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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2003 (27.11.2003)

PCT

(10) International Publication Number
WO 03/098383 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US03/14460

(22) International Filing Date: 8 May 2003 (08.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/142,789 13 May 2002 (13.05.2002) US

(71) Applicant *(for all designated States except US)*: **MESH-NETWORKS, INC.** [US/US]; 485 North Keller Road, Maitland, FL 32751 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHWIESENI, Edward, T.** [GB/US]; 104 Forest Park Ct., Longwood, FL 32779 (US). **WHITE, Eric, D.** [US/US]; 834 Grand Regency Pointe, Apt.4-105, Altamonte Springs, FL 32714 (US).

(74) Agents: **BUCZYNSKI, Joseph** et al.; 1300 19th Street, N.W., Suite 600, Washington, DC 20036 (US).

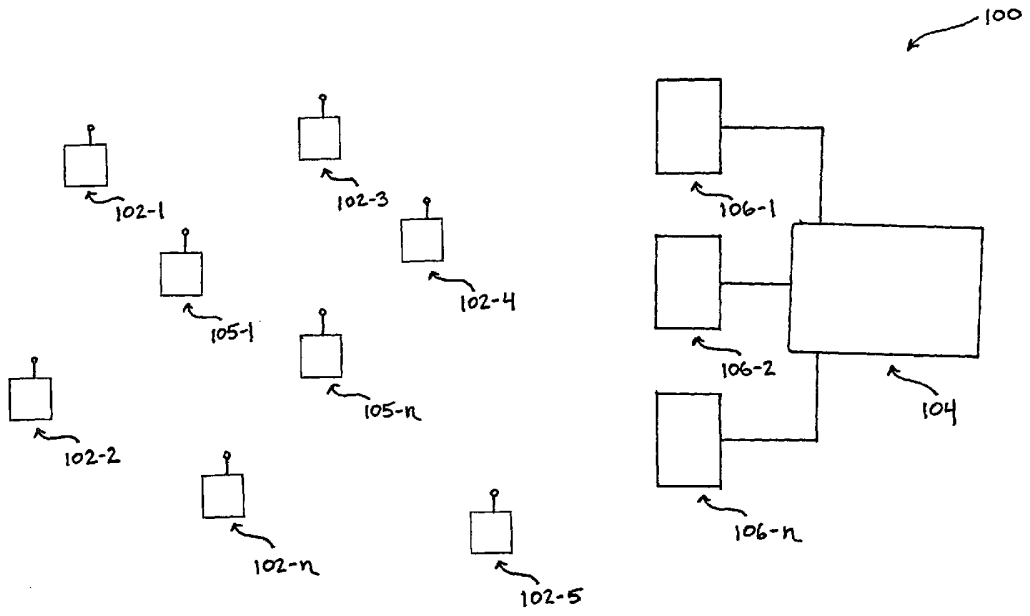
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (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*

[Continued on next page]

(54) Title: A SYSTEM AND METHOD FOR SELF PROPAGATING INFORMATION IN AD-HOC PEER-TO-PEER NETWORKS



(57) Abstract: A system and method for providing network data and system upgrades to individual nodes within an ad-hoc network without requiring network-wide information broadcasts. The system and method identifies adjacent devices authorized to share system and upgrade information. Nodes are directed to prepare and transmit requests for upgrade information from adjacent devices, such that upgrade information may be passed, from one node to the next, reaching each node in the network. The node-to-node upgrade propagation thereby replaces traditional network-wide broadcasts of upgrade information.

WO 03/098383 A2

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.

A SYSTEM AND METHOD FOR SELF PROPAGATING INFORMATION IN AD-HOC PEER-TO-PEER NETWORKS

BACKGROUND OF THE INVENTION

Field of the Invention:

[0001] The present invention relates to a system and method for providing network data and system upgrades to individual devices within an ad-hoc network without requiring network-wide information broadcasts. More particularly, the present invention relates to a system and method for creating and broadcasting requests for data and upgrades between adjacent devices, wherein an individual device can update system parameters from information provided by adjacent devices, where such transfers are authorized.

Description of the Related Art:

[0002] In recent years, a type of mobile communications network known as an "ad-hoc" network has been developed. In this type of network, each user terminal (hereinafter "mobile node") is capable of operating as a base station or router for other mobile nodes, thus eliminating the need for a fixed infrastructure of base stations. Accordingly, data packets being sent from a source mobile node to a destination mobile node are typically routed through a number of intermediate mobile nodes before reaching the destination node.

[0003] More sophisticated ad-hoc networks are also being developed which, in addition to enabling mobile nodes to communicate with each other, as in a conventional ad-hoc network, further enable the mobile nodes to access a fixed network and communicate with other types of user terminals, such as those on the public switched telephone network (PSTN) and on other networks, such as the Internet. Details of these types of ad-hoc networks are described in U.S. Patent Application Serial No. 09/897,790 entitled "Ad Hoc Peer-to-Peer Mobile Radio Access System Interfaced to the PSTN and Cellular Networks", filed on June 29, 2001, in U.S. Patent Application Serial No. 09/815,157 entitled "Time Division Protocol for an Ad-Hoc, Peer-to-Peer Radio Network Having Coordinating Channel Access to Shared Parallel Data Channels with Separate Reservation Channel", filed on March 22, 2001, and in U.S. Patent Application Serial No. 09/815,164 entitled

"Prioritized-Routing for an Ad-Hoc, Peer-to-Peer, Mobile Radio Access System", filed on March 22, 2001, the entire content of each being incorporated herein by reference.

[0004] Generally, all nodes in a wireless ad-hoc peer-to-peer network provide similar services and functionality. Although each node can provide similar services, the workload is typically distributed across many nodes rather than centralized at a single location in the peer-to-peer network. Therefore peer-to-peer networks distinguish themselves from infrastructure networks where one or more nodes offer a superset of the functionality of the rest of the network. Infrastructure nodes in these networks typically can handle Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), as well as other services that depend on broadcast traffic. Dynamic Host Configuration Protocol is defined by IETF RFC 2131 and 2132, and is used by a client node to automatically obtain network settings from a central server. These network settings include the client's IP address, the address of Domain Name Servers (DNS), the IP address of default gateways, and many other network settings. Address resolution protocol is defined by STD 0037 and RFC 0826, and is used by a network node to map IP addresses to MAC addresses so IP traffic can be delivered to specific hardware. These infrastructure nodes are normally discovered by broadcast traffic advertisements from their client nodes in a network.

[0005] Peer-to-peer networks typically do not contain specialized infrastructure nodes. The IEEE 802.11 standard offers a peer-to-peer mode in addition to an infrastructure mode. Details of the 802.11 standards are set forth in ISO/IEC 8802-11, ANSI/IEEE 802.11 "Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Network Specific Requirements", Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, the entire contents of which being incorporated herein by reference. Also, a description of the 802.11 standard is found in a book by Bob O'Hara and Al Petrick entitled *IEEE 802.11 Handbook: A Designer's Companion,* IEEE, 1999, the contents comprising this description being incorporated herein by reference.

[0006] Although broadcast communication may be used to identify and configure nodes within the ad-hoc network, wireless ad-hoc routing networks typically avoid repeating broadcast traffic in an effort to avoid "broadcast storms" which can flood the transmission medium with traffic and cripple the ability of the network to perform.

Broadcast traffic reception is usually limited to nodes in the immediate listening area of the transmitting node. Since ARP and DHCP depend on broadcast traffic, ad-hoc routing networks sometimes "tunnel" this broadcast traffic in directed packets to known infrastructure nodes where it can be handled. Traditional non-ad-hoc networks do not encounter the broadcast problem because their nodes communicate directly with each other.

[0007] However, wireless peer-to-peer ad-hoc routing networks do not contain infrastructure nodes and therefore do not have the option to tunnel their broadcast traffic. Hence, DHCP, ARP and other broadcast network protocols must be handled in another way. In a traditional wired network, system information is usually broadcast to all devices, while upgrades are sent individually from a central location. In an ad-hoc network, however, it is undesirable to broadcast to all devices of the network since the network could become flooded. Accordingly, a need exists for a system and method where adjacent devices within the ad-hoc network, as well as the infrastructure, may be used to distribute system information directly to adjacent devices upon request without the need for network-wide broadcasts.

SUMMARY OF THE INVENTION

[0008] An object of the present invention is to provide a system and method for self-propagating information in an ad-hoc peer-to-peer network.

[0009] Another object of the present invention is to provide a system and method for locating adjacent nodes, or "neighbor" nodes, of a node requesting network data and system upgrades in an ad-hoc network.

[0010] Still another object of the present invention is to provide a system and method for preparing and transmitting a request for specific information between a requesting node and neighbor nodes.

[0011] Still another object of the present invention is to provide a system and method for preparing and transmitting specific information data packets between neighbor nodes and requesting nodes, such that requesting nodes may update network and system information.

[0012] These and other objects are substantially achieved by providing a system and method for identifying adjacent devices within the network which may provide data upgrades. The system and method creates and broadcasts requests for data upgrades between adjacent devices which respond with the requested information. An

individual device can update system parameters from information provided by adjacent devices where such transfers are authorized, without network-wide broadcasts.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] These and other objects, advantages and novel features of the invention will be more readily appreciated from the following detailed description when read in conjunction with the accompanying drawings, in which:

[0014] Figure 1 is a block diagram of an example of an ad-hoc wireless communications network including a plurality of nodes employing an embodiment of the present invention;

[0015] Figure 2 is a block diagram of an example of a wireless node as shown in Figure 1;

[0016] Figure 3A is a block diagram of an example of a broadcast request for information by a node in Figure 1;

[0017] Figure 3B is a block diagram of an example of responses to the broadcast request in Figure 3A;

[0018] Figure 3C is a block diagram of an example of a request for specific information by a node in Figure 1; and

[0019] Figure 3D is a block diagram of an example of a specific response to the broadcast request in Figure 3C.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0020] Figure 1 is a block diagram illustrating an example of an ad-hoc packet-switched wireless communications network 100 employing an embodiment of the present invention. Specifically, the network 100 includes a plurality of mobile wireless user terminals 102-1 through 102-n (referred to generally as nodes 102 or mobile nodes 102), and can, but is not required to, include a fixed network 104 having a plurality of access points 106-1, 106-2, ...106-n (referred to generally as nodes 106 or access points 106), for providing nodes 102 with access to the fixed network 104. The fixed network 104 can include, for example, a core local access network (LAN), and a plurality of servers and gateway routers, to provide network nodes with access to other networks, such as other ad-hoc networks, the public switched telephone network (PSTN) and the Internet. The network 100 further can include a plurality of

fixed routers 105-1 through 105-n (referred to generally as nodes 105 or fixed routers 105) for routing data packets between other nodes 102, 106 or 105. It is noted that for purposes of this discussion, the nodes discussed above can be collectively referred to as "nodes 102, 105 and 106", or simply "nodes".

[0021] As can be appreciated by one skilled in the art, the nodes 102, 105 and 106 are capable of communicating with each other directly, or via one or more other nodes operating as a router or routers for packets being sent between nodes, as described in U.S. Patent No. 5,943,322 to Mayor, which is incorporated herein by reference, and in U.S. Patent Application Serial Nos. 09/897,790, 09/815,157 and 09/815,164, referenced above.

[0022] As shown in Figure 2, each node 102, 105 and 106 includes a transceiver 108, including a transmitter and a receiver, which collectively can be referred to as a modem. The transceiver is coupled to an antenna 110 and is capable of receiving and transmitting signals, such as packetized signals, to and from the node 102, 106 or 105, under the control of a controller 112. The packetized data signals can include, for example, voice, data or multimedia information, and packetized control signals, including node update information.

[0023] Each node 102, 105 and 106 further includes a memory 114, including a read only memory (ROM) for storing information pertaining to the operation of the node, and a random access memory (RAM) for storing information such as routing information pertaining to itself and other nodes in the network 100. The nodes 102, 105 and 106 exchange their respective routing information, referred to as routing advertisements or routing table information, with each other via a broadcasting mechanism periodically, for example, when a new node enters the network 100, or when existing nodes in the network 100 move.

[0024] As further shown in Figure 2, certain nodes, especially mobile nodes 102, can include a host 116 which may consist of any number of devices, such as a notebook computer terminal, mobile telephone unit, mobile data unit, or any other suitable device. Each node 102, 105 and 106 also includes the appropriate hardware and software to perform Internet Protocol (IP) and Address Resolution Protocol (ARP), the purposes of which can be readily appreciated by one skilled in the art. The appropriate hardware and software to perform transmission control protocol (TCP) and user datagram protocol (UDP) may also be included.

[0025] Each node of the network in Figure 1 is required to maintain current network information for proper operation. For instance, the Admission Control (AC) module of transceiver 108 acts on packets flowing between the IP stack module of the host 116 and the IP stack module and the traffic control (TC) module of transceiver 108. In doing so, the AC module relies on local broadcasts, ad hoc routing updates, and unicast requests for information to provide services to the IP stacks. Further details of the operations and protocols are set forth in a U.S. Provisional Patent Application of Eric A. Whitehill entitled "Embedded Routing Algorithms Under the Internet Protocol Routing Layer in a Software Architecture Protocol Stack", Serial No. 60/297,769, filed on June 14, 2001, the entire content of which is incorporated herein by reference.

[0026] As discussed in the Background section, if a mobile node 102 in network 100 of Figure 1 were to broadcast a request for information, such as an ARP request to all the wireless nodes on the network, including all mobile nodes 102 and IAPs 106, such a broadcast could overload the radio network. Therefore, in an embodiment of the present invention shown in Figure 2, when a host 116 sends a request for information, the subscriber device transceiver 108 intercepts the request and determines a neighbor node, or nodes, which may provide the information. Once a neighbor node or nodes are determined, the transceiver forwards the request for information directly to the neighbor node for resolution, instead of performing a traditional broadcast of the request. Specifically, the requesting node 102 unicasts the request for information to the neighbor nodes which are capable of responding.

[0027] The neighbor node or nodes, resolve the query by looking first in the neighbor node's own cache tables, or, if necessary, by querying other adjacent nodes. The neighbor node then returns a message to the requesting node 102 containing the requested information. Specifically, the neighbor node unicasts a reply to the requesting node 102. In addition to reducing network wide broadcasts, an additional benefit results in that the transfer of a unicast message from the neighbor node to the requesting node is much more reliable than the transfer of a broadcast message.

[0028] In yet another embodiment of the present invention, the requesting node may request a listing of data neighbor nodes are authorized to provide. The neighbor nodes, may in turn, provide a list of current data to the requesting node, thereby allowing the requesting node to determine from the data received if data revisions are required, and thereafter requesting the specific data revisions required.

[0029] In an embodiment of the present invention shown in Figure 3A, when a mobile node 102-7 joins an ad-hoc network it can query its neighbors 102-5, 102-6 and 105-2, to determine the network's current state. This can be as simple as obtaining network time values, for operations requiring synchronization, or obtaining network configurations, such as channel usage, carrier location in an area and so forth. In addition, it is possible for nodes to negotiate the correct software and upgrade one another if needed.

[0030] In Figure 3A, when mobile node 102-7 is initialized, it performs a neighborhood discovery process, which determines the proximity of nodes 102-5, 102-6 and 105-2. Once the node has an established list of neighbor devices, it can query them for their system parameters. When the neighbor nodes 102-5, 102-6 and 105-2, receive such a request, they create response packets and send them to the requesting node 102-7. The response packets will contain the information each neighbor node is authorized to share regarding the system data.

[0031] Once all response packets are gathered together, node 102-7 can determine whether it needs to update any of its parameters and which neighbor node is authorized to provide the required data updates. If none of the neighbors are able and/or willing to provide the updates, then node 102-7 can query the infrastructure, such as nodes 106, for the required information. The infrastructure in the network 100, such as the IAPs 106s points, will typically maintain the system information and any network upgrades.

[0032] Once a candidate is identified, node 102-7 can contact the neighbor node and request specific information from that neighbor. If new software is available then a session can be established to transfer the software to the requesting node as well. Once the software has been downloaded, then the controller 112 of node 102-7 can perform the upgrade.

[0033] As shown in Figure 3A, node 102-7 can request information from its neighbors, nodes 102-5, 102-6 and 105-2, at any point in time. The request can be triggered on initialization, by time, or by a specific event. Once the trigger is active, node 102-7 sends a special broadcast to its neighbors, nodes 102-5, 102-6 and 105-2, asking for specific information, such as current software versions or system parameters. If nodes 102-5, 102-6 and 105-2 are authorized to respond to the request, each will create a response packet containing the parameters, or list of parameters authorized to provide, and transmit the packet to the requesting node 102-7, as shown

in Figure 3B. In Figure 3B, neighbor nodes 102-6 and 105-2 have prepared and sent response packets to the requesting node 102-7. For illustration purposes, node 102-5 lacks authorization to provide the requested information, therefore no response packet is prepared or sent to the requesting node.

[0034] As shown in Figure 3B, requesting node 102-7 receives and reads each response packet to discover what upgrades are required, and which neighbor node is authorized to transfer such upgrades. The requesting node 102-7 then requests those items of information it is seeking in Figure 3C.

[0035] In Figure 3C, node 102-7 prepares and sends a request for specific information packets to node 102-6. For illustration purposes, node 102-7 determined no information was required from node 105-2, therefore no further requests are made to node 105-2. Node 102-6 reads the request packet from node 102-7, then initiates transfer of the data to the requesting node in Figure 3D. The transferred data may be a single packet or multiple packets as required and each packet may be acknowledged separately or in blocks. Once all the data is received, the requesting node 102-7 acts on the information. This may be as simple as updating its clock or as complex as overwriting the current software load and performing a restart.

[0036] Also, nodes within the network can be configured to require the requesting node to authenticate themselves or prove authorization for the service being requested. In such an embodiment, proper authentication must be given to the nodes requesting updates. Such node authentication may be provided along with access authorization for nodes entering the network, or may be provided elsewhere.

[0037] Furthermore, the network infrastructure may introduce an upgrade program for all mobile nodes that travels from node to node, validating system information. The network will execute this special program to determine if the information in any node is invalid, at which point the software will request updates from the infrastructure. The propagated upgrade program may be initially broadcast to only those nodes in the proximity of the infrastructure originating the upgrade and thereafter, each node will distribute the upgrades as described above. The system or individual nodes of the network may be enabled or disabled for auto-upgrading and propagation of information from one node to another.

[0038] In addition, the present invention may also be utilized for sending information services. For instance, if two neighbor nodes represent devices having subscribed to the same news service, then each may update the other with the latest news, weather,

and stock information. Paid advertising can be distributed in a similar fashion. In a first mode, such as peer-to-peer networking without any infrastructure, as a new unit enters the network it can compare its status with its neighbors, including system software. If a new version of software is available then it can be shared by all the systems in the group using the process as well.

[0039] Although only a few exemplary embodiments of the present invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the exemplary embodiments without materially departing from the novel teachings and advantages of this invention. Accordingly, all such modifications are intended to be included within the scope of this invention as defined in the following claims.

What is claimed is:

1. A method for controlling a node in a wireless ad-hoc communication network to acquire information from at least one of a plurality of other nodes in said network, comprising:

controlling said node to send a first request for information to a first group of said plurality of nodes;

controlling said first group of nodes to receive said first request and in response, to determine if any node of said first group is authorized to provide said information, and controlling each said authorized node of said first group to send initial reply data to said first node; and

controlling said node to, in response to said initial reply data, send a second request to at least one authorized node for specific reply data and controlling said authorized node to send said specific reply data to said first node.

2. A method as claimed in Claim 1, wherein said first request comprises a request for information available from said authorized nodes of said first group, said information comprises data indicating at least one of the software version, system parameters and information contained at said authorized node.

3. A method as claimed in Claim 1, wherein said initial reply data comprises a response from an authorized node indicating said information available to be sent from said authorized node.

4. A method as claimed in Claim 1, wherein said controlling said node to send said second request comprises:

analyzing said initial reply data to determine whether said second request is required, with said second request comprising a request for specific information available from said authorized node.

5. A method as claimed in Claim 1, wherein said specific reply data comprises a response from an authorized node containing said specific information requested by said node.

6. A method as claimed in Claim 1, further comprising:

controlling said node to operate in accordance with said specific reply data received from an authorized node.

7. A method as claimed in Claim 1, wherein said first and second requests are each sent as a unicast message.

8. A method as claimed in Claim 1, wherein said initial reply data and specific reply data each include at least one data packet.

9. A method as claimed in Claim 1, further comprising:

authenticating said node before said initial reply data is sent by said authorized node.

10. A method as claimed in claim 1, wherein said method further comprises controlling said node to, in response to said initial reply data, send said second request to at least one infrastructure element of said network for specific data and controlling said infrastructure element to send said specific reply data to said first node.

11. A node in an ad-hoc communication network, adapted to acquire information from at least one of a plurality of other nodes in said network, comprising:

a transceiver, adapted to send a first request for information to a first group of said plurality of nodes and to receive initial reply data from nodes of said plurality authorized to provide said information;

a controller adapted to analyze said initial reply data to determine whether a second request is required, with said second request comprising a request for specific information available from said authorized node; and

said transceiver further adapted to send said second request to at least one authorized node for specific reply data and to receive specific reply data from said authorized node.

12. A node as claimed in Claim 11, wherein said first request comprises a request for information available from said authorized nodes of said first group, said

information comprises data indicating at least one of the software version, system parameters and information contained at said authorized node.

13. A node as claimed in Claim 11, wherein said initial reply data comprises a response from an authorized node indicating said information available to be sent from said authorized node.

14. A node as claimed in Claim 11, wherein said specific reply data comprises a response from an authorized node containing said specific information requested by said node.

15. A node as claimed in Claim 11, wherein:

said controller is further adapted to control said node operation in accordance with said specific reply data received from an authorized node.

16. A node as claimed in Claim 11, wherein said first and second requests are each sent as a unicast message.

17. A node as claimed in Claim 11, wherein said initial reply data and specific reply data each include at least one data packet.

18. A node as claimed in Claim 11, wherein:

said controller is further adapted to provide requesting node authentication to each authorized node before said initial reply data is sent.

19. A node as claimed in Claim 11, wherein:

said controller is further adapted to analyze said initial reply data to determine whether said second request should be sent to at least one infrastructure element of said network; and

said transceiver is further adapted to send said second request to at least one infrastructure element and to receive specific reply data from said infrastructure element.

20. A node as claimed in Claim 11, wherein:

said controller is further adapted to determine if said node can operate as an authorized node for other nodes of said plurality.

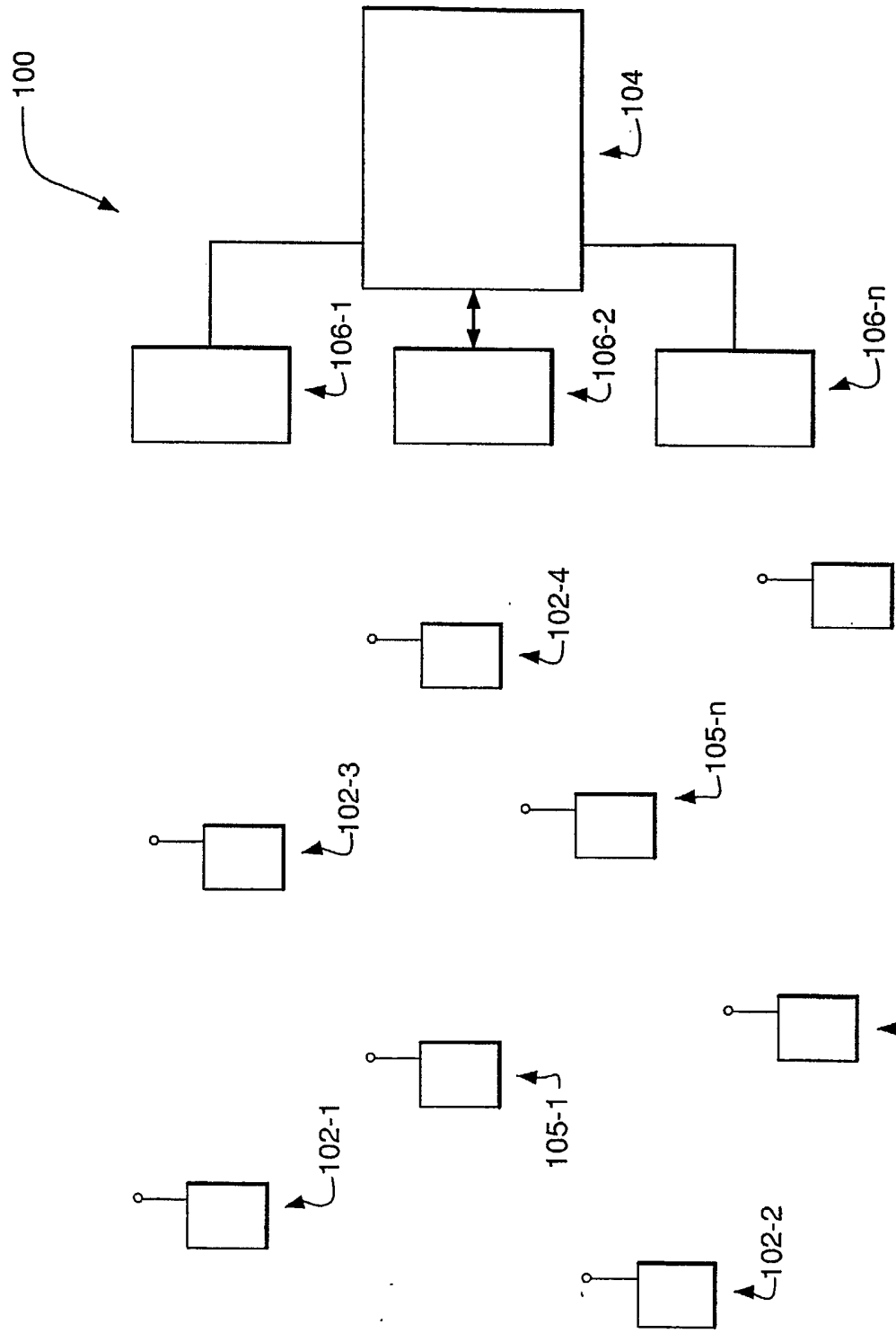

100
104
106-1
106-2
106-n
102-1
102-2
102-3
102-4
102-5
102-n
105-1
105-n

FIGURE 1

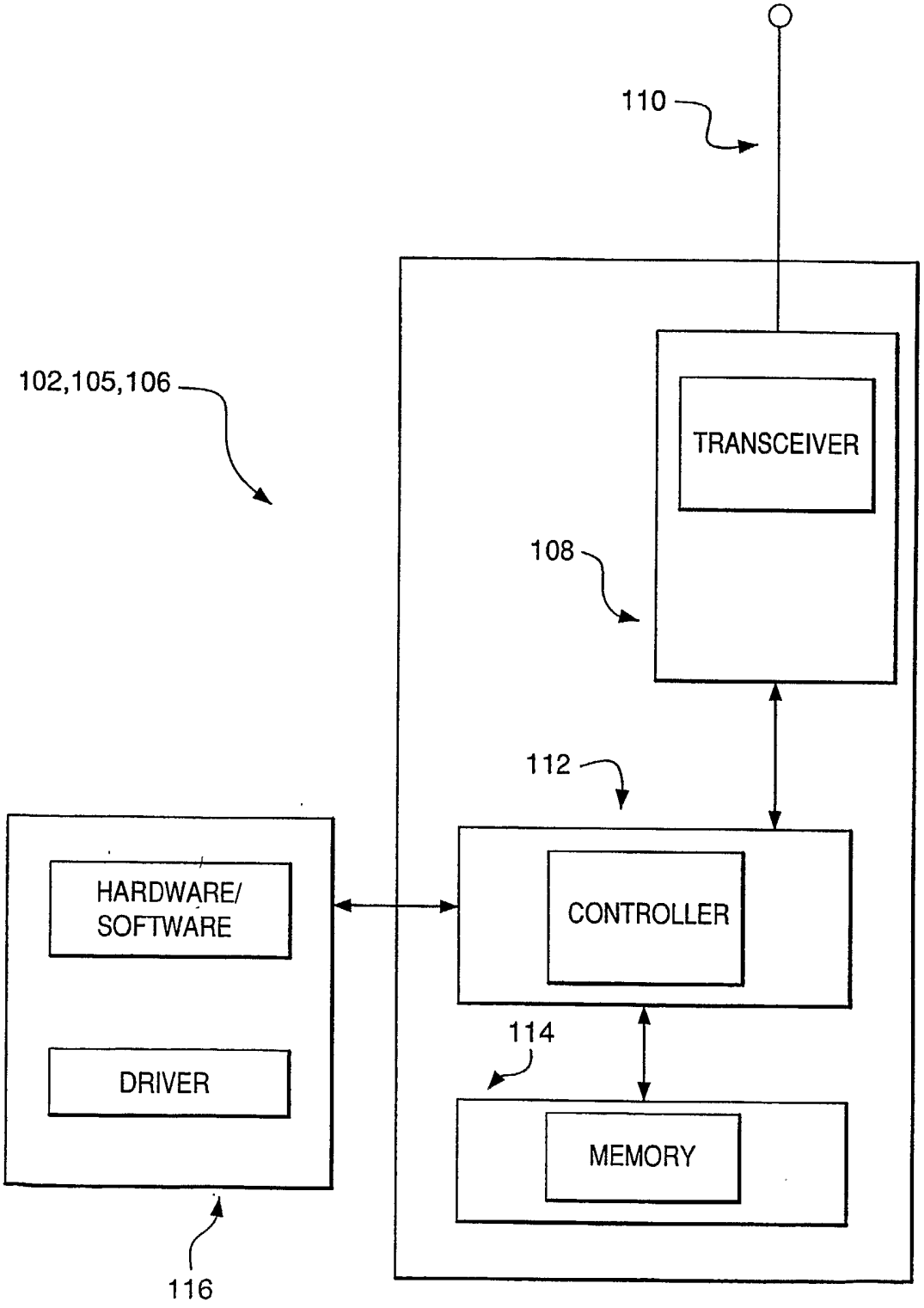

110
102,105,106
TRANSCEIVER
108
112
HARDWARE/
SOFTWARE
CONTROLLER
114
DRIVER
MEMORY
116

FIGURE 2

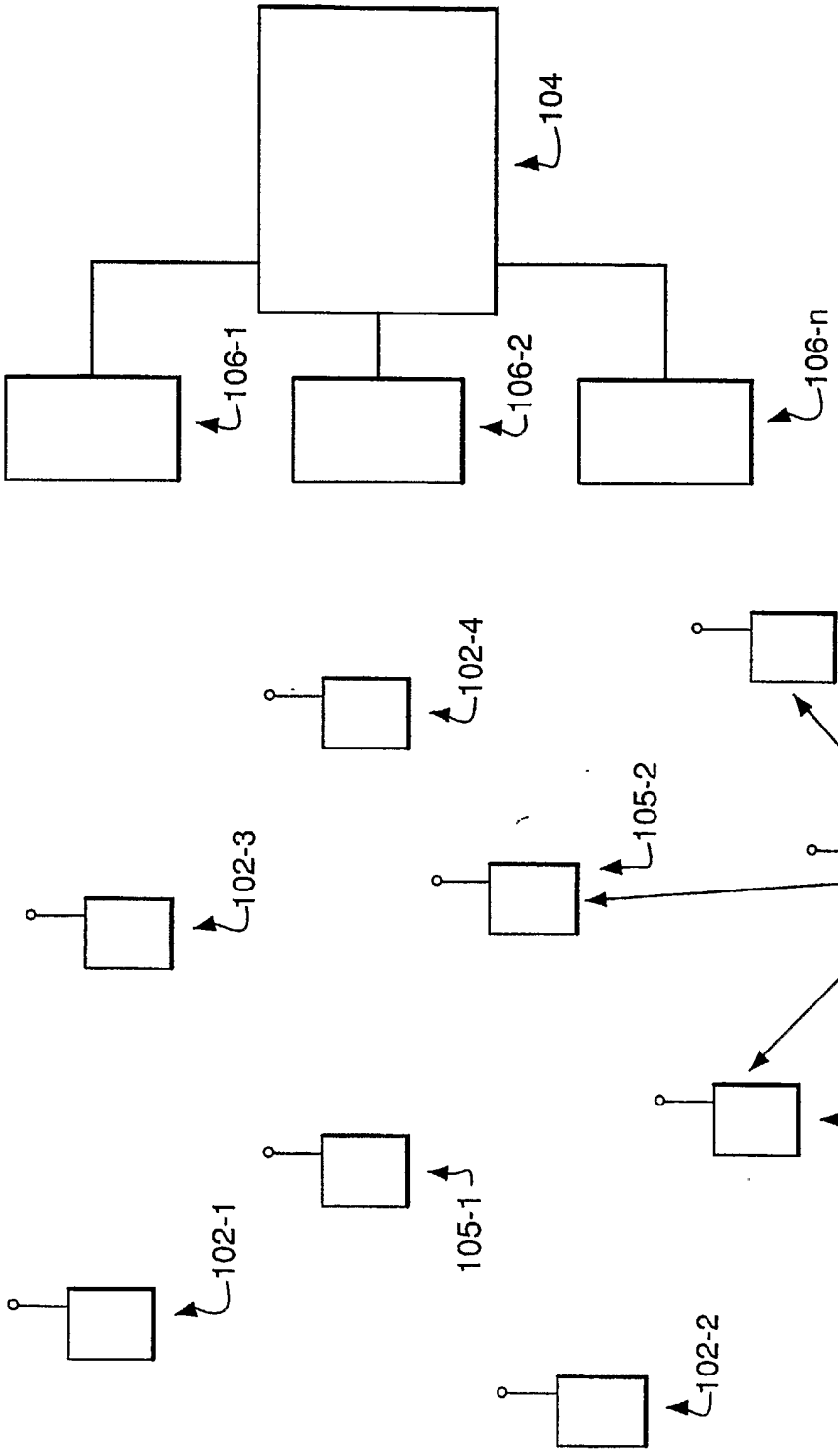

104
106-1
106-2
106-n
102-1
102-2
102-3
102-4
102-5
102-6
102-7
105-1
105-2

FIGURE 3A

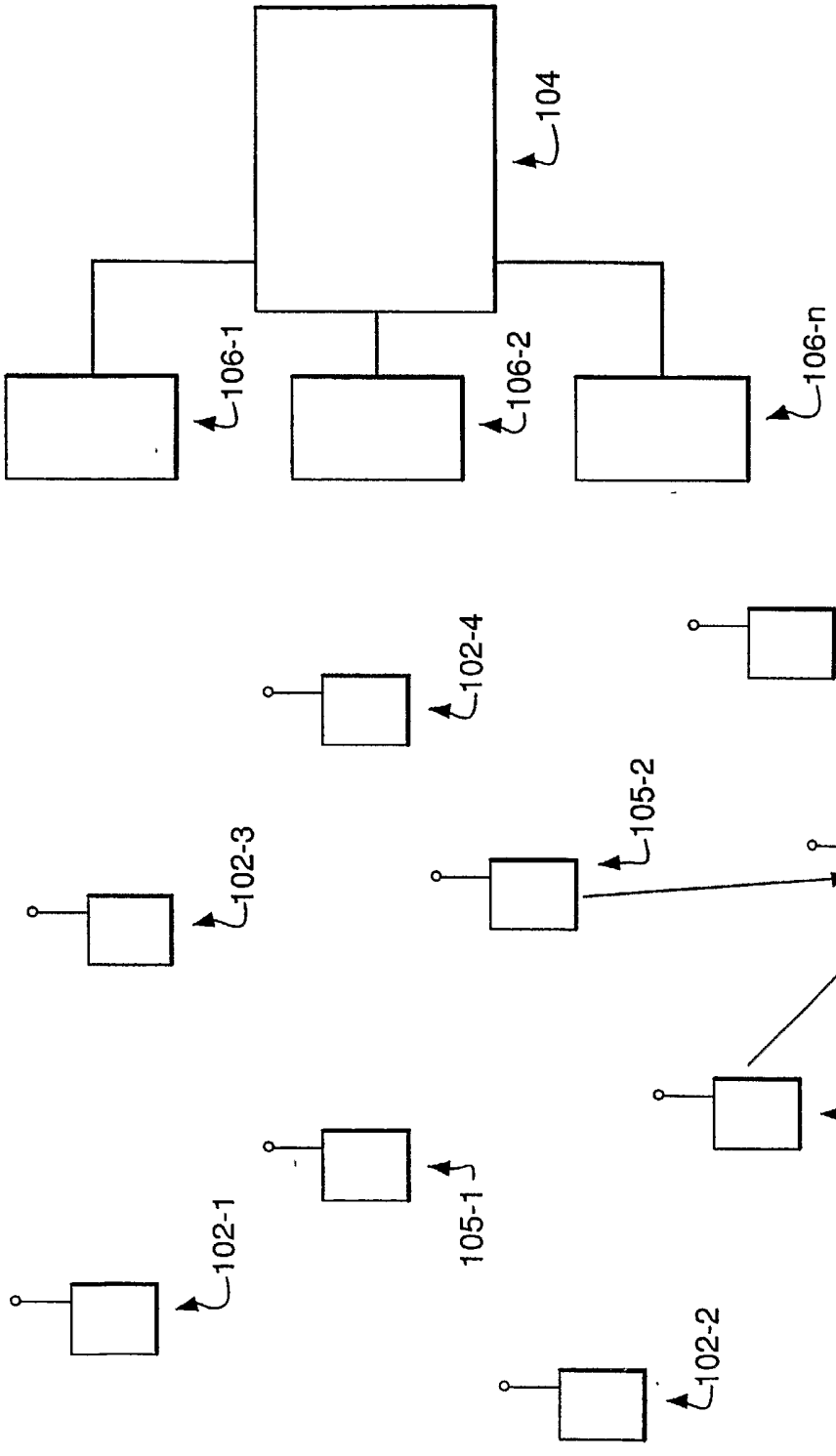


FIGURE 3B

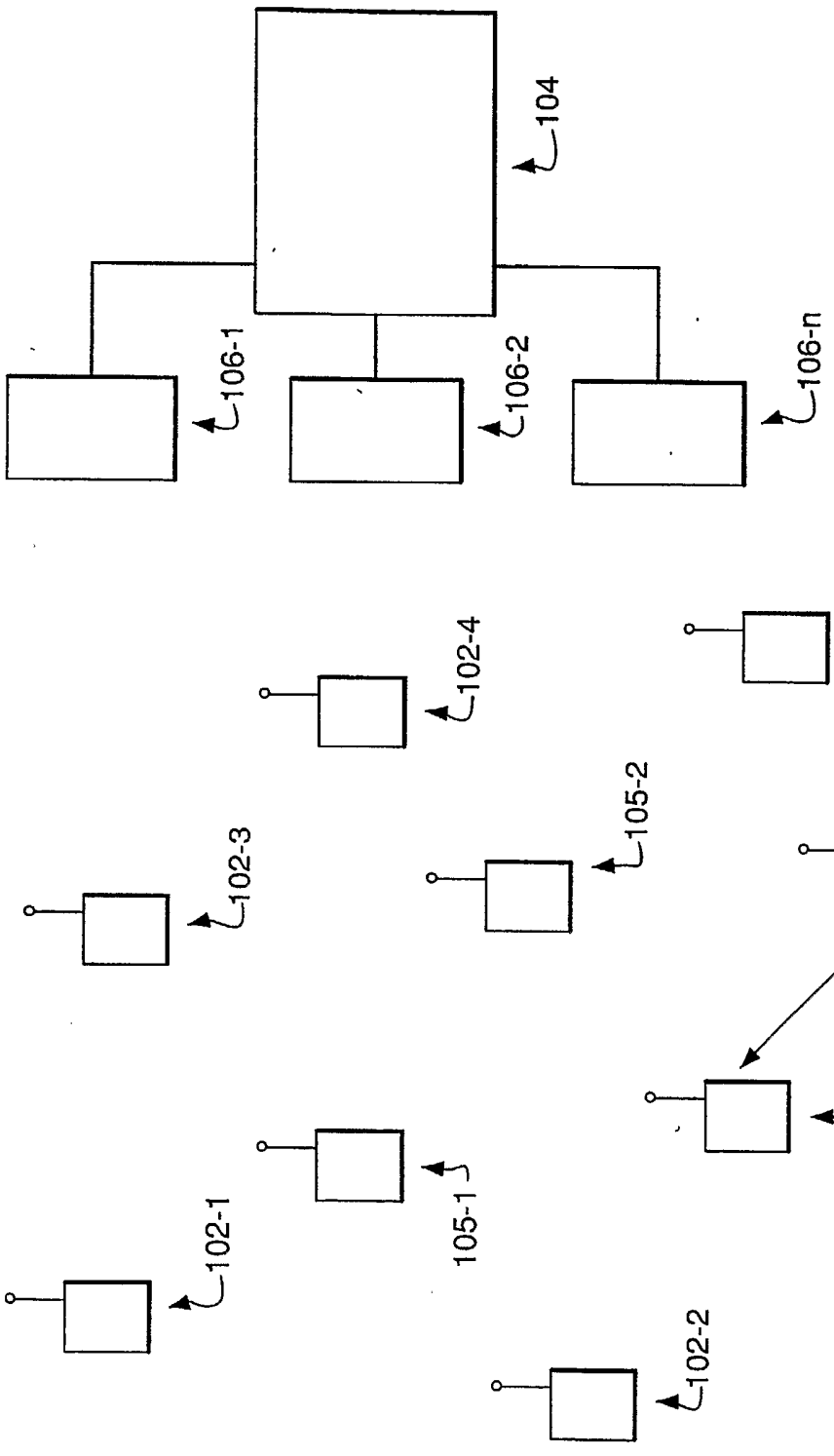

104
106-1
106-2
106-n
102-1
102-2
102-3
102-4
102-5
102-6
102-7
105-1
105-2

FIGURE 3C

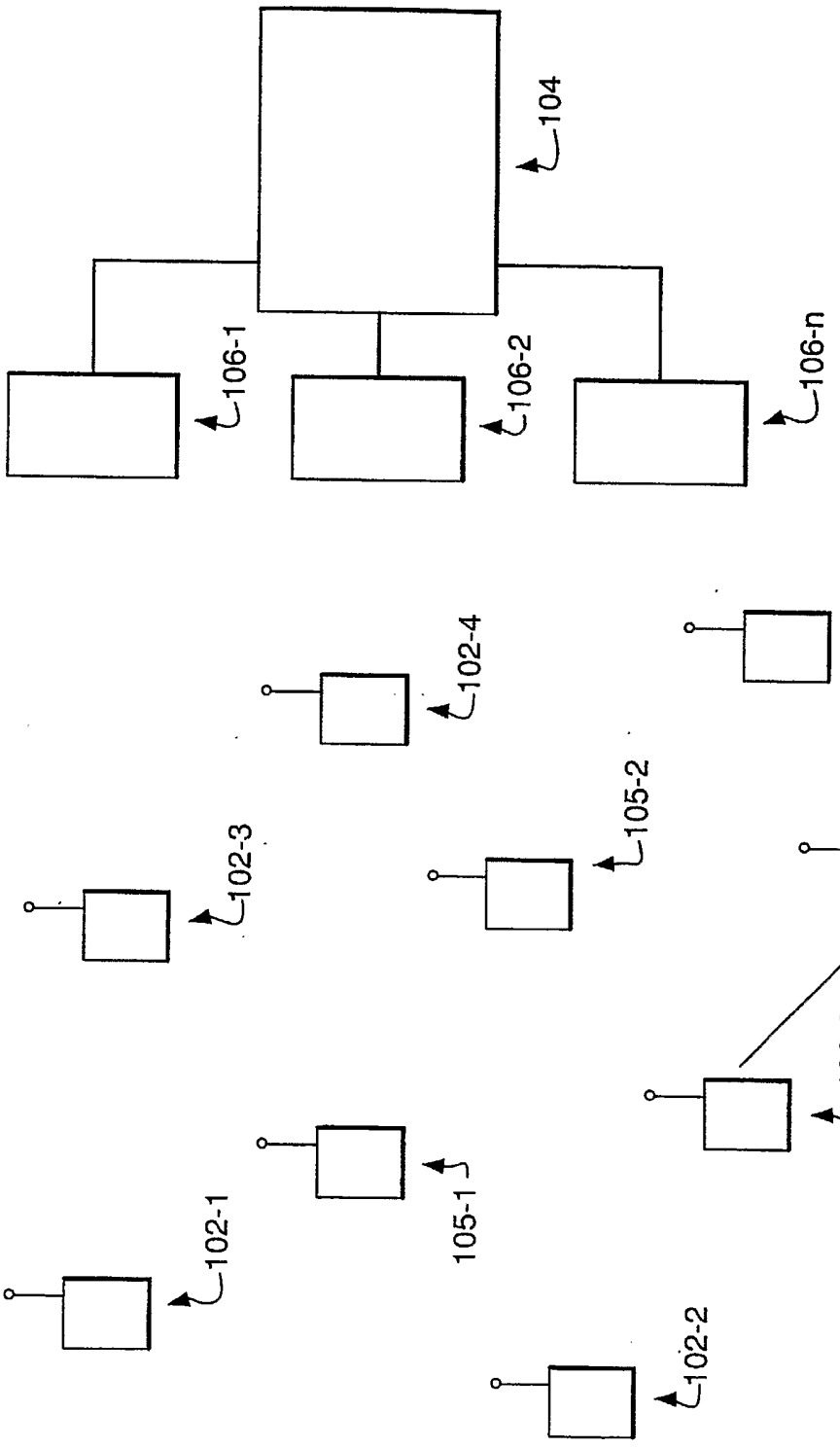

104
106-1
106-2
106-n
102-1
102-2
102-3
102-4
102-5
102-6
102-7
105-1
105-2

FIGURE 3D