firmware version, and a firmware version of an application.

10. The system according to claim 4 wherein the first protocol comprises the SyncML DM protocol.

11. The system according to claim 4 wherein the second protocol comprises the Open Mobile Alliance Download OTA protocol.

12. An electronic device that employs a first protocol to interact with a first server to determine the existence of updating information for updating the electronic device, and employs a second protocol to retrieve the updating information from a second server if the first server indicates the existence of the updating information in the second server.

13. The electronic device according to claim 12 wherein the first server comprises a management server.

14. The electronic device according to claim 12 wherein the electronic device communicates device information to the first server, and

receives from the first server information identifying a second protocol and a remote reference to employ for the download of updating information.

15. The electronic device according to claim 14 wherein the electronic device communicates to the first server the device information and an indication of a download protocol supported by the electronic device as the second protocol.

16. The electronic device according to claim 14 wherein the electronic device employs a first protocol to communicate the device information to the first server and in response, downloads the updating information from the first server employing the first protocol.

17. A method of operating a management server interacting with an electronic device employing a management protocol, the method comprising:

receiving device information from the electronic device;

processing the device information to determine whether updating information exists for updating firmware or software in the electronic device; and

communicating location and protocol information to the electronic device to enable the electronic device to download the updating information employing the location information and the protocol information.

18. The method according to claim 17 wherein the management server communicates a universal resource locator (URL) comprising the location and the protocol information to the electronic device.

19. The method according to claim 17 further comprising instructing the electronic device to employ one of a first protocol and a second protocol to download the updating information based on the device information.

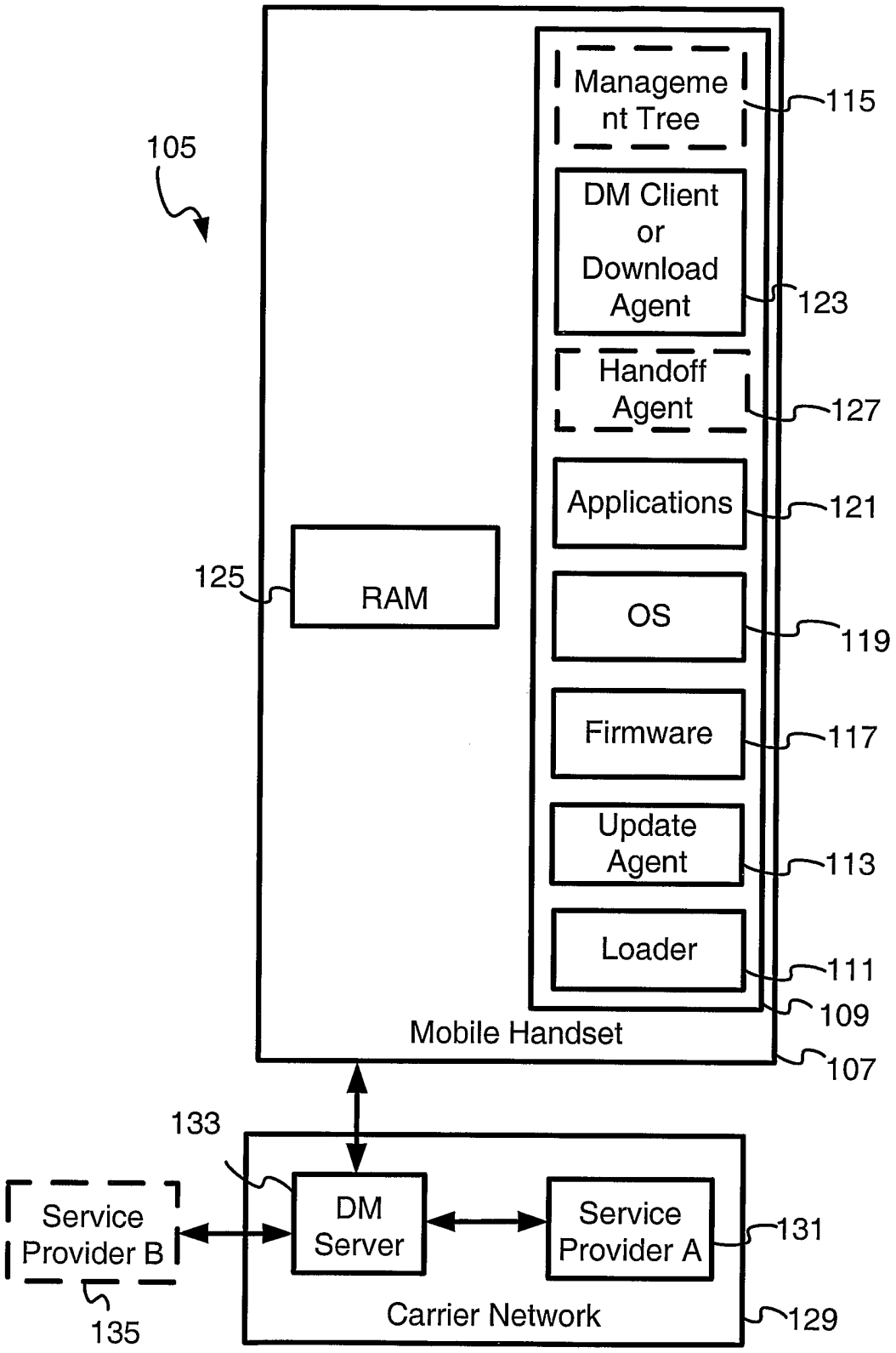

Manageme
nt Tree
115
105
DM Client
or
Download
Agent
123
Handoff
Agent
127
Applications
121
125
RAM
OS
119
Firmware
117
Update
Agent
113
Loader
111
109
Mobile Handset
107
133
Service
Provider B
DM
Server
Service
Provider A
131
135
Carrier Network
129

Fig. 1

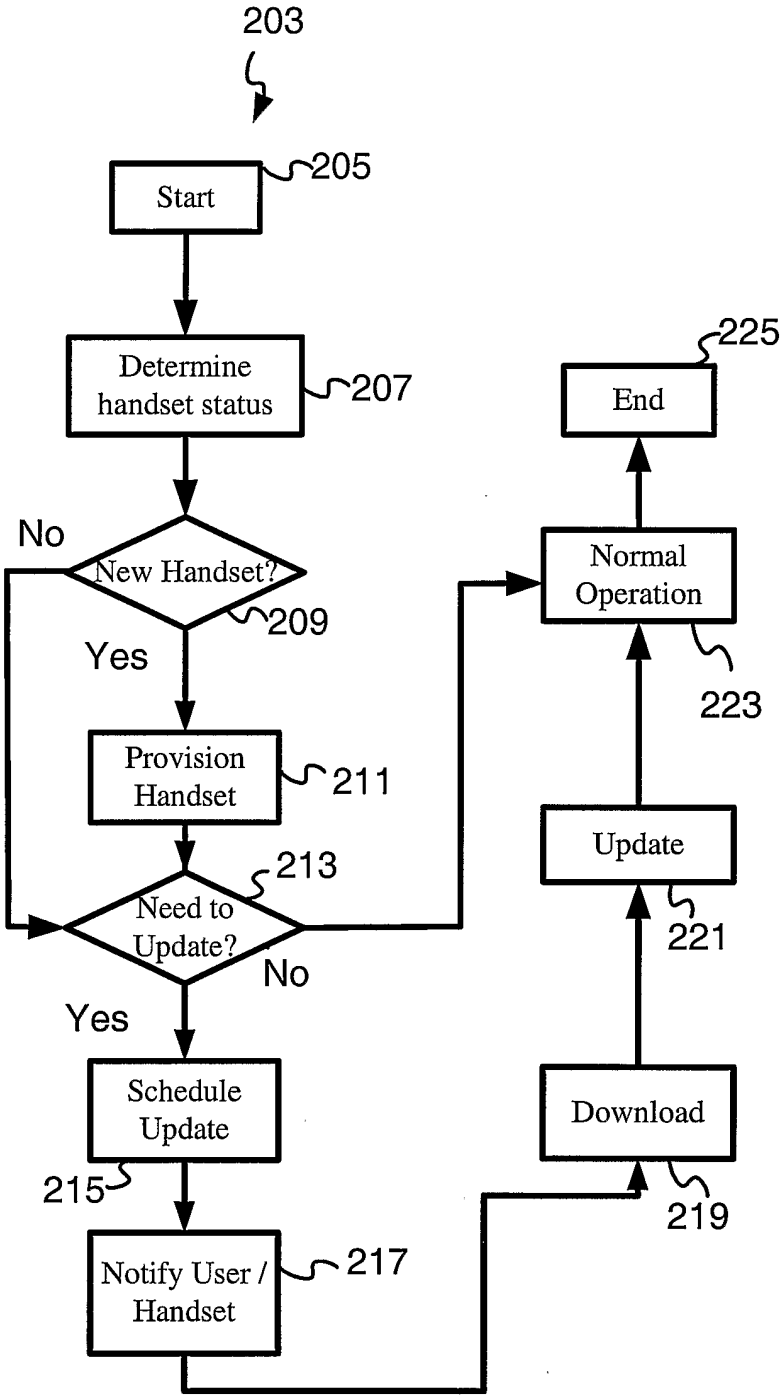

203
Start
205
Determine handset status
207
New Handset?
209
No
Yes
Provision Handset
211
Need to Update?
213
No
Yes
Schedule Update
215
Notify User / Handset
217
Download
219
Update
221
Normal Operation
223
End
225

Fig. 2

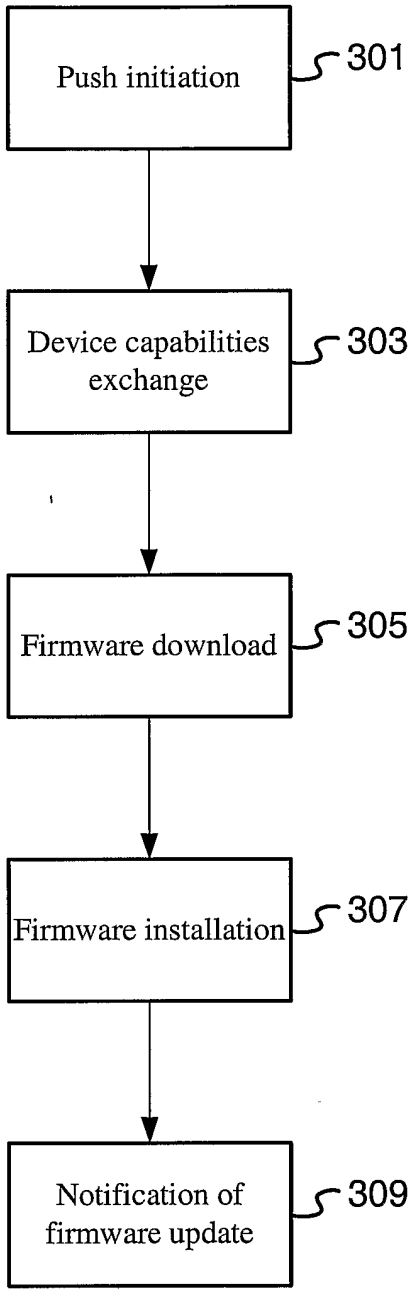

Push initiation
301
Device capabilities exchange
303
Firmware download
305
Firmware installation
307
Notification of firmware update
309

Fig. 3

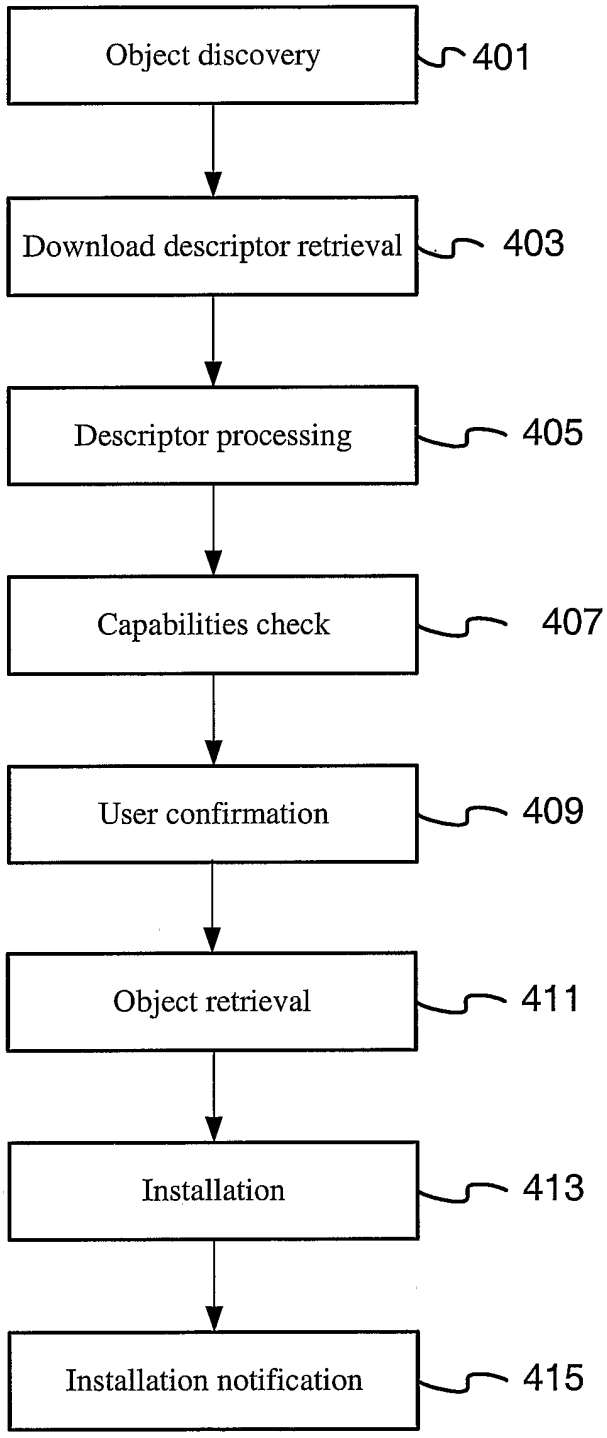

Object discovery
401
Download descriptor retrieval
403
Descriptor processing
405
Capabilities check
407
User confirmation
409
Object retrieval
411
Installation
413
Installation notification
415

Fig. 4