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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 July 2006 (20.07.2006)

PCT

(10) International Publication Number
WO 2006/076404 A2

(51) International Patent Classification:
H04M 3/16 (2006.01)

(21) International Application Number:
PCT/US2006/000935

(22) International Filing Date: 11 January 2006 (11.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/644,064	14 January 2005 (14.01.2005)	US
11/176,999	7 July 2005 (07.07.2005)	US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:

US	10/897,060 (CIP)
Filed on	21 July 2004 (21.07.2004)
US	10/413,443 (CIP)
Filed on	11 April 2003 (11.04.2003)
US	10/377,265 (CIP)
Filed on	28 February 2003 (28.02.2003)

(71) Applicant *(for all designated States except US)*: **SENFORCE TECHNOLOGIES, INC.** [US/US]; 147 W. Election Road, Suite 110, Draper, Utah 84020 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BEACHEM, Brent** [US/US]; 12159 Swensen Circle, Riverton, Utah 84065 (US). **BOUCHER, Peter** [US/US]; 717 East 700 North, Orem, Utah 84097 (US). **NAULT, Gabe** [US/US]; 1194 East Lone Peak Lane, Draper, Utah 84020 (US). **ROLLINS, Richard** [US/US]; 1159 Catherine Street, Salt Lake City, Utah 84118 (US). **WOOD, Jonathan** [US/US]; 438 Rosewood Lane #18, Layton, Utah 84041 (US). **WRIGHT, Michael** [US/US]; 9180 South Granville Circle, Sandy, Utah 84093 (US).

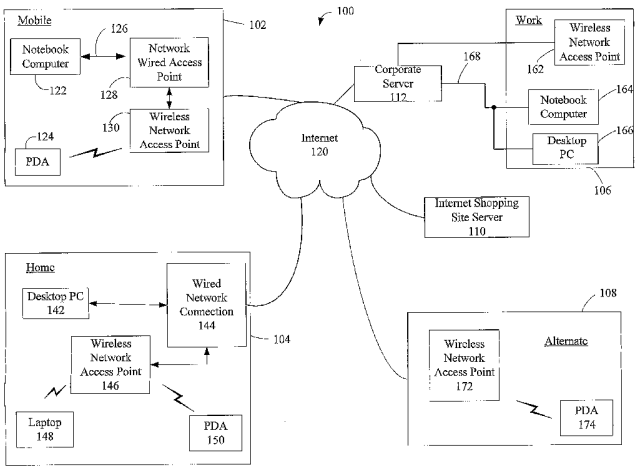
(74) Agent: **SUEOKA, Greg, T.**; FENWICK & WEST LLP, SILICON VALLEY CENTER, 801 California Street, Mountain View, California 94041 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR FILTERING ACCESS POINTS PRESENTED TO A USER AND LOCKING ONTO AN ACCESS POINT



(57) Abstract: The present invention filters access points presented to a user and locks onto an access point. The present invention includes an access point filtering unit and an access point locking unit. The access point filtering unit determines the access points that are accessible by a client device and then filters them to present only the access points that are acceptable to under a security policy in force. The access point locking unit has a plurality of operating modes and can lock onto a user selected access point, a security policy prescribed access point, or the access point with the best signal profile. The present invention also includes several methods such as: a method for filtering access points for presentation to the user, a method for locking onto an access point selected by the user, a method for locking onto an access point with the best signal profile, and a method for locking onto an access point prescribed by a security policy for a given location.

WO 2006/076404 A2

ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

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

SYSTEM AND METHOD FOR FILTERING ACCESS POINTS PRESENTED TO A USER AND LOCKING ONTO AN ACCESS POINT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Patent Application No. 60/644,064, filed on January 14, 2005, entitled "System and Method of Filtering Access Points Presented to a User and Locking Onto an Access Point." This application is a continuation-in-part of U.S. Patent Application No. 10/897,060, filed on July 21, 2004, and entitled "Administration of Protection of Data Accessible by a Mobile Device." This application is also a continuation-in-part of U.S. Patent Application No. 10/413,443, filed April 11, 2003, and entitled "Administration of Protection of Data Accessible by a Mobile Device." This application is also a continuation-in-part of U.S. Patent Application No. 10/377,265, filed February 28, 2003, and entitled "Protection of Data Accessible by a Mobile Device." All of the above applications are incorporated by reference herein in their entirety.

BACKGROUND OF THE INVENTION

1. Field of Invention

[0002] This application relates to the field of wireless communication between computing devices. More particularly, the present invention relates to systems and method for determining which access points are presented to the user or set as default for communication and locking onto a particular access point for communication.

2. Description of Related Art

[0003] The availability of wired and wireless network access points (NAP) allows mobile devices like laptop computers and personal digital assistants (PDAs) to enable users to be more mobile, providing access to corporate networks, e-mail, home networks and the Internet from anywhere. With the advent of the IEEE 802.11 standard for wireless communication, and other popular wireless technologies, software products that protect against unwanted access to information stored on mobile devices and corporate servers is highly desirable.

[0004] Traditional security architectures assume that the information assets being protected are 'tethered'—wired to a particular network infrastructure such as a company's network infrastructure. But mobile users can pick up valuable corporate information, such as by copying files from a server to a laptop, and walk away from the corporate network, and connect to other networks with different security policies. Users with laptops and mobile devices want to take advantage of wireless technologies, to connect wherever they are—at work, at home, in the conference room of another company, at the airport, a hotel, a highway or at the coffee shop on the corner. The mobile device's network environment is constantly changing as the user moves about. Each environment has different needs in terms of security. Each environment presents different challenges to protect the information on the mobile device while allowing access to e-mail, the Internet, and company Virtual Private Networks (VPNs).

[0005] Personal firewalls are designed to deal with static environments. A personal firewall could be ideally suited for mobile users if users knew how to adapt their configuration for their particular mobile application. Unfortunately, security settings for one situation can compromise data security in another. The configuration of popular personal firewalls typically requires a level of expertise on how the technology actually works that average users do not possess. Additionally, personal firewalls don't protect against all 802.11 intrusions. For example, when a user configures a personal firewall off to surf the Internet through their wireless device, their files may be vulnerable to unauthorized malicious wireless attacks on their computer.

[0006] Solutions that secure data in transit, for example a (VPN) connection, from a corporate server to a mobile client device do not protect the data once it is stored on the mobile device. For example, an executive could be retrieving sensitive files or emails from the corporate network, and the VPN will stop eavesdroppers from seeing the data in transit, but once the data is stored on the executive's mobile device, hackers in the parking lot could break

into the mobile device and copy or maliciously alter the data. With the onset of new powerful mobile devices that can store corporate data, IT managers see their network perimeters having to extend to the new limits of these mobile wireless connections.

[0007] Another problem for mobile users is selecting and remaining connected to an access point when multiple access points are accessible within a dynamically changing environment. In a multiple access point environment, the prior art dynamically determines the access point with the strongest signal and switches to that access point. However, this is problematic because changes in the user's environment that cause reflections or disturbances of the wireless signals cause the wireless adapter to switch to another access point. Such switching to another available access point causes a temporary loss of connection, and re-initialization of the connection and other security protocols such as VPNs.

[0008] Thus, there is a need for a system that can control which access point is used and the condition under which the access point is switched.

SUMMARY OF INVENTION

[0009] The present invention provides one or more embodiments of systems and methods for filtering access points presented to a user and locking onto an access point. The present invention includes a computing device that has a location detection module, a policy setting module, a security policy enforcement module, an access point filtering unit, and an access point locking unit cooperatively coupled to a bus. The access point filtering unit determines the access points that are accessible by a client device and then filters them to present only the access points that are acceptable under a security policy in force. The access point locking unit has a plurality of operating modes and can lock onto a user selected access point, a security policy prescribed access point, or the access point with the best signal profile. The signal profile refers to a combination of: the protocol used for communication, the type of encryption use, the key length for encryption, the wireless signal strength, authentication method, and other factors.

[0010] The present invention also includes several methods such as: a method for filtering access points for presentation to the user, a method for locking onto an access point selected by the user, a method for locking onto an access point with the best signal profile, and a method for locking onto an access point prescribed by a security policy for a given location.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Figure 1 illustrates one or more examples of location categories that may be assigned to a mobile device in accordance with an embodiment of the present invention.

[0012] Figure 2A illustrates a server or system for protecting of data accessible by one or more mobile devices based on a location associated with the mobile device and source information for the data requested in accordance with a first embodiment of the present invention.

[0013] Figure 2B illustrates a system in a mobile client device for protecting data accessible by the mobile device based on a location associated with the mobile device and source information for the data requested in accordance with the first embodiment of the present invention.

[0014] Figure 3 illustrates a server system embodiment for administering the protection of data accessible by a mobile client device in accordance with second embodiment of the present invention.

[0015] Figure 4 illustrates an example of a mobile computing device being accessible to a plurality of access points and communicating in accordance with the present invention.

[0016] Figure 5 is a flowchart illustrating a method for locking communication between a mobile client device and a user selected access point.

[0017] Figure 6 is a flowchart illustrating a method for locking communication between a mobile client device and an access point having the best signal profile.

[0018] Figure 7 is a flowchart illustrating a method for locking communication between a mobile client device and an access point authorized by the security policy and having the best signal profile.

[0019] Figure 8 is a flowchart illustrating a method for removing a filter of access points accessible by a mobile client device.

[0020] Figures 9A and 9B are exemplary signal profiles for a plurality of access points at different points in time.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0021] Figure 1 illustrates examples of location categories 102, 104, 106, 108 that may be assigned based on the network environment in which a mobile device is operating in

accordance with an embodiment of the present invention. One example of a location category is "Home" 104. The network environment in which each of the mobile devices 148, 150 communicates via a network connection at a user's home is detected. Upon detection of this home network environment, each of the mobile devices 148, 150 is assigned a location indicator or type of "Home" 104. In the illustrated example, the laptop 148 and the PDA 150 communicating with the illustrated wireless network access point will have its location set to "Home."

[0022] The location "Work" 106 is an example of a location associated with a network environment maintained by a user's employer. In the illustrated example, a notebook computer 164 has a wired Ethernet connection 168 to the corporate server 112 of his or her employer. However, the notebook computer 164 may also communicate with the server 112 through a wireless NAP 162 as illustrated.

[0023] Another example of a location category is "Mobile" 102. For example, at an airport, a mobile device such as the illustrated notebook computer 122 accesses a network environment respectively through a wired connection 126 (in this example a T1 line) to a wired network access point 128. This wired network access point 128 may provide access to an Internet shopping site server 110 because the user desires to browse the site while waiting for departure. The notebook computer 122 and the personal digital assistant (PDA) 124 alternatively have a wireless connection to a wireless NAP 130, in this example an 802.11b connection through which they may communicate at the airport. Additionally, as discussed below, the security policy associated with the "Mobile" location may take into account the connection type of wired or wireless. In this example, the network environment provided at the airport does not match with a defined environment associated with a location such as "Work" 106 or "Home" 104 so "Mobile" 102 is assigned or associated with the PDA 124 and the notebook computer 122 as a default location.

[0024] The last location example is "Alternate" 108. In one example, a specific environment (e.g. an environment associated with a university computer lab or an environment associated with a type of network class) may be associated with "Alternate." Similarly, a "Custom" or another named location may also be defined. In this example, the wireless network access point 172 is associated with a cellular base station providing network access through a General Packet Radio Services (GPRS) system, Global System for Mobile communication (GSM) system, third generation wireless 3G system or other kind of mobile

wireless communication system. A PDA 174 communicates wirelessly to the NAP 172 for access to the network 120.

System Overview

[0025] Figures 2A and 2B illustrate interaction between a computer system 200 (Figure 2A) acting in a server role with respect to a mobile computer system 201 (Figure 2B) acting in a client role for the purposes of managing security in accordance with an embodiment of the invention. Similarly, Figures 2A and 2B also illustrate interaction between the server computer system 200 and the mobile client computer system 201 for the purpose of providing diagnostic assistance to the client computer system. The system 200 in Figure 2A may be implemented as software executing in a standalone computer having a processor being accessible to memory, the processor being communicatively coupled with one or more network interfaces, a display and input/output devices such as a keyboard and a pointing device. Similarly, the system 200 may be implemented by a series of networked computers as may typically be implemented by an enterprise. Additionally, the system 200 of Figure 2A may be implemented on another mobile computing device 201. The server or server-side system 200 allows an administrator to manage and distribute policies and software upgrades, analyze logs, and perform remote diagnostics. The client system 201 in Figure 2B may be implemented as software executing in a mobile computing device having a processor being accessible to memory, the processor being communicatively coupled with one or more network interfaces, a display and input/output devices such as a keyboard and a pointing device. The client side system 201 monitors the user's changes in location and/or security features and applies the appropriate policies automatically as the user moves about or different security features are activated or deactivated. The client 201 enforces the policies set up by the administrator, and performs diagnostics. The client 201 can also create and manage policies for the client mobile device when run in a self-managed mode. The server system 200 is discussed first.

Server System

[0026] Figure 2A illustrates a system 200 for administering protection of data accessible by a mobile device based on a location associated with a network environment in which the mobile device is operating and the access point in use. The illustrated system embodiment 200 comprises an authorization module 232, a policy distribution module 234, a policy management module 236, illustrated here with an optional policy setting module 238 and

an optional policy enforcement module 244, a remote diagnostics module 224 and a user interface module 240. The system 200 protects data accessible by the mobile device that may be resident (See Figure 2B, 220) or data 242 that is accessible by the mobile device over a network 204. Examples of such data may include security policies, corporate data, group files indicating the organization of personnel into various groups, client device management data, and diagnostic information related to the mobile devices or computers internal to the corporate network. As is apparent, these are examples of information valuable to a company. As illustrated, each of these modules has a communication interface or is communicatively coupled to each of the other modules and has access to data objects 242 stored in memory of the server 200 and also has access to a network 204 (e.g. Internet).

[0027] The policy management module 236 manages security policies. One aspect of managing security policies is defining the policies. In this example, the policy management module 236 comprises instructions for establishing this pre-defined criteria based upon user input processed by the communicatively coupled user interface module 240. Defining policies includes the creation of policies and the modification of policies. Examples of aspects of a policy includes specification of rules and permissions (e.g. policy override), defining one or more locations associated with network environments, defining or identifying security features to be monitored, ports to be monitored, network services to be monitored, applications to be monitored, enforcement mechanisms to be put in place for a particular policy, level identification for a policy or policy aspect for flexibility (optional, recommended, mandatory, invisible), and feedback (e.g. custom error messages) to alert an administrator via a user interface screen using the server system 200 of certain conditions or to alert a client device user via a user interface screen of certain conditions.

[0028] There may be several layers of policies. There may be a base policy applicable to a group of entities. Examples of entities may be users or the mobile devices themselves. In these examples, the group may include one instance of an entity. The attributes of the base policy may be incorporated into other policies that add on additional attributes. For example, a base policy for the group including engineers in the user interface design department may be allowed access to files on a certain disk drive. Another policy based on location that incorporates the attributes of the base policy may only allow access to encrypted versions of the files if a mobile device through which a UI design engineer is logged in is operating in a "Home" network location. The optional policy setting module 238 is discussed below in the discussion of the client policy setting module 212 of Figure 2B. The optional policy

enforcement module 244 is discussed below in the discussion of the client policy enforcement control module 214 of Figure 2B.

[0029] In one embodiment, the policy management module 236 is provided with an enterprise's existing group structures. The policy management module 236 compensates for a failing in the traditional makeup of groups. Since groups are not hierarchical, it is common for one person to be a member of several groups, and if each group has its own security policy, an issue arises as to how to determine which policy to apply to a particular user. The policy management module 236 inputs a prioritized list of groups from a memory location 242. The policy management module 236 searches the groups in priority order of the list. Thus, if a person is a member of "engineering" and "executive staff," that person will get the security policy for whichever of those two groups comes first in the prioritized list. There is a default policy for users who are not members of any of the groups on the prioritized list. Further, there is a highest priority group that always has the highest priority. An example of such a group is a "stolen mobile device" group that always has the highest priority, because it doesn't matter what other groups the device is associated with if the device is in the hands of a thief.

[0030] The policy distribution module 234 distributes security information to the one or more client mobile devices. The policy distribution module 234 has a communication interface or is communicatively coupled to the policy management module 236 for receiving notifications of updated security information. Examples of security information are versions of existing policies, policies, or software. An example of communication interface is a bus between a processor executing one or more of the modules and a memory controller responsible for memory reads/writes. Another example is one module reading a parameter stored in a memory location by another module. Of course, other communication interfaces known to those of ordinary skill in the art may also be used.

[0031] In this embodiment, the authorization module 232 authorizes a communication exchange between the client mobile device and the policy distribution or policy management modules. The authorization module 232 is a further safeguard against unauthorized or rogue mobile devices trying to hijack the security policies or corporate data. Various authorization protocols and techniques may be used. One example is a simple username and password verification scheme. Another example of a type of authorization protocol is a cryptographic authentication protocol. The authorization module 232 may also be used to authorize a communication exchange between the client system 201 and the remote diagnostics module 224.

[0032] The remote diagnostics module 224 is illustrated in the context of a server 200 in Figure 2A concerned with security or protection of data accessible by mobile client devices. However, the remote diagnostics module 224 may also function to provide diagnostic support for computer problems generally encountered by mobile client devices independently of security related software. In this embodiment, the remote diagnostics module 224 provides diagnostic assistance and/or corrective instructions with respect to problems not only associated with security but also provides such support with other problems generally encountered by mobile client devices. The remote diagnostics module 224 has a communication interface or is communicatively coupled with the user interface module 240, the authorization module 232, the policy management module 236 and the policy distribution module 234. This allows a person using the mobile device to get the device repaired where they are as opposed to having to mail the device or wait until he or she is back in the office to get help.

[0033] The remote diagnostics module 224 comprises three modules or sub-modules: a monitoring module 226, a diagnosis module 228, and a diagnosis distribution module 230. The monitoring module 226 receives diagnostic information such as events or audit logs from a client device and stores the information in a data object (242) for the client device. In one embodiment, a client diagnostics module (e.g. Figure 2B, 246) periodically and automatically initiates tests. Results including errors from these tests are reported over a network 204 (e.g. Internet) to the remote diagnostics module 224. Other examples of diagnostic information retrieved from the client are debug output files, examples of which include system event logs, crash dumps, and diagnostic outputs from a client diagnostics module (e.g. 246, Figure 2B). This information may be received periodically over a network 204 from the client diagnostics module 246, or upon an initial network connection by the mobile device with the server, or because the client diagnostics module 246 requests diagnostic assistance.

[0034] The diagnosis module 228 analyzes diagnostic information stored for the mobile device. For example the diagnosis module 228 may perform analysis according to pre-stored diagnostic programs or according to an interactive user environment or a combination of the two. The diagnosis module 228 may provide a repair to a problem in the client device, determine that a trend is occurring for the device, or determine that preventive maintenance is to be scheduled for the client device. In one example, the diagnosis module 228 initiates requests to the client mobile device for additional information. The additional information may be based on input received via the user interface module 240 or according to a pre-stored diagnosis method. In one embodiment, the diagnosis module 228 provides requested information to the

user interface module 240 responsive to user input. In another embodiment, the diagnosis module 228 may provide requested information transmitted via the diagnostics distribution module 230 over the network 204 to the client mobile device responsive to requests received at a user interface module on the client device (e.g. Figure 2B, 218). Once a diagnosis has been made with respect to a problem, support information may be distributed to the mobile device under the control of the diagnosis distribution module 230. For example, support information may be in the form of instructions or code to the client device to repair a problem or perform maintenance. This provides an advantage of taking corrective or preventive actions without requiring user intervention or action. Another example of support information that may be forwarded is messages for display by the client device providing a diagnostic report or requesting specific input from a user of the device.

[0035] Either the monitoring module 226 or the diagnosis module 228 may initiate tests and/or queries to determine the readiness or robustness of the existing client device population. Trends may be noted. Again, these tests may be run during a connection with a device without requiring user intervention.

[0036] The remote diagnostics module 224 may also probe a particular client to verify its status. For example, client configuration information may be retrieved such as the current version of the security policy software components on the client device, the current policy settings on the device, and attributes in accordance with those settings, for example, which ports are blocked. This information may be stored for later assistance in a diagnostics situation or for use with a current diagnostics situation.

[0037] In the system embodiment of Figure 2A, the policy management module 236 defines a security policy applicable to a client mobile device based upon criteria. One example of criteria is the location associated with the network environment in which the mobile device is operating and source information. Other examples of criteria are the presence or the activity status of one or more security features. Of course, a combination of location and one or more security features may also form a criteria basis for defining a security policy. The policy management module 236 designates one or more client devices associated with the policy. In one example, this association may be based on an entity or class to which the security policy is applicable. An example of an entity is a group with one or more members. An example of a member may be a user of the client mobile device. A policy may be set that is applicable to the group of all engineers in the software development department. Another example of a member is the mobile device itself. For example, the capabilities of different mobile devices may be the

basis for classifying them into different groups. In a secure manner, the policy management module 236 provides the one or more designated client mobile devices with authorization information for use in contacting the server system securely. One example of authorization information is an encrypted token provided by the authorization module to the mobile client device during a trusted connection between the two. An example of a trusted connection may be an internal connection behind the firewall of and within the internal network of the enterprise with which both the server system and the mobile client device system are associated. In one embodiment, a management server within the firewall in the internal network provides the authorization information. When a client mobile device connects via the Internet, it interacts with one or more of the enterprise side servers external to the firewall. The client contacts the external servers to retrieve policies and instructions. The external servers also perform key / identity management and policy persistence. The external servers communicate with the management server through the firewall for client management information such as a key, a user, a group, and version information associated with a client mobile device system. In a similar manner, responsive to security information such as a policy or software being designated for encryption, the policy management module 236 provides the designated client mobile device with cryptographic information that the client device can store and use to decrypt the security information. An example of cryptographic information is a key for use with a cryptographic authentication protocol. In one example, Microsoft® web keys may be used. The policy management module 236 sets the permissions for the one or more associated mobile devices with respect to the one or more policies. In one aspect, permissions typically relate to the allowable modification that may be made to a downloaded policy or client software by the client mobile device. Permissions may be applied to various policies and to the criteria upon which policies are defined. For example, there may be permissions set for a policy, but permissions may also be set with respect to a location. Some examples of permissions specific to policies are as follows:

- Ability to see the tray icon
- Ability to shut down the service
- Ability to go to unmanaged mode
- Ability to go to self-managed mode
- Ability to change to a different policy server, or get a policy from another server in the same enterprise
- Ability to not pull down new policies when they are available

- Ability to get software updates directly from a vendor
- Ability to launch the settings application
- Ability to modify visual settings
- Ability to modify feedback levels
- Ability to see/modify server-defined global objects (for each type of object)
- Ability to create new global objects (for each type of object)
- Ability to see/modify global objects in the policy (for each type of object)
- Ability to change the global objects used in the policy (for each type of object)
- Ability to remove adapters from the policy.

Some examples of permissions specific to locations are as follows:

- Ability to manually switch to a location
- Ability to override a location.
- Ability to manually switch to a different location
- Ability to change enforcement mechanisms.

[0038] In one embodiment, in setting the permissions, for flexibility, a permission setting or a level of identification for each of the permissions may also be set. Some examples of these possible settings or levels are as follows:

- Modifiable: The user has permission to modify the setting freely.
- Recommended: The user has permission to modify the setting, but the application will recommend the policy's default.
- Mandatory: The user does not have permission to modify the setting.
- Hidden: The user does not have permission to view or modify the setting.

[0039] The policy management module 236 determines whether the security information is to be encrypted. If not, the policy management module 236 stores the security policy. If it is to be encrypted, the policy is encrypted. Similarly the policy management module 236 may also encrypted other types of security information such as software updates before they are stored. For example, the security policy may be stored as a data object in a memory 242 accessible via an internal enterprise network. In another example, security policies may be included in XML documents that may themselves be encrypted. In an alternate embodiment, the policy management module 236 may store the policy unencrypted, the policy distribution module 234 makes the determination of whether encryption applies to the policy or other security information, and the policy distribution module 234 encrypts the security

information before distributing it. Additionally, in the embodiment of Figure 2A, the policy management module 236 manages the one or more client devices for security purposes. One aspect of client management is that the policy management module 236 maintains client management information for the mobile device and the one or more policies associated with it. The following list of information fields is an example of the types of information that may be included in client management information.

- User Name
- Group
- Connection state, which is one of:
    - Connected
    - Last connected time
    - Never connected
- Policy for this user
- Policy version for this user
- Software version for this user
- Current enforcement mechanisms
- Diagnostic level, including diagnostic options available in the client settings
- Diagnostic information
- Auditing level
- Auditing information
- Locations Previously Detected

[0040] The information may be organized in a data object stored in a memory 242 accessible to the server computer system.

[0041] Through a user interface, a system administrator provides input indicating actions to be taken with respect to managing clients. In the embodiment of Figure 2A, the user interface module 240 provides the input to the policy management module 236. In one example, a graphical user interface (GUI) for managing mobile client devices provides a list of information identifying directly or indirectly all mobile client devices that have connected to the server system, and has controls for managing them. Information displayed may be based on information sent during client-server negotiation. Below are some examples of actions to be taken for one or more client devices selected in accordance with user input.

- Remove this client device from the current list of connected client devices (although the client device is re-added the next time he connects).

- Change auditing level (to one of the options described below).
- Change the diagnostic level.
- View the diagnostic or event log for this client device.
- Reassign this client device to another group.
- Define Properties (e.g. required hardware, required software, data accessibility rights, data visibility rights.)

Mobile Device/Client System

[0042] Figure 2B illustrates a system 201 for protecting data accessible by a mobile device based on a location associated with a network environment in which the mobile device is operating and an access point being used. Additionally, the system 201 in Figure 2B illustrates a system for determining and enforcing security policies based upon the activity status of a security feature in a communication session between the mobile device and another computer. The system 201 comprises a location detection module 208, a policy setting module 212, security features determination module 210, a policy enforcement control module 214, a user interface module 218, memory location(s) 216, an authorization module 245, and a client diagnostics module 246. The system 201 protects data accessible by the mobile device 201 that may be in resident memory 220 on the device or data 242 accessible over a network 204. In this illustrated example, each of these modules has a communication interface or is communicatively coupled to each of the other modules. One or more of these modules may access resident memory 220.

[0043] The authorization module 245 provides authorization information to the authorization module 232 of the server 200 to establish communication exchanges with the client mobile device 201 for the exchange of security information or diagnostic information or both. The client diagnostics module 246 collects diagnostic information that is sent to the remote diagnostics module 224 of the server system embodiment 200.

[0044] In one embodiment, the location detection module 208 receives network parameters from network 204 and detects or determines the location associated with the current network environment based upon criteria defined in a downloaded policy from the server system 200. In this example, the policy setting module 212 receives, installs and updates the security information including security policies and / or software updates received from the policy management module 236 via the policy distribution module 234 over the network connection 204. The policy setting module 212 may define criteria or if permissions set by the

policy management module 236 allow, supplemental policy definitions or customization of policy definitions based upon user input processed by the mobile device user interface module 218. Similarly, if operating in a standalone mode not under the control of the server system, the policy setting module 212 defines an aspect of a policy such as location criteria or security features criteria based upon user input processed by user interface module 218.

[0045] In this embodiment, memory locations 216, including indicators of security features and/or location indicators, have a communication interface (e.g. a bus between a processor executing one or more of the modules and a memory controller responsible for memory reads / writes) to the location detection module 208, the security features determination module 210, the policy setting module 212, the policy enforcement control module 214, the authorization module 245, and the client diagnostics module 246. The location detection module 208 has a communication interface to the policy setting module 212. In the embodiment, the policy setting module 212 determines a security policy based upon the location detected by the location detection module 208 and communicated via a communication interface. In one example of the communication interface, the policy setting module 212 may read a current location indicator 216 updated in a memory location 216 by the location detection module 208. The policy setting module 212 may then read the location indicator 216 periodically or responsive to a notification message from the location detection module 208. In another example, the location detection module 208 may pass the currently detected location to the policy setting module 212 as a parameter in a message. Of course, other communication interfaces known to those of ordinary skill in the art for use in notifying the policy setting module 212 of the current location may also be used.

[0046] In an alternate embodiment, an optional policy setting module 238 may operate on a server computer system such as the one illustrated in Figure 2A that determines the selection of the current security policy for the mobile device based on criteria information received from the mobile device 201 including location and activity status of one or more security features or based on network parameters received from network 204. In this embodiment, a module on the client device such as the policy enforcement control module 214 receives commands from the policy setting module 238 and executes them on the mobile device.

[0047] The policy setting module 212 also has a communication interface to a policy enforcement module 214. The policy enforcement module 214 comprises instructions for enforcing the security policy currently set by the policy setting module 212. The

enforcement module 214 comprises instructions for one or more enforcement mechanisms associated with a security policy. Again, in an alternate embodiment, an optional policy enforcement module 244 in a server computer system 200 with which the client device has a network connection 204 may send instructions to the mobile device for the enforcement of a security policy as determined by the optional policy setting module 238 for the local device on the server side.

[0048] Furthermore, the policy enforcement control module 214 may include an access point filtering unit, and an access point locking unit cooperatively coupled to the other components noted above. The access point filtering unit determines the access points that are accessible by the client device, filters the access points using the security policy in force and presents only access points authorized for use to a user for selection. The access point locking unit locks communication between the access point and the mobile client device so that the mobile client device will not jump to connect with other access points having stronger signal strength. For the present invention the term "lock" or "locking" means only that the connection to the same access point is maintained. The connection is not switched and others are prevented from connecting to the mobile computing device 201. Locking is not meant to imply any type of required coding or encryption. The access point locking unit has a plurality of operating modes and can lock onto a user selected access point, a security policy prescribed access point, or the access point with the best signal profile. The signal profile refers to a combination of: the protocol used for communication, the type of encryption used, the key length for encryption, the wireless signal strength, authentication method and other factors. The operation of these units is explained further below with reference to the flowcharts of Figures 5-8 and the example in Figures 9A and 9B.

[0049] In this embodiment, a user interface module 218 has a communication interface to one or more of these modules 208, 210, 212, 214, 245, and 246. In one embodiment, the user interface module 218 receives input from a user input device such as a keyboard, mouse, or touchpad, and causes user interfaces to be displayed for use by a user for establishing criteria for defining an aspect of a security policy as allowed by permissions associated with the policy or when operating in a standalone mode not under the control of the server system 200.

[0050] The system 201 further comprises a security feature module 210 for determining whether one or more security features have an activity status of inactive or active in a communication session between the mobile device and another computer. An example of a

security feature is a connection type of wired or wireless. In one example, this connection type may be indicated by the association of the port over which data is communicated with a wireless or wired network adapter or network interface card (NIC). In another example, this connection type may be indicated by the association of a local IP address with data communicated over a wireless or wired network adapter or network interface card (NIC). In other embodiments, policies may be set based on particular features besides simply connection type. For example, a different security policy may be applied for different brands of NICs or particular classes (e.g. 802.3, 802.11a, 802.11b, GPRS, GSM) of NICs. Furthermore, different security policies may be assigned based on the operating system employed or the version of the operating system because different systems or versions provide different security features. Furthermore, different policies may be employed based on the security features (e.g. a firewall) provided by different types of network access points (NAP). Additionally, the presence or absence of upgraded NIC support for enhanced security protocols (e.g. 802.11i), or the presence or absence of security software such as virtual private network (VPN), or antivirus software, or intrusion-detection software may be the basis for setting different policies on a particular port, network adapter or data.

[0051] As with the location detection module 208, the security features module 210 has a communication interface to the policy setting module 212 in this embodiment as well as the memory locations 216. An activity status indicator field for the feature stored in the memory locations 216 may indicate the activity status of active or inactive for a security feature. The policy setting module 212 may be notified of the active features via the communication interface implemented in the same manner described in any one of the examples discussed above with respect to the location detection module 208 or in any manner known to those of ordinary skill in the art.

[0052] The policy setting module 212 communicates the current security policy to the policy enforcement control module 214 via a communication interface implemented in the same manner described in any one of the examples discussed above with respect to the location detection module 208 or in any manner known to those of ordinary skill in the art. The policy enforcement module 214 comprises one or more enforcement mechanism modules as specified by the policy. For example, in a communication session between the mobile device and another computer in which data is being transferred over a wireless connection, based on this connection type, in one example, the enforcement module 214 may prevent certain files from being transferred over the wireless connection as opposed to the cases in which the data is being

transferred over a wired connection, or the case in which 802.11i cryptography is being used over the wireless connection. Again, in an alternate embodiment the policy enforcement control module 244 may operate as part of a separate computer system that transfers commands over a network to the mobile device. In the illustrated embodiment of Figure 2B, a client diagnostics module 246 processes events and performs audits relating to processing performed by one or more of the modules. The remote diagnostics module 246 transmits over a network 204 diagnostic information to the remote diagnostic module 224 on the server computer system. Examples of tasks that the diagnostics module 246 performs in order to obtain diagnostics information are as follows:

- Verify that correct files are in correct locations.
- Verify (e.g. checksum) all files to verify no corruption.
- Verify time/date stamps for correct versions.
- Check for outdated installation (INF, PNF) files.
- Verify that all registry entries are correct and correct any errors found. For example, it is verified whether the indications of the installation of the network interface cards (NICs) is accurate.

[0053] Examples of other tasks that the client diagnostics module 246 may perform to provide diagnostic information to the remote diagnostics module 224 on the server computer system 200 include enabling and disabling advanced debugging and sending debugging output to the server computer system 200. For example, enabling and disabling advanced debugging includes turning on system event logging with options including which parameters to log, when to log, etc. and allowing a debug version of a system component to be installed. In this example, the system event log or portions of it and any special debug output files that debug components generate are sent to the remote diagnostics module 224 on the server.

Second Embodiment Of Server And Mobile/Client Devices

[0054] Figure 3 illustrates a system including a server and mobile client device for protection of data accessible by the mobile client device in accordance with second embodiment of the present invention. As illustrated, the system 300 comprises a policy server 350 having an administrator user interface 346. This system 350 is communicatively coupled over a network with the client side system through a communication port 342. Also, as is apparent to those of ordinary skill in the art, the policy server 350 may be implemented in one or more computers or

computer systems. For example, it may comprise a management server executing on one machine for establishing communication sessions and a number of computers with which client devices may communicate in order to obtain their updates and receive diagnostic assistance.

[0055] The client side system embodiment comprises a policy engine 332 operating in application space having a communication interface to management tools 316 of the operating system, a communication interface to a file filter 324 operating in the kernel space that controls access to the file system 326, a communication interface to a user interface module 302, and also having a communication interface to a packet filter engine 318 operating within a driver 334. In this example, the driver 334 is an NDIS intermediate driver 334 operating within the kernel of the operating system of the mobile device.

[0056] The policy engine 332 further comprises a diagnostics module 344, a rule processing module 308, rules 340 and representative examples of rules subsets, packet rules 310 and file rules 312. In addition to the packet filter engine 318, the driver 334 further comprises an application filter 322, in this example, implemented as a transport driver interface (TDI) filter 322 and a VPN module 320 embodied here as a VPN Lite 320 implementation discussed below. The TDI filter 322 comprises a communication interface with the packet rules subset 310 and the file rules 312 subset in this example. It also communicates with the packet filter engine 318 as part of the driver 334. The TDI filter 322 further comprises a communication interface with a Windows Socket (Winsock) layer 328 in application space. The Winsock layer implemented in this example as a Windows socket filter and communicates with one or more applications 330 in application space.

[0057] In this embodiment, network environment location detection is performed by the policy engine 332, in accordance with rules implementing one or more location detection tests in the Rules set 340, based on network parameters obtained by the NDIS driver for OSI layers 2–5, and by the TDI filter 322 for OSI layers 6 and 7. For example, the Winsock 328 captures information about network applications starting and stopping and what ports the applications will be using. This information is provided to the filter 318 and the policy engine 332 to provide application awareness. Furthermore, the policy engine 332, in accordance with the current security policy, provides rules with respect to applications. For example, the engine 332 may provide a list of which applications can or cannot access the network, as well as the target IP addresses and ports that they are or not allowed to use. The policy engine 332 then enforces the current policy in accordance with these rules applicable to applications.

[0058] In this example, windows socket 328 is used to determine which application (e.g. browser e-mail application such as Outlook Exchange®) is accessing the network and what networking services the application will be using. An example of an application's network service usage could include Outlook Express opening a specific set of Winsock ports, each using a separate protocol and target I.P. address. The windows socket 328 will pass this information to the packet filter engine 318, which then informs the policy engine 332 using an event signaling mechanism. An example of an event signaling mechanism is to use named events to signal the policy engine 332 that some event has occurred.

[0059] Filtering of specific applications provides further resolution for location detection and enforcement mechanisms. The context of Microsoft® Networking provides an example of the benefits of such a filter. Several applications such as Exchange and Microsoft® File Sharing can and do use the same TCP and UDP ports. The NDIS filter driver 334 cannot determine which application is active based solely on TCP and UDP ports. The NDIS filter driver will act on the low level information i.e. TCP or UDP port numbers. When the packet arrives at the TDI layer 322, the TDI filter driver 322 determines based on one or more application parameters for which Microsoft Networking application a packet is destined and if the packet should be forwarded or filtered. For example, the TDI filter 322 provides to the driver, via IOCTL calls, "sessions" which provide information about applications opening ports for sending, listening (receiving), and details such as what protocol is being used and the target IP address of sent packets. Once the application closes the Winsock port, the TDI filter 322 can inform the packet driver that the session is now closed. These sessions allow the driver to be able to detect what incoming and outgoing packets should be allowed through the system and which packets should be forwarded or filtered.

[0060] A benefit of this embodiment is that it allows the NDIS filter driver 334 to do low level filtering based on port or protocol information and not have the overhead of application specific parsing. A modular approach to packet and application filtering is allowed.

[0061] The policy engine 332 also has a communication interface to management tools 316 of the operating system. The management tools 316 provide information to the policy engine 332 such as the types of adapters connected to the mobile device and specific information about each of them such as their brand name. The policy engine 332 also receives from the management tools 316 the local IP address associated with each adapter. Additionally management tools 316 alert the policy engine 332 that applications are running. For example, a process table maintained by the operating system may be monitored and notifications sent by

the management tools 316 to the policy engine 332. For example, it may be determined whether 802.11i wired equivalency protection (WEP) software is running on a network adapter card through which wireless data is being sent and received. In this way, the policy engine 332 determines which security features are available in a system.

[0062] The policy engine 332 may create a security policy that is not inconsistent with the policies downloaded from the policy server 350. Additionally, modification and local management of policies as allowed, for example in accordance with permissions of policies set by the policy server 350. The policy engine 332 receives user input and sends output via a communication interface with the user interface module 302 to display and change policy settings responsive to user input.

[0063] Rules 340 comprise rules that define one or more security policies to be enforced by the policy engine 332. The policy engine 332 comprises a rule processing module 308 which executes tasks in accordance with determinations to be made as set by the rules for the current security policy and for directing the appropriate results dictated by the rules of the current policy.

[0064] In one embodiment, rules are pairings of logically grouped conditions with results. The following are examples of conditions, which may be connected by logical operators:

- Check for the existence of a registry key
- Check for a registry value
- Check for the existence of a file
- Check for a currently running application
- Check for a currently running service
- Check for the existence of network environment settings (includes a list of environments)
- Verify that specified applications are running
- Verify that specified protocols are enabled
- Verify that specified VPN is running

The following are examples of results:

- Can/Can't use the network
- Can/Can't use the machine
- Locked in to a certain location

- Can/Can't access the file
- Can/Can't use the application
- Only transfer encrypted version of file.

[0065] Examples of subsets of rules are illustrated in Figure 3, packet rules 310 and file rules 312. These subsets illustrate examples of enforcement mechanisms that may work at different layers of a communication model, for example at the network layer and at the application layer.

[0066] One example of an enforcement mechanism is referred to as stateful filtering. In one example, a security policy is called a type of shield or is referred to as a particular type of shield level. The state may hereafter be referred to as the shield state or shield.

[0067] If the filtering is performed on a packet basis, it is referred to as stateful packet filtering. In stateful packet filtering, a packet filter such as the packet filter engine 318 as it name suggests filters packets based on a state set by the currently enforced policy with respect to a parameter. Examples of such a parameter include source IP addresses (for received packets) or target IP addresses (for sent packets), port numbers, port types or a port group. A port group is a list of ports that are used by a particular application, network service or function. For example, a port group can be created that includes all the ports for a particular instant messaging application, or for all supported instant messaging applications, or for all applications used internally at a company. Examples of port groups that may be selected for processing by a policy include web surfing ports, gaming ports, FTP and SMTP ports, file sharing and network ports, and anti-virus updates and administration ports. A port group can contain individual port items or other port groups.

[0068] In this example, we discuss a version of stateful filtering called adaptive port blocking. In this example, there are rules comprising a mapping between a set of ports, port types, and actions. The ports are the actual port numbers, the port types enumerate the possible port types e.g. UDP, TCP, IP, or Ethertype, and the actions are what is to be done with this particular port e.g. filter, forward, or inform. The inform action will post an event to the policy engine 332 when a packet is sent or received on the specified port. Filter and forward action control the sending and receiving of packets on the specified port.

[0069] In one example, a policy is in effect that each port is in one of three modes: open, closed, or stateful. When the port is open, all traffic (both incoming and outgoing) on that port is permitted to flow through the packet filter. When the port is closed, all traffic on that

port is blocked (both incoming and outgoing). When the port is stateful, all outgoing traffic on that port is permitted to flow through the packet filter, and incoming responses to that outgoing traffic are allowed back through, but unsolicited incoming traffic is blocked. In another example, incoming and outgoing traffic may be blocked on a basis, examples of which are a network service or an application.

[0070] In the system embodiment illustrated in Figure 3, components such as the policy engine 332, the packet filter engine 318 and the TDI filter 322 may be employed for supporting stateful filtering. In one example, a session is created when a mobile device initiates communications with a particular remote or a specified set of remote computing devices. The stateful filtering, as may be performed by the packet filter engine 318 and /or the TDI filter 322 in accordance with rules 340, for example rules in the subset of the packet rules 310, applicable to the current policy, may use the transport protocol to determine when a session is starting and the address of the remote device. Forward and filter decisions in accordance with rules in the set of rules 340 or the subset of the packet rules 310 may be based upon the session information obtained at session startup. Additionally, forward and filter decisions may be based on application parameters received via the TDI filter 322. This provides the benefit of more refined application filtering as illustrated in the example discussed above.

[0071] The policy engine will pass the rules to the packet filter engine as commands using the existing IOCTL interface. In one example, the policy engine determines based upon its current rules which ports or range of ports should do stateful filtering. These rules are then passed to the packet filter engine 318 by an IOCTL command. In another example, the policy engine 332 determines that rules of the current security policy do not support certain applications accessing a network. These rules are passed to the packet filter engine 318 as well as the TDI filter 322 for application specific filtering. The policy engine 332 may also pass rules about application-specific network access to the TDI filter 322 via an IOCTL interface.

[0072] Each component of the system may also provide health checks on the others. For example, the policy engine 332, the file filter 324, and the packet filter engine 318 report whether any of the other services have been disabled or removed from the system to the diagnostics module 344. This information may be relayed to the policy server 350 as it indicates a possible compromise of the protective system. The policy server 350 in that case provides diagnostic support information to the diagnostics module 344.

[0073] Stateful packet filtering deals with packets with different types of address. Outgoing packets have three different types of addresses: directed, multicast, or broadcast. Directed addresses are specific devices. Broadcast packets are typically used to obtain network configuration information whereas multicast packets are used for group applications such as NetMeeting®.

[0074] To establish session state information with a directed address is straightforward. The IP address and the port number are recorded in a session control block. When the remote responds the receive side of the filter engine will forward the packet because a session control block will exist for that particular session.

[0075] When the outgoing packet is a multicast packet there is a problem. Multicast packets are sent to a group; however, a multicast address is not used as a source address. Hence any replies to the outgoing multicast will have directed addresses in the source IP address. In this case the filter engine will examine the port to determine a response to a given multicast packet. When a response to the specified port is found session control block will be completed i.e. the source address of this incoming packet will be used as the remote address for this particular session. However, more than one remote may respond to a given multicast packet, which will require a session control block be created for that particular remote. The broadcast packets may be handled in the same manner as the multicast.

[0076] The file rules subset 312 have a communications interface such as an IOCTL interface with a file filter 324 having a communication control interface with a file system 326. The file filter 324 may implement one or more filter related enforcement mechanisms. A policy may protect files based on the location in which they are created and/or modified as well as the location in which the mobile device is operating. The policy specifies a set of locations in which the files are to be made available, and whenever the mobile device is not operating in one of those locations, those files are unavailable. In another embodiment, policies may require that files be encrypted only if they were copied from certain network drives.

[0077] One reason for requiring that all files created and/or modified in one of the specified locations is so that copies of sensitive files or data derived from the sensitive files are also protected. Specific mechanisms for protecting the files include file hiding and file encryption.

[0078] When the mobile device is operating in one of the specified locations, the files can be located (e.g., they are not hidden). When the mobile device is operating in some

other location, the files are hidden. One purpose of this mechanism is to prevent the user from accidentally revealing the contents of sensitive files while in locations where access to those files is not authorized.

[0079] One mechanism for hiding the files is to simply mark them "hidden" in their Windows properties pages, and to cache the access control list (ACL) on the file and then modify the permissions to deny all access by non-administrators. Other versions may use the file-system filter to more effectively render the files unavailable.

[0080] In one embodiment, files that are subject to location-based protection by the policy are always stored encrypted. When the mobile device is associated with one of the specified locations, the files can be decrypted. When the mobile device is associated with some other location, the files cannot be decrypted. This mechanism provides a benefit of preventing unauthorized persons who may have stolen the device from gaining access to sensitive files.

[0081] One mechanism for encrypting the files is to simply mark them "encrypted" in their properties pages, and to rely on the file hiding feature (see above) to stop the files from being decrypted in an unauthorized location. Other versions may use the file-system filter to more effectively encrypt the files in a way that does not depend on the operating system to prevent them from being decrypted in an unauthorized location.

[0082] Policies can have rules controlling the use of VPNs. For example, a rule can require that when the VPN is in use, all other ports are closed. This prevents hackers near the user from co-opting the user's device and coming in to the corporate network over the user's VPN connection. In one embodiment, a lightweight web-based VPN is used that allows traffic from selected applications (e.g., email) to be encrypted with Transport Layer Security (TLS).

[0083] In one embodiment, a VPN Lite 320 having a communication interface with the packet filter engine 318 establishes a TLS-encrypted, authenticated connection with the server, and then sends and receives traffic over this connection. The TDI filter 322 diverts the outgoing traffic from the application to a VPN client piece 320, and incoming traffic from the VPN client piece 320 to the application.

[0084] In one implementation example in accordance with the present invention a layer is inserted into the Winsock environment, which opens up a Transport Layer Security (TLS) or Secure Socket Layer (SSL) socket to the VPN server, and tunnels all application network traffic through that connection to the VPN server. The applications are unaware that the VPN is active. The VPN has a very small footprint, since TLS is included in Windows®. In this example, using the Winsock Environment, all communication between client and server

is routed through a secure channel. Unlike current clientless VPNs, all existing applications are supported

[0085] As seen in the embodiment of Figure 3, the packet filter engine 318 and the TDI filter 322 comprise implementation examples of functionality for processing network traffic. The policy engine 332 performs implementation examples of functions of determining location analogous to those of the location detection module 208, of determining policies analogous to those of the policy setting module 212 and of identifying active security features analogous to those of the security features determination module 210. Furthermore, the packet filter engine 318, and the TDI filter 322 also perform implementation examples of enforcement mechanisms that the policy enforcement control module 214 may analogously perform.

[0086] The diagnostics module 344 of the policy engine 332 performs similar functions discussed with respect to the client diagnostics module 246 of Figure 2B. For example, it provides status, configuration, error logs, audit logs, and debug information to the server system. Similarly, it would assist a server side remote diagnostics module such as module 224 in Figure 2A in debugging an error, for example in a method such as that described in Figure 11.

[0087] In one embodiment, policy documents are XML documents. XML allows great flexibility in design, usage, and enhancement of policies. Using the flexibility of XML as the means to distribute enterprise wide policies simplifies the complex problem of distributing and enforcing enterprise wide policies. Policies are defined by the enterprise including but not limited to program usage, network access, hardware restrictions, VPN access, data access, and many other policies. The definition of these polices is performed at the enterprise level using XML Schemas and documents. The policies may then be distributed to the enterprise clients via various forms of data transfer. Furthermore, the policies may also be protected from hacking by encryption or signatures (i.e. XKMS, XMLDSIG, XMLENC, or proprietary encryptions). The policy is then enforced on the client by a process that can interpret the policy distributed by the enterprise. This approach allows a policy to be extensible and easily changed by the administrator. Furthermore, policy management, compilation and interpretation are performed by policy aware application interfaces. Also, the administrator can configure elements of the policy such that they are configurable by the end user. In one example, the XML schema or XSD is derived from the standard XML schema http://www.w3.org/2001/XMLSchema (May 2001). In this example, a schema defines one set of types that is used by both the server (group) and the client policies. Policies may be signed to

ensure integrity. Additionally individual policy elements will be signed to ensure integrity of policy enforcement.

[0088] In one embodiment, a very thin client host application resides on a client mobile device. For example, it may be part of the policy setting module 212 for the embodiment of Figure 2B or part of the policy engine 332 in Figure 3. The central policy server or server system 350 pushes execution instructions to the client, described by XML. As a result, a small relatively stable execution environment is available as part of the client device. When additional or different functionality is needed on the client, this new functionality is pushed to the client in an XML format.

[0089] For example, assume version vX.01 of a product supports two types of security policies. For version X.02 it is necessary to implement a third type of security policy. The implementation and associated behaviors of the policy would be described within XML and published to the clients via the policy server. Clients running vX.01 would then effectively be upgraded without user intervention. In another example, this approach could be used for instantiating portions of an application to clients in a cafeteria style – e.g. they want feature 1, 2, 3, 6, 8 and not 4, 5, 7. If the client requires a change to their implementation, they change their menu selections and implementation and behaviors are pushed to their respective client instances.

Access Point Filter and Lock Units

[0090] Referring now to Figure 4, an example of a mobile client device 201 being accessible to a plurality of access points 402-410 and communicating in accordance with the present invention is shown. Figure 4 is only an exemplary environment for describing the features and function of the present invention, and the mobile client device 201 may be in range of any number of access points 402-410. As shown in Figure 4, each of the access points 402-410 is a different distance 430-438 from the mobile client device 201 and may also have different obstacles or disturbances in the communication to the mobile client device 201, and therefore each may provide a different signal strength for communication.

[0091] One key aspect of the present invention is the ability to control which access points 402-410 are presented to the user of a mobile client device 201, and with which the mobile client device 201 can communicate. The visible and accessible access points 402-410 are preferably set by the policy server 350 in Figure 3 which sends a list of access points

with which the mobile client device 201 can present to the user and establish communication. The policy server 350 preferably provides a different list suitable for each location.

[0092] For example, a security policy for the location shown in Figure 4 may be provided from the policy server 350 (not shown in Figure 4) to the mobile client device 201. Such a security policy may provide that communication is only permitted under the security policy with access points A 402, B 404 and C 406. When the user tries to connect to the mobile client device 201 to available access points at the location shown in Figure 4, only access points A 402, B 404 and C 406 are presented to the user as possible connection points, and only connection to those points will be allowed by the security policy enforcement control module 214 in Figure 2B. Even though access points D 408 and n 410 are accessible to the client mobile device 201, they will not be presented to the user as a possible connection, and connection to them will not be permitted.

[0093] Another key aspect of the present invention is the ability to lock the mobile client device 201 to communicate with a specific access point. The present invention advantageously overrides the default switching protocol of the wireless communication adapter such that the mobile client device 201 continues to communicate with a specific access point even though another access point may provide a signal with greater strength so long as the signal strength for the specified access point is above a predefined minimum strength threshold. The specific access point to which the mobile client device 201 is locked is determined using a variety of factors as will be described in more detail below with reference to Figures 9A and 9B. This is particularly advantageous because it prevents the loss of connection between the mobile client device 201 and the specific access point, and having to establish a connection to a new access point.

[0094] For example in Figure 4, the mobile client device 201 may be locked to access point C 406. Even though the signal strength of access points A 402, B 404, D 408 and n 410 may be greater than that of access point C 406, the mobile client device 201 will continue to communicate with access point C 406 until the signal strength is below a predetermined minimum. The security policy enforcement control module 214 locks to access point C 406 by masking the appearance of competing access points A 402, B 404, D 408 and n 410 from the list that the mobile client device 201 can detect. This allows the mobile client device 201 to remain connected to access point C 406, the access point of interest, regardless of signal fluctuations until the signal becomes totally unusable.

[0095] Yet another aspect of the present invention is that a plurality or group of access points may be set to be a virtual access point such that plurality of access points are presented to the user as a single access point. The virtual access point interacts with the mobile client device 201 in the same way a single access point would interact with the mobile client device 201, and the user may not be aware and need not care that communication is actually roaming between any one of multiple access points in the set of access points that forms the virtual access point. Moreover, the visibility and lock features described above are applicable to the virtual access point and the security policy enforcement control module 214 treats it as a single access point such that a virtual access point is visible or not, and the access points it represents are never presented, and switching between access points forming a virtual access point does not affect the user. This feature is particularly advantageous for managing multiple access points and making them appear the user the same as a location definition.

[0096] For example, as shown in Figure 4, access point A 402 and access point B 404 may be combined into a virtual access point 420 for communication with the mobile client device 201. As such virtual access point 420 will be visible to the user only if 1) the virtual access point 420 is defined under the security policy to be visible and accessible, or 2) both access point A 402 and access point B 404 are defined under the security policy to be visible and accessible. Similarly, the mobile client device 201 can be locked to communicate with the virtual access point 420 and will continue to communicate with the virtual access point 420 until the signal strength is below a predetermined minimum. In other words, the signal strength between the mobile client device 201 and both access point A 402 and access point B 404 must be unusable, otherwise the mobile client device 201 could maintain communication with either access point A 402 or access point B 404. While Figure 4 only shows the virtual access point 420 as comprising two other access points 402, 404, those skilled in the art will recognize that a virtual access point 420 may include any number of other access points and that two virtual access points may include overlapping sets of access points.

[0097] Referring now to Figure 5, the method for locking communication between a mobile client device 201 and a user selected access point will be described. The method begins by determining 502 the available access points for the location that the mobile client device 201 is operating. Then the method determines 540 if the security policy enforced at the mobile client device 201 for the current location allows user selection of access points. If not, this method is complete and ends because under such a security policy the user is not permitted

to connect to access points. Such a security to policy prevents users from connecting to unsecured networks such as when the location is a publicly available hot spots.

[0098] However, if the security policy does allow user selection of access points for this location, the method continues in step 506, where the method determines whether the security policy limits the access points that are selectable. If not, the method continues by displaying 508 all the accessible access points to the user. The user uses an input device to select an access point, and the access point selected by user is received 510. Then the mobile client device 201 locks 512 into communication with the access point and filters the presence and appearance of competing access points to the user. As has been described above, the mobile client device 201 will remain locked in communication with the selected access point until provides a signal that is below a predetermined threshold of acceptability. In one embodiment, that predetermined threshold is a signal that has an unusable strength. It should be understood that the predetermined threshold of acceptability could also be signal strength of a preset level or other factor relating to the signal such as protocol, encryption, etc.

[0099] If in step 506 it is determined that the security policy limits the access points that are selectable, then the method continues in step 514. In step 514, the mobile client device 201 retrieves 514 permitted access points for this location. This is preferably done by policy enforcement control module 214 accessing memory location 216 storing permitted access points for the location. Then the mobile client device 201displays or presents 516 the permitted access points to user. An access point selected by user is received 518 by the mobile client device 201. It should be understood that if there is only a single access point permitted for this location, steps 516 and 518 are omitted, and the method proceeds directly to step 520. In this case, the access point is set by the security policy and pushed from the policy server 350 to the mobile client device 201 and the user does not select the access point. Finally, the mobile client device 201 locks 520 onto selected access point and filters the appearance of competing access points. This step is similar to that described above as step 512 but limited to the permissible access points, and the method is complete.

[00100] Referring now to Figure 6, the method for locking communication between the mobile client device 201 and an access point having the best signal profile is described. The method begins by determining 602 available access points for the location of the mobile client device 201. Then the method retrieves 604 an available access point from the group determined in step 602. If there are no available access points the method ends. If there is at least one available access point, the method continues to determine 606 a signal "profile" for connection

to the retrieved access point. The signal "profile" is preferably data about the connection between the mobile client device 201 and the access point that is used to determine the quality of the connection. The signal profile preferably includes one or more from the group of signal strength, communication protocol, encryption type, encryption key length, service set identifier (SSID), media access control (MAC) address, authentication type, authentication method, and other information. Once the signal profile for the retrieved access point is determined, the method tests 608 whether there are more available access points that were found to be available for the location in step 602. If so, the method returns to step 604 and repeats steps 604 and 606 for each available access point. If not, the method continues by selecting 610 the access point with the most desirable signal profile. In one embodiment, any access point that has a signal profile criterion that matches a preset requirement may be in the group of desirable access points. In another embodiment, defining multiple criteria the signal must meet sets desirability. For example, each of the factors included in the signal profile could be weighted for desirability such that the most desirable signal profile was one that had encryption, with the key length of 64 or greater, and the greatest signal strength. Those skilled in the art will recognize a variety of rules that could be applied to the signal profiles to determine which signals are the best or most desirable for a give location. In addition, the security policy can provide a default access point in the event there is not a signal profile that is most desirable. Once the most desirable signal profile and its corresponding access point are selected 610, the method locks 612 onto selected access point by filtering the appearance of competing access points in a similar manner to that described above with reference to steps 512 and 520.

[00101] Figure 7 shows a method for locking communication between a mobile client device and an access point authorized by the security policy and having the best signal profile. This method is a combination of the methods described above in Figures 5 and 6, so where appropriate like reference numerals have been used for ease understanding and convenience. The method begins by determining 602 available access points for the location of the mobile client device 201. Then the method determines 704 the security setting for the location of the mobile client device 201. Next, the method creates 706 a subset of usable access points based on the security setting for the location of the mobile client device 201. This is preferably done by starting with a list of available access points from step 602 and selecting those access points that are acceptable under the security policy for this location from the list of available access points. Then in step 708, the method retrieves 604 an available access point from the subset created in step 706. Again, if there are no access points in the subset the

method is complete and ends. However, if there is an access point in the subset, the method determines 606 a signal profile for connection to the retrieved access point in step 606 and then completes step 608, 610 and 612 as has been described above with reference to Figure 6. If in step 608 there are more available access points from the subset, the method returns to step 708 to repeat steps 708 and 606 for each access point. Those skilled in the art will recognize that this method has the advantage of allowing enforcement of a security policy while preserving some flexibility to select the access point with the best signal profile.

[00102] Figure 8 is a flowchart of a method for removing the filter of access points accessible by the mobile client device 201. Once the mobile client device 201 has activated the filter such that only a given access point or a small set of access points are visible and usable, a method to remove the filter and allow all access points accessible by the mobile client device 201 for a location to be presented to the user is needed. The method of Figure 8 illustrates one embodiment for that process. The method begins with a series of tests. First, the method tests 802 whether the mobile client device 201 is transitioning from a secure location to a mobile location. If so, the method proceeds to step 814 where all the available access points for the location are made usable. If not, the method determines 804 whether there is a wireless policy for the location of the mobile client device 201. If so, the wireless policy controls which access points that are usable, and the method proceeds to step 814 where all the available access points for the location are made usable consistent with the wireless policy for this location. Next, the method tests 806 whether the network environment for the location has been stamped. If not, the method continues in step 814 where all the available access points for the location are made usable. If the method the network environment for the location has been stamped, the method tests 808 whether the mobile client device 201 is communicating via a wireless adapter. If not, it is assumed it is a wired connection and the method continues to step 814 to make usable all the available access points for the location. However, if the mobile client device 201 is communicating via a wireless adapter, the method locks 810 into communication with the access point and filters the presence and appearance of competing access points to the user. Next, the method tests 812 whether the filter should be removed. The filter should be removed in various circumstances such as 1) if the user manually requests a clear network environment operation; 2) if a location change for the mobile client device 201 moves to the mobile location; or 3) if the user manually performs a change location operation. If filter should not be removed, the method loops through steps 810 and 812 on a periodic basis. If the filter should be removed,

the method proceeds to step 814 to remove the filter and make all available access points for the location usable.

[00103] Figures 9A and 9B show exemplary signal profiles for a plurality of access points at different points in time. Figure 9A shows signals profiles 902-910 for a plurality of access points a first time (t1). As can be seen, signals A-E have different signal strengths, protocols, encryption types, and key lengths. These signal profiles are provided just by way of example and the signal profile may include any of the information about the communication link provided by an access point. As an example, signal C may have the best signal profile because of a combination of signal strength, protocol and encryption type are the most desirable. This is completely dependent on rules set forth by the security policy. As such, the present invention would lock onto signal C and remain connected to the access point providing signal profile 906. This may be the case even though the signal strength for signal E is greater than the signal strength 912 for signal C. Even at a later time (t2) as shown in Figure 9B, the mobile client device 201 would continue to communicate with the access point providing signal profile 906. The mobile client device 201 is locked into communication with the access point providing Signal C, and is unaffected by signal strength amplitude changes such as the signal strength of signal E being reduced 916 or the signal strength of signal B increasing 914. Thus, the present invention avoids the switching and bounce effects of the prior art that switches to the signal with the greatest signal strength.

[00104] The foregoing description of the embodiments of the present invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the present invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the present invention be limited not by this detailed description, but rather by the claims of this application. As will be understood by those familiar with the art, the present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Likewise, the particular naming and division of the modules, routines, features, attributes, methodologies and other aspects are not mandatory or significant, and the mechanisms that implement the present invention or its features may have different names, divisions and/or formats. Furthermore, as will be apparent to one of ordinary skill in the relevant art, the modules, routines, features, attributes, methodologies and other aspects of the present invention can be implemented as software, hardware, firmware or any combination of the three. Of course, wherever a component, an example of which is a module, of the present

invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of ordinary skill in the art of computer programming.

[00105] Additionally, the present invention is in no way limited to implementation in any specific programming language, or for any specific operating system or environment. For example, one embodiment of the present invention is applicable to AdHoc peer-to-peer connections as well. Access using such connections could be allowed based on key length. Accordingly, the disclosure of the present invention is intended to be illustrative, but not limiting, of the scope of the present invention, which is set forth in the following claims.

CLAIMS

1. A method for connecting to an access point by a mobile computing device, the method comprising the steps of:

determining available access points for a location of the mobile computing device;

connecting the mobile computing device to the access point; and

locking a connection between the mobile computing device to the access point.

2. The method of claim 1, wherein the step of locking is performed until a signal profile between the mobile computing device and the access point falls below a predetermined threshold.

3. The method of claim 2, wherein signal profile includes one from the group of: signal strength, communication protocol, encryption type, encryption key length, service set identifier (SSID), media access control (MAC) address, authentication method and other information about the communication channel.

4. The method of claim 1, wherein the step of locking is performed until a request to perform a clear network environment operation is received, a location change for the mobile computing device is detected; or a request to change location operation is received.

5. The method of claim 1, wherein the step of locking is performed by filtering an appearance of competing access points.

6. The method of claim 1, wherein the step of connecting further comprises:

displaying available access points for the location to the user;

receiving a selected access point selected by the user from the displayed available access points; and

connecting the mobile computing device to the selected access point.

7. The method of claim 1, further comprising the step of determining whether a security policy for the location of the mobile computing device allows user selection of the access point.

8. The method of claim 7, wherein if the security policy for the location of the mobile computing device allows user selection of the access point, the step of connecting further comprises:

displaying available access points for the location to the user;

receiving a selected access point selected by the user from the displayed available access points; and

connecting the mobile computing device to the selected access point.

9. The method of claim 1, wherein the step of connecting further comprises a step of determining whether a security policy for the location of the mobile computing device limits access points selectable by a user.

10. The method of claim 9, wherein if the security policy for the location of the mobile computing device limits access points selectable by the user, the step of connecting further comprises:

displaying to the user permitted access points for the location that the mobile computing device may be connected to under the security policy;

receiving a selected access point selected by the user from the permitted access points; and

connecting the mobile computing device to the selected access point.

11. The method of claim 1, wherein the step of connecting further comprises connecting to the access point prescribed by a security policy for the location of the mobile computing device.

12. The method of claim 1, wherein the step of connecting the mobile computing device to the access point further comprises the steps of:

determining a signal profile for two of the available access points; and

selecting the access point with a most desirable profile to connect to the mobile computing device.

13. The method of claim 1, wherein the step of connecting the mobile computing device to the access point further comprises the steps of:

determining a signal profile for each of the available access points; and

selecting the access point with a most desirable profile to connect to the mobile computing device.

14. The method of claim 12, wherein the signal profile includes one from the group signal strength, communication protocol, encryption type, encryption key length, service set identifier (SSID), media access control (MAC) address, and other information about the communication channel.

15. The method of claim 14, wherein the most desirable signal profile is determined based on encryption type and signal strength.

16. The method of claim 14, wherein the most desirable signal profile is determined based on communication protocol and signal strength.

17. The method of claim 12, wherein the step of connecting further comprises a step of determining whether a security policy for the location of the mobile computing device limits access points selectable.

18. The method of claim 17, wherein if the security policy for the location of the mobile computing device limits access points selectable, the step of connecting further comprises:

providing a group of permitted access points for the location that the mobile computing device may be connected to under the security policy; and

wherein the step of determining the signal profile for two of the available access points, selects access points from the group of permitted access points.

19. A method for connecting to an access point by a mobile computing device, the method comprising the steps of:

determining available access points for a location of the mobile computing device;

filtering the available access points for the location to a group of permitted access points for the location that the mobile computing device may be connected to under a security policy; and

connecting the mobile computing device to one from the group of permitted access points.

20. The method of claim 19, wherein the step of connecting further comprises connecting to an access point from the group of permitted access points and prescribed by a security policy for the location of the mobile computing device.

21. The method of claim 19, further comprising the step of determining whether a security policy for the location of the mobile computing device allows user selection of the access point.

22. The method of claim 21, wherein if the security policy for the location of the mobile computing device allows user selection of the access point, the step of connecting further comprises:

displaying the group of permitted access points for the location to a user;

receiving a selected access point selected by the user from the group of permitted access points; and

connecting the mobile computing device to the selected access point.

23. An apparatus for establishing communication between an access point and a mobile computing device, the apparatus comprising:

a location detection module having an input and an output for determining a location of the mobile computing device;

a security policy module having an input and an output and including a security policy for a mobile computing device;

a security enforcement module having an input and an output for enforcing the security policy on the mobile computing device based on location, the security

enforcement module coupled to the security policy module and the location detection module; and

an access point filtering unit for determining access points that are accessible by the mobile computing device and filters accessible access points using the security policy, the access point filtering unit coupled to the security enforcement module and the security policy module.

24. The apparatus of claim 23 further comprising an access point locking unit for locking communication between the access point and the mobile computing device so that the mobile computing device will not connect to another access points having stronger signal strength, the access point locking unit coupled to the security enforcement module.

25. An apparatus for establishing communication between an access point and a mobile computing device, the apparatus comprising:

a location detection module having an input and an output for determining a location of the mobile computing device;

a security enforcement module having an input and an output for enforcing the security policy on the mobile computing device based on location, the security enforcement module coupled to the location detection module; and

an access point locking unit for locking communication between the access point and the mobile computing device so that the mobile computing device will not connect to another access points having stronger signal strength, the access point locking unit coupled to the security enforcement module.

26. The apparatus of claim 25 wherein the access point locking unit has a plurality of operating modes and can lock onto a user selected access point, a security policy prescribed access point, or the access point with the best signal profile.

27. The apparatus of claim 26 wherein the signal profile refers to a combination of two from the group of: a protocol used for communication, a type of encryption used, a key length for encryption, an authentication method, a wireless signal strength or other factors.

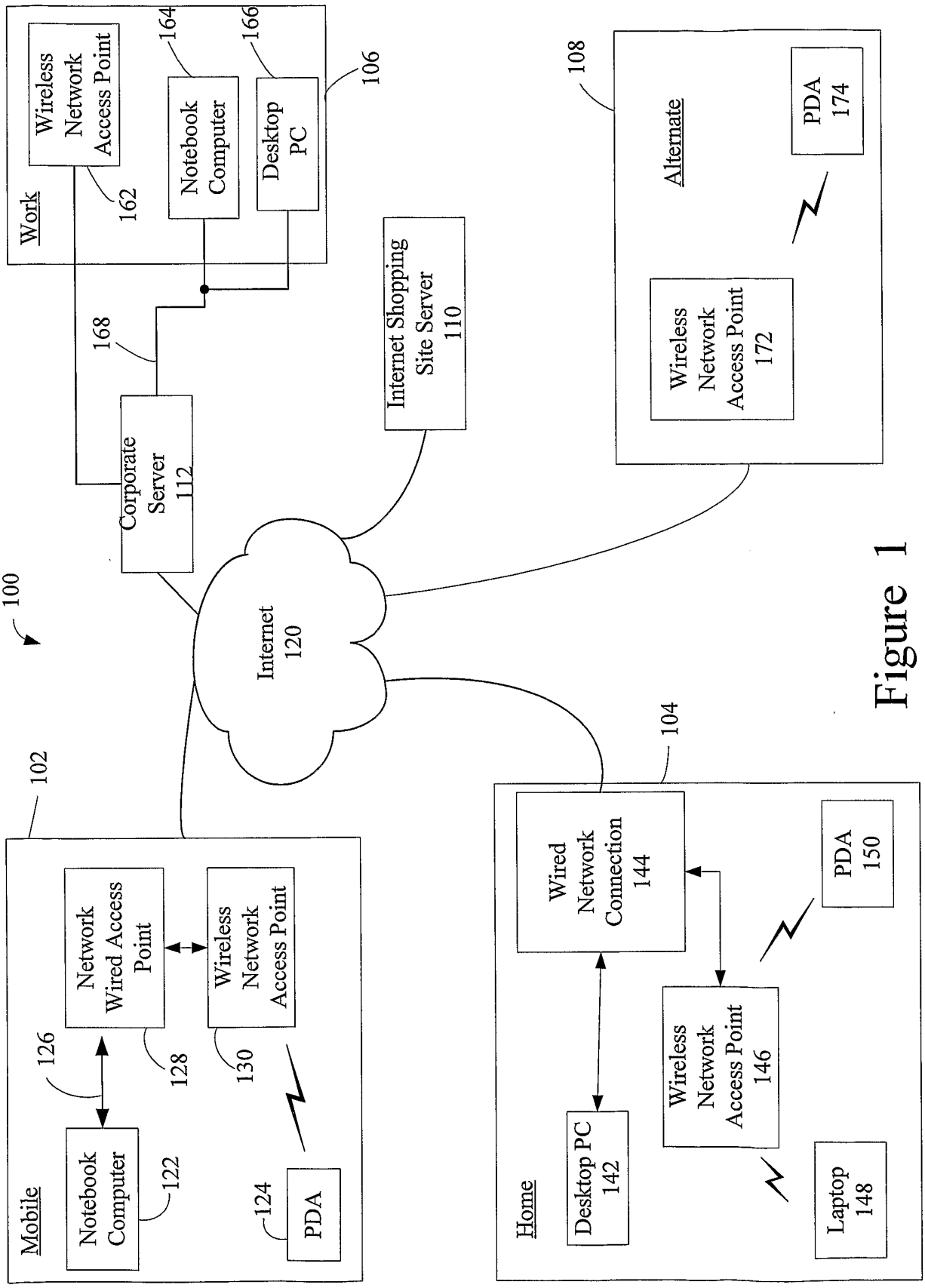

100
Work
Wireless Network Access Point
162
Notebook Computer
164
Desktop PC
166
106
168
Corporate Server 112
Internet Shopping Site Server 110
Alternate
108
PDA 174
Wireless Network Access Point 172
Internet 120
102
Mobile
Network Wired Access Point
126
128
Wireless Network Access Point
130
Notebook Computer
122
PDA
124
104
Wired Network Connection 144
PDA 150
Wireless Network Access Point 146
Desktop PC 142
Laptop 148
Home

Figure 1

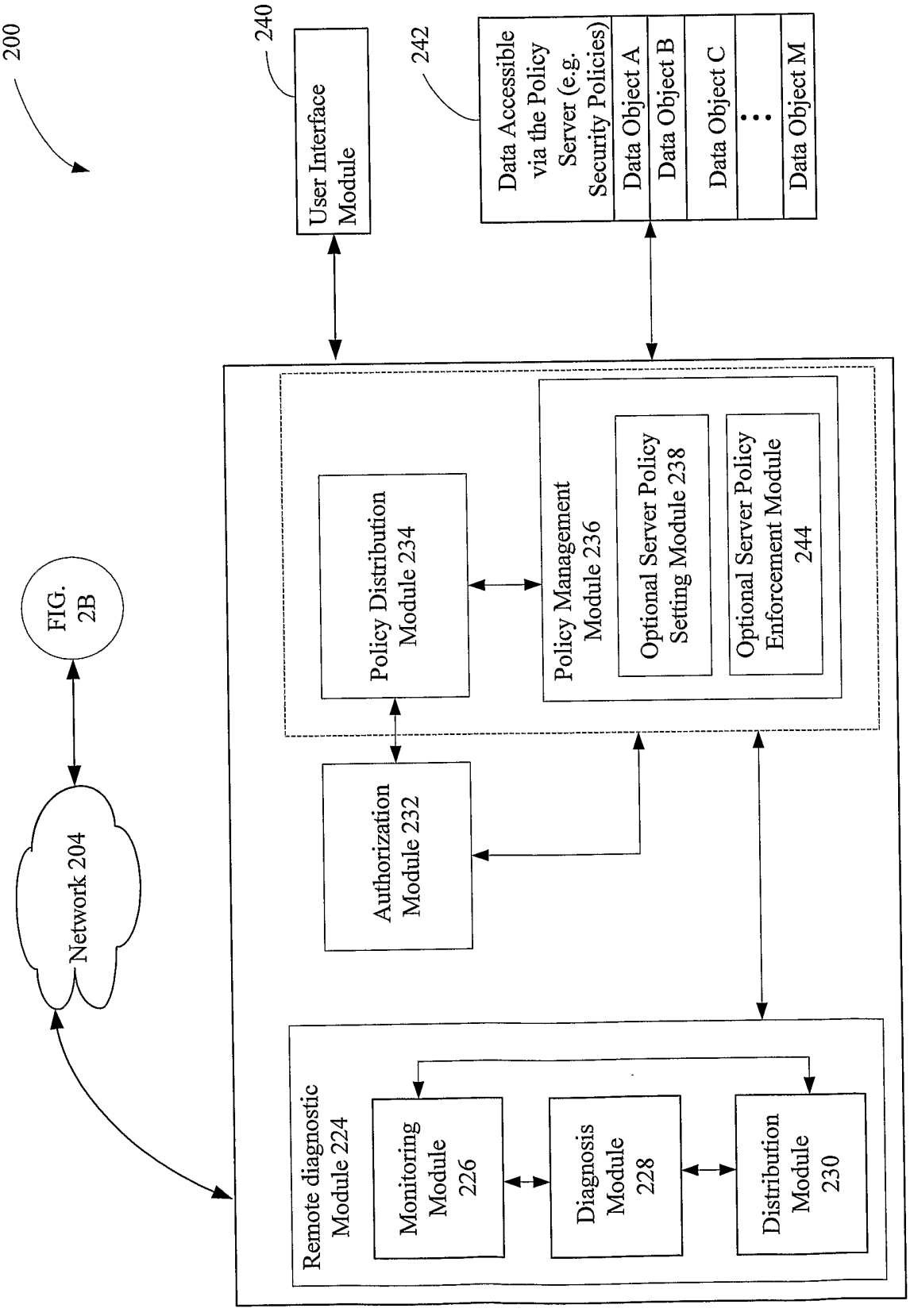

200
240
User Interface Module
242
Data Accessible via the Policy Server (e.g. Security Policies)
Data Object A
Data Object B
Data Object C
Data Object M
Policy Distribution Module 234
Policy Management Module 236
Optional Server Policy Setting Module 238
Optional Server Policy Enforcement Module 244
Authorization Module 232
Remote diagnostic Module 224
Monitoring Module 226
Diagnosis Module 228
Distribution Module 230
Network 204
FIG. 2B

Figure 2A

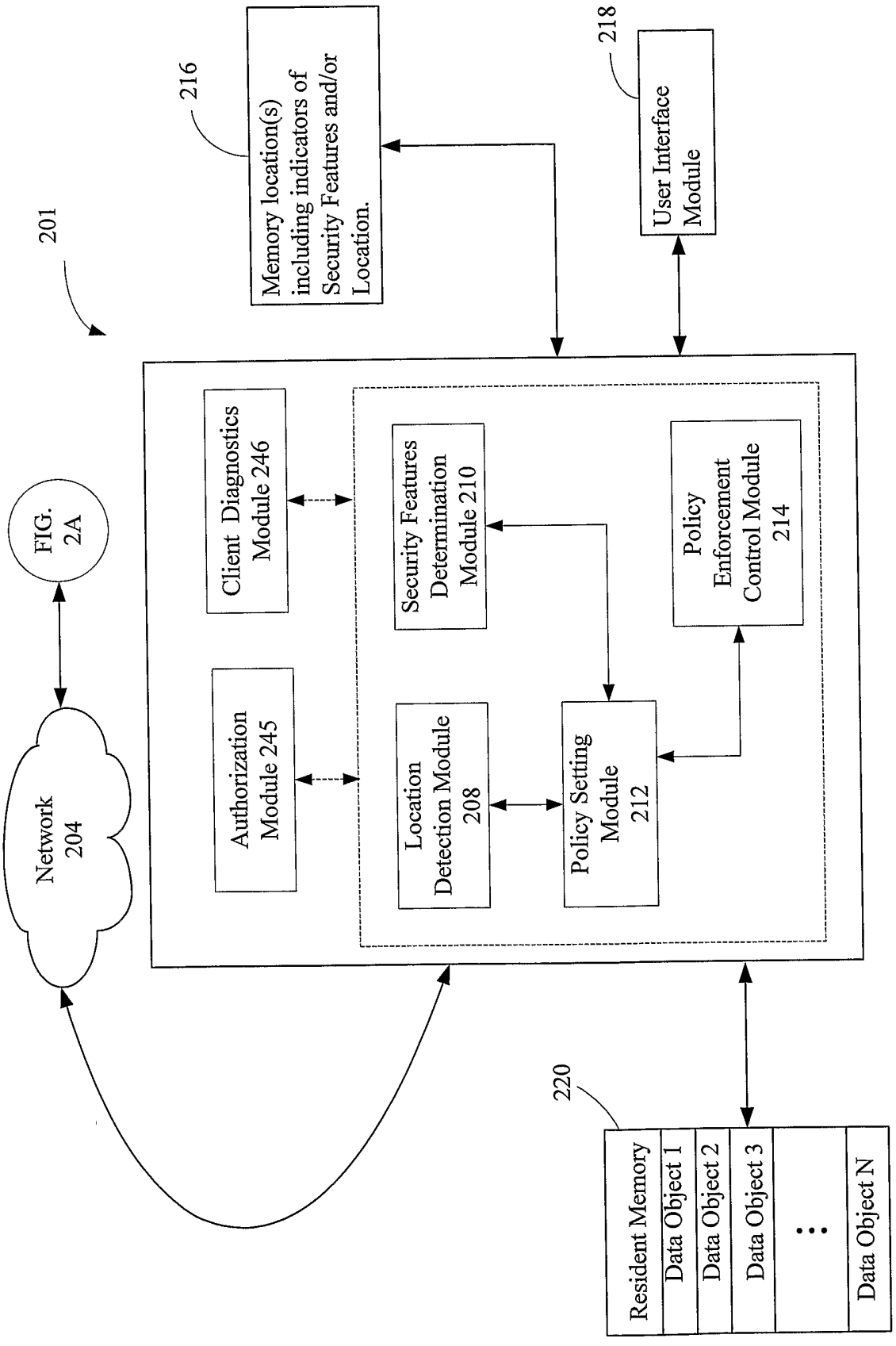

201
216
Memory location(s) including indicators of Security Features and/or Location.
218
User Interface Module
Client Diagnostics Module 246
Security Features Determination Module 210
Policy Enforcement Control Module 214
Authorization Module 245
Location Detection Module 208
Policy Setting Module 212
FIG. 2A
Network 204
220
Resident Memory
Data Object 1
Data Object 2
Data Object 3
Data Object N

Figure 2B

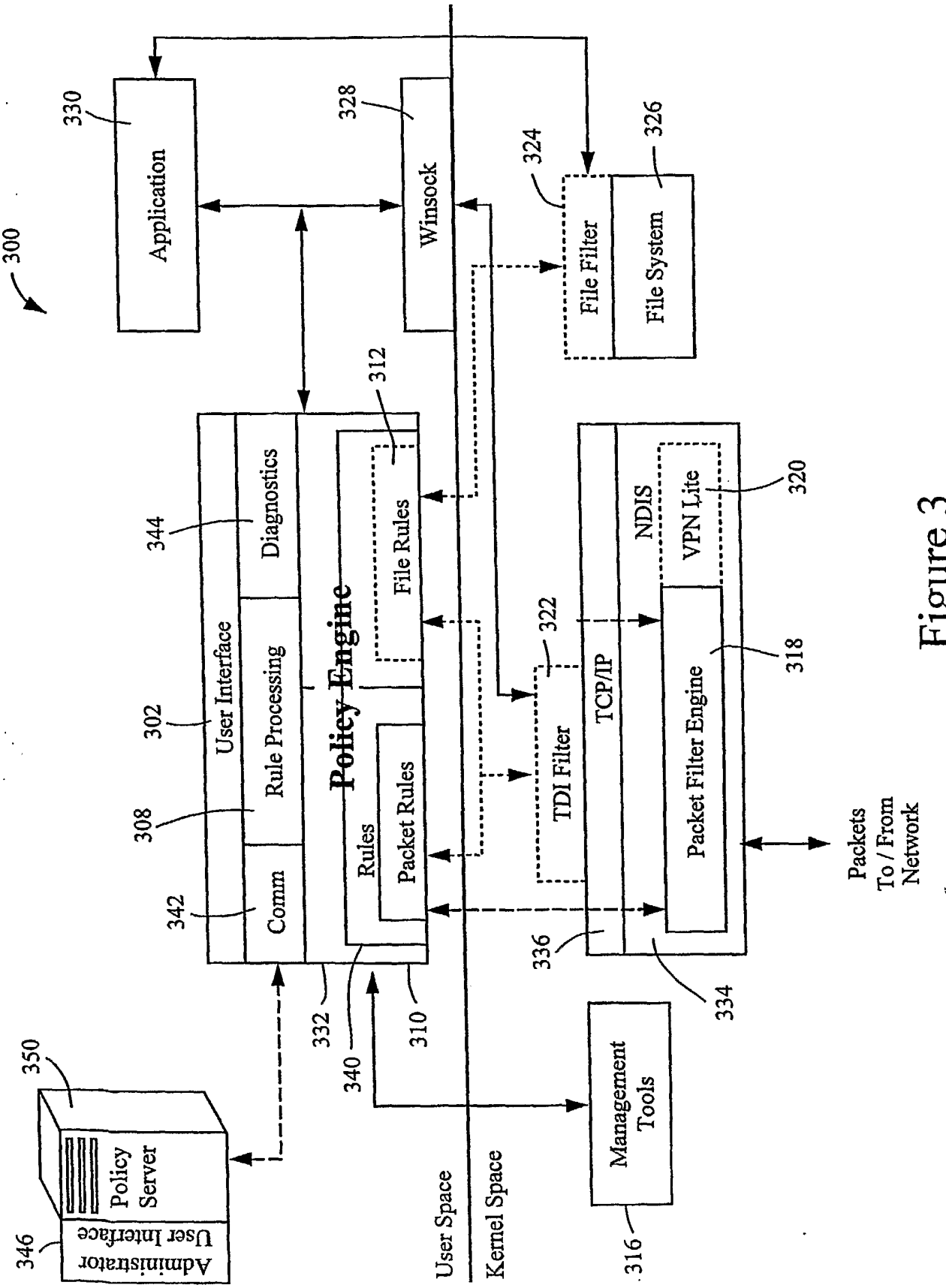

300
Application
330
Winsock
328
File Filter
324
File System
326
Policy Engine
312
User Interface
302
Diagnostics
344
Rule Processing
308
Comm
342
Rules
File Rules
Packet Rules
TDI Filter
322
TCP/IP
NDIS
VPN Lite
320
Packet Filter Engine
318
Packets
To / From
Network
336
334
332
340
310
Management
Tools
316
User Space
Kernel Space
Policy
Server
350
Administrator
User Interface
346

Figure 3

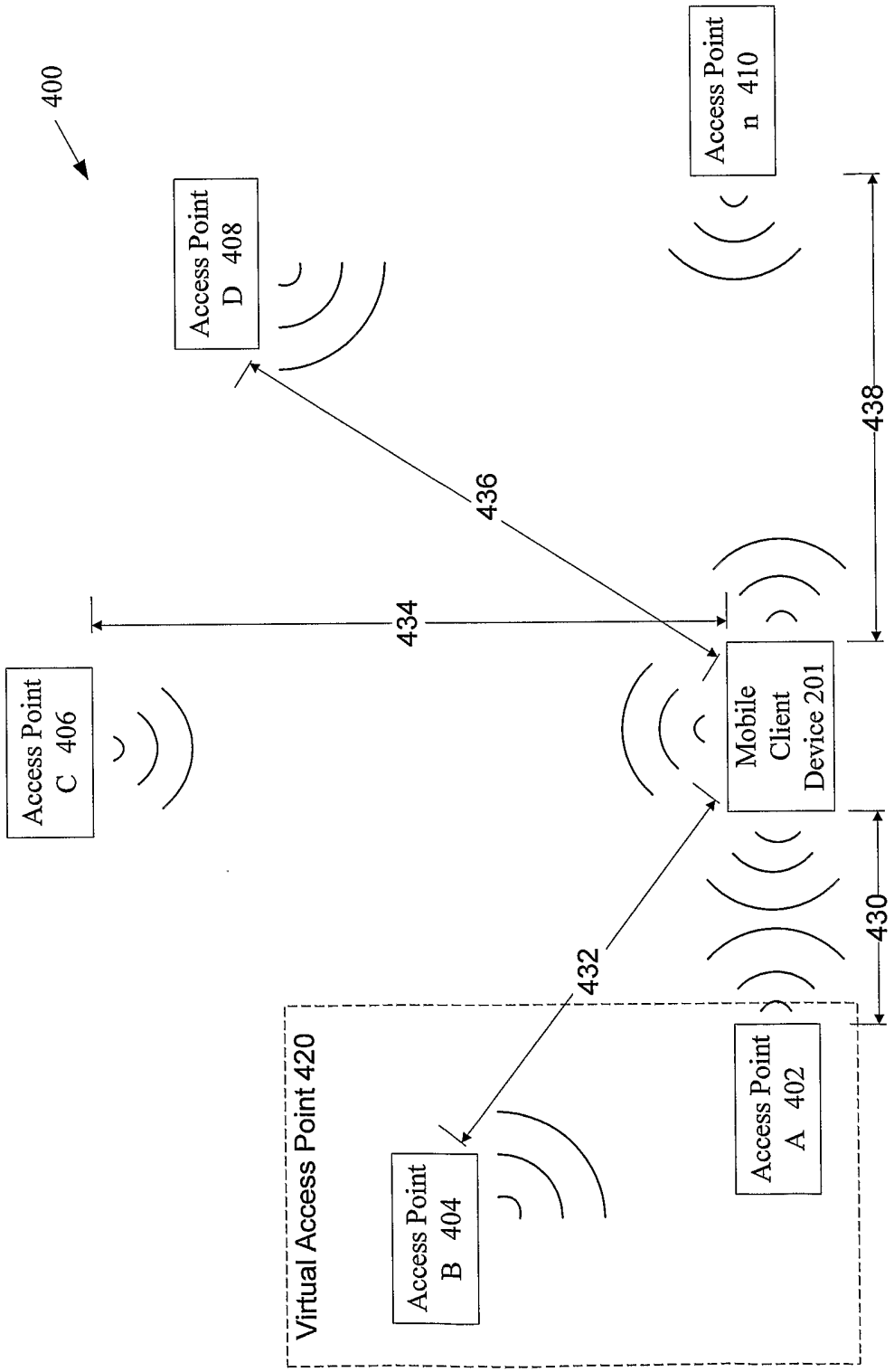

400
Access Point
n 410
Access Point
D 408
436
438
434
Access Point
C 406
Mobile
Client
Device 201
430
432
Virtual Access Point 420
Access Point
B 404
Access Point
A 402

Figure 4

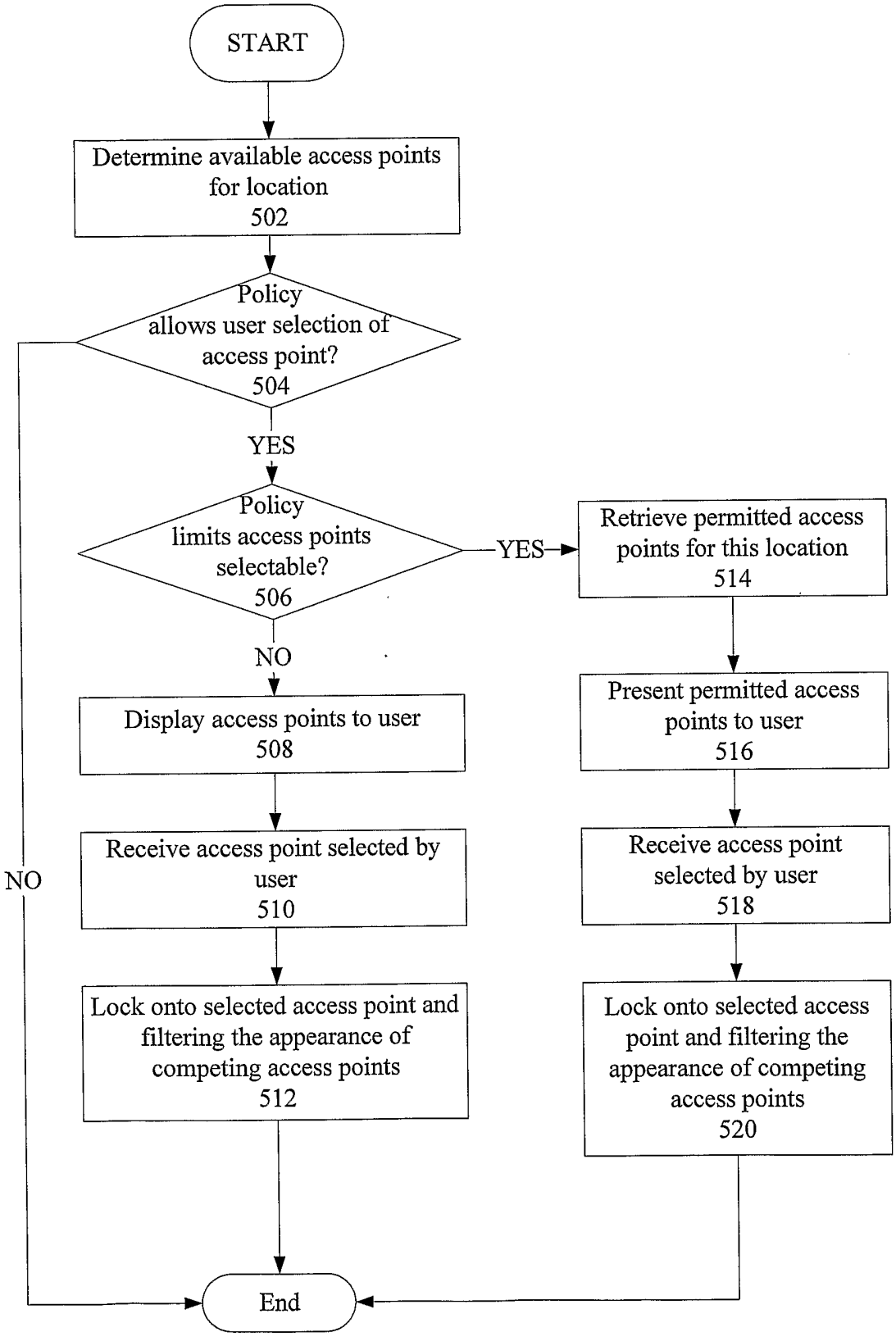

START
Determine available access points for location 502
Policy allows user selection of access point? 504
YES
NO
Policy limits access points selectable? 506
YES
NO
Retrieve permitted access points for this location 514
Present permitted access points to user 516
Receive access point selected by user 518
Lock onto selected access point and filtering the appearance of competing access points 520
Display access points to user 508
Receive access point selected by user 510
Lock onto selected access point and filtering the appearance of competing access points 512
End

Figure 5

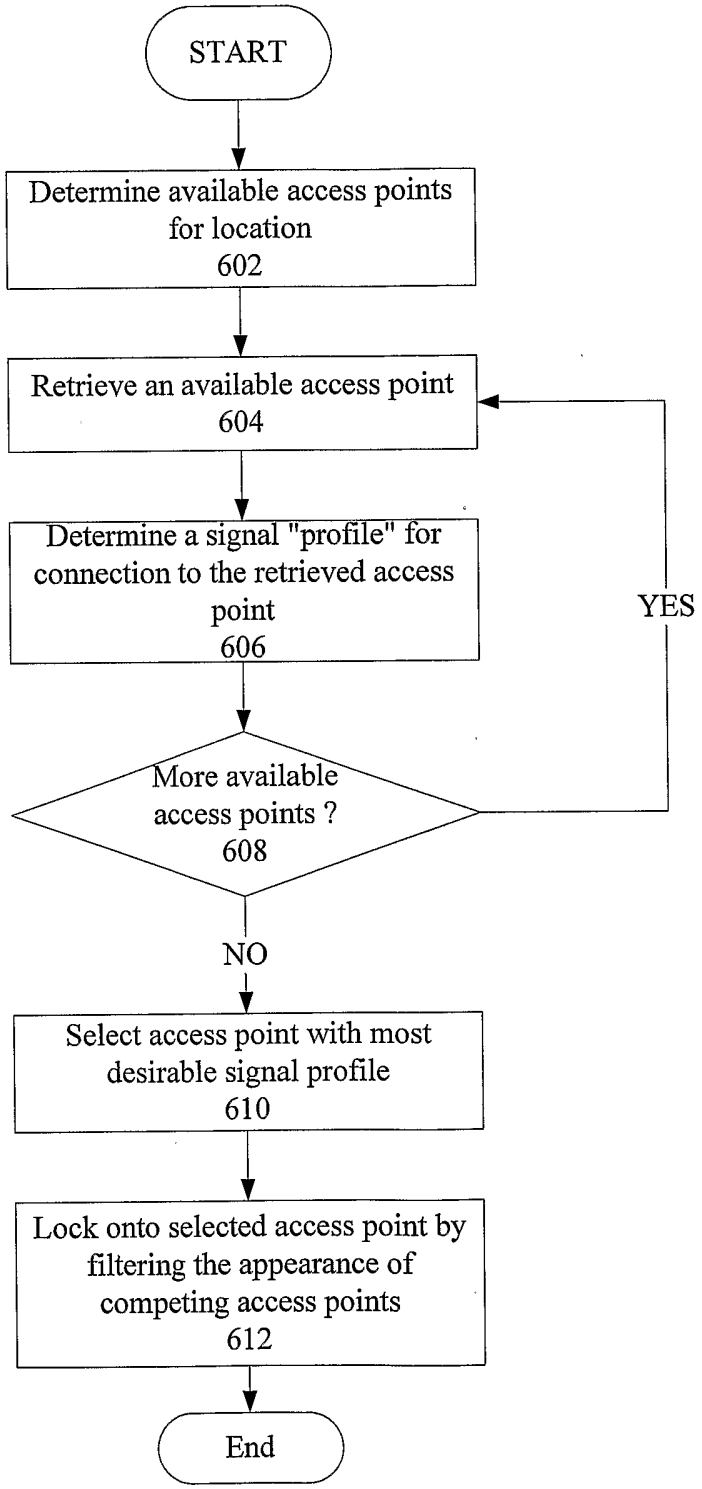

START
Determine available access points for location
602
Retrieve an available access point
604
Determine a signal "profile" for connection to the retrieved access point
606
More available access points ?
608
YES
NO
Select access point with most desirable signal profile
610
Lock onto selected access point by filtering the appearance of competing access points
612
End

Figure 6

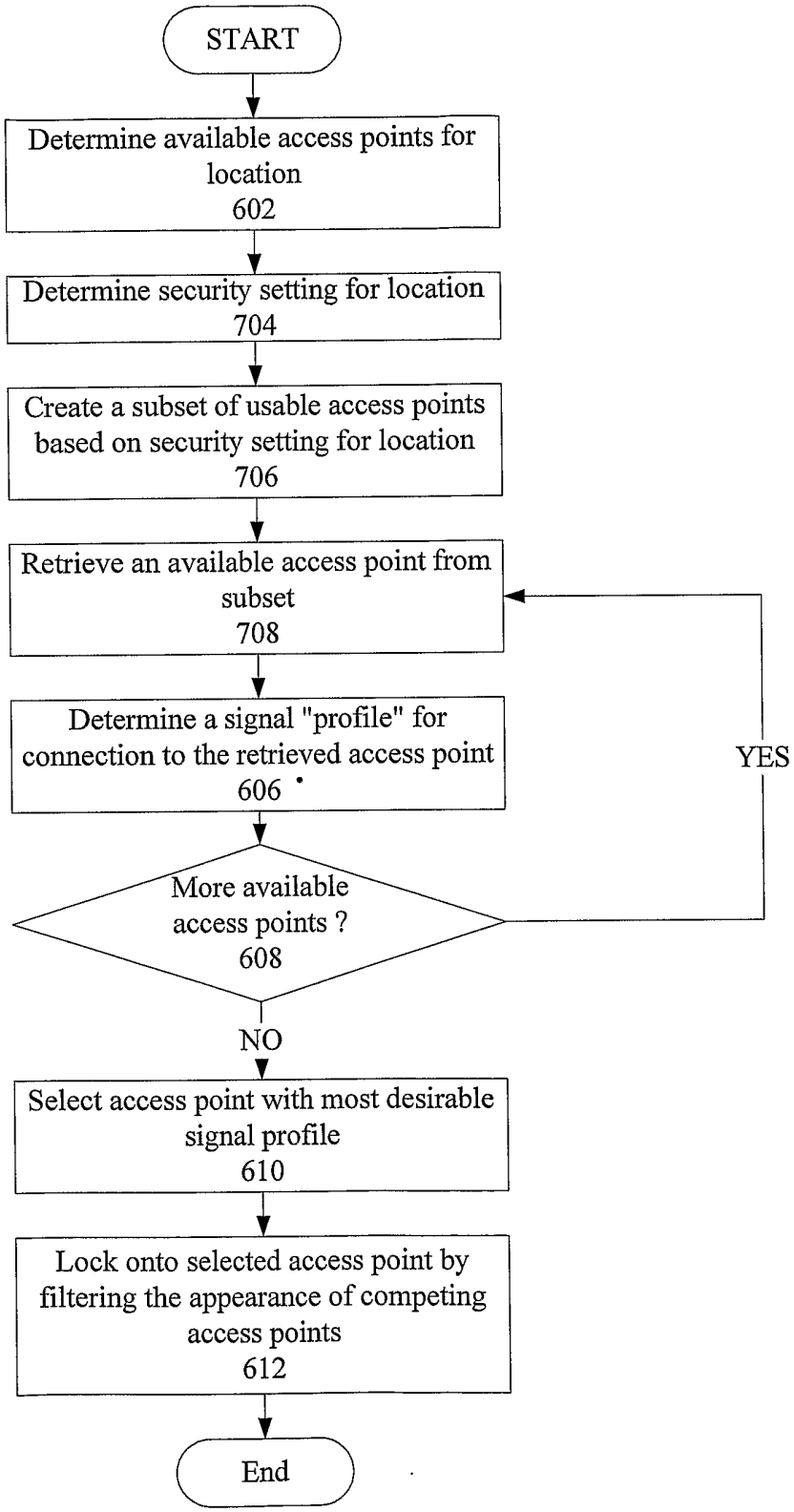

START
Determine available access points for location
602
Determine security setting for location
704
Create a subset of usable access points based on security setting for location
706
Retrieve an available access point from subset
708
Determine a signal "profile" for connection to the retrieved access point
606
More available access points ?
608
YES
NO
Select access point with most desirable signal profile
610
Lock onto selected access point by filtering the appearance of competing access points
612
End

Figure 7

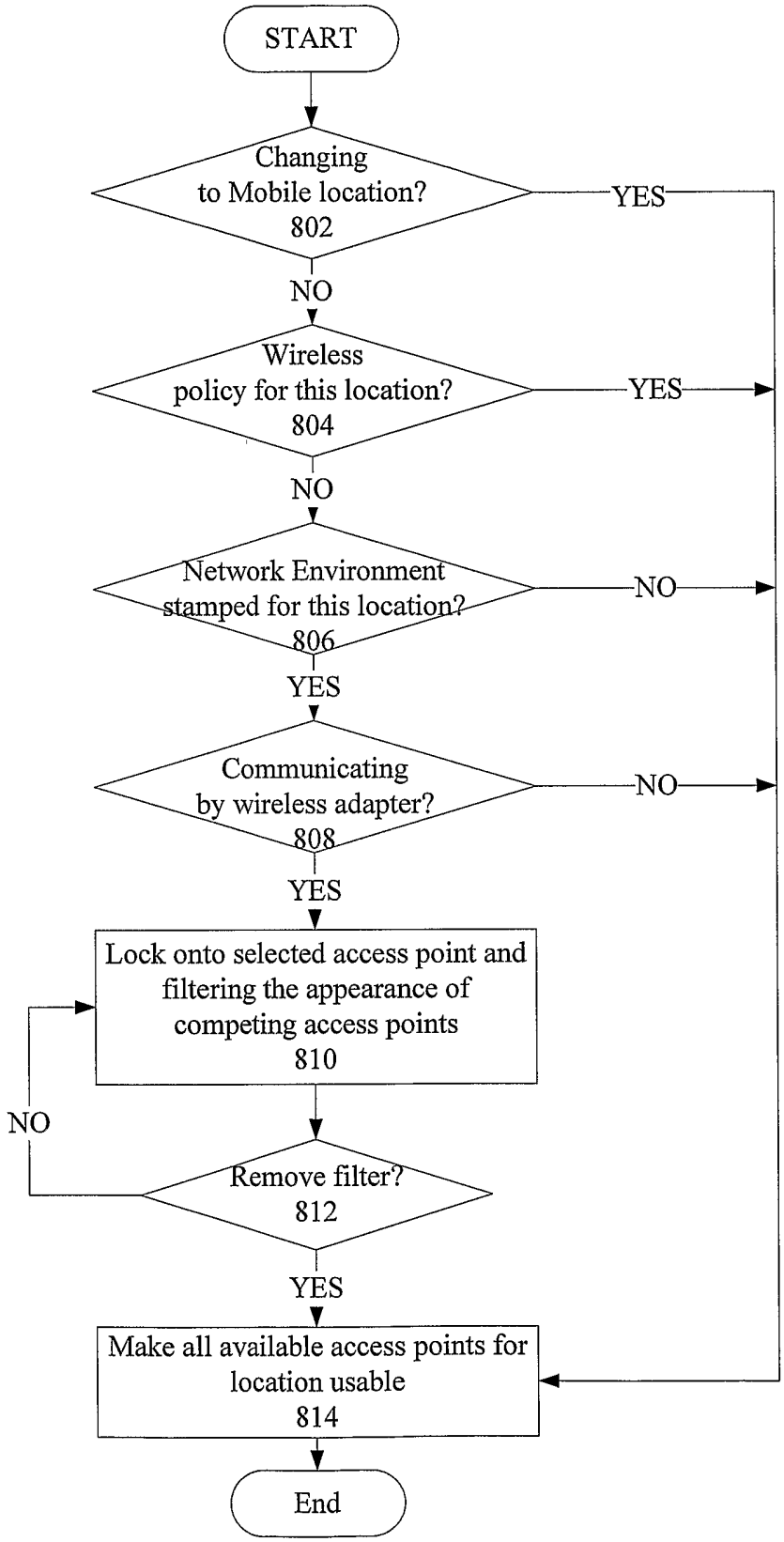

START
Changing to Mobile location? 802
YES
NO
Wireless policy for this location? 804
YES
NO
Network Environment stamped for this location? 806
NO
YES
Communicating by wireless adapter? 808
NO
YES
Lock onto selected access point and filtering the appearance of competing access points 810
NO
Remove filter? 812
YES
Make all available access points for location usable 814
End

Figure 8

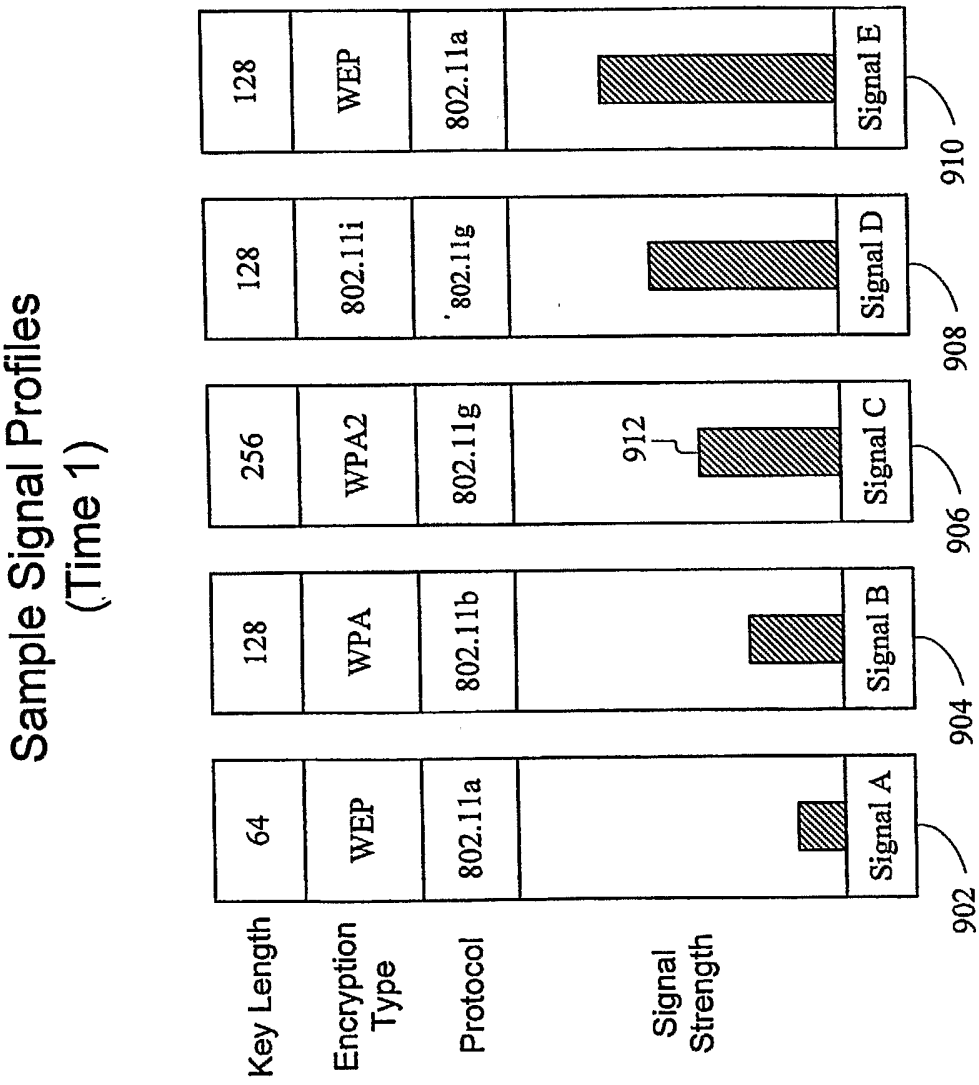

Sample Signal Profiles
(Time 1)
Key Length
Encryption Type
Protocol
Signal Strength
64
WEP
802.11a
Signal A
902
128
WPA
802.11b
Signal B
904
256
WPA2
802.11g
912
Signal C
906
128
802.11i
802.11g
Signal D
908
128
WEP
802.11a
Signal E
910

Figure 9A

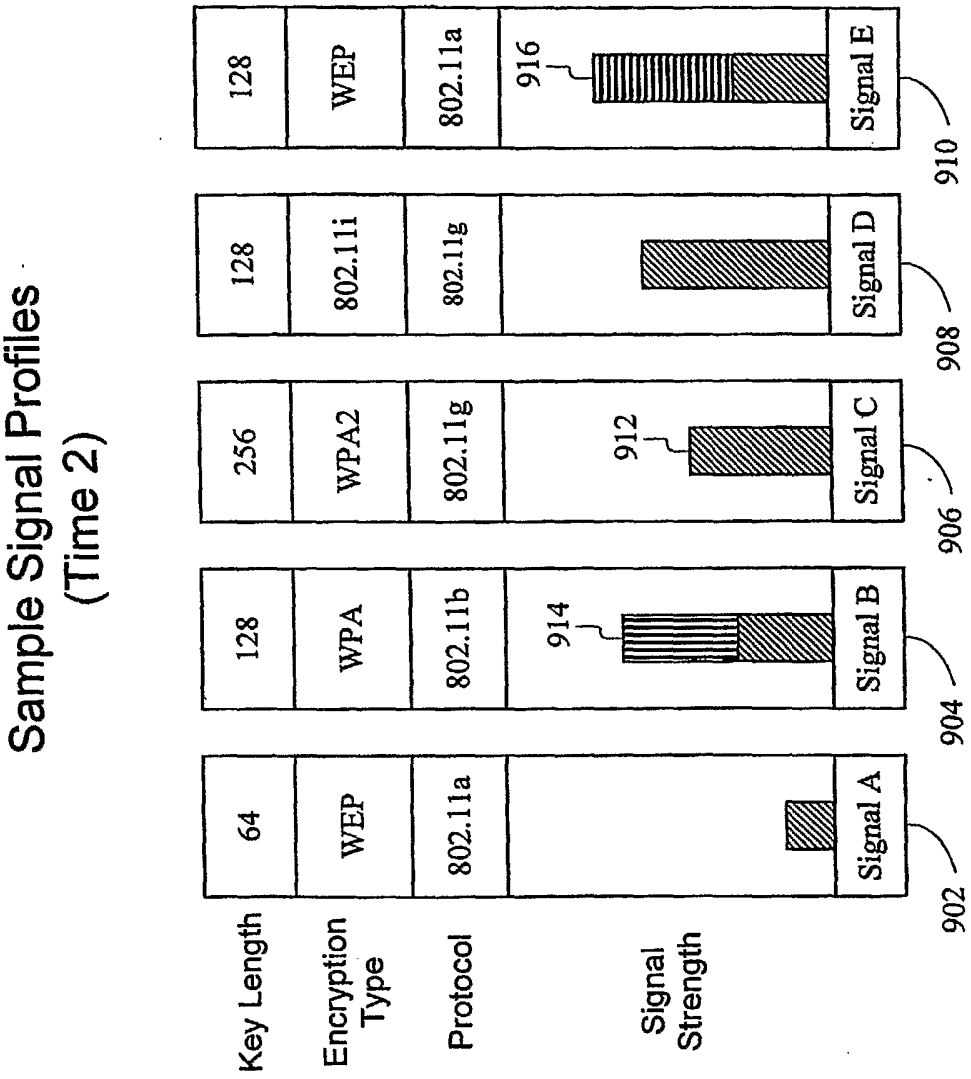

Sample Signal Profiles
(Time 2)
Key Length
Encryption Type
Protocol
Signal Strength
64
WEP
802.11a
Signal A
902
128
WPA
802.11b
914
Signal B
904
256
WPA2
802.11g
912
Signal C
906
128
802.11i
802.11g
Signal D
908
128
WEP
802.11a
916
Signal E
910

Figure 9B