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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 February 2009 (26.02.2009)

PCT

(10) International Publication Number
WO 2009/026109 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 36/08* (2009.01)

(21) International Application Number:
PCT/US2008/073218

(22) International Filing Date: 14 August 2008 (14.08.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/956,658	17 August 2007 (17.08.2007)	US
60/980,557	17 October 2007 (17.10.2007)	US
12/188,990	8 August 2008 (08.08.2008)	US

(71) Applicant *(for all designated States except US)*: **QUALCOMM Incorporated** [US/US]; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KRISHNASWAMY, Dilip** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agent: **TAM, Kam T.**; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, Califonia 92121 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

[Continued on next page]

(54) Title: HANDOFF AT AN AD-HOC MOBILE SERVICE PROVIDER

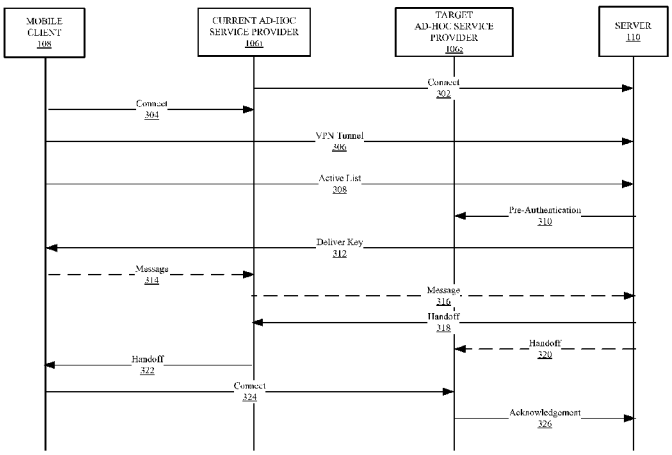

FIG. 3

(57) Abstract: An ad-hoc service provider is configured to support pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider. The ad-hoc service provider is further configured to enable the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

WO 2009/026109 A1

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

HANDOFF AT AN AD-HOC MOBILE SERVICE PROVIDER

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application for patent claims priority under 35 U.S.C. § 119 to Provisional Application No. 60/956,658 entitled, "Method for a Heterogeneous Wireless Ad Hoc Mobile Service Provider," filed August 17, 2007 and Provisional Application No. 60/980,557 entitled, "Handoff In Ad-Hoc Mobile Broadband Networks," filed October 17, 2007.

BACKGROUND

Field

[0002] The present disclosure relates generally to telecommunications, and more specifically to handoff in an ad-hoc mobile broadband network.

Background

[0003] Wireless telecommunication systems are widely deployed to provide various services to consumers, such as telephony, data, video, audio, messaging, broadcasts, etc. These systems continue to evolve as market forces drive wireless telecommunications to new heights. Today, wireless networks are providing broadband Internet access to mobile subscribers over a regional, a nationwide, or even a global region. Such networks are sometimes referred as Wireless Wide Area Networks (WWANs). WWAN operators generally offer wireless access plans to their subscribers such as subscription plans at a monthly fixed rate.

[0004] Accessing WWANs from all mobile devices may not be possible. Some mobile devices may not have a WWAN radio. Other mobile devices with a WWAN radio may not have a subscription plan enabled. Ad-hoc networking allows mobile devices to dynamically connect over wireless interfaces using protocols such as WLAN, Bluetooth, UWB or other protocols. There is a need in the art for a methodology to allow a user of a mobile device without WWAN access to dynamically subscribe to wireless access service provided by a user with a WWAN-capable mobile device using wireless ad-hoc networking between the mobile devices belong to the two users.

SUMMARY

[0005] In one aspect of the disclosure, an ad-hoc service provider includes a processing system configured to support pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider, the processing system being further configured to enable the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

[0006] In another aspect of the disclosure, a method of receiving a handoff at an ad-hoc service provider includes supporting pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider, and enabling the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

[0007] In a further aspect of the disclosure, an ad-hoc service provider includes means for supporting pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider, and means for enabling the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

[0008] In yet a further aspect of the disclosure, a machine-readable medium includes instructions executable by a processing system in a mobile server provider, the instructions include code for supporting pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider, and code for enabling the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

[0009] It is understood that other aspects of the disclosure will become readily apparent to those skilled in the art from the following detailed description, wherein various aspects of an ad-hoc mobile broadband network are shown and described by way of illustration. As will be realized, these aspects of the disclosure are capable of other and different configurations and its several details are capable of modification in various other respects. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] FIG. 1 is a simplified block diagram illustrating an example of a telecommunications system.

[0011] FIG. 2 is a simplified block diagram illustrating an example of a handoff in a telecommunications system.

[0012] FIG. 3 is a call flow diagram illustrating an example of a pre-authentication process for handoff.

[0013] FIG. 4 is a simplified block diagram illustrating an example of the functionality of an ad-hoc service provider.

[0014] FIG. 5 is a simplified block diagram illustrating an example of a hardware configuration for a processing system in an ad-hoc service provider.

DETAILED DESCRIPTION

[0015] The detailed description set forth below in connection with the appended drawings is intended as a description of various aspects of an ad-hoc mobile broadband network and is not intended to represent the only aspects which are encompassed by the claims. The detailed description includes specific details for the purpose of providing a thorough understanding of these aspects. However, it will be apparent to those skilled in the art that various aspects of an ad-hoc mobile broadband network may be practiced without these specific details. In some instances, well-known structures and components are shown in block diagram form in order to avoid obscuring the various concepts presented throughout this disclosure.

[0016] FIG. 1 is a simplified block diagram illustrating an example of a telecommunications system. The telecommunications system 100 is shown with multiple WWANs that provide broadband access to a network 102 for mobile subscribers. The network 102 may be a packet-based network such as the Internet or some other suitable network. For clarity of presentation, two WWANs 104 are shown with a backhaul connection to the Internet 102. Each WWAN 104 may be implemented with multiple fixed-site base stations (not shown) dispersed throughout a geographic region. The geographic region may be generally subdivided into smaller regions known as cells. Each base station may be configured to serve all mobile subscribers within its

respective cell. A base station controller (not shown) may be used to manage and coordinate the base stations in the WWAN 104 and support the backhaul connection to the Internet 102.

[0017] Each WWAN 104 may use one of many different wireless access protocols to support radio communications with mobile subscribers. By way of example, one WWAN 104 may support Evolution-Data Optimized (EV-DO), while the other WWAN 104 may support Ultra Mobile Broadband (UMB). EV-DO and UMB are air interface standards promulgated by the 3rd Generation Partnership Project 2 (3GPP2) as part of the CDMA2000 family of standards and employs multiple access techniques such as Code Division Multiple Access (CDMA) to provide broadband Internet access to mobile subscribers. Alternatively, one of WWAN 104 may support Long Term Evolution (LTE), which is a project within the 3GPP2 to improve the Universal Mobile Telecommunications System (UMTS) mobile phone standard based primarily on a Wideband CDMA (W-CDMA) air interface. . One of WWAN 104 may also support the WiMAX standard being developed by the WiMAX forum. The actual wireless access protocol employed by a WWAN for any particular telecommunications system will depend on the specific application and the overall design constraints imposed on the system. The various techniques presented throughout this disclosure are equally applicable to any combination of heterogeneous or homogeneous WWANs regardless of the wireless access protocols utilized.

[0018] Each WWAN 104 has a number of mobile subscribers. Each subscriber may have a mobile node 106 capable of accessing the Internet 102 directly through the WWAN 104. In the telecommunications system shown in FIG. 1, these mobile nodes 106 access the WWAN 104 using a EV-DO, UMB or LTE wireless access protocol; however, in actual implementations, these mobile nodes 106 may be configured to support any wireless access protocol.

[0019] One or more of these mobile nodes 106 may be configured to create in its vicinity an ad-hoc network based on the same or different wireless access protocol used to access the WWAN 104. By way of example, a mobile node 106 may support a UMB wireless access protocol with a WWAN, while providing an IEEE 802.11 access point for mobile nodes 108 that cannot directly access a WWAN. IEEE 802.11 denotes a set of Wireless Local Access Network (WLAN) standards developed by the IEEE 802.11

committee for short-range communications (e.g., tens of meters to a few hundred meters). Although IEEE 802.11 is a common WLAN wireless access protocol, other suitable protocols may be used.

[0020] A mobile node 106 that may be used to provide an access point for another mobile node 108 will be referred to herein as an "ad-hoc service provider." A mobile node 108 that may use an access point of an ad-hoc service provider 106 will be referred to herein as a "mobile client." A mobile node, whether an ad-hoc service provider 106 or a mobile client 108, may be a laptop computer, a mobile telephone, a personal digital assistant (PDA), a mobile digital audio player, a mobile game console, a digital camera, a digital camcorder, a mobile audio device, a mobile video device, a mobile multimedia device, or any other device capable of supporting at least one wireless access protocol.

[0021] The ad-hoc service provider 106 may extend its wireless broadband Internet access service to mobile clients 108 that would otherwise not have Internet access. A server 110 may be used as an "exchange" to enable mobile clients 108 to purchase unused bandwidth from ad-hoc service providers 106 to access, for example, the Internet 102 across WWANs 104.

[0022] An ad-hoc service provider 106, a server 110, and one or more mobile clients 108 may establish a network that is an ad-hoc heterogeneous wireless network. By way of example, a heterogeneous wireless network may include at least two types of wireless networks (e.g., a WWAN and a WLAN). By way of example, an ad-hoc network may be a network whose specific configuration may change from time to time or from the formation of one network to the next. The network configuration is not pre-planned prior to establishing the network. Examples of configurations for an ad-hoc network may include a configuration as to which members are to be in the network (e.g., which ad-hoc service provider, which server, and/or which mobile client(s) are to be included in a network), a configuration as to the geographic locations of an ad-hoc service provider and mobile client(s), and a configuration as to when and how long a network is to be established.

[0023] In one example of an exchange, mobile clients 108 register with the server 110. Once registered, a mobile client 108 may search for available ad-hoc service providers 106 when Internet access is desired. When the mobile client 108 detects the presence of one or more ad-hoc service providers 106, it may select a ad-hoc service provider 106 to

initiate a session with based on various parameters such as bandwidth, Quality of Service (QoS) and cost. Another parameter that may be used by the mobile client 108 to select a ad-hoc service provider 106 is availability in terms of time. By way of example, a mobile subscriber in an airport may turn on his mobile node (e.g., a laptop computer or a mobile telephone) and use it as an ad-hoc service provider 108 for 30 minutes as he awaits his flight. A mobile client 108 requiring access to the Internet 102 for 45 minutes may choose not to select this ad-hoc service provider 106 even if the ad-hoc service provider 108 can provide adequate bandwidth with good QoS. Another mobile client 108, however, requiring Internet access for 15 minutes, may select this ad-hoc service provider 106 because of its bandwidth and QoS. In any event, once a mobile client 108 selects an ad-hoc service provider 106, a session may be established based on the parameters negotiated be the two (e.g., bandwidth, QoS, duration of the session, etc.). A link encryption key may be established between the mobile client 108 and the ad-hoc service provider 106 during the establishment of the session. A Secured Socket Layer Virtual Private Network (SSL VPN) session may be established between the mobile client 108 and the server 110. The transport layer ports may be kept in the open and not encrypted to provide visibility for the network address translation functionality at the ad-hoc service provider 106. In this example, all Internet traffic is routed through the server 110 via a client-server tunnel 112 to provide security.

[0024] In some telecommunication systems, once a mobile client 108 has gained access to the Internet 102, it listens for other ad-hoc service providers 106 and measures the signal strength of the ad-hoc service providers 106 it can hear. The mobile client 108 uses these measurements to create an active list. The active list is a list of ad-hoc service providers 106 that can provide service to the mobile client 108. The mobile client 108 will continue to measure the signal strength of other ad-hoc service providers 106 and may add or remove ad-hoc service providers 106 from the active list as the configuration of the ad-hoc network changes.

[0025] One function of the active set is to allow the mobile client 108 to quickly switch between ad-hoc service providers 106 while maintaining the current session with the server 110. The mobile client 108 may consider a handoff to another ad-hoc service provider 106 based on any number of factors. These factors may include, by way of example, the inability of the ad-hoc service provider 106 to provide the bandwidth or QoS negotiated at the beginning of the session. Alternatively, the ad-hoc service

provider 106 may not be able to provide Internet access to the mobile client 108 for the entire duration of the session. It would not be uncommon for a mobile subscriber on an ad-hoc service provider 106 that negotiates a 30 minute session with a mobile client 108 to leave the vicinity 15 minutes into the session for whatever reason. In that event, the mobile client 108 would need to select a new ad-hoc service provider from the active list for handoff. The server 110 uses the active list to pre-authenticate other ad-hoc service providers for handoff during the session between the mobile client 108 and the current ad-hoc service provider 106. By pre-authenticating the ad-hoc service provider 106 in the active list before the ad-hoc service provider 106 currently serving the mobile client 108 goes down, the time required to handoff the mobile client 108 can be reduced.

[0026] The term "pre-authenticating" as used herein means authenticating a target ad-hoc service 106 provider for handoff prior to receiving a message from the ad-hoc service provider 106 currently serving the mobile client 108 relating to the unavailability of the current ad-hoc service provider 106. The message may provide notification to the server 110 that the current ad-hoc service provider 106 has gone down and a hard handoff must be performed to another ad-hoc service provider 106 if the session between the mobile client 108 and the server 110 is to be maintained. Alternatively, the message may provide notification to the server 110 that the current ad-hoc service provider 106 will be going down shortly, or that it can no longer provide the mobile client 108 with the service agreed upon (e.g., QoS, bandwidth, etc.). This provides the server 110 with the option of enabling a soft handoff of the mobile client 108 to another ad-hoc service provider 106.

[0027] Pre-authentication includes provisioning, prior to handoff, a potential new service provider 106 and a mobile client 108 with encryption/decryption keys that may be needed for communication between the potential new service provider 106 and the mobile client 108.

[0028] Pre-authentication also includes provisioning, prior to handoff, the current service provider 106 and the new service provider 106 with encryption/decryption keys that may be needed for communication between the current service provider 106 and the new service provider 106.

[0029] Pre-authentication also includes authorization of communication between the potential new service provider 106 and the current service provider 106. It also includes authorization of communication between the potential new service provider 106 and the mobile client 108.

[0030] FIG. 2 is a simplified block diagram illustrating an example of a handoff in a telecommunications system. In this example, the mobile client 108 is being handed off from a current ad-hoc service provider 106_1 to a target service provider 106_2. A persistent tunnel 112 between the two ad-hoc service providers 106_1, 106_2 is used to maintain the mobile client's session with the server 110 during handoff. Data packets received by the current ad-hoc service provider 106_1 during handoff may be forwarded to the target ad-hoc service provider 106_2 through the tunnel 112. Alternatively, or in addition to, the data packets received by the current service provider 106_1 may be forwarded to the target ad-hoc service provider 106_2 directly over a wireless link 114 between the two as shown in FIG. 2, or through another ad-hoc service provider (not shown).

[0031] The mobile client 108 may have an IPv4, IPv6, or other suitable address that is used by the server 110 to maintain the session. The address may be provided to the mobile client 108 by the server 110 or one of the ad-hoc service providers 106 in the telecommunications network 100 (see FIG. 1). Alternatively, the address may be stored on the mobile client 108. In at least one configuration, the address may be a MobileIP address.

[0032] The tunneling anchor is shown in FIG. 2 as a server. However, the tunneling anchor may be any suitable entity or distributed across multiple entities in the telecommunications system 100. The tunneling anchor may be coupled to the Internet 102 as shown in FIG. 2 or located elsewhere. By way of example, the tunneling anchor may be located anywhere on the Internet 102 or within the network operator's infrastructure. Those skilled in the art will be readily able to determine the optimal implementation of the tunneling anchor for any particular application based on the performance requirements, the overall design constraints imposed on the system, and/or other relevant factors.

[0033] FIG. 3 is a call flow diagram illustrating an example of the authentication process for handoff. For clarity of presentation, various signaling for the ad-hoc service

providers 106 and clients 108 to authenticate the server 110 and register with the server 110 will be omitted.

[0034] In step 302, a connection may be initiated by an ad-hoc service provider 106_1 with the server 110 when the ad-hoc service provider 106_1 is mobile and desires to provide service. Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) may be used for Authentication, Authorization and Accounting (AAA) and secure session establishment for this connection. In step 304, a connection may be initiated by a mobile client 108 with the ad-hoc service provider 106_1 (hereinafter referred to as the "current ad-hoc service provider") when the mobile client 108 requires Internet access. EAP-TTLS may also be used for AAA and secure session establishment. In particular, the ad-hoc service provider 106_1 sends the mobile client's credentials to the server 110 for EAP-AAA authentication. The EAP-TTLS authentication response from the server 110 is then used to generate a master shared key. Subsequently, a link encryption key may be established between the current ad-hoc service provider 106_1 and the mobile client 108. A SSL VPN session may then be established, in step 306, between the mobile client 108 and the server 110.

[0035] It should be noted that information flow may be encrypted using encryption/decryption keys between any pair of nodes (where the nodes comprise the server 110, the current service provider 106_1, the target service provider 106_2, and the mobile client 108). Such encryption/decryption keys can be set up in the system when nodes in the system connect with the server. Typically symmetric key cryptography such as using AES may be used for such encryption or decryption for message-flow between any pair of nodes in the system.

[0036] In step 308, the mobile client 108 provides the active list to the server 110. Alternatively, the mobile client 108 can send a report identifying ad-hoc service providers that it can hear accompanied by data indicating the signal strength measurements for each, and any other service parameters for the service providers that it can infer. The server 110 may use the report to generate the active list at its end.

[0037] The server 110 pre-authenticates one or more of the ad-hoc service providers in the active list. During pre-authentication of a target service provider 106_2 with a client 108, the server 110 provisions the target-service provider 106_2 with an encryption/decryption key for communication with the client 108. The server may

additionally provision the target service provider 106_2 with an encryption/decryption key for communication with the current service provider 106_1. The server 110 also provisions the client 108 with the encryption/decryption key to communicate with the target service provider 106_2. The current service provider 106_1 can be provisioned by the server 110, either at the time of a handoff or anytime earlier, with the encryption/decryption key to communicate with the target service provider 106_2. The exact number of ad-hoc service providers in the active list that are pre-authenticated may depend on the admission control policies implemented by the server 110. By way of example, the server 110 may limit the number of ad-hoc service providers at a given location if it determines that additional ad-hoc service providers will adversely affect performance in the WWAN. Additional constraints may be imposed by the WWAN operators that may not want its mobile subscribers to provide service in a given geographic location depending on various network constraints. In any event, the server 110 pre-authenticates one or more ad-hoc service providers by providing each of them with a key to encrypt the data link between the mobile client 108 and the new ad-hoc service provider 106 following handoff. In FIG. 3, the server 110 is shown, in step 310, providing the key to one ad-hoc service provider 106_2 (hereinafter referred to as the target ad-hoc service provider). In step 312, the server 110 also provides the key to the mobile client 108.

[0038] In step 314, the mobile client 108 sends a message to the current ad-hoc service provider 106 requesting a handoff to an alternate service provider. Step 314 is optional and is indicated by a dotted line from the client to the ad-hoc service provider.

[0039] In step 316, the current ad-hoc service provider 106_1 sends a message to the server 110 requesting a handoff. Such a message is tagged with an identifier that indicates that the handoff was initiated by the mobile client 108, or that it was initiated by the current ad-hoc service provider 106_1. The message may be created at the current ad-hoc service provider 106_1 as a consequence of the current ad-hoc service provider's unavailability to continue to provide service to the mobile client. Alternatively, the message could have been created at the mobile client (step 314), which needs to be sent by the current ad-hoc service provider 106_1 to the server 110. For a handoff that is initiated directly by the server, step 316 is optional. For a handoff that is initiated by the mobile client 108, or by the ad-hoc service provider 106_1, in step 318, the server 110 responds to step 316 by sending a message back to current ad-hoc service provider 106_1

authorizing handoff. Alternatively, step 318 could be a message from the server initiating a handoff, in the absence of a message 316 from the current ad-hoc service provider 106_1. The message sent to the current ad-hoc service provider 106_1 may identify the target ad-hoc service provider 106_2 for handoff, or alternatively, allow the mobile client 108 to make the decision. In the latter case, the user on the mobile client 108 selects a target ad-hoc service provider for handoff in accordance with any admission control policy constraints imposed by the server 110. The server 110 may also provide the mobile client 108 with a quality metric for each ad-hoc service provider available to the mobile client. This quality metric may be used to assist the user on a mobile client 108 to select a new ad-hoc service provider for handoff. In the example shown in FIG. 3, the mobile client 108 selects the target ad-hoc service provider 106_2 for handoff.

[0040] In step 320, the server may optionally send a message regarding the handoff to one or more target service providers 106_2. In step 322, the handoff message received from the server 110 is sent by the current service provider 106_1 to the mobile client 108.

[0041] In step 324, the mobile client 108 establishes a connection with the target ad-hoc service provider 106_2 by sending a message encrypted with a key. Since the target ad-hoc service provider 106_2 received the same key during the pre-authentication process, it can decrypt the message and establish a session with the mobile client 108 to complete the handoff. The target ad-hoc service provider 106_2 may also send a message back to the server 110, in step 326, to signify that the handoff has been successfully completed.

[0042] Packets that have left the mobile client 108 may be in transit to the current ad-hoc service provider 106_1, or could be at the current ad-hoc service provider 106_1. These packets need to continue to be supported by the current ad-hoc service provider 106_1. Other packets that have left the mobile client 108 may be in transit to the server 110, or may be waiting at server 110 for further processing, or may be in transit to their final destination beyond the tunneling server. Future packets that leave the mobile client 108 are sent to the target ad-hoc service provider 106_2 after handoff. Packets that are destined to the mobile client 108 may be waiting at the server. Such packets are sent to the target ad-hoc service provider 106_2 after handoff. Other packets destined for the mobile client 108 may be in transit to the current ad-hoc service provider 106_1, or may

be waiting at the current ad-hoc service provider 106_1, or may be in transit from the current service provider to the mobile client 108, and the current ad-hoc service provider 106_1 needs to continue to support such packets to be delivered to the mobile client 108. The delivery of such packets can be done over a wireless link or a multi-hop wireless path between the current ad-hoc service provider 106_1 and the target ad-hoc service provider 106_2. Alternatively, such packets can be delivered by the current ad-hoc service provider 106_1 to the server 110, which then sends them through the target ad-hoc service provider 106_2. Messages between the current ad-hoc service provider 106_1 and the target ad-hoc service provider 106_2 may be exchanged either through the server 110, or over a wireless link or multi-hop wireless path between the service providers.

[0043] FIG. 4 is a simplified block diagram illustrating an example of the functionality of an ad-hoc service provider. The ad-hoc service provider 106 has the ability to enable interconnection between wireless links over homogeneous or heterogeneous wireless access protocols. This may be achieved with a WWAN network interface 402 that supports a wireless access protocol for a WWAN to the Internet 102, and a WLAN network interface 404 that provides a wireless access point for mobile clients 108. By way of example, the WWAN network interface 402 may include a transceiver function that supports EV-DO for Internet access through a WWAN, and the WLAN network interface 404 may include a transceiver function that provides an 802.11 access point for mobile clients 108. More generally, each of the WWAN and WLAN network interfaces 402, 404 may be configured to implement the physical layer by providing the means to transmit raw data bits in accordance with the physical and electrical specifications required to interface to its respective transmission medium. Each of the WWAN and WLAN network interfaces 402, 404 may also be configured to implement the lower portion of the data link layer by managing access to its respective transmission medium.

[0044] The ad-hoc service provider 106 is shown with a filtered interconnection and session monitoring module 406. The module 406 provides filtered processing of content from mobile clients 108 so that the interconnection between the ad-hoc wireless links to the WWAN interface 402 is provided only to mobile clients 108 authenticated and permitted by the server to use the WWAN network. The module 406 also maintains tunneled connectivity between the server and the authenticated mobile clients 108.

[0045] The ad-hoc service provider 106 also includes a service provider application 408 that (1) enables the module 406 to provide ad-hoc services to mobile clients 108, and (2) supports WWAN or Internet access to a mobile subscriber or user of the ad-hoc service provider 106. The latter function is supported by a user interface 412 that communicates with the WWAN interface 402 through the module 406 under control of the service provider application 408.

[0046] As discussed above, the service provider application 408 enables the module 406 to provide ad-hoc services to mobile clients 108. The service provider application 408 maintains a session with the server to exchange custom messages with the server. In addition, the service provider application 408 also maintains a separate session with each mobile client 108 for exchanging custom messages between the service provider application 408 and the mobile client 108. The service provider application 408 provides information on authenticated and permitted clients to the filtered interconnection and session monitoring module 406. The filtered interconnection and session monitoring module 408 allows content flow for only authenticated and permitted mobile clients 108. The filtered interconnection and session monitoring module 406 also optionally monitors information regarding content flow related to mobile clients 108 such as the amount of content outbound from the mobile clients and inbound to the mobile clients, and regarding WWAN and WLAN network resource utilization and available bandwidths on the wireless channels. The filtered interconnection and session monitoring module 406 can additionally and optionally provide such information to the service provider application 408. The service provider application 408 can optionally act on such information and take appropriate actions such as determining whether to continue maintaining connectivity with the mobile clients 108 and with the server, or whether to continue to provide service. It should be noted that the functions described in modules 406 and 408 can be implemented in any given platform in one or multiple sets of modules that coordinate to provide such functionality at the ad-hoc service provider 106.

[0047] When the ad-hoc service provider 106 decides to provide these services, the service provider application 408 sends a request to the server for approval. The service provider application 408 requests authentication by the server and approval from the server to provide service to one or more mobile clients 108. The server may authenticate the ad-hoc service provider 106 and then determine whether it will grant

the ad-hoc service provider's request. As discussed earlier, the request may be denied if the number of ad-hoc service providers in the same geographic location is too great or if the WWAN operator has imposed certain constraints on the ad-hoc service provider 106.

[0048] Once the ad-hoc service provider 106 is authenticated, the service provider application 408 may advertise an ad-hoc WLAN Service Set Identifier (SSID). Interested mobile clients 108 may associate with the SSID to access the ad-hoc service provider 106. The service provider application 408 may then authenticate the mobile clients 108 with the server and then configure the filtered interconnection and session monitoring module 406 to connect the mobile clients 108 to the server. During the authentication of a mobile client 108, the service provider application 408 may use an unsecured wireless link.

[0049] The service provider application 408 may optionally choose to move a mobile client 108 to a new SSID with a secure link once the mobile client 108 is authenticated. In such situations, the service provider application 408 may distribute the time it spends in each SSID depending on the load that it has to support for existing sessions with mobile clients 108.

[0050] The service provider application 408 may also be able to determine whether it can support a mobile client 108 before allowing the mobile client 108 to access a network. Resource intelligence that estimates the drain on the battery power and other processing resources that would occur by accepting a mobile client 108 may assist in determining whether the service provider application 408 should consider supporting a new mobile client 108 or accepting a handoff of that mobile client 108 from another ad-hoc service provider.

[0051] The service provider application 408 may admit mobile clients 108 and provide them with a certain QoS guarantee, such as an expected average bandwidth during a session. Average throughputs provided to each mobile client 108 over a time window may be monitored. The service provider application 408 may monitor the throughputs for all flows going through it to ensure that resource utilization by the mobile clients 108 is below a certain threshold, and that it is meeting the QoS requirement that it has agreed to provide to the mobile clients 108 during the establishment of the session.

[0052] The service provider application 408 may also provide a certain level of security to the wireless access point by routing content through the filtered interconnection and session monitoring module 406 without being able to decipher the content. Similarly, the service provider application 408 may be configured to ensure content routed between the user interface 410 and the WWAN 104 via the module 406 cannot be deciphered by mobile clients 108. The service provider application 408 may use any suitable encryption technology to implement this functionality.

[0053] The service provider application 408 may also maintain a time period for a mobile client 108 to access a network. The time period may be agreed upon between the service provider application 408 and the mobile client 108 during the initiation of the session. If the service provider application 408 determines that it is unable to provide the mobile client 108 with access to the network for the agreed upon time period, then it may notify both the server and the mobile client 108 regarding its unavailability. This may occur due to energy constraints (e.g., a low battery), or other unforeseen events. The server may then consider a handoff of the mobile client to another ad-hoc service provider, if there is such an ad-hoc service provider in the vicinity of the mobile client 108. The service provider application 408 may support the handoff of the mobile client 108.

[0054] The service provider application 408 may also dedicate processing resources to maintain a wireless link or limited session with mobile clients 108 served by other ad-hoc service providers. This may facilitate the handoff of mobile clients 108 to the ad-hoc service provider 106.

[0055] The service provider application 408 may manage the mobile client 108 generally, and the session specifically, through the user interface 412. Alternatively, the service provider application 408 may support a seamless operation mode with processing resources being dedicated to servicing mobile clients 108. In this way, the mobile client 108 is managed in a way that is transparent to the mobile subscriber. The seamless operation mode may be desired where the mobile subscriber does not want to be managing mobile clients 108, but would like to continue generating revenue by sharing bandwidth with mobile clients 108.

[0056] In at least one configuration of an ad-hoc service provider, a processing system may be used to implement the filtered interconnection and session monitoring module

406, the service provider application 408, and the service provider user interface 412. The WWAN interface 402 and WLAN interface 404 may be separate from the processing system as shown in FIG. 4, or alternatively, may be integrated, either in part or whole, into the processing system.

[0057] FIG. 5 is a simplified diagram illustrating an example of a hardware configuration for a processing system in an ad-hoc service provider. In this example, the processing system 500 may be implemented with a bus architecture represented generally by bus 502. The bus 502 may include any number of interconnecting buses and bridges depending on the specific application of the processing system 500 and the overall design constraints. The bus links together various circuits including a processor 504, machine-readable media 506, and a service provider user interface 510. The bus 502 may also link various other circuits such as timing sources, peripherals, voltage regulators, power management circuits, and the like, which are well known in the art, and therefore, will not be described any further. A network adapter 508 provides an interface between the WWAN and WLAN network interfaces 402, 404 (see FIG. 4) and the bus 502.

[0058] The processor 504 is responsible for managing the bus and general processing, including the execution of software stored on the machine-readable media 506. The processor 304 may be implemented with one or more general-purpose and/or special-purpose processors. Examples include microprocessors, microcontrollers, DSP processors, and other circuitry that can execute software. Software shall be construed broadly to mean instructions, data, or any combination thereof, whether referred to as software, firmware, middleware, microcode, hardware description language, or otherwise. Machine-readable media may include, by way of example, RAM (Random Access Memory), flash memory, ROM (Read Only Memory), PROM (Programmable Read-Only Memory), EPROM (Erasable Programmable Read-Only Memory), EEPROM (Electrically Erasable Programmable Read-Only Memory), registers, magnetic disks, optical disks, hard drives, or any other suitable storage medium, or any combination thereof.

[0059] In the hardware implementation illustrated in FIG. 5, the machine-readable media 506 is shown as part of the processing system 500 separate from the processor 504. However, as those skilled in the art will readily appreciate, the machine-readable

media 506, or any portion thereof, may be external to the processing system 504. By way of example, the machine-readable media 506 may include a transmission line, a carrier wave modulated by data, and/or a computer product separate from the ad-hoc service provider, all which may be accessed by the processor 504 through the network interface 508. Alternatively, or in addition to, the machine readable media 306, or any portion thereof, may be integrated into the processor 504, such as the case may be with cache and/or general register files.

[0060] The processing system 504 may be configured as a general-purpose processing system with one or more microprocessors providing the processor functionality and external memory providing at least a portion of the machine-readable media 306, all linked together with other supporting circuitry through an external bus architecture. Alternatively, the processing system 504 may be implemented with an ASIC (Application Specific Integrated Circuit) with the processor 504, the network interface 508, the service provider user interface 510, supporting circuitry (not shown), and at least a portion of the machine-readable media 506 integrated into a single chip, or with one or more FPGAs (Field Programmable Gate Array), PLDs (Programmable Logic Device), controllers, state machines, gated logic, discrete hardware components, or any other suitable circuitry, or any combination of circuits that can perform the various functionality described throughout this disclosure. Those skilled in the art will recognize how best to implement the described functionality for the processing system 500 depending on the particular application and the overall design constraints imposed on the overall system.

[0061] The machine-readable media 506 is shown with a number of software modules. The software modules include instructions that when executed by the processor 504 cause the processing system to perform various functions. Each software module may reside in a single storage device or distributed across multiple memory devices. By way of example, a software module may be loaded into RAM from a hard drive when a triggering event occurs. During execution of the software module, the processor 504 may load some of the instructions into cache to increase access speed. One or more cache lines may then be loaded into a general register file for execution by the processor 504. When referring to the functionality of a software module below, it will be understood that such functionality is implemented by the processor 504 when executing instructions from that software module.

[0062] A protocol stack module 511 may be used to implement the protocol architecture, or any portion thereof, for the ad-hoc service provider. In the implementation described thus far, the protocol stack module 511 is responsible for implementing several protocol layers running on top of the data link layers implemented by the WWAN and WLAN network interfaces 402, 404 (see FIG. 4). By way of example, the protocol stack module 511 may be used to implement the upper portion of the data link layer by providing flow control, acknowledgement, and error recovery. The protocol stack module 511 may also be used to implement the network layer by managing source to destination data packet transfer, as well as the transport layer by providing transparent transfer of data between end users. Although described as part of the processing system, the protocol stack module 511, or any portion thereof, may be implemented by the WWAN and WLAN network adapters 402, 404.

[0063] The machine-readable media 506 is also shown with a filtered interconnection and session monitoring module 512 and service provider application 514. These software modules, when executed by the processor 504, cause the processing system to carry out the process steps as shown and described in FIGS. 1-4 in connection with the ad-hoc service provider.

[0064] The user interface 510 may include a keypad, display, speaker, microphone, joystick, and/or any other combination user interface devices that enable a mobile subscriber or user to access the WWAN or the Internet 102.

[0065] Turning now to the mobile client, a TLS session may be used by the mobile client 108 to register with the server 110. Once registered, the mobile client 108 may search for available ad-hoc service providers 106. When the mobile client 108 detects the presence of one or more ad-hoc service providers 106, it may initiate a session using EAP-TTLS with an ad-hoc service provider 106 based on parameters such as the available bandwidth that the ad-hoc service provider 106 can support, the QoS metric of the ad-hoc service provider 106, and the cost of the service advertised. As described earlier, a link encryption key may be established between the mobile client 108 and the ad-hoc service provider 106 during the establishment of the session. An SSL VPN session may be established between the mobile client 108 and the server 110 so that all traffic between the two is encrypted. The transport layer ports may be kept in the open and not encrypted to provide visibility for the network address translation functionality at the ad-hoc service provider 106.

[0066] The handoff of the mobile client 108 may be performed in a variety of ways. In one configuration, the mobile client 108 may maintain a limited session with multiple ad-hoc service providers 106, while using one ad-hoc service provider 106 to access the Internet. As described earlier, this approach may facilitate the handoff process. In an alternative configuration, the mobile client 108 may consider a handoff only when necessary. In this configuration, the mobile client 108 may maintain an active list of ad-hoc service providers 106 in its vicinity for handoff. The mobile client 108 may select an ad-hoc service provider 106 for handoff from the active list when the current ad-hoc service provider 106 needs to discontinue its service. When handoff is not possible, a mobile client 108 may need to reconnect through a different ad-hoc service provider 106 to access the Internet. Persistence of the tunnel between the mobile client and the server can enable a soft handoff of a mobile client from one service provider to another service provider.

[0067] If the bandwidth needs of a mobile client 108 are greater than the capabilities of the available ad-hoc service providers 106, then the mobile client 108 may access multiple ad-hoc service providers 106 simultaneously. A mobile client 108 with multiple transceivers could potentially access multiple ad-hoc service providers 106 simultaneously using a different transceiver for each ad-hoc service provider 106. If the same wireless access protocol can be used to access multiple ad-hoc service providers 106, then different channels may be used. If the mobile client 108 has only one transceiver available, then it may distribute the time that it spends accessing each ad-hoc service provider 106.

[0068] Those of skill in the art would appreciate that the various illustrative blocks, modules, elements, components, methods, and algorithms described herein may be implemented as electronic hardware, computer software, or combinations of both. To illustrate this interchangeability of hardware and software, various illustrative blocks, modules, elements, components, methods, and algorithms have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application.

[0069] It is understood that the specific order or hierarchy of steps in the processes disclosed is an illustration of exemplary approaches. Based upon design preferences, it is understood that the specific order or hierarchy of steps in the processes may be rearranged. The accompanying method claims present elements of the various steps in a sample order, and are not meant to be limited to the specific order or hierarchy presented.

[0070] The previous description is provided to enable any person skilled in the art to practice the various aspects described herein. Various modifications to these aspects will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other aspects. Thus, the claims are not intended to be limited to the aspects shown herein, but is to be accorded the full scope consistent with the language claims, wherein reference to an element in the singular is not intended to mean "one and only one" unless specifically so stated, but rather "one or more." Unless specifically stated otherwise, the term "some" refers to one or more. Pronouns in the masculine (e.g., his) include the feminine and neuter gender (e.g., her and its) and vice versa. All structural and functional equivalents to the elements of the various aspects described throughout this disclosure that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the claims. Moreover, nothing disclosed herein is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the claims. No claim element is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase "means for" or, in the case of a method claim, the element is recited using the phrase "step for."

CLAIMS

WHAT IS CLAIMED IS:

1. An ad-hoc service provider, comprising:

a processing system configured to support pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider, the processing system being further configured to enable the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

2. The ad-hoc service provider of claim 1 wherein the processing system is further configured to support pre-authentication by receiving a key from the server to support an encrypted link between the ad-hoc service provider and the mobile client.

3. The ad-hoc service provider of claim 2 wherein the processing system is further configured to establish a connection with the mobile client to receive the handoff in response to a message encrypted with the key from the mobile client.

4. The ad-hoc service provider of claim 1 wherein the processing system is further configured to support pre-authentication by receiving authorization from the server to communicate with the mobile client.

5. The ad-hoc service provider of claim 1 wherein the processing system is further configured to support pre-authentication by receiving a key from the server to support an encrypted link between the ad-hoc service provider and said another ad-hoc service provider.

6. The ad-hoc service provider of claim 1 wherein the processing system is further configured to support pre-authentication by receiving authorization from the server to communicate with said another ad-hoc service provider.

7. The ad-hoc service provider of claim 1 wherein the processing system is further configured to enable the mobile client to maintain a session with the server while receiving the handoff by supporting a tunnel with said another ad-hoc service provider.

8. The ad-hoc service provider of claim 7 wherein the processing system is further configured to receive through the tunnel at least some packets received by said another ad-hoc service provider from the mobile client.

9. The ad-hoc service provider of claim 1 which the processing system is further configured to receive at least some packets from said another ad-hoc service provider over a wireless link while receiving the handoff.

10. The ad-hoc service provider of claim 9 wherein the processing system is further configured to receive one or more of said at least some packets from said another ad-hoc service provider through yet another ad-hoc service provider.

11. The ad-hoc service provider of claim 1 wherein the processing system is further configured to provide an IPv4 or IPv6 address to the mobile client.

12. The ad-hoc service provider of claim 11 wherein the IPv4 or IPv6 address comprises a MobileIP address.

13. The ad-hoc service provider of claim 1 wherein the processing system is further configured to receive from the server a message to receive the handoff of the mobile client from said another ad-hoc service provider.

14. The ad-hoc service provider of claim 1 wherein the processing system is further configured to support a hard handoff.

15. The ad-hoc service provider of claim 1 wherein the processing system is further configured to support a soft handoff.

16. The ad-hoc service provider of claim 1 wherein the processing system is further configured to send a message to the server indicating that the handoff is complete.

17. A method of receiving a handoff at an ad-hoc service provider, comprising:

supporting pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider; and

enabling the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

18. The method of claim 17 wherein the pre-authentication is supported by receiving a key from the server to support an encrypted link between the ad-hoc service provider and the mobile client.

19. The method of claim 18 further comprising establishing a connection with the mobile client to receive the handoff in response to a message encrypted with the key from the mobile client.

20. The method of claim 17 wherein the pre-authentication is supported by receiving authorization from the server to communicate with the mobile client.

21. The method of claim 17 wherein the pre-authentication is supported by receiving a key from the server to support an encrypted link between the ad-hoc service provider and said another ad-hoc service provider.

22. The method of claim 17 wherein the pre-authentication is supported by receiving authorization from the server to communicate with said another ad-hoc service provider.

23. The method of claim 17 wherein the mobile client is enabled to maintain the session with the server while receiving the handoff by supporting a tunnel with said another ad-hoc service provider.

24. The method of claim 23 further comprising receiving through the tunnel at least some packets received by said another ad-hoc service provider from the mobile client.

25. The method of claim 17 further configured to receive at least some packets from said another ad-hoc service provider over a wireless link while receiving the handoff.

26. The method of claim 25 wherein one or more of said at least some packets received from said another ad-hoc service provider are received through yet another ad-hoc service provider.

27. The method of claim 17 further comprising providing an IPv4 or IPv6 address to the mobile client.

28. The method of claim 27 wherein the IPv4 or IPv6 address comprises a MobileIP address.

29. The method of claim 17 further comprising receiving from the server a message to receive the handoff of the mobile client from said another ad-hoc service provider.

30. The method of claim 17 wherein the handoff comprises a hard handoff.

31. The method of claim 17 wherein the handoff comprises a soft handoff.

32. The method of claim 17 further comprising sending a message to the server indicating that the handoff is complete.

33. An ad-hoc service provider, comprising:

means for supporting pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider; and

means for enabling the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

34. The ad-hoc service provider of claim 33 wherein the means for supporting pre-authentication comprises means for receiving a key from the server to support an encrypted link between the ad-hoc service provider and the mobile client.

35. The ad-hoc service provider of claim 34 further comprising means for establishing a connection with the mobile client to receive the handoff in response to a message encrypted with the key from the mobile client.

36. The ad-hoc service provider of claim 33 wherein the means for supporting pre-authentication comprises means for receiving authorization from the server to communicate with the mobile client.

37. The ad-hoc service provider of claim 33 wherein the means for supporting pre-authentication comprises means for receiving a key from the server to

support an encrypted link between the ad-hoc service provider and said another ad-hoc service provider.

38. The ad-hoc service provider of claim 33 wherein the means for supporting pre-authentication comprises means for receiving authorization from the server to communicate with said another ad-hoc service provider.

39. The ad-hoc service provider of claim 33 wherein the means for enabling the mobile client to maintain the session with the server while receiving the handoff comprises means for supporting a tunnel with said another ad-hoc service provider.

40. The ad-hoc service provider of claim 39 further comprising means for receiving through the tunnel at least some packets received by said another ad-hoc service provider from the mobile client.

41. The ad-hoc service provider of claim 33 further configured means for receiving at least some packets from said another ad-hoc service provider over a wireless link while receiving the handoff.

42. The ad-hoc service provider of claim 41 wherein the means for receiving at least some packets is configured to receive one or more of said at least some packets received from said another ad-hoc service provider through yet another ad-hoc service provider.

43. The ad-hoc service provider of claim 33 further comprising means for providing an IPv4 or IPv6 address to the mobile client.

44. The ad-hoc service provider of claim 43 wherein the IPv4 or IPv6 address comprises a MobileIP address.

45. The ad-hoc service provider of claim 33 further comprising means for receiving from the server a message to receive the handoff of the mobile client from said another ad-hoc service provider.

46. The ad-hoc service provider of claim 33 further comprising means for receiving a hard handoff.

47. The ad-hoc service provider of claim 33 further comprising means for receiving a soft handoff.

48. The ad-hoc service provider of claim 33 further comprising means for sending a message to the server indicating that the handoff is complete.

49. A machine-readable medium comprising instructions executable by a processing system in a mobile server provider, the instructions comprising code for:

supporting pre-authentication with a server for the purpose of receiving a handoff of a mobile client from another ad-hoc service provider; and

enabling the mobile client to maintain a session with the server while receiving the handoff from said another ad-hoc service provider.

50. The machine-readable medium of claim 49 wherein the code for supporting pre-authentication comprises code for receiving a key from the server to support an encrypted link between the ad-hoc service provider and the mobile client.

51. The machine-readable medium of claim 50 wherein the instructions further comprise code for establishing a connection with the mobile client to receive the handoff in response to a message encrypted with the key from the mobile client.

52. The machine-readable medium of claim 49 wherein the code for supporting pre-authentication comprises code for receiving authorization from the server to communicate with the mobile client.

53. The machine-readable medium of claim 49 wherein the code for supporting pre-authentication comprises code for receiving a key from the server to support an encrypted link between the ad-hoc service provider and said another ad-hoc service provider.

54. The machine-readable medium of claim 49 wherein the code for supporting pre-authentication comprises code for receiving authorization from the server to communicate with said another ad-hoc service provider.

55. The machine-readable medium of claim 49 wherein the code for enabling the mobile client to maintain the session with the server while receiving the handoff comprises code for supporting a tunnel with said another ad-hoc service provider.

56. The machine-readable medium of claim 55 wherein the instructions further comprise code for receiving through the tunnel at least some packets received by said another ad-hoc service provider from the mobile client.

57. The machine-readable medium of claim 49 wherein the instructions further comprise code for receiving at least some packets from said another ad-hoc service provider over a wireless link while receiving the handoff.

58. The machine-readable medium of claim 57 wherein the code for receiving at least some packets is configured to receive one or more of said at least some packets received from said another ad-hoc service provider through yet another ad-hoc service provider.

59. The machine-readable medium of claim 49 wherein the instructions further comprise code for providing an IPv4 or IPv6 address to the mobile client.

60. The machine-readable medium of claim 59 wherein the IPv4 or IPv6 address comprises a MobileIP address.

61. The machine-readable medium of claim 49 wherein the instructions further comprise code for receiving from the server a message to receive the handoff of the mobile client from said another ad-hoc service provider.

62. The machine-readable medium of claim 49 wherein the instructions further comprise code for receiving a hard handoff.

63. The machine-readable medium of claim 49 wherein the instructions further comprise code for receiving a soft handoff.

64. The machine-readable medium of claim 49 wherein the instructions further comprise code for sending a message to the server indicating that the handoff is complete.

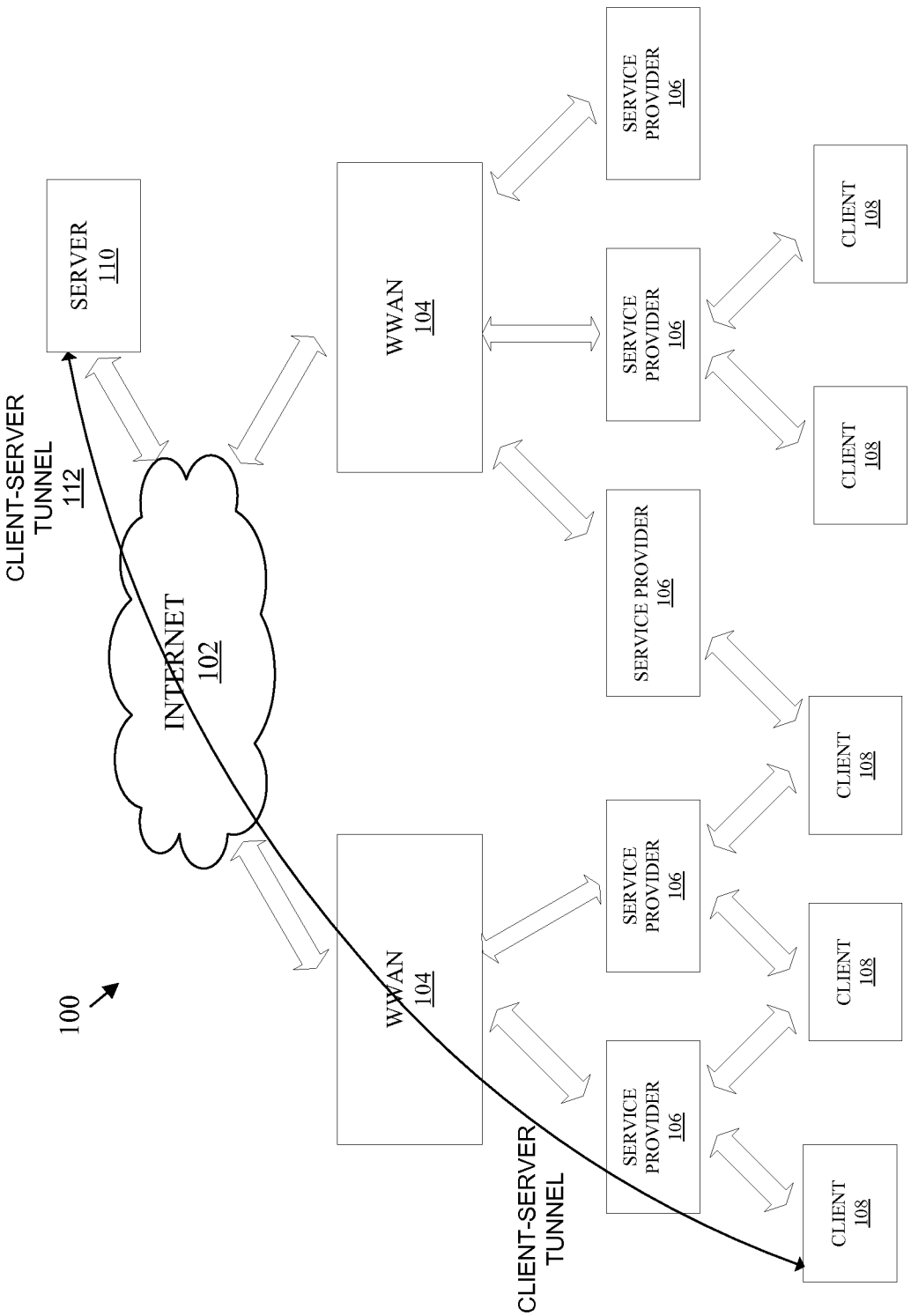
100
SERVER 110
CLIENT-SERVER TUNNEL 112
INTERNET 102
WWAN 104
WWAN 104
SERVICE PROVIDER 106
SERVICE PROVIDER 106
SERVICE PROVIDER 106
SERVICE PROVIDER 106
SERVICE PROVIDER 106
CLIENT 108
CLIENT 108
CLIENT 108
CLIENT 108
CLIENT 108
CLIENT 108
CLIENT-SERVER TUNNEL

FIG. 1

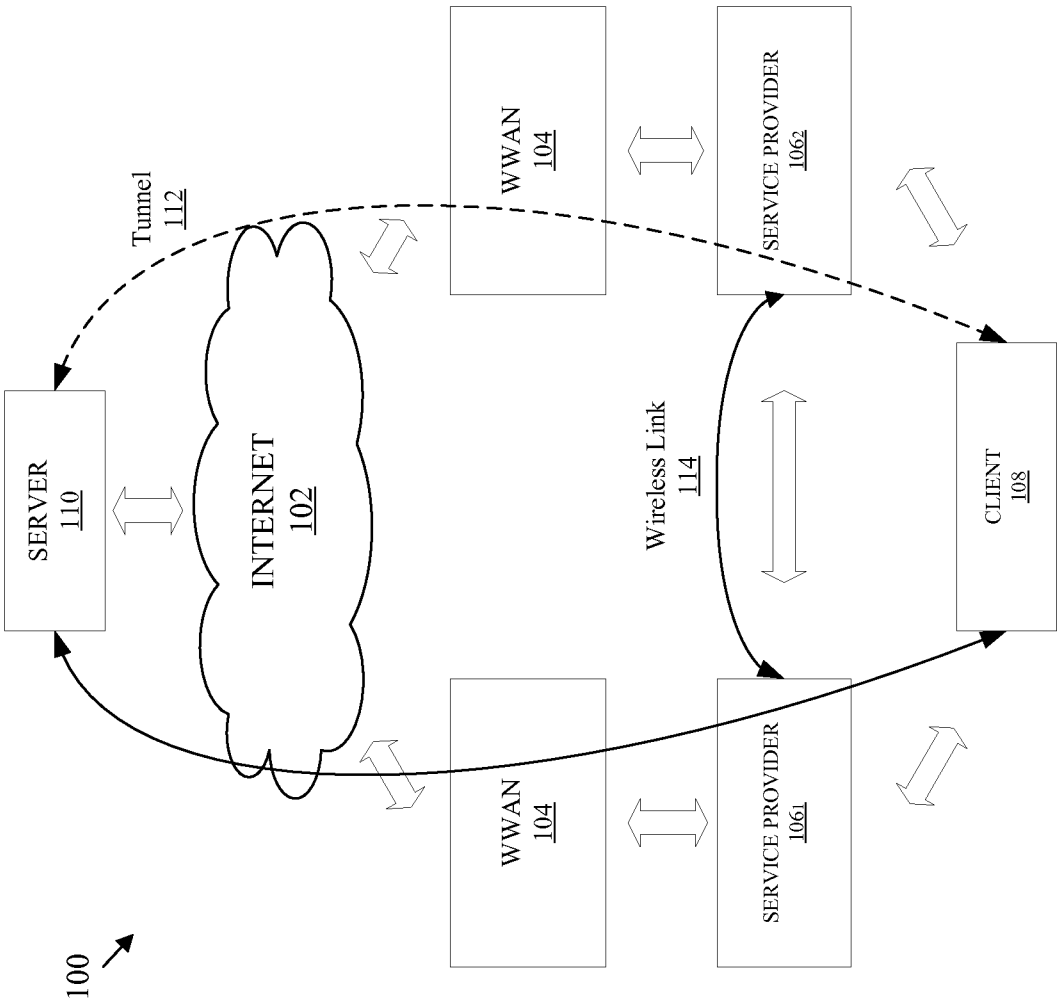
100
SERVER
110
INTERNET
102
Tunnel
112
WWAN
104
WWAN
104
SERVICE PROVIDER
1062
SERVICE PROVIDER
1061
Wireless Link
114
CLIENT
108

FIG. 2

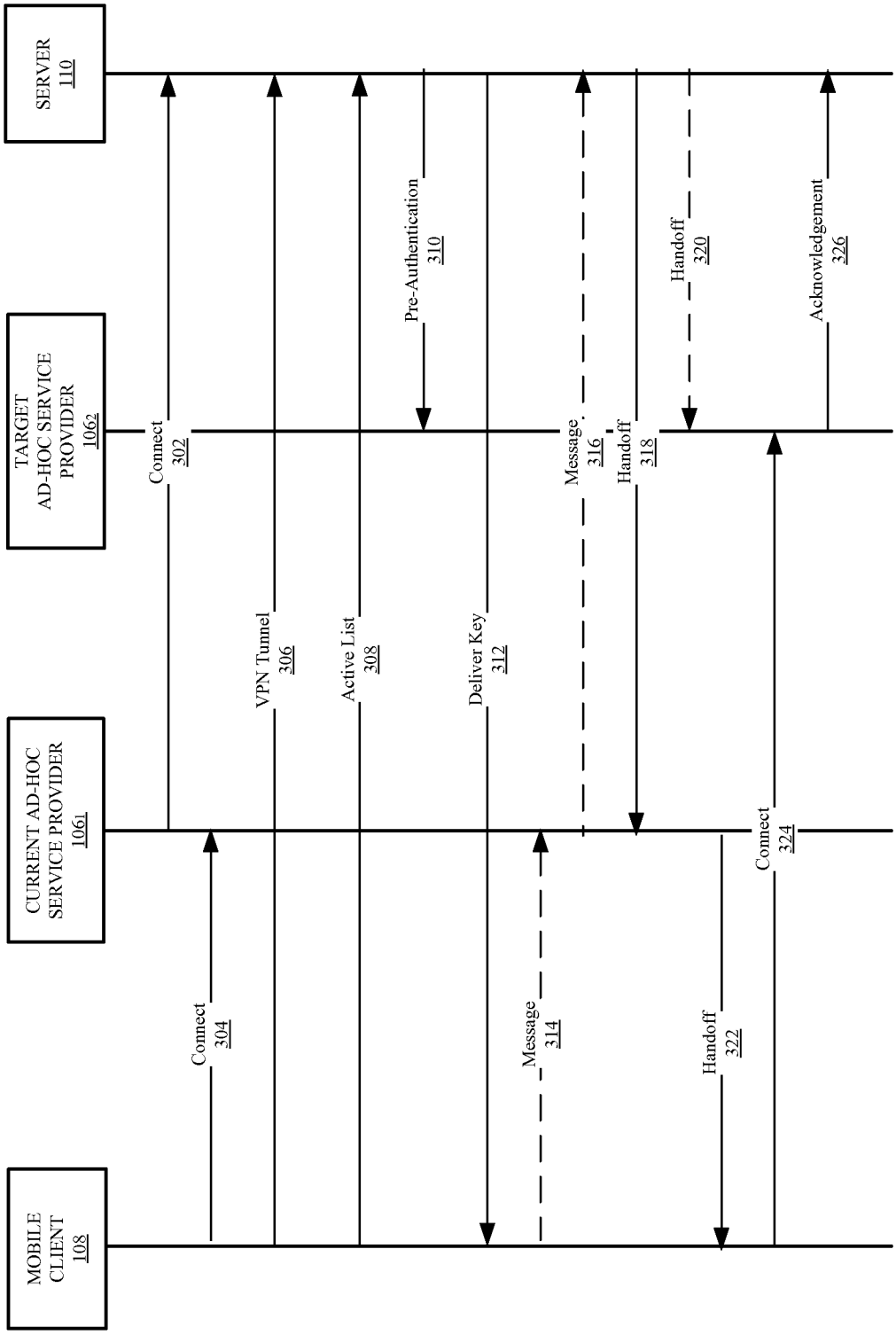
SERVER 110
TARGET AD-HOC SERVICE PROVIDER 1062
CURRENT AD-HOC SERVICE PROVIDER 1061
MOBILE CLIENT 108
Connect 302
Pre-Authentication 310
Handoff 320
Acknowledgement 326
VPN Tunnel 306
Active List 308
Deliver Key 312
Message 316
Handoff 318
Connect 304
Message 314
Handoff 322
Connect 324

FIG. 3

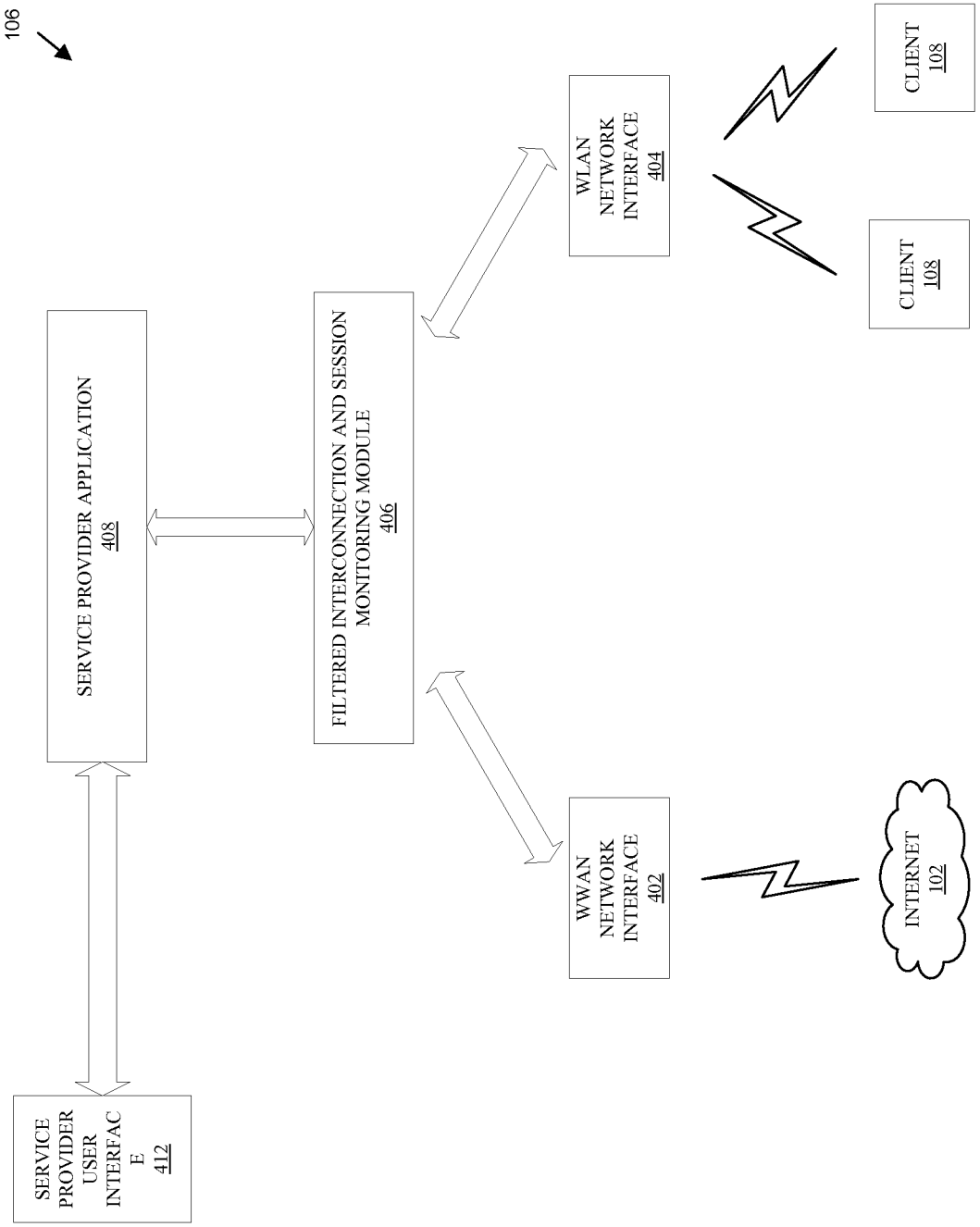
106
SERVICE PROVIDER APPLICATION 408
FILTERED INTERCONNECTION AND SESSION MONITORING MODULE 406
WLAN NETWORK INTERFACE 404
WWAN NETWORK INTERFACE 402
CLIENT 108
CLIENT 108
INTERNET 102
SERVICE PROVIDER USER INTERFACE 412

FIG. 4

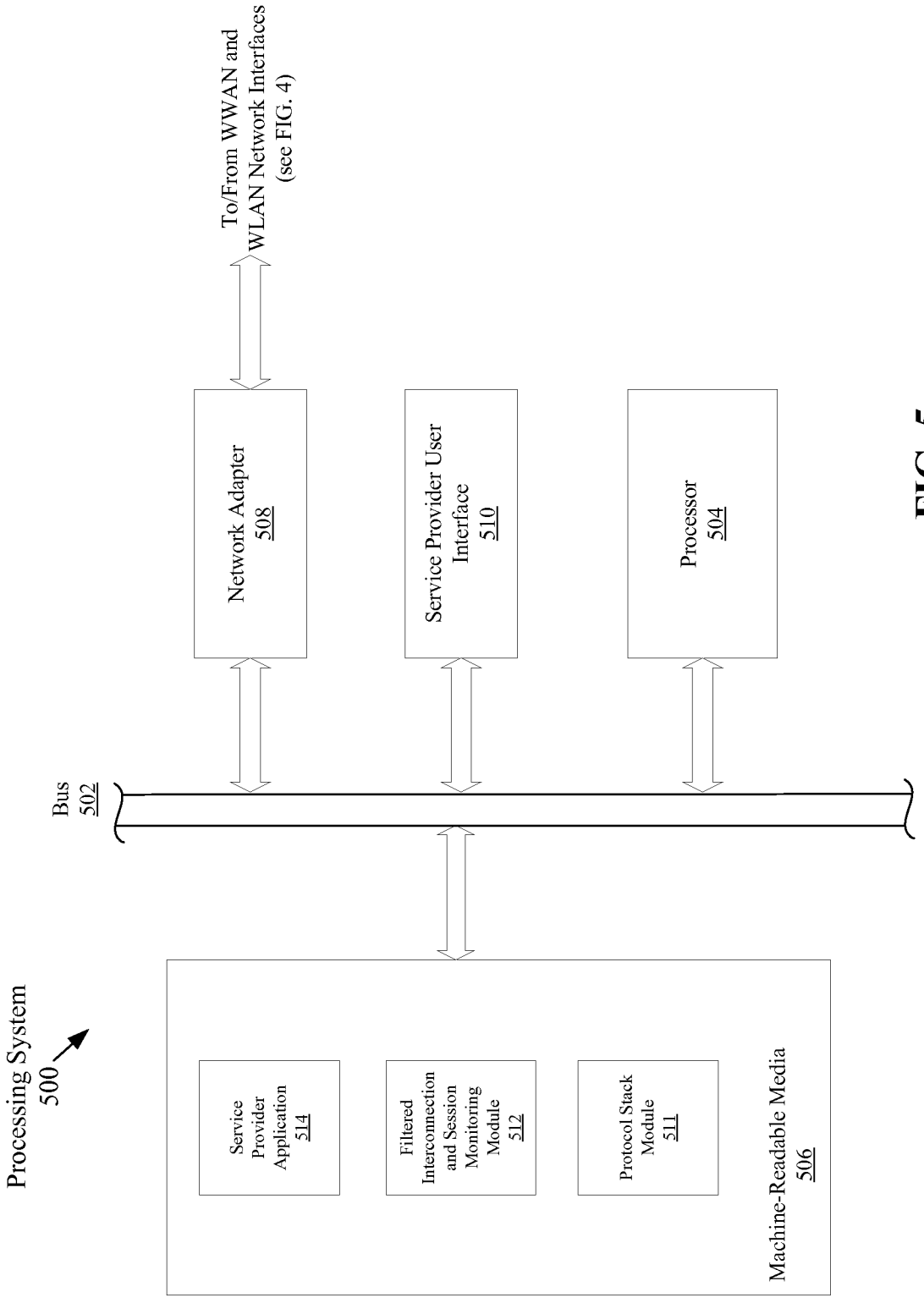
Processing System
500
Bus
502
To/From WWAN and
WLAN Network Interfaces
(see FIG. 4)
Network Adapter
508
Service Provider User
Interface
510
Processor
504
Service
Provider
Application
514
Filtered
Interconnection
and Session
Monitoring
Module
512
Protocol Stack
Module
511
Machine-Readable Media
506

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/073218

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06
ADD. H04W36/08

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 practical, 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	US 2006/176852 A1 (WU KO-CHING [TW] ET AL) 10 August 2006 (2006-08-10)	1-7, 9-23, 27-39, 43-55, 59-64
Y	paragraph [0008]	8-10, 24-26, 40-42, 56-58
	paragraph [0015] - paragraph [0031]	
Y	WO 2007/004051 A (NOKIA CORP [FI]; NOKIA INC [US]; FORSBERG DAN [FI]) 11 January 2007 (2007-01-11)	8-10, 24-26, 40-42, 56-58
A	figures 14A-15B2	1,17,33, 49

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document 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
18 December 2008	05/01/2009

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	Behringer, Lutz

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/073218

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SETHOM K ET AL: "Secure and seamless mobility support in heterogeneous wireless networks" GLOBAL TELECOMMUNICATIONS CONFERENCE, 2005. GLOBECOM '05. IEEE ST. LOIUS, MO, USA 28 NOV.-2 DEC. 2005, PISCATAWAY, NJ, USA,IEEE, vol. 6, 28 November 2005 (2005-11-28), pages 3403-3407, XP010882678 ISBN: 978-0-7803-9414-8 page 3404, right-hand column, line 6 - page 3405, right-hand column, line 35	1,17,33, 49

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2008/073218

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006176852 A1	10-08-2006	TW 262683 B	21-09-2006
WO 2007004051 A	11-01-2007	CN 101243719 A	13-08-2008
		EP 1900245 A1	19-03-2008