

SECURITY FOR A HETEROGENEOUS AD HOC MOBILE BROADBAND NETWORK

CROSS-REFERENCE TO RELATED APPLICATION

[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.

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. Adhoc 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 adhoc networking between the mobile devices belong to the two users.

SUMMARY

[0005] In one aspect of the disclosure, a server includes a processing system configured to maintain an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support an encrypted data tunnel through the ad-hoc service provider.

[0006] In another aspect of the disclosure, a server includes means for enabling a mobile client to support an encrypted data tunnel through an ad-hoc service provider, and means for maintaining an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support the encrypted data tunnel through the ad-hoc service provider.

[0007] In yet another aspect of the disclosure, a method of providing security to a network from a server includes enabling a mobile client to support an encrypted data tunnel through an ad-hoc service provider, and maintaining an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support the encrypted data tunnel through the ad-hoc service provider.

[0008] In a further aspect of the disclosure, a machine-readable medium includes instructions executable by a processing system in a server. The instructions include code for enabling a mobile client to support an encrypted data tunnel through the ad-hoc service provider, and maintaining an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support the encrypted data tunnel through the ad-hoc service provider.

[0008] 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

[0009] FIG. 1 is a conceptual diagram illustrating an example of a telecommunications system.

[0010] FIG. 2 is a conceptual diagram illustrating an example of the hardware configuration for a server.

[0011] FIG. 3 is a conceptual diagram illustrating an example of the hardware configuration for a processing system in a server.

[0012] FIG. 4A is a flow chart illustrating an example of the functionality of a server supporting a connection with an ad-hoc service provider.

[0013] FIG. 4B is a flow chart illustrating an example of the functionality of a server supporting a mobile client.

[0014] FIG. 5 is a conceptual block diagram illustrating an example of the functionality of 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 conceptual 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. In one configuration of a telecommunications system 100, the server 110 charges the mobile clients 108 based on usage. For the occasional user of mobile Internet services, this may be an attractive alternative to the monthly fixed rate wireless access plans. The revenue generated from the usage charges may be allocated to the various entities in the telecommunications system 100 in a way that tends to perpetuate the vitality of the exchange. By way of example, a portion of the revenue may be distributed to the ad hoc service providers, thus providing a financial incentive for mobile subscribers to become ad hoc service providers. Another portion of the revenue may be distributed to the WWAN operators to compensate them for the bandwidth that would otherwise go unutilized. Another portion of the revenue may be distributed to the manufacturers of the mobile nodes.

[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] FIG. 2 illustrates an example of a hardware implementation for a server. The server 110 may be a centralized server or a distributed server. A centralized server may be a dedicated server or integrated into another network-related entity, such as a desktop or laptop computer, mainframe, or other suitable entity. A distributed server may be distributed across multiple servers and/or one or more network-related entities, such as a desktop or laptop computer, mainframe, or some other suitable entity. In at least one configuration, the server may be integrated, either in whole or part, into one or more ad-hoc service providers.

[0024] The server 110 is shown with a network interface 202, which may support a wired and/or wireless connection to the Internet 102. The network interface 202 may be used 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 the transmission medium. The network 202 may also be configured to implement the lower portion of the data link layer by managing access to the transmission medium.

[0025] The server 110 is also shown with a processing system 204 that provides various functions, including registration and authentication of the ad-hoc service providers and mobile clients, control session management for the ad-hoc service providers and mobile clients, handoff support between ad-hoc service providers, data tunneling for mobile clients, and services to mobile clients. The processing system 204 is shown separate from the network interface 202, however, as those skilled in the art will readily appreciate, the network interface 202, or any portion thereof, may be integrated into the processing system 204.

[0026] FIG. 3 illustrates an example of a hardware implementation for a processing system in a server. In this example, the processing system 204 may be implemented with a bus architecture represented generally by bus 302. The bus 302 may include any number of interconnecting buses and bridges depending on the specific application of the processing system 204 and the overall design constraints. The bus links together various circuits including a processor 304 and machine-readable media 306. The bus

302 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 308 provides an interface between the network interface 202 (see FIG. 2) and the bus 302.

[0027] The processor 304 is responsible for managing the bus and general processing, including the execution of software stored on the machine-readable media 306. 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.

[0028] In the hardware implementation illustrated in FIG. 3, the machine-readable media 306 is shown as part of the processing system 204 separate from the processor 304. However, as those skilled in the art will readily appreciate, the machine-readable media 306, or any portion thereof, may be external to the processing system 204. By way of example, the machine-readable media 306 may include a transmission line, a carrier wave modulated by data, and/or a computer product separate from the server, all which may be accessed by the processor 304 through the network interface 308. Alternatively, or in addition to, the machine readable media 306, or any portion thereof, may be integrated into the processor 304, such as the case may be with cache and/or general register files.

[0029] The processing system 204 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 204 may be implemented with an ASIC (Application Specific Integrated Circuit) with the processor 304, the network interface

308, supporting circuitry (not shown), and at least a portion of the machine-readable media 306 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 204 depending on the particular application and the overall design constraints imposed on the overall system.

[0030] The machine-readable media 306 is shown with a number of software modules. Each module includes a set of instructions that when executed by the processor 304 cause the processing system 204 to perform the various functions described below. The software modules include a protocol stack module 309, a security module 310, a service provider control session manager module 312, a mobile client control session manager module 314, a tunneling/routing module 316, a handoff module 318, and a services module 320. 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 (e.g., a mobile node decides to become an ad-hoc service provider). During execution of the software module, the processor 304 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 304. When referring to the functionality of a software module below, it will be understood that such functionality is implemented by the processor 304 when executing instructions from that software module.

[0031] The protocol stack module 309 may be used to implement the protocol architecture, or any portion thereof, for the server. In the implementation described thus far, the protocol stack module 309 is responsible for implementing several protocol layers running on top of the data link layer implemented by the network interface 202 (see FIG. 2). By way of example, the protocol stack module 309 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 309 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 309, or any portion thereof, may be implemented by the network adapter 202.

[0032] The security module 310 may be used for registration. Registration of a mobile client or an ad-hoc service provider can be static (non-mobile) or dynamic (mobile). A server certificate may be supplied to the mobile client or the ad-hoc service provider. This certificate contains the public key of the server signed with the private key of an external certificate authority. The mobile client and the ad-hoc service provider are provisioned with the public key of that certificate authority, and therefore, are able to verify the signature of the certificate authority, and to then use the public key to communicate privately with the server. A mobile client and ad-hoc service provide may register with the server to set up a user name and password with payment information. Similarly, an ad-hoc service provider may register with the server setting up a user name and password. The user names and passwords are set up by the security module 310 and stored in an authentication database 322.

[0033] Once registered, the security module 310 may authenticate an ad-hoc service provider when the ad-hoc service provider desires to provide a wireless access point to other mobile clients. In this example, the ad-hoc service provider requests a certificate from the server, which is forwarded by the security module 310. Upon receipt of the certificate, and after validating the server certificate, the ad-hoc service provider suggests a session key ($K_{SP,S}$) encrypted with the public key of the server. This is received by the server and provided to the security module 310 to encrypt all subsequent messages with the session key $K_{SP,S}$. The ad-hoc service provider provides its username and password encrypted with the session key $K_{SP,S}$. The security module 310 authenticates the ad-hoc service provider based on the information stored in the authentication database 322.

[0034] The security module 310 may also be used to authenticate mobile clients that have registered with the server. Authentication will generally require connectivity over an ad-hoc wireless link between the mobile client and the ad-hoc service provider, but may be performed in some cases directly between the mobile client and the server. Existing connectivity between an ad-hoc service provider and the server is used to establish connectivity between the mobile client and the server. In this example, the mobile client is the supplicant, the ad-hoc service provider is the authenticator, and the server is the authentication server. The mobile client requests a certificate from the

server. The ad-hoc service provider forwards this request to the server, receives a certificate from the security module 310, and forwards that certificate to the mobile client. The mobile client receives the certificate. After validating the server certificate, the mobile client suggests a session key ($K_{C,S}$) encrypted with the public key of the server. This is received by the server and provided to the security module 310 so that all subsequent messages between the server and the mobile client can be encrypted with the session key $K_{C,S}$. The mobile client provides its username and password encrypted with the session key $K_{C,S}$ to the server. The security module 310 authenticates the mobile client based on the information stored in the authentication database 322. Upon completion of authentication, the security module 310 communicates to the ad-hoc service provider and to the mobile client that the mobile client is now authenticated and may receive service.

[0035] Once the ad-hoc service provider is authenticated, the control session manager module 312 establishes and maintains a secure session $X_{SP,S}$ between the ad-hoc service provider and the server using the key $K_{SP,S}$. Similarly, once the mobile client is authenticated, the control session manager module 314 establishes and maintains a secure session $X_{C,S}$ between the mobile client and the server using the key $K_{C,S}$. A key $K_{SP,C}$ may be generated at the mobile client and communicated to the control session manager module 314 server over the session $X_{C,S}$. The key $K_{SP,C}$ may then be provided to the ad-hoc service provider via the control session manager module 312 over the session $X_{SP,S}$. This allows a secure session $X_{SP,C}$ to be established and maintained between the mobile client and the ad-hoc service provider using the key $K_{SP,C}$. In alternative configurations, the key $K_{SP,C}$ may be generated by the security module 204 in the server or the ad-hoc service provider.

[0036] The session keys described thus far, $K_{SP,S}$, $K_{C,S}$ and $K_{SP,C}$, are exchanged at the application layer. IP-headers and information regarding the message type may be exposed. To prevent any visibility into information flowing over the ad-hoc wireless link between the mobile client and the ad-hoc service provider, securing the transmissions over the wireless link can be performed. The mobile client and the ad-hoc service provider can agree to a data link encryption key $WK_{SP,C}$ for the wireless link. Such a key may be generated at either the mobile client, the ad-hoc service provider, or the security module 204 in the server. Once the mobile client and the ad-

hoc service provider agree to using this data link encryption key, all transmissions between them can be communicated using this key.

[0037] Over the secure session $X_{C,S}$, information can be exchanged between the mobile client and the control session manager module 314 in the server to establish an encrypted VPN tunnel to transport data to the Internet through the server. In at least one configuration of a telecommunications system, all data from the mobile client destined to any location on the Internet is tunneled through the tunnel/routing module 316 in the server. This is done to ensure that the ad-hoc service provider has no visibility into data associated with the mobile client, and hence ensures the privacy of the mobile client. This tunneling also provides security to the ad-hoc service provider by ensuring that all data associated with the mobile client flows through the tunnel/routing module 316, leaving the responsibility of such mobile client transactions to the server and the mobile client, with the ad-hoc service provider merely serving as a transport to allow data associated with the mobile client to reach the server. The tunnel/routing module 316 is depicted with short-dashed lines to emphasize that it may be located in the server or elsewhere in the telecommunications system.

[0038] Once the tunnel is established between the mobile client 108 and the tunnel/routing module 316 in the server, the services module 320 may be used to provide various services to the mobile client. By way of example, the services module 320 may support audio or video services to the mobile client 108. The services module 320 may also support advertising services to the mobile client 108. Other functions of the services module 320 may include routing to and from the Internet for mobile client data as well as providing network address translation to and from the Internet for the mobile client.

[0039] The handoff module may also provide support for a handoff of a mobile client from one ad-hoc service provider to another based on any number of factors. These factors may include, by way of example, the quality of service (QoS) required by the mobile client, the duration of the session required by the mobile client, and the loading, link conditions, and energy level (e.g., battery life) at the ad-hoc service provider.

[0040] An example will now be presented where a mobile client connected to a through a “serving ad-hoc service provider” (SP1) is handed off to a “target ad-hoc service provider” (SP2). Initially, three secure sessions $X_{SP1,S}$, $X_{C,S}$ and $X_{SP1,C}$ exist using session keys $K_{SP1,S}$, $K_{C,S}$ and $K_{SP1,C}$, respectively. When the target ad-hoc service

provider SP2 becomes available, a secure session $X_{SP2,S}$ may be established with the control session manager module 312 using a session key $K_{SP2,S}$ negotiated between the target ad-hoc service provider SP2 and the security module 310. A handoff request may be initiated by either the mobile client, the serving ad-hoc service provider SP1, or the handoff module 316 over the secure session $X_{SP2,S}$. The security module 310 can provide information to target ad-hoc service provider SP2 indicating that the mobile client is authenticated. Over the secure session $X_{C,S}$, the mobile client may be informed by the security module 310 that it has been authenticated with the target ad-hoc service provider SP2. A session key $K_{SP2,C}$ may be generated by the mobile client, the target ad-hoc service provider SP2, or the security module 310 in the server to establish and maintain a secure session $X_{SP2,C}$. The mobile client disassociates with serving ad-hoc service provider SP1 and associates with target service provider SP2. The session key $K_{SP2,C}$ may be used for the secure session $X_{SP2,C}$ between the mobile client and the target ad-hoc service provider SP2, which has now become the serving ad-hoc service provider. Information (such as residual packets associated with the mobile client) can be exchanged between the service providers through the server with the assistance of the handoff module 318 for both service providers. A session key $K_{SP1,SP2}$ may be established for secure exchange of messages between the service providers. Alternatively, such exchange of information can occur over a direct wireless link between the service providers if the service providers can reach each other over a local wireless link. It is possible that a multi-hop wireless path between the service providers is used in a wireless mesh network topology if such a path is available. It is possible that some information (such as control flow information) may go through the server with the assistance of the handoff module 318, while other information (such as data flow information) may go over the direct wireless link/path between the service providers.

[0041] The functionality of the processing system in the server will now be described with reference to FIGS. 4A and 4B. FIG. 4A is a flow chart illustrating an example of a process implemented by the server to support an ad-hoc service provider. FIG. 4B is a flow chart illustrating an example of a process implemented by the server to support a mobile client.

[0042] Referring to FIG. 4A, in block 402A, the server may allow an ad-hoc service provider to register to provide an access point to a wireless broadband network for

mobile clients. When the ad-hoc service provider actually desires to provide an access point, the server may authenticate the ad-hoc service provider in block 404A from the information obtained during the registration process. The authentication process may include the creation of a session key $K_{SP,S}$ between the server and the ad-hoc service provider. Once authenticated, the server establishes and manages a secure control session with the ad-hoc service provider in block 406A using the session key $K_{SP,S}$. The server continues to manage the secure control session until the connection is terminated as shown in block 412A. Once the connection is terminated, the server closes the control session with the ad-hoc service provider in block 414A. Since the ad-hoc service provider remains registered, it may later serve as an access point again by invoking the authentication process of the server in block 404A.

[0043] Turning to FIG. 4B, the server may allow a mobile client to register in block 402B in order to receive service from an ad-hoc service provider for wireless broadband access to a network. When the mobile client actually desires to connect to an ad-hoc service provider, the server may authenticate the mobile client in block 404B from the information obtained during the registration process. The authentication process may include the creation of a session key $K_{C,S}$ between the server and the mobile client. Once authenticated, the server establishes and manages a secure control session with the mobile client in block 406B using the session key $K_{C,S}$. The server also establishes and maintains an encrypted data tunnel to transport data through the server to the network in block 408B. Once the tunnel is established, the server may provide various services to the mobile client in block 410B. Should a handoff of the mobile client to another ad-hoc service provider be required in step 412B, the server may support the handoff in block 414B and continue to provide services to the mobile client in step 410B during and after the handoff. These services may be provided by the service until the connection is terminated as shown in block 416B. Once the connection is terminated, the server closes the control session and tunnel with the mobile client in block 418B. Since the mobile client remains registered, it may later connect to an ad-hoc service provider by invoking the authentication process of the server in block 404B.

[0044] FIG. 5 is a conceptual block diagram illustrating an example of the functionality of an ad-hoc service provider. The ad-hoc service provider 106 has the ability to bridge wireless links over homogeneous or heterogeneous wireless access protocols. This may be achieved with a WWAN network adapter 502 that supports a wireless access

protocol for a WWAN to the Internet 102, and a WLAN network adapter 504 that provides a wireless access point for mobile clients 108. By way of example, the WWAN network adapter 502 may include a transceiver function that supports EV-DO for Internet access through a WWAN, and the WLAN network adapter 504 may include a transceiver function that provides an 802.11 access point for mobile clients 108. Each network adapter 502, 504 may be configured to implement the physical layer by demodulating wireless signals and performing other radio frequency (RF) front end processing. Each network adapter 502, 504 may also be configured to implement the link layer by managing data transfer across the physical layer, and the network layer by managing source to destination packet delivery.

[0045] The ad-hoc service provider 106 is shown with a filtered interconnection and session monitoring module 506. The module 506 provides filtered processing of content from mobile clients 108 so that the interconnection between the adhoc wireless links to the WWAN network adapter 502 is provided only to mobile clients 108 authenticated and permitted by the server to use the WWAN network. The module 506 also maintains tunneled connectivity between the server and the authenticated mobile clients 108.

[0046] The ad-hoc service provider 106 also includes a service provider application 508 that (1) enables the module 506 to provide adhoc 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 512 that communicates with the WWAN network adapter 502 through the module 506 under control of the service provider application 508. The user interface 512 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 104 or the Internet 102 (see FIG. 1).

[0047] As discussed above, the service provider application 508 enables the module 506 to provide adhoc services to mobile clients 108. The service provider application 508 maintains a control session with the server to exchange custom messages with the server. In addition, the service provider application 508 also maintains a separate control session with each mobile client 108 for exchanging custom messages between the service provider application 508 and the mobile client 108. The service provider application 508 provides information on authenticated and permitted clients to the

filtered interconnection and session monitoring module 506. The filtered interconnection and session monitoring module 508 allows content flow for only authenticated and permitted mobile clients 108. The filtered interconnection and session monitoring module 506 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 506 can additionally and optionally provide such information to the service provider application 508. The service provider application 508 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 506 and 508 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.

[0048] When the ad-hoc service provider 106 decides to provide these services, the service provider application 508 sends a request to the server for approval. The service provider application 508 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.

[0049] Once the ad-hoc service provider 106 is authenticated, the service provider application 508 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 508 may then authenticate the mobile clients 108 with the server and then configure the filtered interconnection and session monitoring module 506 to connect the mobile clients 108 to the server. During the authentication of a mobile client 108, the service provider application 508 may use an unsecured wireless link.

[0050] The service provider application 508 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 508 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.

[0051] The service provider application 508 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 508 should consider supporting a new mobile client 108 or accepting a handoff of that mobile client 108 from another ad-hoc service provider.

[0052] The service provider application 508 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 508 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.

[0053] The service provider application 508 may also provide a certain level of security to the wireless access point by routing content through the filtered interconnection and session monitoring module 506 without being able to decipher the content. Similarly, the service provider application 508 may be configured to ensure content routed between the user interface 510 and the WWAN 104 via the module 506 cannot be deciphered by mobile clients 108. The service provider application 508 may use any suitable encryption technology to implement this functionality.

[0054] The service provider application 508 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 508 and the mobile client 108 during the initiation of the session. If the service provider application 508 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 508 may support the handoff of the mobile client 108.

[0055] The service provider application 508 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.

[0056] The service provider application 508 may manage the mobile client 108 generally, and the session specifically, through the user interface 512. Alternatively, the service provider application 508 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.

[0057] Turning now to the mobile client, a 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 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. A 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.

[0058] 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.

[0059] 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.

[0060] 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.

[0061] 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.

[0062] 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.”

WHAT IS CLAIMED IS:

1. A server, comprising:
a processing system configured to maintain an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support an encrypted data tunnel through the ad-hoc service provider.
2. The server of claim 1 wherein the processing system is further configured to enable the mobile client to support the encrypted data tunnel through the ad-hoc service provider to the server.
3. The server of claim 1 wherein the processing system is further configured to use a first session key for the encrypted control session with the ad-hoc service provider and a second session key for the encrypted control session with the mobile client, wherein the first session key is different from the second session key.
4. The server of claim 3 wherein the processing system is further configured to receive from the ad-hoc service provider the first session key encrypted with a public key for the server and receive from the mobile client the second session key encrypted with the public key for the server.
5. The server of claim 1 wherein the processing system is further configured to authenticate the ad-hoc service provider to establish the encrypted control session with the ad-hoc service provider.
6. The server of claim 1 wherein the processing system is further configured to authenticate the mobile client to establish the encrypted control session with the mobile client.
7. The server of claim 6 wherein the processing system is further configured to authenticate the mobile client through the ad-hoc service provider.
8. The server of claim 7 wherein the processing system is further configured to communicate to the ad-hoc service provider and the mobile client that the mobile client is authenticated.

9. The server of claim 1 wherein the processing system is further configured to assist in establishing an encrypted control session between the ad-hoc service provider and the mobile client.

10. The server of claim 9 wherein the processing system is further configured to assist in establishing the encrypted control session between the ad-hoc service provider and the mobile client by receiving a session key from one of the mobile client and ad-hoc service provider and providing the session key to the other one of the mobile client and ad-hoc service provider.

11. The server of claim 9 wherein the processing system is further configured to assist in establishing the encrypted control session between the ad-hoc service provider and the mobile client by generating a session key and providing the session key to the ad-hoc service provider and the mobile client.

12. The server of claim 1 wherein the processing system is further configured to assist in establishing an encrypted wireless link between the ad-hoc service provider and the mobile client.

13. The server of claim 12 wherein the processing system is further configured to assist in establishing the encrypted wireless link between the ad-hoc service provider and the mobile client by generating a wireless link encryption key and providing the wireless link encryption key to the ad-hoc service provider and the mobile client.

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

15. The server of claim 14 wherein the processing system is further configured to support the handoff by establishing an encrypted control session with said another ad-hoc service provider.

16. The server of claim 14 wherein the processing system is further configured to authenticate the mobile client with said another ad-hoc service provider.

17. The server of claim 16 wherein the processing system is further configured to communicate to the mobile client that the mobile client has been authenticated with said another ad-hoc service provider.

18. The server of claim 14 wherein the processing system is further configured to support the handoff by assisting in establishing an encrypted control session between said another ad-hoc service provider and the mobile client.

19. The server of claim 18 wherein the processing system is further configured to assist in establishing the encrypted control session between said another ad-hoc service provider and the mobile client by generating a session key and providing the session key to said another ad-hoc service provider and the mobile client.

20. A server, comprising:
means for enabling a mobile client to support an encrypted data tunnel through an ad-hoc service provider; and
means for maintaining an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support the encrypted data tunnel through the ad-hoc service provider.

21. The server of claim 20 wherein the means for enabling the mobile client to support an encrypted data tunnel is configured to enable the mobile client to support the encrypted data tunnel through the ad-hoc service provider to the server.

22. The server of claim 20 wherein the means for maintaining an encrypted control session with an ad-hoc service provider and a mobile client comprises means for using a first session key for the encrypted control session with the ad-hoc service provider and means for using a second session key for the encrypted control session with the mobile client, wherein the first session key is different from the second session key.

23. The server of claim 22 further comprising means for receiving from the ad-hoc service provider the first session key encrypted with a public key for the server and means for receiving from the mobile client the second session key encrypted with the public key for the server.

24. The server of claim 20 further comprising means for authenticating the ad-hoc service provider to establish the encrypted control session with the ad-hoc service provider.

25. The server of claim 20 further comprising means for authenticating the mobile client to establish the encrypted control session with the mobile client.

26. The server of claim 25 wherein the means for authenticating the mobile client is configured to authenticate the mobile client through the ad-hoc service provider.

27. The server of claim 26 further comprising means for communicating to the ad-hoc service provider and the mobile client that the mobile client is authenticated.

28. The server of claim 20 further comprising means for assisting in establishing an encrypted control session between the ad-hoc service provider and the mobile client.

29. The server of claim 28 wherein the means for assisting in establishing an encrypted control session between the ad-hoc service provider and the mobile client comprises means for receiving a session key from one of the mobile client and ad-hoc service provider and means for providing the session key to the other one of the mobile client and ad-hoc service provider.

30. The server of claim 28 wherein the means for assisting in establishing an encrypted control session between the ad-hoc service provider and the mobile client comprises means for generating a session key and means for providing the session key to the ad-hoc service provider and the mobile client.

31. The server of claim 20 further comprising means for assisting in establishing an encrypted wireless link between the ad-hoc service provider and the mobile client.

32. The server of claim 31 wherein the means for assisting in establishing an encrypted wireless link between the ad-hoc service provider and the mobile client comprises means for generating a wireless link encryption key and means for providing the wireless link encryption key to the ad-hoc service provider and the mobile client.

33. The server of claim 20 further comprising means for supporting a handoff of the mobile client from the ad-hoc service provider to another ad-hoc service provider.

34. The server of claim 33 wherein the means for supporting a handoff is configured to support the handoff by establishing an encrypted control session with said another ad-hoc service provider.

35. The server of claim 33 further comprising means for authenticating the mobile client with said another ad-hoc service provider.

36. The server of claim 35 further comprising means for communicating to the mobile client that the mobile client has been authenticated with said another ad-hoc service provider.

37. The server of claim 33 wherein the means for supporting a handoff is configured to support the handoff by assisting in establishing an encrypted control session between said another ad-hoc service provider and the mobile client.

38. The server of claim 37 wherein the means for supporting a handoff is further configured to assist in establishing the encrypted control session between said another ad-hoc service provider and the mobile client by generating a session key and providing the session key to said another ad-hoc service provider and the mobile client.

39. A method of providing security to a network from a server, comprising:
enabling a mobile client to support an encrypted data tunnel through an ad-hoc service provider; and
maintaining an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support the encrypted data tunnel through the ad-hoc service provider.

40. The method of claim 39 wherein the mobile client is enabled to support the encrypted data tunnel through the ad-hoc service provider to the server.

41. The method of claim 39 wherein the encrypted control session is maintained with the ad-hoc service provider and the mobile client by for using a first session key for the encrypted control session with the ad-hoc service provider and using

a second session key for the encrypted control session with the mobile client, wherein the first session key is different from the second session key.

42. The method of claim 41 further comprising receiving from the ad-hoc service provider the first session key encrypted with a public key for the server and receiving from the mobile client the second session key encrypted with the public key for the server.

43. The method of claim 39 further comprising authenticating the ad-hoc service provider to establish the encrypted control session with the ad-hoc service provider.

44. The method of claim 39 further comprising authenticating the mobile client to establish the encrypted control session with the mobile client.

45. The method of claim 44 wherein the mobile client is authenticated through the ad-hoc service provider.

46. The method of claim 45 further comprising communicating to the ad-hoc service provider and the mobile client that the mobile client is authenticated.

47. The method of claim 39 further comprising assisting in establishing an encrypted control session between the ad-hoc service provider and the mobile client.

48. The method of claim 47 wherein the establishment of the encrypted control session between the ad-hoc service provider and the mobile client is assisted by receiving a session key from one of the mobile client and ad-hoc service provider and providing the session key to the other one of the mobile client and ad-hoc service provider.

49. The method of claim 47 wherein the establishing an encrypted control session between the ad-hoc service provider and the mobile client is assisted by generating a session key and providing the session key to the ad-hoc service provider and the mobile client.

50. The method of claim 39 further comprising assisting in establishing an encrypted wireless link between the ad-hoc service provider and the mobile client.

51. The method of claim 50 wherein the establishment of the encrypted wireless link between the ad-hoc service provider and the mobile client is assisted by generating a wireless link encryption key and providing the wireless link encryption key to the ad-hoc service provider and the mobile client.

52. The method of claim 39 further comprising supporting a handoff of the mobile client from the ad-hoc service provider to another ad-hoc service provider.

53. The method of claim 52 wherein the handoff is supported by establishing an encrypted control session with said another ad-hoc service provider.

54. The method of claim 52 further comprising authenticating the mobile client with said another ad-hoc service provider.

55. The method of claim 54 further comprising communicating to the mobile client that the mobile client has been authenticated with said another ad-hoc service provider.

56. The method of claim 52 wherein the handoff is supported by assisting in establishing an encrypted control session between said another ad-hoc service provider and the mobile client.

57. The method of claim 56 wherein the handoff is supported by assisting in establishing the encrypted control session between said another ad-hoc service provider and the mobile client by generating a session key and providing the session key to said another ad-hoc service provider and the mobile client.

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

enabling a mobile client to support an encrypted data tunnel through the ad-hoc service provider; and

maintaining an encrypted control session with an ad-hoc service provider and a mobile client while enabling the mobile client to support the encrypted data tunnel through the ad-hoc service provider.

59. The machine-readable medium of claim 58 wherein the code for enabling the mobile client to support an encrypted data tunnel is configured to enable the mobile

client to support the encrypted data tunnel through the ad-hoc service provider to the server.

60. The machine-readable medium of claim 58 wherein the code for maintaining an encrypted control session with an ad-hoc service provider and a mobile client comprises code for using a first session key for the encrypted control session with the ad-hoc service provider and code for using a second session key for the encrypted control session with the mobile client, wherein the first session key is different from the second session key.

61. The machine-readable medium of claim 60 wherein the instructions further comprise code for receiving from the ad-hoc service provider the first session key encrypted with a public key for the server and code for receiving from the mobile client the second session key encrypted with the public key for the server.

62. The machine-readable medium of claim 20 wherein the instructions further comprise code for authenticating the ad-hoc service provider to establish the encrypted control session with the ad-hoc service provider.

63. The machine-readable medium of claim 58 wherein the instructions further comprise code for authenticating the mobile client to establish the encrypted control session with the mobile client.

64. The machine-readable medium of claim 63 wherein the code for authenticating the mobile client is configured to authenticate the mobile client through the ad-hoc service provider.

65. The machine-readable medium of claim 64 wherein the instructions further comprise code for communicating to the ad-hoc service provider and the mobile client that the mobile client is authenticated.

66. The machine-readable medium of claim 58 wherein the instructions further comprise code for assisting in establishing an encrypted control session between the ad-hoc service provider and the mobile client.

67. The machine-readable medium of claim 66 wherein the code for assisting in establishing an encrypted control session between the ad-hoc service provider and the

mobile client comprises code for receiving a session key from one of the mobile client and ad-hoc service provider and code for providing the session key to the other one of the mobile client and ad-hoc service provider.

68. The machine-readable medium of claim 66 wherein the code for assisting in establishing an encrypted control session between the ad-hoc service provider and the mobile client comprises code for generating a session key and code for providing the session key to the ad-hoc service provider and the mobile client.

69. The machine-readable medium of claim 58 wherein the instructions further comprise code for assisting in establishing an encrypted wireless link between the ad-hoc service provider and the mobile client.

70. The machine-readable medium of claim 69 wherein the code for assisting in establishing an encrypted wireless link between the ad-hoc service provider and the mobile client comprises code for generating a wireless link encryption key and code providing the wireless link encryption key to the ad-hoc service provider and the mobile client.

71. The machine-readable medium of claim 58 wherein the instructions further comprise code for supporting a handoff of the mobile client from the ad-hoc service provider to another ad-hoc service provider.

72. The machine-readable medium of claim 71 wherein the code for supporting a handoff is configured to support the handoff by establishing an encrypted control session with said another ad-hoc service provider.

73. The machine-readable medium of claim 71 wherein the instructions further comprise code for authenticating the mobile client with said another ad-hoc service provider.

74. The machine-readable medium of claim 73 wherein the instructions further comprise code for communicating to the mobile client that the mobile client has been authenticated with said another ad-hoc service provider.

75. The machine-readable medium of claim 71 wherein the code for supporting a handoff is configured to support the handoff by assisting in establishing an

encrypted control session between said another ad-hoc service provider and the mobile client.

76. The machine-readable medium of claim 75 wherein the code for supporting a handoff is further configured to assist in establishing the encrypted control session between said another ad-hoc service provider and the mobile client by generating a session key and providing the session key to said another ad-hoc service provider and the mobile client.