



US 20040157557A1

(19) **United States**

(12) **Patent Application Publication**
Barnett et al.

(10) **Pub. No.: US 2004/0157557 A1**

(43) **Pub. Date: Aug. 12, 2004**

(54) **SYSTEM FOR A DYNAMIC AD-HOC
WIRELESS NETWORK**

(22) Filed: **Feb. 3, 2004**

(75) Inventors: **Bruce Barnett**, Troy, NY (US);
Stephen F. Bush, Latham, NY (US);
Scott Evans, Burnt Hills, NY (US);
Amit Kulkarni, Clifton Park, NY (US);
Richard Spackmann, Saratoga Springs,
NY (US); **Harold Tomlinson JR.**,
Scotia, NY (US)

Related U.S. Application Data

(60) Provisional application No. 60/445,579, filed on Feb.
7, 2003.

Publication Classification

(51) **Int. Cl.⁷** **H04Q 7/20**

(52) **U.S. Cl.** **455/41.2; 455/445**

Correspondence Address:

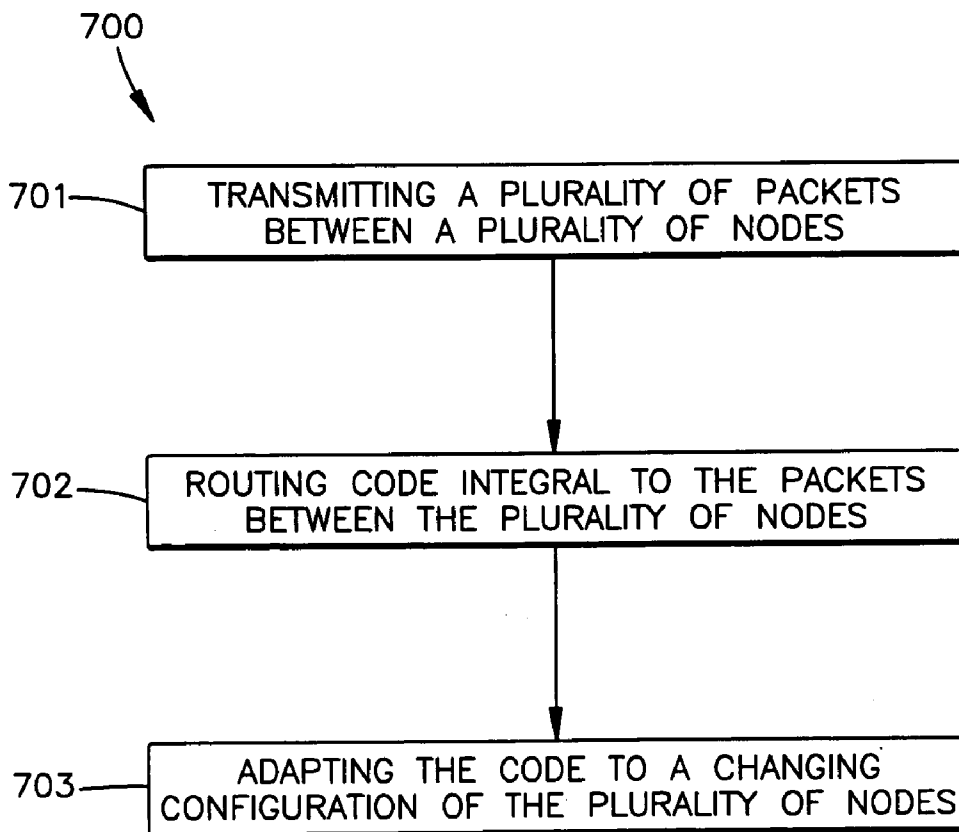
**TROLLI, SUNDHEIM, COVELL &
TUMMINO LLP**
Suite 1111
526 Superior Avenue
CLEVELAND, OH 44114 (US)

(57) **ABSTRACT**

(73) Assignee: **Lockheed Martin Corporation**, Owego,
NY (US)

(21) Appl. No.: **10/771,026**

A system operates a wireless ad hoc network. The system includes a plurality of nodes and a plurality of packets for transmission between the plurality of nodes. The packets contain code for routing the packets between the plurality of nodes. The code adapts to a changing configuration of the plurality of nodes.



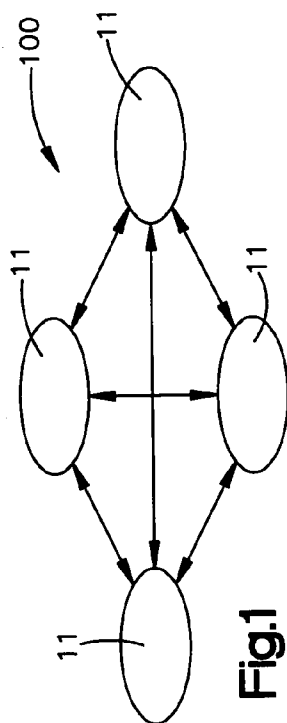


Fig.1

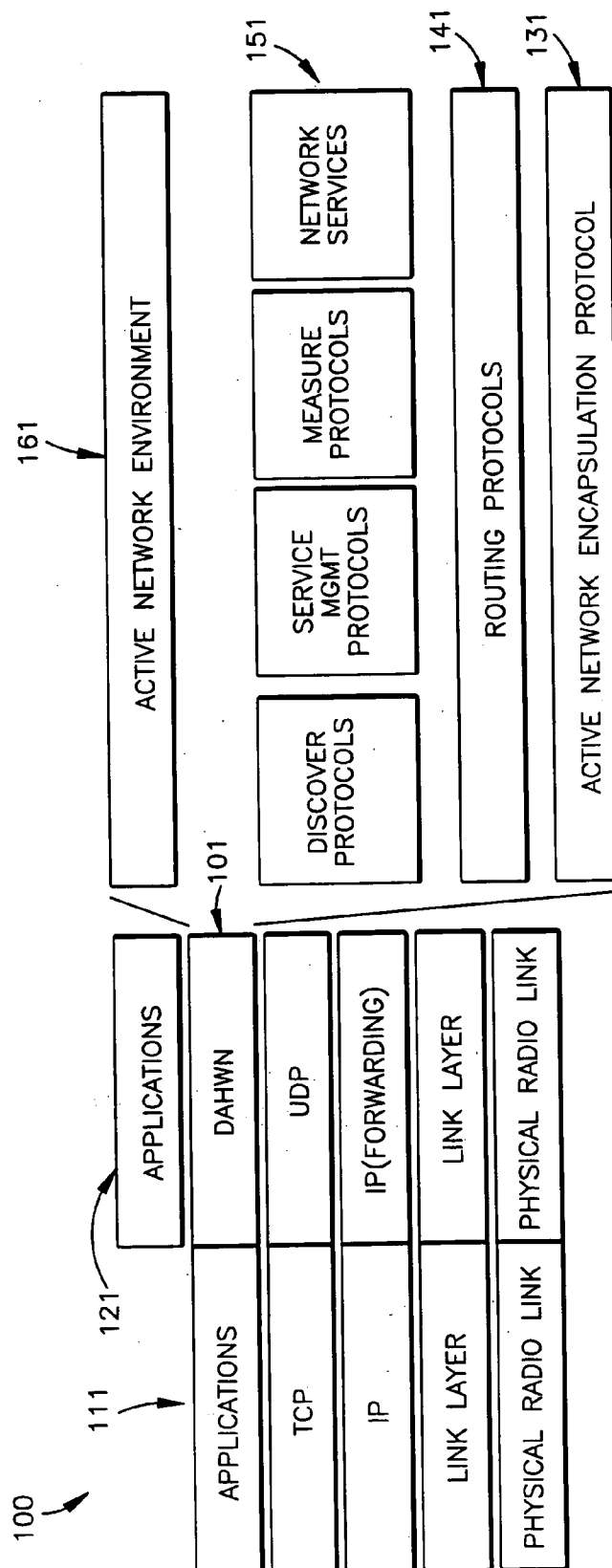


Fig.2

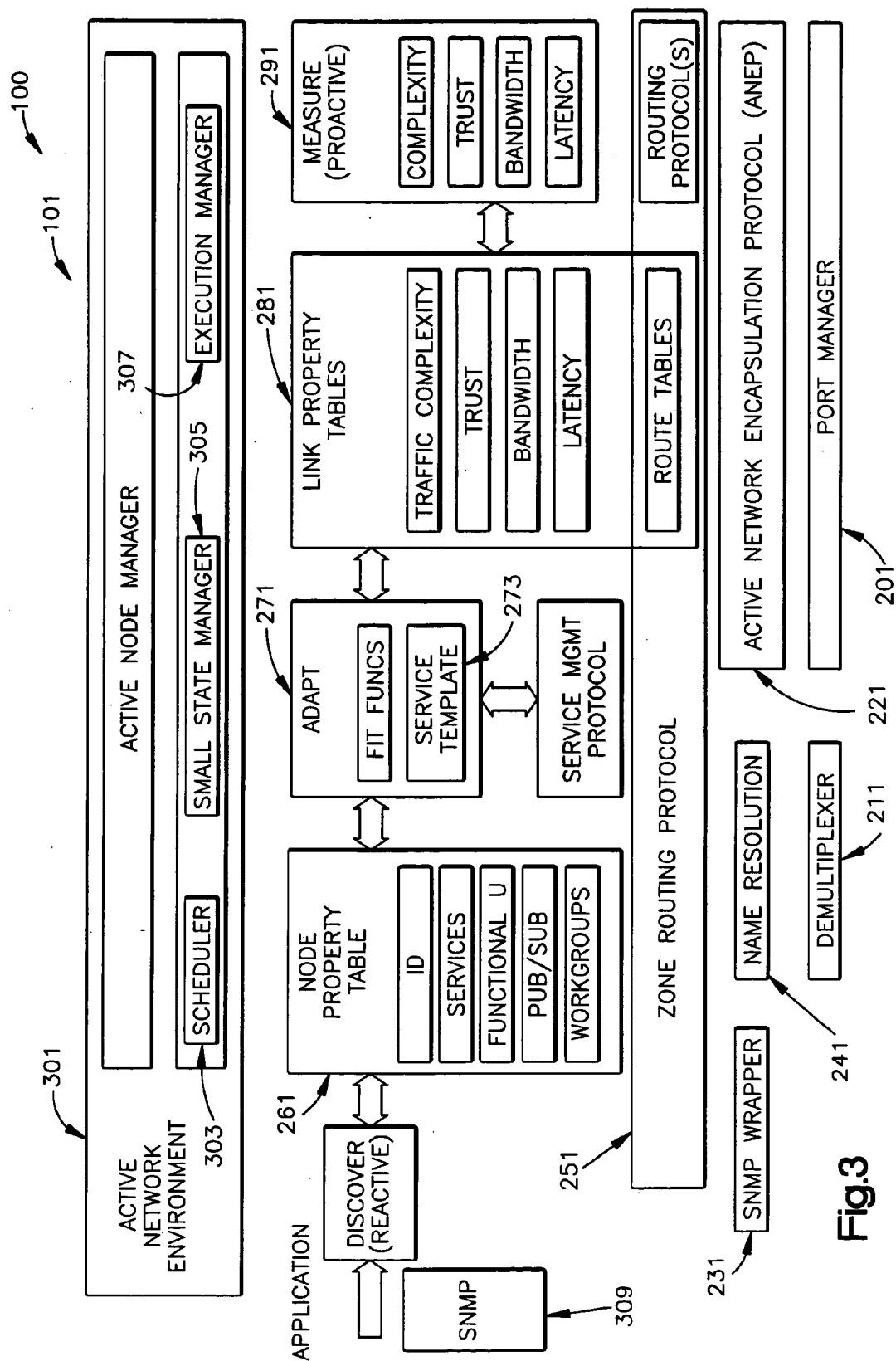


Fig.3

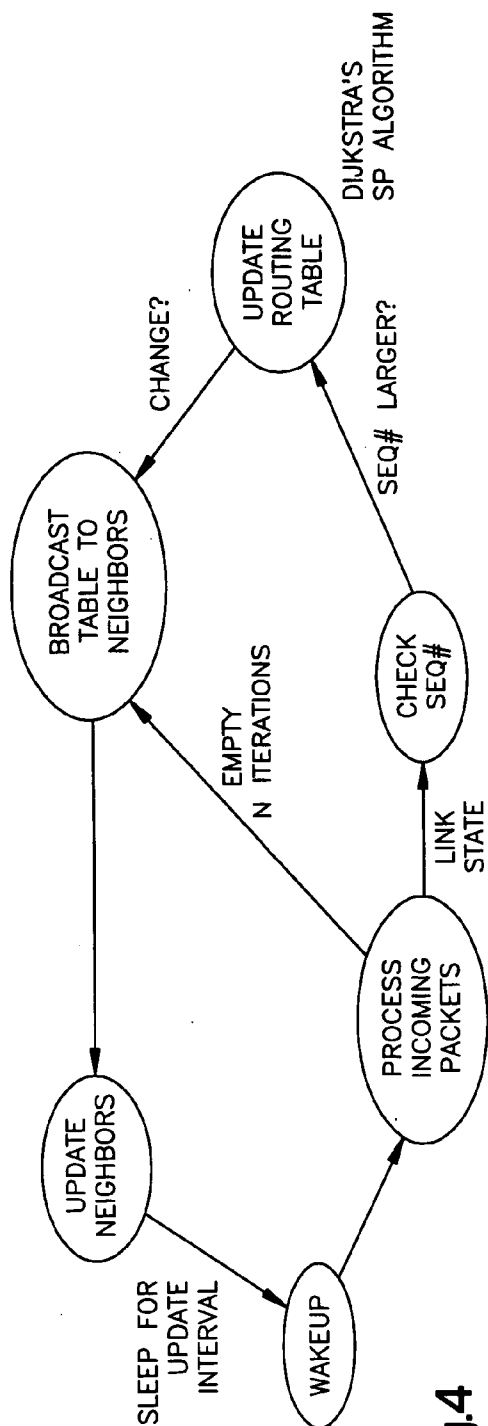


Fig.4

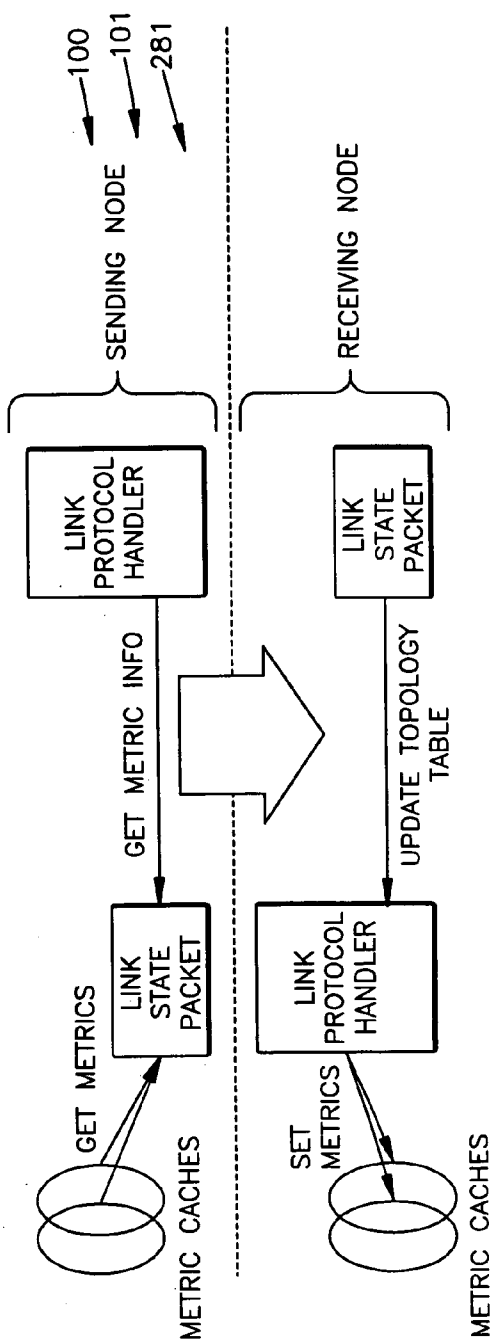
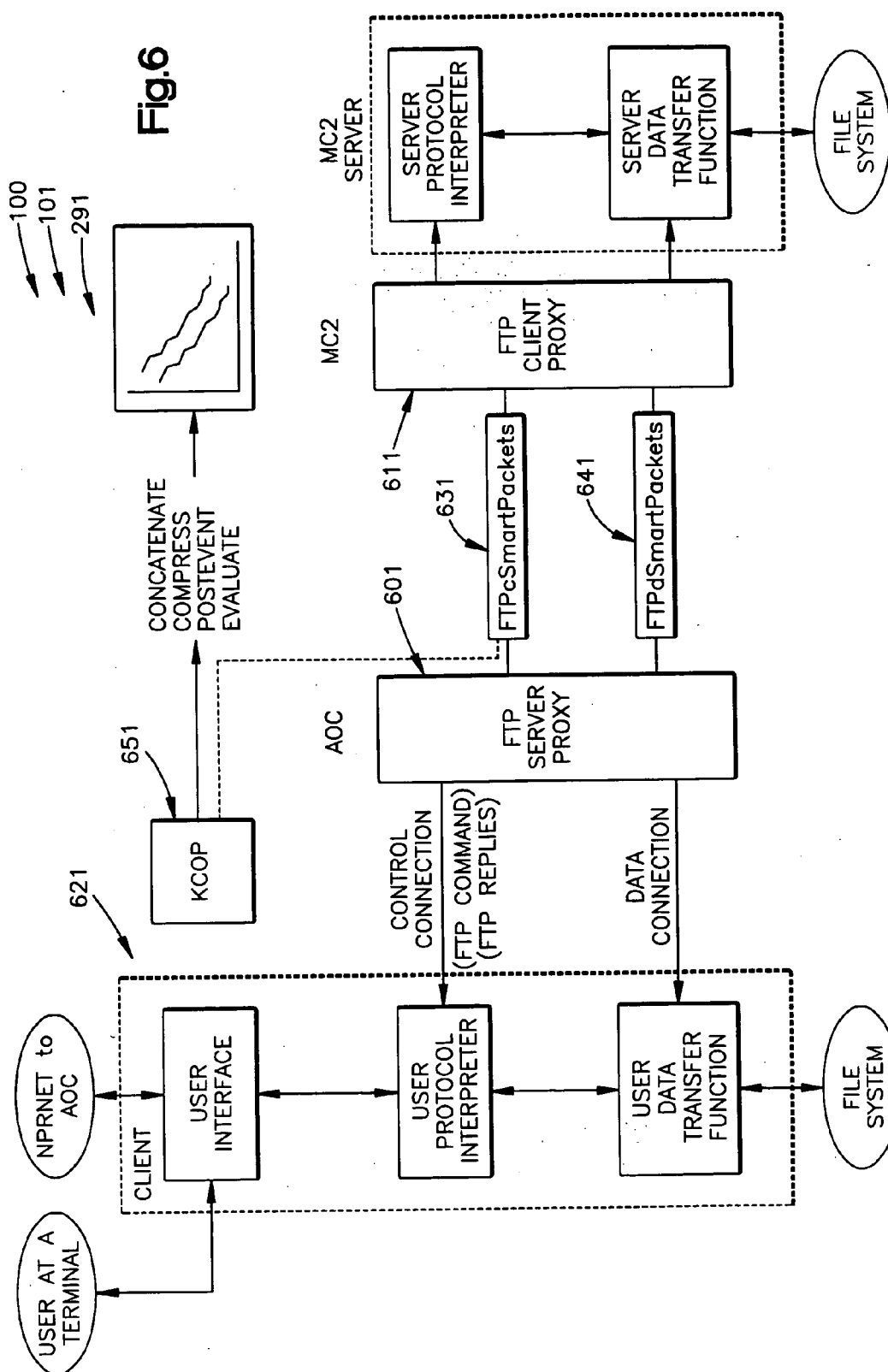


Fig.5



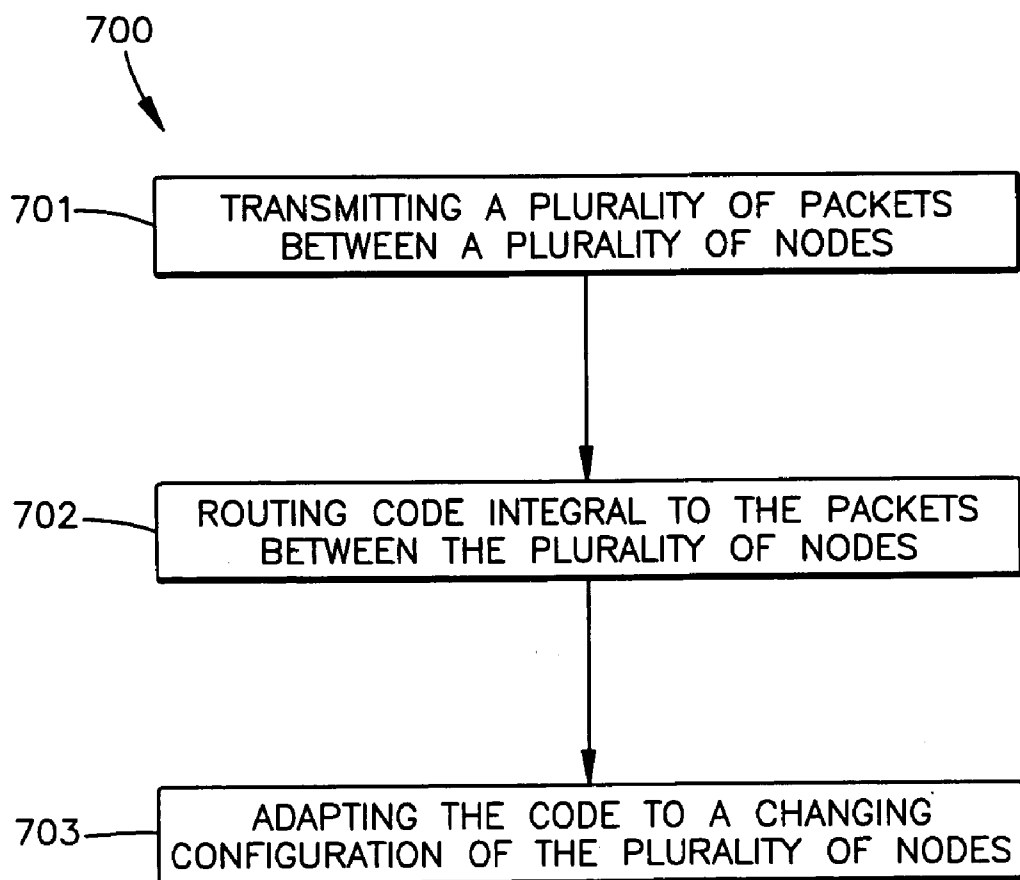


Fig.7

SYSTEM FOR A DYNAMIC AD-HOC WIRELESS NETWORK

RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Application No. 60/445,579, filed Feb. 7, 2003.

FIELD OF INVENTION

[0002] The present invention relates to a system for a wireless network and, more specifically, a system for a dynamic ad-hoc wireless network architecture.

BACKGROUND OF THE INVENTION

[0003] A wireless ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Since the nodes communicate over wireless links, the nodes have to contend with the effects of radio communication, such as noise, fading, and interference. In addition, the links typically have less bandwidth than in a wired network. Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is generally dynamic because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. Hence, there is a need for efficient routing protocols to allow the nodes to communicate over multi-hop paths consisting of possibly several links in a way that does not use any more of the network "resources" than necessary. Some of these features are characteristic of the type of packet radio networks that were studied extensively in the 1970s and 1980s. Yet, research in the area of ad hoc networking is receiving much attention from academia, industry, and government. Since these networks pose many complex issues, there are many open problems for research and opportunities for making significant contributions.

[0004] There are two major conventional types of wireless ad hoc networks: mobile ad hoc networks (MANET's) and smart sensor networks. Conventional MANET's are the next generation of wireless communication systems. MANET's provide rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, military networks, etc. Such deployment scenarios cannot rely on centralized and organized connectivity, but may be conceived as applications of MANETs.

[0005] Specifically, a MANET is an autonomous collection of mobile users that communicate over wireless links with relatively constrained bandwidths. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The MANET is decentralized with all network activity being executed by the nodes themselves, i.e., discovering topology, delivering messages, routing functionality incorporated into mobile nodes, etc.

[0006] The applications of MANET's are extremely diverse ranging from small, static networks that are constrained by power sources to large-scale, mobile, highly dynamic networks. Thus, the design of network protocols

for MANET's is a complex issue. Regardless of the application, MANET's need efficient algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANET's. Factors such as variable wireless link quality, propagation path loss, fading, multi-user interference, power expended, and topological changes may become relevant issues.

[0007] Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, MANET's should radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of a MANET. A MANET should ideally be able to adaptively alter routing paths to alleviate any of these effects and adapt to any of these requirements.

[0008] A conventional smart sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and sufficient intelligence for signal processing and networking of the data.

[0009] An example of smart sensor network is a military sensor network for detecting enemy movements, the presence of hazardous material (such as poison gases or radiation), explosions, etc. Another example is an environmental sensor network (such as in plains, in deserts, on mountains, or on ocean surfaces) for detecting and monitoring environmental changes. Still another example is a wireless traffic sensor network for monitoring vehicle traffic on a highway or in a congested part of a city. Yet another example is a wireless surveillance sensor network for providing security in a shopping mall, parking garage, or other facility. Still another example is a wireless parking lot sensor network for determining occupied spots and free spots. Besides offering certain capabilities and enhancements in operational efficiency in these conventional applications, smart sensor networks may assist in the national effort to increase alertness to potential terrorist threats.

[0010] Two conventional ways to classify smart sensor networks are whether the nodes are individually addressable and whether the data in the network is aggregated. The sensor nodes in a parking lot network, for example, should be individually addressable, so that one may determine the location of each free space. Thus, it may be necessary to broadcast a message simultaneously to all the nodes in the network.

[0011] However, if one wants to determine the temperature in a corner of a room, then addressability may not be so important. Any node in the given corner region may respond. The ability of the smart sensor network to aggregate the data collected ("data fusion") may greatly reduce the number of messages that are transmitted across the network.

[0012] The basic goals of a smart sensor network generally depend upon the application. One goal is to determine

the value of some parameter at a given location. In an environmental network, the parameter may be the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations. A node at this location may be connected to a number of different types of sensors, each with a different sampling rate and range of allowed values.

[0013] Another goal of a smart sensor network may be to detect the occurrence of events of interest and estimate parameters of the detected event(s). In a traffic sensor network, this event may be a vehicle moving through an intersection and the resulting estimate of the speed and direction of the vehicle.

[0014] Another goal of a smart sensor network may be to classify a detected object. In a vehicle in a traffic sensor network, the detected object may be a car, a minivan, a light truck, a bus, SUV, etc.

[0015] Another goal of a smart sensor network may be to track an object. In a military sensor network, the object may be an enemy tank moving through the area occupied by the network.

[0016] With these four goals, an important requirement of the sensor network is that the required data be disseminated to the proper end users. In some cases, there are fairly strict time requirements on this communication. For example, the detection of an intruder in a surveillance network should be immediately communicated to the police so that action may be taken.

[0017] In accordance with these goals, a conventional smart sensor network may require a large number of mostly stationary sensors. Aside from the deployment of sensors on the ocean surface or the use of mobile, unmanned, robotic sensors in military operations, most nodes in a smart sensor network are stationary. Smart sensor networks of 10,000 or even 100,000 nodes are envisioned, so scalability is also a major issue.

[0018] A smart sensor network may also require a low energy use. Since in many applications the sensor nodes will be placed in a remote area, maintenance of a node may not be possible. In this case, the lifetime of a node may be determined by the battery life, thereby requiring the minimization of energy expenditure.

[0019] A smart sensor network may further require network self-organization. Given the large number of nodes and their potential placement in hostile locations, it may be essential that the network self-organize since manual configuration may not be feasible. Moreover, nodes may fail (either from lack of energy or from physical destruction), and new nodes may join the smart sensor network. Therefore, the smart sensor network must be able to periodically reconfigure itself so that it can continue to function. Individual nodes may become disconnected from the rest of the network, but a high degree of connectivity should ideally be maintained.

[0020] A smart sensor network may still further require collaborative signal processing. A factor that distinguishes smart sensor networks from MANETs is the end goal of detection/estimation of some event(s) of interest, and not just communication. To improve detection performance and efficiency, it may be quite useful to "fuse" data from multiple

sensors. This data fusion requires the transmission of data and control messages, and thus puts constraints on the network architecture.

[0021] A smart sensor network may also require querying ability. A user may want to query an individual node or a group of nodes for information collected in a region. Depending upon the amount of data fusion performed, it may not be feasible to transmit a large amount of data across the network. Instead, various local "sink" nodes may collect data from a given region and create summary messages. A query will be directed to the sink node nearest to the desired region.

[0022] With the coming availability of low cost, short range radios, along with advances in wireless networking, smart sensor networks may become commonly deployed. In these networks, each node may be equipped with a variety of sensors such as acoustic, seismic, infrared, still/motion, video camera, etc. These nodes may be organized in clusters such that a locally occurring event can be detected by most of, if not all, the nodes in a cluster. Each node will have sufficient processing power to make a decision, and that node will be able to broadcast this decision to the other nodes in the cluster. One node may act as the cluster master with a long range radio using a conventional protocol.

[0023] The design and construction of today's legacy tactical battlefield networks are centered on well-defined, pre-configured, and fixed infrastructures. Such network infrastructures are often characterized by reliable and high-capacity links and the availability of well-identified and pre-established network services. Over the years, various communication protocols and application layer services have been developed and fielded to support end-user applications under the assumption of fixed infrastructures. However, as discussed above, emerging tactical battlefield networks are characterized by nodes that are mobile, often unpredictably so, moving into and out of communication range with each other, and that cannot, in general, rely on a pre-defined fixed infrastructure within their environment. In other words, the network environment is mobile, wireless, dynamically changing, and is "infrastructure-less". Therefore, there is a strong need in military and other environments to consider and apply Dynamic Ad-Hoc Wireless Networking (DAHWN) concepts and technologies.

[0024] Conventional ad hoc wireless networks have addressed active network intelligent packet routing capability. However, these conventional approaches assume incremental changes to the Internet Protocol (IP) and do not consider packets carrying code as an inherent part of the network, thereby resulting in inefficient implementations.

[0025] Complexity-based intrusion detection networks are currently based upon detecting physical anomalies and abnormal events. There have been suggestions of entropy based techniques, but complexity-based techniques have never been proposed. Further, trust-based routing as an integral part of routing has not been attempted. Active publish/subscribe servers (PSS) are common, but none has been implemented using active network technology. Service migration of dynamically moving network services has also never been attempted. Moving applications from node to node in a network has been done semi-manually, but not as a fully integrated and dynamic mechanism to maintain quality of service (QoS) in an ad hoc network. While the use

of routing metrics may be common, the ability to dynamically integrate new routing metrics has not been attempted. Complexity-based intrusion detection, using Kolmogorov Complexity estimation to support information assurance, has not been attempted.

SUMMARY OF THE INVENTION

[0026] In accordance with the present invention, a system operates a wireless ad hoc network. The system includes a plurality of nodes and a plurality of packets for transmission between the plurality of nodes. The packets contain code for routing the packets between the plurality of nodes. The code adapts to a changing configuration of the plurality of nodes.

[0027] In accordance with another aspect of the present invention, a system operates a wireless ad hoc network. The system includes a plurality of nodes and a plurality of packets for transmission between the plurality of nodes. The plurality of nodes utilizes a complexity metric for determining the route of at least one of the plurality of packets from one of the plurality of nodes to another of the plurality of nodes.

[0028] In accordance with still another aspect of the present invention, a computer program product operates a wireless ad hoc network. The computer program product includes a first instruction for transmitting a plurality of packets between a plurality of nodes, a second instruction for routing code integral to the packets between the plurality of nodes, and a third instruction for adapting the code to a changing configuration of the plurality of nodes.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] The foregoing and other features of the present invention will become apparent to one skilled in the art to which the present invention relates upon consideration of the following description of the invention with reference to the accompanying drawings, wherein:

[0030] FIG. 1 is a schematic view of an example system for use with the present invention;

[0031] FIG. 2 is a schematic view of an example system in accordance with the present invention;

[0032] FIG. 3 is a detailed schematic view of part of the system of FIG. 2;

[0033] FIG. 4 is a detailed schematic view of part of the system of FIG. 3;

[0034] FIG. 5 is a detailed schematic view of another part of the system of FIG. 3;

[0035] FIG. 6 is a detailed schematic view of still another part of the system of FIG. 3; and

[0036] FIG. 7 is a schematic view of another example system in accordance with the present invention.

DESCRIPTION OF AN EXAMPLE EMBODIMENT

[0037] A dynamic wireless ad hoc network (DAHWN) in accordance with the present invention encompasses multiple disciplines including not only the conventional aspects of networking technology per se, but also the theory and technology of signal processing at the application layer,

statistical communication theory, and technology at the physical/hardware level. In seeking to advance the performance of wireless ad hoc networks, the DAHWN network uses analysis, simulation, and hardware testbeds to characterize and assess the performance of new network designs and protocols. Each of these tools provides a reference by which to measure the DAHWN network's performance, and each may be used as a means for validating the other.

[0038] One goal of the DAHWN network is the investigation of the performance of routing protocols for MANETs that have been submitted for possible standardization. Another goal is the investigation of schemes for implementing user and traffic-type priority in a distributed ad hoc network. A further goal of the DAHWN network is the carrying out of a comparative study of wireless network simulation tools with an emphasis on scalability of these tools to large networks, increased traffic loads, increased mobility, etc. A still further goal is the development of efficient distributed detection and estimation algorithms for smart sensor networks. Other goals may be the investigation of methods of network self-organization and clustering in smart sensor networks, development of sensor networks capable of transmitting video information at very low bit rates in a multi-hop ad-hoc manner, and the development of kinetic spanning tree concepts for wireless network routing and collaboration.

[0039] The DAHWN network in accordance with the present invention develops analytical methods for predicting the outcomes of particular simulations as a means for validating the simulations. The result may be in dynamic source routing (DSR) protocol and ad hoc on-demand distance vector (AODV) protocol.

[0040] The DAHWN network thus allows the dynamic injection of network algorithms, such as various types of routing protocols (i.e., DSR, AODV, etc.). The intended use of this capability is to provide more flexible and optimized behavior than that found in conventional networks.

[0041] The DAHWN network may predict the distribution of link distances in a network of randomly deployed radio terminals and measurements of the probability of n-hop routing paths. The DAHWN network may thereby provide intermediate results for assessing network performance based on the underlying connectivity at a given time.

[0042] The DAHWN network 10 may provide an extension to an nth root, parity distributed detection algorithm. Instead of making a single "hard" decision at each sensor node 11, a two bit quantizer may be used to choose the hypothesis and also to provide a confidence measure of this decision (FIG. 1). The DAHWN network 10 may broadcast these "soft" decisions to all nodes 11, thus creating a stopping rule that reduces the number of parleys.

[0043] For a Bayesian criterion, the probability of error may be unchanged. The probability may be equal to that of a central processor. For a Neyman-Pearson criterion, the receiver operating curve may be essentially the same as that of a central processor. The performance may also be compared to that obtained using one-bit decision makers and the majority fusion rule. Simulation results may be provided for a Gaussian shift in means problem assuming an ideal channel and the binary symmetric channel.

[0044] As a first step in studying self-organization algorithms for wireless sensor networks, a C++ implementation

of the Linked Cluster Algorithm (LCA) of Baker and Ephremides may be created. Given a set of sensor nodes **11**, the LCA may use a fixed TDMA frame structure to form clusters so that all the nodes of the cluster are within one hop of a distinguished node called the cluster head. If the cluster heads of two adjacent clusters are not within transmission range of each other, gateway nodes **11s** may be designated to connect them. The set of cluster heads and gateways form a backbone network. The interaction of the LCA and the parley distributed detection algorithm may then be studied.

[0045] A primary goal may be the determination of the parameters that are responsible for performance and the drawing of conclusions about how to optimize the parameters. One of the primary performance metrics of a smart sensor network may be the ability to detect events of interest.

[0046] The self-configuration architecture of the DAHWN network may produce a hierarchical network with address auto-configuration and various other properties. Consequently, a set of distributed algorithms and message formats may also allow an actual implementation. Specifically, protocols may organize the sensor nodes **11** into clusters and then merge the clusters to form groups. Groups may merge to form larger groups, in a hierarchical process that dynamically assigns a unique address to each sensor node **11**. Additionally, a broadcast tree may be constructed to reduce the maximum number of hops along the tree. A number of important parameters may be identified and their effects on the overall system performance may be studied.

[0047] An unstructured mobile network ideally may support emergency responses to natural disasters, surveillance and information gathering in hostile territories, and robotic search and rescue operations where existing communication infrastructures are not available. Rapid deployment of this unstructured mobile network, where each unit is capable of transmitting video information and sensor data, would be highly desirable. The requirements may include some or all of the following: a higher upstream bandwidth (for transmitting video data), geographic mobility, sufficient area coverage, communications beyond line of sight, and low energy consumption.

[0048] The functionality required in the DAHWN network may be abstracted into four areas: (1) discovery of resources in the network; (2) operational routing and services information establishment; (3) continuous measurement of key performance metrics such as available bandwidth, latency and trust, etc.; and (4) adaptation of network protocols and services to changing topology and environmental parameters. The DAHWN network architecture may be able to discover and configure new nodes **11**, measure and monitor network operations, and adapt network services to the Dynamic Ad-Hoc Wireless Networking environment.

[0049] The DAHWN network in accordance with the present invention may provide Active Network Encapsulation Packets (ANEP) for carrying code and data thus distributing the intelligence throughout the network and adapting to network topology changes. The Complexity-Based Intrusion Detection of abnormal changes in the estimation of complexity along a key control channels by the DAHWN network may also indicate suspicious behavior in the electromagnetic environment. The DAHWN network may also allow Link Quality Tables and Metric Routing Decisions to

be more finely tuned to match network topology changes to application requirements. The DAHWN network may allow the movement of network services to optimal locations within the network in order to maintain a high QoS, particularly as the network topology changes.

[0050] A network **10** may further create trust-based routing patterns of behavior learned via intermediate nodes **11**. These routing patterns may be used to establish a measure of trust in those intermediate nodes **11**. As the behavior is consistently and successfully verified, the trust level increases. Trust of intermediate nodes **11** may be integrated into the routing mechanism as a Link Property Table entry.

[0051] The left side of **FIG. 2** illustrates a high-level diagram of a DAHWN system **100** in accordance with the present invention. Packets enter from the bottom of the stacks on the left and flow to the top. Packet payload is processed at the top of the stack. Packets are transmitted downward through the bottom of the stack.

[0052] The right side of **FIG. 2** is a detailed view of the DAHWN layer **101**. The left most stack of **FIG. 2** is a conventional legacy TCP/IP stack **111** that resides in parallel with the DAHWN protocol stack **121**. Packets enter and exit via the "Active Network Encapsulation Protocol" box **131**. This protocol may reside on top of a conventional protocol. Packets pass through the routing protocol box **141**. Packets then pass through any one of the four middle boxes **151** depending upon their function. These four boxes **151** operate within the Active Network Environment box **161** (i.e., a Java thread execution control mechanism, etc.).

[0053] **FIG. 3** detailed view the DAHWN block in **FIG. 2**. Packets arrive at the Port Manager **201**. Packets are demultiplexed at the Demultiplexer box **211**. Packet payloads are extracted in the Active Network Encapsulation Protocol box **221**.

[0054] Legacy (UDP/IP) Simple Network Management Protocol (SNMP) packets are executed in parallel via the left side stacks **309** of **FIG. 2**. SNMP payload is extracted upon reception (or wrapped upon transmission) in the SNMP Wrapper **231**. Returning to the DAHWN layer, Internet Protocol to Active Network node name translation occurs in the Name Resolution box **241**.

[0055] Packets containing routing information are processed in the Zone Routing Protocol box **251**. **FIG. 4** is a detailed flow diagram of an example operation algorithm for the Zone Routing Protocol box **251**. Packets controlling operation of the ad hoc network **100** continue through one of the following boxes: Node Properties (Discovery Module) **261**, Adapt (Adaptation Module) **271**, Link Property Tables (Routing) **281**, or Measure **291** Modules. Each of the code threads that implements one of the above stated modules **261**, **271**, **281**, **291** is maintained within the Active Network Environment box **301**. The Adaptation Module **271** includes a service template **273** for generating new services via a programming technique.

[0056] The Scheduler **303** (**FIG. 3**) controls when packet code may be executed. The Small State Manager **305** contains memory where information from a packet may be retained for use by other packets. The Execution Manager **307** runs and controls the code. The SNMP **309** gathers and sets general management information within the system **100**.

[0057] FIG. 5 is a detailed view of the Link Property Tables box 281 of FIG. 3. General metrics regarding link state are propagated along with routing information and maintained along with typical topological information.

[0058] FIG. 6 is a detailed view of the Measure box 291 of FIG. 3 related to security in the example case of an FTP protocol. A user at terminal may connect through the ad hoc network 100 to the NPRnet, a specific military network. AOC and MC2 are example nodes in this network (unrelated to technical implementation).

[0059] FTP is a conventional protocol and is executed in the FTP Server Proxy 601, FTP Client Proxy 611, and Client 621 boxes. The FTP Server Proxy 601 and Client Proxy 611 interface with the DAHWN wireless ad hoc network 100 and packetize the legacy FTP packets appropriately for transmission over the DAHWN wireless ad hoc network. FTPcSmartPackets 631 may be FTP control data packets. FTPdSmartPackets 641 may be FTP data packets. These packets 631, 641 flow within the DAHWN wireless ad hoc network 100 wrapped in active packets. The complexity of the FTPcSmartPacket 631 contents is monitored via the Kolmogorov Complexity Operations Policar (KCOP) 651. Any deviation from normal complexity indicates suspicious activity.

[0060] In accordance with the present invention, a computer program product 700 operates a wireless ad hoc network (FIG. 7). The computer program product 700 includes a first instruction 701 for transmitting a plurality of packets between a plurality of nodes, a second instruction 702 for routing code integral to the packets between the plurality of nodes, and a third instruction 703 for adapting the code to a changing configuration of the plurality of nodes.

[0061] In order to provide a context for the various aspects of the present invention, the following discussion is intended to provide a brief, general description of a suitable computing environment in which the various aspects of the present invention may be implemented. While the invention has been described above in the general context of computer-executable instructions of a computer program that runs on a computer, those skilled in the art will recognize that the invention also may be implemented in combination with other program modules.

[0062] Generally, program modules include routines, programs, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the inventive methods may be practiced with other computer system configurations, including single-processor or multi-processor computer systems, minicomputers, mainframe computers, as well as personal computers, hand-held computing devices, microprocessor-based or programmable consumer electronics, and the like. The illustrated aspects of the invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications argument model. However, some, if not all aspects of the invention can be practiced on stand-alone computers. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

[0063] An exemplary system for implementing the various aspects of the invention includes a conventional server

computer, including a processing unit, a system memory, and a system bus that couples various system components including the system memory to the processing unit. The processing unit may be any of various commercially available processors. Dual microprocessors and other multi-processor architectures also can be used as the processing unit. The system bus may be any of several types of bus structure including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of conventional bus architectures. The system memory includes read only memory (ROM) and random access memory (RAM). A basic input/output system (BIOS), containing the basic routines that help to transfer information between elements within the server computer, such as during start-up, is stored in ROM.

[0064] The server computer further includes a hard disk drive, a magnetic disk drive, e.g., to read from or write to a removable disk, and an optical disk drive, e.g., for reading a CD-ROM disk or to read from or write to other optical media. The hard disk drive, magnetic disk drive, and optical disk drive are connected to the system bus by a hard disk drive interface, a magnetic disk drive interface, and an optical drive interface, respectively. The drives and their associated computer-readable media provide nonvolatile storage of data, data structures, computer-executable instructions, etc., for the server computer. Although the description of computer-readable media above refers to a hard disk, a removable magnetic disk and a CD, it should be appreciated by those skilled in the art that other types of media which are readable by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, and the like, may also be used in the exemplary operating environment, and further that any such media may contain computer-executable instructions for performing the methods of the present invention.

[0065] A number of program modules may be stored in the drives and RAM, including an operating system, one or more application programs, other program modules, and program data. A user may enter commands and information into the server computer through a keyboard and a pointing device, such as a mouse. Other input devices (not shown) may include a microphone, a joystick, a game pad, a satellite dish, a scanner, or the like. These and other input devices are often connected to the processing unit through a serial port interface that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor or other type of display device is also connected to the system bus via an interface, such as a video adapter. In addition to the monitor, computers typically include other peripheral output devices (not shown), such as speaker and printers.

[0066] The server computer may operate in a networked environment using logical connections to one or more remote computers, such as a remote client computer. The remote computer may be a workstation, a server computer, a router, a peer device or other common network node, and typically includes many or all of the elements described relative to the server computer. The logical connections include a local area network (LAN) and a wide area network (WAN). Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the internet.

[0067] When used in a LAN networking environment, the server computer is connected to the local network through a network interface or adapter. When used in a WAN networking environment, the server computer typically includes a modem, or is connected to a communications server on the LAN, or has other means for establishing communications over the wide area network, such as the internet. The modem, which may be internal or external, is connected to the system bus via the serial port interface. In a networked environment, program modules depicted relative to the server computer, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0068] In accordance with the practices of persons skilled in the art of computer programming, the present invention has been described with reference to acts and symbolic representations of operations that are performed by a computer, such as the server computer, unless otherwise indicated. Such acts and operations are sometimes referred to as being computer-executed. It will be appreciated that the acts and symbolically represented operations include the manipulation by the processing unit of electrical signals representing data bits which causes a resulting transformation or reduction of the electrical signal representation, and the maintenance of data bits at memory locations in the memory system (including the system memory, hard drive, floppy disks, and CD-ROM) to thereby reconfigure or otherwise alter the computer system's operation, as well as other processing of signals. The memory locations where such data bits are maintained are physical locations that have particular electrical, magnetic, or optical properties corresponding to the data bits.

[0069] It will be understood that the above description of the present invention is susceptible to various modifications, changes and adaptations, and the same are intended to be comprehended within the meaning and range of equivalents of the appended claims. The presently disclosed embodiments are considered in all respects to be illustrative, and not restrictive. The scope of the invention is indicated by the appended claims, rather than the foregoing description, and all changes that come within the meaning and range of equivalence thereof are intended to be embraced therein.

Having described the invention, we claim:

1. A system for operating a wireless ad hoc network, said system comprising:

a plurality of nodes; and

a plurality of packets for transmission between said plurality of nodes, said packets containing code for routing of said packets between said plurality of nodes, said code adapting to a changing configuration of said plurality of nodes.

2. The system as set forth in claim 1 wherein said plurality of nodes utilizes a complexity metric for determining the route of at least one of said plurality of packets from one of said plurality of nodes to another of said plurality of nodes.

3. The system as set forth in claim 2 wherein said complexity metric is a Kolmogorov complexity metric.

4. The system as set forth in claim 1 wherein a service template module generates services for said plurality of nodes.

5. The system as set forth in claim 1 wherein a complexity operations policer monitors said plurality of nodes for high complexity and determines whether to shut down particular nodes.

6. A system for operating a wireless ad hoc network, said system comprising:

a plurality of nodes; and

a plurality of packets for transmission between said plurality of nodes, said plurality of nodes utilizing a complexity metric for determining the route of at least one of said plurality of packets from one of said plurality of nodes to another of said plurality of nodes.

7. The system as set forth in claim 6 wherein said packets contain code for routing of said packets between said plurality of nodes, said code adapting to a changing configuration of said plurality of nodes.

8. The system as set forth in claim 6 wherein said complexity metric is a Kolmogorov complexity metric.

9. The system as set forth in claim 6 wherein a complexity operations policer monitors said plurality of nodes for high complexity and determines whether to shut down particular nodes.

10. The system as set forth in claim 6 wherein a service template module generates services for said plurality of nodes.

11. A computer program product for operating a wireless ad hoc network, said computer program product comprising:

a first instruction for transmitting a plurality of packets between a plurality of nodes;

a second instruction for routing code integral to the packets between the plurality of nodes; and

a third instruction for adapting the code to a changing configuration of the plurality of nodes.

12. The computer program product as set forth in claim 11 further including a fourth instruction for utilizing a complexity metric for determining the route of at least one of the plurality of packets from one of the plurality of nodes to another of the plurality of nodes.

13. The computer program product as set forth in claim 12 wherein the complexity metric is a Kolmogorov complexity metric.

14. The computer program product as set forth in claim 11 further including a fourth instruction for generating services for the plurality of nodes.

15. The computer program product as set forth in claim 11 further including a fourth instruction for monitoring the plurality of nodes for high complexity and determining whether to shut down particular nodes.

* * * * *