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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2007 (21.12.2007)

PCT

(10) International Publication Number
WO 2007/146690 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2007/070469

(22) International Filing Date: 6 June 2007 (06.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/423,308 9 June 2006 (09.06.2006) US

(71) Applicant *(for all designated States except US)*: **SECURE COMPUTING CORPORATION** [US/US]; 2340 Energy Park Drive, St. Paul, Minnesota 55108 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JUDGE, Paul** [US/US]; 10090 Jones Bridge Road, Unit 3, Alpharetta, Georgia 30022 (US). **ALPEROVITCH, Dmitri** [US/US]; 3338 Peachtree Road NE, #1003, Atlanta, Georgia 30326 (US). **KRASSER, Sven** [US/DE]; 250 10th Street NE, Apartment 3206, Atlanta, Georgia 30309 (US). **SELLAKANNU, Arasendran** [US/IN]; 3166 Vickery Drive, Marietta, Georgia 30066 (US). **WILLIS, Lamar L.** [US/US]; 604 Springharbor Drive, Woodstock, Georgia 30188 (US).

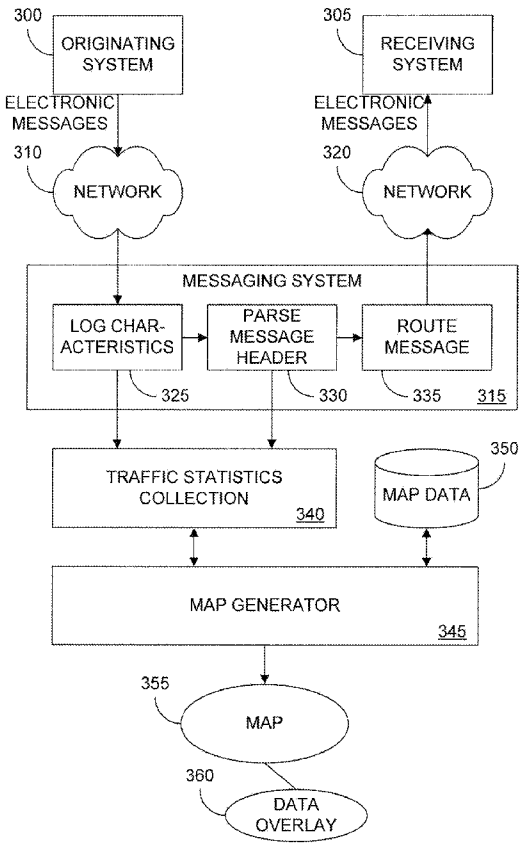
(74) Agent: **VAN AACKEN, Troy A.**; Fish & Richardson P.C., P.O. Box 1022, 3300 Dain Rauscher Plaza, Minneapolis, Minnesota 55440-1022, (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH,

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR GRAPHICALLY DISPLAYING MESSAGING TRAFFIC



(57) Abstract: Systems and methods for graphically displaying messaging traffic flows by collecting messaging data, converting a portion of the messaging data to a geographical position and collecting statistics related to the messaging data for overlaying upon a geographical map.

WO 2007/146690 A2

GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, 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).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

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

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.

SYSTEMS AND METHODS FOR GRAPHICALLY DISPLAYING MESSAGING TRAFFIC

TECHNICAL FIELD

This disclosure relates to enhancing security associated with electronic communications, and more particularly, without limitation, this disclosure relates to computer-based systems and methods for mapping data traffic flow for a messaging system.

BACKGROUND

The Internet is a global network of connected computer networks. Over the last several years, the Internet has grown in significant measure. A large number of computers on the Internet provide information in various forms. Anyone with a computer connected to the Internet can potentially tap into this vast pool of information.

The information available via the Internet encompasses information available via a variety of types of application layer information servers such as SMTP (simple mail transfer protocol), POP3 (Post Office Protocol), Instant Messaging, GOPHER (RFC 1436), WAIS, HTTP (Hypertext Transfer Protocol, RFC 2616) and FTP (file transfer protocol, RFC 1123).

One of the most wide spread method of providing information over the Internet is via the World Wide Web (the Web). The Web consists of a subset of the computers connected to the Interne; the computers in this subset run Hypertext Transfer Protocol (HTTP) servers (Web servers). Several extensions and modifications to HTTP have been proposed including, for example, an extension framework (RFC 2774) and authentication (RFC 2617). Information on the Internet can be accessed through the use of a Uniform Resource Identifier (URI, RFC 2396). A URI uniquely specifies the location of a

particular piece of information on the Internet. A URI will typically be composed of several components. The first component typically designates the protocol by which the address piece of information is accessed (e.g., HTTP, GOPHER, etc.). This first component is separated from the remainder of the URI by a colon (':'). The remainder of the URI will depend upon the protocol component. Typically, the remainder designates a computer on the Internet by name, or by IP number, as well as a more specific designation of the location of the resource on the designated computer. For instance, a typical URI for an HTTP resource might be:

http://www.server.com/dir1/dir2/resource.htm

where http is the protocol, www.server.com is the designated computer and /dir1/dir2/resouce.htm designates the location of the resource on the designated computer. The term URI includes Uniform Resource Names (URN's) including URN's as defined according to RFC 2141.

Web servers host information in the form of Web pages; collectively the server and the information hosted are referred to as a Web site. A significant number of Web pages are encoded using the Hypertext Markup Language (HTML) although other encodings using eXtensible Markup Language (XML) or XHTML. The published specifications for these languages are incorporated by reference herein; such specifications are available from the World Wide Web Consortium and its Web site (http://www.w3c.org). Web pages in these formatting languages may include links to other web pages on the same web site or another. As will be known to those skilled in the art, web pages may be generated dynamically by a server by integrating a variety of elements into a formatted page prior to transmission to a web client. Web servers, and

information servers of other types, await requests for the information from Internet clients.

Client software has evolved that allows users of computers connected to the Internet to access this information. Advanced clients such as Netscape's Navigator and Microsoft's Internet Explorer allow users to access software provided via a variety of information servers in a unified client environment. Typically, such client software is referred to as browser software.

Electronic mail (e-mail) is another wide spread application using the Internet. A variety of protocols are often used for e-mail transmission, delivery and processing including SMTP and POP3 as discussed above. These protocols refer, respectively, to standards for communicating e-mail messages between servers and for server-client communication related to e-mail messages. These protocols are defined respectively in particular RFC's (Request for Comments) promulgated by the IETF (Internet Engineering Task Force). The SMTP protocol is defined in RFC 821, and the POP3 protocol is defined in RFC 1939.

Since the inception of these standards, various needs have evolved in the field of e-mail leading to the development of further standards including enhancements or additional protocols. For instance, various enhancements have evolved to the SMTP standards leading to the evolution of extended SMTP. Examples of extensions may be seen in (1) RFC 1869 that defines a framework for extending the SMTP service by defining a means whereby a server SMTP can inform a client SMTP as to the service extensions it supports and in (2) RFC 1891 that defines an extension to the SMTP service, which allows an SMTP client to specify (a) that delivery status notifications (DSNs) should be generated under certain conditions, (b) whether such notifications should return

the contents of the message, and (c) additional information, to be returned with a DSN, that allows the sender to identify both the recipient(s) for which the DSN was issued, and the transaction in which the original message was sent.

In addition, the IMAP protocol has evolved as an alternative to POP3 that supports more advanced interactions between e-mail servers and clients. This protocol is described in RFC 2060.

The various standards discussed above by reference to particular RFC's are hereby incorporated by reference herein for all purposes. These RFC's are available to the public through the IETF and can be retrieved from its website (http://www.ietf.org/rfc.html). The specified protocols are not intended to be limited to the specific RFC's quoted herein above but are intended to include extensions and revisions thereto. Such extensions and/or revisions may or may not be encompassed by current and/or future RFC's.

A host of e-mail server and client products have been developed in order to foster e-mail communication over the Internet. E-mail server software includes such products as sendmail-based servers, Microsoft Exchange, Lotus Notes Server, and Novell GroupWise; sendmail-based servers refer to a number of variations of servers originally based upon the sendmail program developed for the UNIX operating systems. A large number of e-mail clients have also been developed that allow a user to retrieve and view e-mail messages from a server; example products include Microsoft Outlook, Microsoft Outlook Express, Netscape Messenger, and Eudora. In addition, some e-mail servers, or e-mail servers in conjunction with a Web server, allow a Web browser to act as an e-mail client using the HTTP standard.

As the Internet has become more widely used, it has also created new risks for corporations. Breaches of computer security by hackers and intruders and the potential

for compromising sensitive corporate information are a very real and serious threat. Organizations have deployed some or all of the following security technologies to protect their networks from Internet attacks:

Firewalls have been deployed at the perimeter of corporate networks. Firewalls act as gatekeepers and allow only authorized users to access a company network. Firewalls play an important role in controlling traffic into networks and are an important first step to provide Internet security.

Intrusion detection systems (IDS) are being deployed throughout corporate networks. While the firewall acts as a gatekeeper, IDS act like a video camera. IDS monitor network traffic for suspicious patterns of activity, and issue alerts when that activity is detected. IDS proactively monitor your network 24 hours a day in order to identify intruders within a corporate or other local network.

Firewall and IDS technologies have helped corporations to protect their networks and defend their corporate information assets. However, as use of these devices has become widespread, hackers have adapted and are now shifting their point-of-attack from the network to Internet applications. The most vulnerable applications are those that require a direct, "always-open" connection with the Internet such as web and e-mail. As a result, intruders are launching sophisticated attacks that target security holes within these applications.

Many corporations have installed a network firewall, as one measure in controlling the flow of traffic in and out of corporate computer networks, but when it comes to Internet application communications such as e-mail messages and Web requests and responses, corporations often allow employees to send and receive from or to anyone or anywhere inside or outside the company. This is done by opening a port, or hole in

their firewall (typically, port 25 for e-mail and port 80 for Web), to allow the flow of traffic. Firewalls do not scrutinize traffic flowing through this port. This is similar to deploying a security guard at a company's entrance but allowing anyone who looks like a serviceman to enter the building. An intruder can pretend to be a serviceman, bypass the perimeter security, and compromise the serviced Internet application.

The security risks do not stop there. After taking over the mail server, it is relatively easy for the intruder to use it as a launch pad to compromise other business servers and steal critical business information. This information may include financial data, sales projections, customer pipelines, contract negotiations, legal matters, and operational documents. This kind of hacker attack on servers can cause immeasurable and irreparable losses to a business. interconnected world, applications such as e-mail serve as a transport for easily and widely spreading viruses. Viruses such as "I Love You" use the technique exploited by distributed Denial of Service (DDoS) attackers to mass propagate. Once the "I Love You" virus is received, the recipient's Microsoft Outlook sends emails carrying viruses to everyone in the Outlook address book. The "I Love You" virus infected millions of computers within a short time of its release. Trojan horses, such as Code Red use this same technique to propagate themselves. Viruses and Trojan horses can cause significant lost productivity due to down time and the loss of crucial data.

The Nimda worm simultaneously attacked both email and web applications. It propagated itself by creating and sending infectious email messages, infecting computers over the network and striking vulnerable Microsoft IIS Web servers, deployed on Exchange mail servers to provide web mail.

Most e-mail and Web requests and responses are sent in plain text today, making it just as exposed as a postcard. This includes the e-mail message, its header, and its

attachments, or in a Web context, a user name and password and/or cookie information in an HTTP request. In addition, when you dial into an Internet Service Provider (ISP) to send or receive e-mail messages, the user ID and password are also sent in plain text, which can be snooped, copied, or altered. This can be done without leaving a trace, making it impossible to know whether a message has been compromised.

The following are additional security risks caused by Internet applications:

- E-mail spamming consumes corporate resources and impacts productivity. Furthermore, spammers use a corporation's own mail servers for unauthorized email relay, making it appear as if the message is coming from that corporation.
- E-mail and Web abuse, such as sending and receiving inappropriate messages and Web pages, are creating liabilities for corporations. Corporations are increasingly facing litigation for sexual harassment or slander due to e-mail their employees have sent or received.
- Regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (regulating financial institutions) create liabilities for companies where confidential patient or client information may be exposed in e-mail and/or Web servers or communications including e-mails, Web pages and HTTP requests.

Using the "always open" port, a hacker can easily reach an appropriate Internet application server, exploit its vulnerabilities, and take over the server. This provides hackers easy access to information available to the server, often including sensitive and confidential information. The systems and methods according to this disclosure provide enhanced security for communications involved with such Internet applications requiring an "always-open" connection.

SUMMARY

The present disclosure is directed to systems and methods for graphically displaying messaging traffic. Systems and methods can include a system data store (SDS), a system processor and one or more interfaces to one or more communications networks over which electronic communications are transmitted and received. The processor includes processing elements for receiving electronic communications having headers, the headers containing source and destination addresses and parsing the source and destination addresses associated with the electronic communications. Additional processing elements can convert source and destination addresses into a geographical position, assemble statistical information based upon the source and destination addresses of the electronic communications received at the communications interface. The processing elements can further provide a graphical user interface component comprising a geographical information pane configured to display a geographical map to a user via a display device and a map generator to generate the geographical map for use by the graphical user interface based upon user input, the map generator being configured to overlay statistical information onto the geographical map to show traffic flow associated with source and destination addresses.

Methods for graphically displaying messaging traffic can include the steps of: receiving a plurality of electronic communications, the electronic communications having source and destination addresses associated with the communications; parsing the source and destination addresses associated with the electronic communications; converting the source and destination addresses into a geographical position; assembling statistical information based upon at least the source and destination addresses of at least a sample of electronic communications received at the communications interface; storing

the statistical information in the system data store; generating a geographical map; displaying the geographical map to a user; and overlaying the geographical map with traffic information based upon the statistical information and geographical position associated with the statistical information

The details of one or more embodiments of this disclosure are set forth in the accompanying drawings and the description below.

DESCRIPTION OF DRAWINGS

FIG. 1 is a depicts a hardware diagram for an environment using one preferred embodiment according to this disclosure.

FIG. 2A is a block diagram depicting a system that has been configured to receive map data and statistics related to messaging traffic and provide a map with the overlayed messaging statistics.

FIG. 2B is a block diagram depicting a system that has been configured to receive map data and statistics related to messaging traffic and provide a user selectable map with a messaging statistics overlay.

FIG. 3 is a block diagram depicting a system that has been configured to compile messaging traffic statistics and to generate a map based upon the messaging traffic statistics.

FIG. 4 is a block diagram depicting a system that has been configured to use an existing message filtering system to collect messaging traffic statistics used to generate a map based upon the messaging traffic statistics.

FIG. 5 is a block diagram depicting a system that has been configured to use a messaging client to collect messaging traffic statistics used to generate a map based upon the messaging traffic statistics.

FIG. 6 is a block diagram depicting a system that has been configured to use a local messaging client having a messaging filter to collect messaging traffic statistics used to generate a map based upon the messaging traffic statistics.

FIG. 7 is a flowchart depicting an operational scenario for generating a map showing messaging traffic flow.

FIG. 8 is a flowchart depicting an operational scenario for gathering messaging traffic statistics and generating a map showing messaging traffic flow.

FIG. 9 is a flowchart depicting an operational scenario for generating an interactive map showing messaging traffic flow.

FIG. 10 is a flowchart depicting an operational scenario for gathering messaging traffic statistics and generating an interactive map showing messaging traffic flow.

FIG. 11 depicts an example of a graphical user interface for a map pane in accordance with the present disclosure.

FIG. 12 depicts another example of a graphical user interface for a map pane in accordance with the present disclosure.

FIG. 13 depicts another example of a graphical user interface for a map pane in accordance with the present disclosure and showing types of traffic flowing between nodes.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

Embodiments of this disclosure are now described in detail. Referring to the drawings, like numbers indicate like parts throughout the views. As used in the description herein and throughout the claims that follow, the meaning of "a," "an," and

"the" includes plural reference unless the context clearly dictates otherwise. Also, as used in the description herein and throughout the claims that follow, the meaning of "in" includes "in" and "on" unless the context clearly dictates otherwise. Finally, as used in the description herein and throughout the claims that follow, the meanings of "and" and "or" include both the conjunctive and disjunctive and may be used interchangeably unless the context clearly dictates otherwise.

Ranges may be expressed herein as from "about" one particular value, and/or to "about" another particular value. When such a range is expressed, another embodiment includes from the one particular value and/or to the other particular value. Similarly, when values are expressed as approximations, by use of the antecedent "about," it will be understood that the particular value forms another embodiment. It will be further understood that the endpoints of each of the ranges are significant both in relation to the other endpoint, and independently of the other endpoint.

FIG. 1 depicts a typical environment according to this disclosure. The access environment using systems and methods according to this disclosure may include a hardware device 195 connected to a local communication network such as Ethernet 180 and logically interposed between firewall system 140, local servers 120 and clients 130. Application related electronic communications attempting to enter or leave the local communications network through the firewall system 140 are routed to the hardware device 195 for application level security assessment and/or anomaly detection. Hardware device 195 need not be physically separate from existing hardware elements managing the local communications network. For instance, the methods and systems according to this disclosure could be incorporated into a standard firewall system 140 or router (not shown) with equal facility. In environments not utilizing a firewall system, the hardware

device 195 may still provide application level security assessment and/or anomaly detection.

For convenience and exemplary purposes only, the foregoing discussion makes reference to hardware device 195; however, those skilled in the art will understand that the hardware and/or software used to implement the systems and methods according to this disclosure may reside in other appropriate network management hardware and software elements. Moreover, hardware device 195 is depicted as a single element. In various embodiments, a multiplicity of actual hardware devices may be used. Multiple devices that provide security enhancement for application servers of a particular type such as e-mail, instant messaging or web may be used where communications of the particular type are allocated among the multiple devices by an appropriate allocation strategy such as (1) serial assignment that assigns a communication to each device sequentially, or (2) via the use of a hardware and/or software load balancer that assigns a communication to the device based upon current device burden. A single device may provide enhanced security across multiple application server types, or each device may only provide enhanced security for a single application server type.

In one embodiment, hardware device 195 may be a rack-mounted Intel-based server at either 1U or 2U sizes. The hardware device 195 can be configured with redundant components such as power supplies, processors and disk arrays for high availability and scalability. The hardware device 195 may include SSL/TLS accelerators for enhanced performance of encrypted messages.

The hardware device 195 will include a system processor potentially including multiple processing elements where each processing element may be supported via Intel-compatible processor platforms preferably using at least one PENTIUM III or CELERON

(Intel Corp., Santa Clara, Calif.) class processor; alternative processors such as UltraSPARC (Sun Microsystems, Palo Alto, Calif.) could be used in other embodiments. In some embodiments, security enhancement functionality, as further described below, may be distributed across multiple processing elements. The term processing element may refer to (1) a process running on a particular piece, or across particular pieces, of hardware, (2) a particular piece of hardware, or either (1) or (2) as the context allows.

The hardware device 195 would have an SDS that could include a variety of primary and secondary storage elements. In one preferred embodiment, the SDS would include RAM as at least part of the primary storage; the amount of RAM might range from 128 MB to several gigabytes although these amounts could vary and represent overlapping use such as where security enhancement according to this disclosure is integrated into a firewall system. The primary storage may in some embodiments consist of, or include in combination, other forms of memory such as cache memory, registers, non-volatile memory (e.g,, FLASH, ROM, EPROM, etc.), etc.

The SDS may also include secondary storage including single, multiple and/or varied servers and storage elements. For example, the SDS may use internal storage devices connected to the system processor. In embodiments where a single processing element supports all of the security enhancement functionality, a local hard disk drive may serve as the secondary storage of the SDS, and a disk operating system executing on such a single processing element may act as a data server receiving and servicing data requests.

It will be understood by those skilled in the art that the different information used in the security enhancement processes and systems according to this disclosure may be logically or physically segregated within a single device serving as secondary storage for

the SDS; multiple related data stores accessible through a unified management system, which together serve as the SDS; or multiple independent data stores individually accessible through disparate management systems, which may in some embodiments be collectively viewed as the SDS. The various storage elements that comprise the physical architecture of the SDS may be centrally located, or distributed across a variety of diverse locations.

The architecture of the secondary storage of the system data store may vary significantly in different embodiments. In several embodiments, database(s) are used to store and manipulate the data; in some such embodiments, one or more relational database management systems, such as DB2 (IBM, White Plains, N.Y.), SQL Server (Microsoft, Redmond, Wash.), ACCESS (Microsoft, Redmond, Wash.), ORACLE 8i (Oracle Corp., Redwood Shores, Calif.), Ingres (Computer Associates, Islandia, N.Y.), MySQL (MySQL AB, Sweden) or Adaptive Server Enterprise (Sybase Inc., Emeryville, Calif.), may be used in connection with a variety of storage devices/file servers that may include one or more standard magnetic and/or optical disk drives using any appropriate interface including, without limitation, IDE and SCSI. In some embodiments, a tape library such as Exabyte X80 (Exabyte Corporation, Boulder, Colo.), a storage area network (SAN) solution such as available from (EMC, Inc., Hopkinton, Mass.), a network attached storage (NAS) solution such as a NetApp Filer 740 (Network Appliances, Sunnyvale, Calif.), or combinations thereof may be used. In other embodiments, the data store may use database systems with other architectures such as object-oriented, spatial, object-relational or hierarchical or may use other storage implementations such as hash tables or flat files or combinations of such architectures. Such alternative approaches may use data servers other than database management systems such as a hash table look-

up server, procedure and/or process and/or a flat file retrieval server, procedure and/or process. Further, the SDS may use a combination of any of such approaches in organizing its secondary storage architecture.

The hardware device 195 would have an appropriate operating system such as WINDOWS/NT, WINDOWS 2000 or WINDOWS/XP Server (Microsoft, Redmond, Wash.), Solaris (Sun Microsystems, Palo Alto, Calif.), or LINUX (or other UNIX variant). In one preferred embodiment, the hardware device 195 includes a pre-loaded, pre-configured, and hardened UNIX operating system based upon FreeBSD (FreeBSD, Inc., http://www.freebsd.org). In this embodiment, the UNIX kernel has been vastly reduced, eliminating non-essential user accounts, unneeded network services, and any functionality that is not required for security enhancement processing. The operating system code has been significantly modified to eliminate security vulnerabilities.

Depending upon the hardware/operating system platform, appropriate server software may be included to support the desired access for the purpose of configuration, monitoring and/or reporting. Web server functionality may be provided via an Internet Information Server (Microsoft, Redmond, Wash.), an Apache HTTP Server (Apache Software Foundation, Forest Hill, Md.), an iPlanet Web Server (iPlanet E-Commerce Solutions--A Sun--Netscape Alliance, Mountain View, Calif.) or other suitable Web server platform. The e-mail services may be supported via an Exchange Server (Microsoft, Redmond, Wash.), sendmail or other suitable e-mail server. Some embodiments may include one or more automated voice response (AVR) systems that are in addition to, or instead of, the aforementioned access servers. Such an AVR system could support a purely voice/telephone driven interface to the environment with hard copy output delivered electronically to suitable hard copy output device (e.g., printer, facsimile, etc.),

and forward as necessary through regular mail, courier, inter-office mail, facsimile or other suitable forwarding approach. In one preferred embodiment, an Apache server variant provides an interface for remotely configuring the hardware device 195. Configuration, monitoring, and/or reporting can be provided using some form of remote access device or software. In one embodiment, SNMP is used to configure and/or monitor the device. In one embodiment, any suitable remote client device is used to send and retrieve information and commands to/from the hardware device 195. Such a remote client device can be provided in the form of a Java client or a Windows-based client running on any suitable platform such as a conventional workstation or a handheld wireless device or a proprietary client running on an appropriate platform also including a conventional workstation or handheld wireless device.

FIG. 2A is block diagram depicting the generation of a geographical map having a messaging traffic overlay. Messaging statistics 200 and a maps database 205 are provided to a map generator 210. It should be understood that messages typically include internet protocol (IP) addresses, these addresses can therefore be assembled from the messages. The IP addresses can then be traced to a location associated with the message. As known to those skilled in the art, software can be used to trace IP addresses to locations based upon known locations of registered IP addresses stored in associated databases. However, it should be understood that this disclosure is not intended to be limited to current location methods, but is intended to include all known methods for locating a computing device based upon its IP or media-access-control address. For example, in a wireless network, a computing device may be located through triangulation based on the signal strength received at more than one base station or access point. Enhanced 911 (e911) now allows mobile communications devices to be located in case of emergency. e911 can

use a variety of techniques to locate a mobile communications device, and can include using a GPS signal alone or in combination with other techniques. Similarly, VoIP enhanced 911 is a geographic location system for packet switched voice, which is conceptually similar to any other packet switched data network.

Using the information provided the map generator 210 creates a map 220 for display to a user. The map includes an overlay of the data traffic flow 225, such that a system administrator can view the geographical locations from which traffic is being received, and to which traffic is being sent.

FIG. 2B is a block diagram depicting a system for graphically displaying a map having a data traffic flow overlay. Messaging statistics 250 and a maps database 255 are provided to a map generator 260. The map generator 260 can generate a map 265 for display to a user based upon the input received from the messaging statistics 250 and the maps database 255. It should be understood that the map 265 can be generated based upon user input to a computing device. The map 265 includes an overlay of data traffic flow 270, thereby enabling a user to view the locations to which messaging data is being sent, and from which messaging data is being received. Moreover, the map 265 is selectable 275, thereby enabling a user to pan to different geographical locations, zoom in/zoom out to/from a location , zoom in/out to/from a particular traffic flow, such that a user can obtain a complete picture of messaging traffic.

With regard to zooming in to a traffic flow or zooming out from a traffic flow, it should be understood that in various systems and methods of this disclosure that messaging traffic can be isolated down to the message level, or at any abstraction therefrom, for example, traffic can be shown as flowing between states, between cities, between street address, among many others. Traffic can also be separated and displayed

as, for example, incoming traffic, outgoing traffic, virus traffic, spam traffic, confidential traffic, personal traffic, encrypted traffic, among many other types of classifications, and combinations thereof. Additionally, in some examples, the types of attachments included in messages between endpoints may be displayed to a user. Types of attachments can be file types, such as, for example, images, binary, text documents, etc. Furthermore, the frequency with which messages travel between nodes can be provided to the user. For example, two addresses may exchange messages once a week, once a day, several times a day, several times an hour, etc.

The interface can be configured to turn on or off types of traffic being displayed. For example, if an administrator wants to view malicious traffic, the administrator might select to only display spam and virus traffic. Thus, it should be recognized that in some examples, the types of traffic displayed can be toggled on or off based upon user input.

Moreover, visualization of messaging traffic and statistical information can use visual cues such as color, size, shape, pattern, etc. In some examples, the visual cues are consistent between different views, queries, and/or sessions.

FIG. 3 depicts a system for collecting statistics from messaging traffic and generating maps using the collected messaging statistics. Messaging traffic can originate from a computing device 300 bound for a recipient device 305. Messaging traffic originating from computing device 300 typically passes through a network 310 before reaching some sort of messaging system 315. The messaging system then forwards the message to network 320 which routes the message to the receiving system 305. It should be understood that in various examples, networks 310 and 320 can comprise different networks, the same network or overlapping networks. Moreover, it should be understood that the sending an receiving systems often have different messaging systems, therefore

depending on whether the messaging system is associated with the sender or receiver networks 310, 320 can include a messaging system for storage of electronic messages until they are delivered (e.g., downloaded) to the receiving system 305, or sometimes messages may be stored until deletion is requested by policy or by the receiving system 305. Further, it should be recognized that networks 310, 320 can take a variety of different forms, including public switched telephone networks (PSTN), local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), intranets, extranets, among many others.

The messaging system 315 can perform a variety of functions, including a logging the characteristics 325 associated with the message. For example, the component could monitor any message characteristics, including, among others, message size, message content classification, intermediate systems through which the message has passed, and combinations thereof. The messaging system can further parse the message header 330 to determine source and destination addresses associated with the message, such that the messaging system can also route the message 335. As is known to those skilled in the art, the message header typically includes information about the originating system and receiving systems. Moreover, this information is not encrypted so that the messaging systems, and any intermediate routers, understand how to route the message to the recipient.

The message characteristics 325 and message header parsing 330 are sent to a traffic statistics collection system 340, which can be part of a system data store. Alternatively, the traffic statistics collection system could optionally include functionality to determine a location of IP or MAC addresses included in the message statistics,

although it should be understood that this functionality could alternatively be embodied in the map generator 345.

The traffic statistics collection system 340 communicates with the map generator 345 to supply data related to a particular geographic location to the map generator 345. The map generator also communicates with a map database 350 to retrieve map data for the particular geographic location. The map generator 345 then uses the information received from the map database 350 and the traffic statistics collection system 345 to generate a map 355. The map 355 may be sent to a display device (not shown) for display to a user. The map 355 may further include a data overlay 360 depicting the traffic flow between the locations depicted on the map 355.

FIG. 4 depicts a system for collecting statistics from messaging traffic and generating maps using the collected messaging statistics. Messaging traffic can originate from a computing device 400 bound for a recipient device 405. Messaging traffic originating from computing device 400 typically passes through a network 410 before reaching some sort of messaging system 415. The messaging system then forwards the message to network 420 which routes the message to the receiving system 405. It should be understood that in various examples, networks 410 and 420 can comprise different networks, the same network or overlapping networks. Moreover, it should be understood that the sending an receiving systems often have different messaging systems, therefore depending on whether the messaging system is associated with the sender or receiver networks 410, 420 (or is associated with neither of the sender or receiver networks) can include a messaging system for storage of electronic messages until they are delivered (e.g., downloaded) to the receiving system 405, or sometimes messages may be stored until deletion is requested by policy or by the receiving system 405. Further, it should be

recognized that networks 410, 420 can take a variety of different forms, including public switched telephone networks (PSTN), local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), intranets, extranets, among many others.

The messaging system 415 can perform a variety of functions, including a logging the characteristics 425 associated with the message. For example, the component could monitor any message characteristics, including, among others, message size, message content classification, intermediate systems through which the message has passed, and combinations thereof. The messaging system can further parse the message header 430 to determine source and destination addresses associated with the message, such that the messaging system can also route the message 435. As is known to those skilled in the art, the message header typically includes information about the originating system and receiving systems. Moreover, this information is not encrypted so that the messaging systems, and any intermediate routers, understand how to route the message to the recipient.

The parsed message may also be used for message filtering 440. For example, a message may contain known spam, virus content, policy violation, security violation, etc., and combinations thereof. These messages may therefore be filtered by the messaging filter 440 to protect the receiving system. Messages that are filtered could be for example, sent to a quarantine 445, the messages could be dropped altogether, or the messages could be held for further analysis, among many others handling options for filtered messages.

The message characteristics 425, results of message header parsing 430, and results of message filtering 440 are sent to a traffic statistics collection system 450, which can be part of a system data store. Alternatively, the traffic statistics collection system

could optionally include functionality to locate of IP or MAC addresses included in the message statistics, although it should be understood that this functionality could alternatively be embodied in the map generator 455.

The traffic statistics collection system 450 communicates with the map generator 455 to supply data related to a particular geographic location to the map generator 455. The map generator also communicates with a map database 460 to retrieve map data for the particular geographic location. The map generator 455 then uses the information received from the map database 460 and the traffic statistics collection system 455 to generate a map 465. The map 465 may be sent to a display device (not shown) for display to a user. The map 465 may further include a data overlay 470 depicting the traffic flow between the locations depicted on the map 465.

It should be understood from this disclosure that the traffic statistics collection system 455 may collect statistics from hundreds or thousands of messaging systems in various examples of this disclosure. Moreover, the traffic statistics collection system 455 in some examples can collect statistics from many unrelated nodes, and be operable to present statistics on any internet node based upon input from a user, such as an IP address. It should also be recognized that the traffic statistics collection system, in some examples, collects information related to different messaging and communication protocols and aggregates traffic across different platforms and protocols.

FIG. 5 depicts a system for collecting statistics from messaging traffic and generating maps using the collected messaging statistics. Messaging traffic can originate from a computing device 500 bound for a recipient device (not shown). Messaging traffic originating from computing device 500 is typically composed using a messaging client 505 installed on the computing device via one or more I/O devices 510. passes through a

network 515 before reaching some sort of messaging system 520. The messaging system then forwards the message to be routed to a receiving system (not shown). It should be understood that in various examples, the messaging client is the receiving system, and that it receives a message via the network 515 from the messaging server 520. Further, it should be recognized that networks 515 can take a variety of different forms, including public switched telephone networks (PSTN), local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), intranets, extranets, among many others.

Systems and methods for collecting messaging statistics can use functionality included in a messaging client to log characteristics 525 of received/sent messages, and to log the header 530 of received/sent messages. The messaging client 505 can then send the messaging statistics to a map server 540 via a network 535. Again, it should be understood that networks 535 and 515 can be the same network, different networks, or overlapping networks, and can use myriad different architectures, protocols, and/or components, each of which is intended to be within the scope of this disclosure.

A map server 540 can include a traffic statistics collection system 545 to collect statistics received from the messaging client 505, as well as a map generator 550 and a map database 545. It should be understood that messaging statistics can be sent in real time as messages are sent/received, but that the messaging client 505 could also store statistics in volatile or non-volatile memory for transfer at regular intervals determined by a schedule, or at irregular intervals when usage of the computing device 500 is low.

The traffic statistics collection system 545 communicates with the map generator 540 to supply data related to a particular geographic location to the map generator 540. The map generator 550 also communicates with a map database 555 to retrieve map data

for the particular geographic location. The map generator 550 then uses the information received from the map database 555 and the traffic statistics collection system 545 to generate a map 560. The map 550 may be sent to a display device (not shown) for display to a user. The map 560 may further include a data overlay 565 depicting the traffic flow between the locations depicted on the map 560. It should also be understood that the map server can be used as a central repository to graphically depict data traffic flow between a multitude of devices associated with and providing data to the map server 540. Moreover, it should be understood that the map server 540 in some examples could be used transmit a map 560 across a network to one or more remote users.

FIG. 6 depicts systems and methods for collecting statistics from messaging traffic and generating maps using the collected messaging statistics. Messaging traffic can originate from a computing device 600 bound for a recipient device (not shown). Messaging traffic originating from computing device 600 is typically composed using a messaging client 605 installed on the computing device via one or more I/O devices 610. passes through a network 615 before reaching some sort of messaging system 620. The messaging system then forwards the message to be routed to a receiving system (not shown). It should be understood that in various examples, the messaging client is the receiving system, and that it receives a message via the network 615 from the messaging server 620. Further, it should be recognized that networks 615 can take a variety of different forms, including public switched telephone networks (PSTN), local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), intranets, extranets, among many others.

Systems and methods for collecting messaging statistics can use functionality included in a messaging client to log characteristics 625 of received/sent messages and to

log the header 630 of received/sent messages. It should also be understood that in some systems and methods, the message may be filtered by a local message filtering system 635. For example, a message may contain known spam, virus content, policy violation, security violation, etc., and combinations thereof. These messages may therefore be filtered by the local messaging filter 635 to protect the receiving and/or sending system. Messages that are filtered could be for example, sent to a quarantine, the messages could be dropped altogether, or the messages could be held for further analysis, among many other handling options for filtered messages.

The messaging client 605 can then send the messaging statistics (including the parsed header information, message characteristics, and classification, among others) to a map server 645 via a network 640. Again, it should be understood that networks 640 and 615 can be the same network, different networks, or overlapping networks, and can use myriad different architectures, protocols, and/or components, each of which is intended to be within the scope of this disclosure.

A map server 645 can include a traffic statistics collection system 650 to collect statistics received from the messaging client 605, as well as a map generator 655 and a map database 650. It should be understood that messaging statistics can be sent in real time as messages are sent/received, but that the messaging client 605 could also store statistics in volatile or non-volatile memory for transfer at regular intervals determined by a schedule, or at irregular intervals when usage of the computing device 600 is low. The traffic statistics collection system 650 in some examples can optionally include functionality to locate of IP or MAC addresses included in the message statistics, although it should be understood that this functionality could alternatively be embodied in the map generator 655.

The traffic statistics collection system 650 communicates with the map generator 645 to supply data related to a particular geographic location to the map generator 645. The map generator 655 also communicates with a map database 660 to retrieve map data for the particular geographic location. The map generator 655 then uses the information received from the map database 660 and the traffic statistics collection system 650 to generate a map 665. The map 665 may be sent to a display device (not shown) for display to a user. The map 665 may further include a data overlay 670 depicting the traffic flow between the locations depicted on the map 655. It should also be understood that the map server 645 can be used as a central repository to graphically depict data traffic flow between a multitude of devices associated with and providing data to the map server 645. Moreover, it should be understood that the map server 645 in some examples could be used transmit a map 665 across a network to one or more remote users.

FIG. 7 depicts an operational scenario 700 for systems and methods for graphically displaying messaging traffic. In step 710, the operational receives data flow statistics from some form of statistics collection and/or aggregation system. At step 720, the operational scenario generates a map based upon the received statistics. The operational scenario then overlays the generates map with the compiled statistics as shown in step 730. It should be understood that points on the map can be correlated with nodes associated with the data flow. For example, the node information can include latitude and longitude information in addition to data traffic associated with the various nodes identified by the data flow statistics. In step 740, the operational scenario sends the map with the traffic statistics overlay to a be displayed to a user.

FIG. 8 depicts an operational scenario 800 for systems and methods for graphically displaying messaging traffic. In step 810, the operational scenario logs

electronic communications. In some examples, the scenario could log only headers and other characteristics associated with the messages. At step 820, the operational scenario parses the headers of the messages and compiles statistics associated with the logged messages or message characteristics. The operational scenario then generates a map based upon the compiled statistics, as shown by step 830. At step 840, the operational scenario overlays the map using the compiled statistics. It should be understood that the compilation of statistics can be performed by a messaging system, by a messaging filtering system, by a messaging client, or by any other suitable mechanisms by which statistics can be collected regarding the data traffic flow. The operational scenario then sends the generated map to for display to a user, as shown by step 850.

FIG. 9 depicts an operational scenario 900 for systems and methods for graphically displaying messaging traffic. In step 910, the operational receives data flow statistics from some form of statistics collection and/or aggregation system. It should be understood that in various example systems and methods that the statistics collection and/or aggregation system could also provide latitudinal and longitudinal information, or other information to assist in linking the statistics to a map. The operational scenario then generates a map based upon the compiled statistics, as shown by step 920. In various example systems and methods, the map generation can include a location system for using the addresses provided by the statistics collection and/or aggregation system to locate the nodes identified by the statistical information, and thereby use this information to link the statistics to the map. At step 930, the operational scenario overlays the map using the compiled statistics. It should be understood that the compilation of statistics can be performed by a messaging system, by a messaging filtering system, by a messaging client, or by any other suitable mechanisms by which statistics can be

collected regarding the data traffic flow. The operational scenario then sends the generated map to for display to a user, as shown by step 940.

The operational scenario then determines whether input from the user has been received in step 950. If the operational scenario determines that input from the user has been received, the operational scenario instructs the map generation system to perform the action requested by the user. It should be understood that the action requested by the user can include, in various example systems an methods, zooming in on a location, zooming out from a location, zooming in on a traffic flow, zooming out on a traffic flow, separating traffic flows based upon the characteristics of individual data stream included in the traffic flow, combining individual streams to show an overall traffic flow, among many others. The operational scenario then returns to generate a map (920) and overlay compiled statistics onto the map (930) and send the map for display to a user (940), as shown by step 960.

If the operational scenario determines that no input from the user has been received in step 950, the operational scenario then determines whether an exit command has been received at step 970. If no exit command has been received, the operation scenario waits until it is determined that an exit command has been received or that an input from the user has been received. Upon determining that an exit command has been received from the user, the operational scenario ends at step 980.

FIG. 10 depicts an operational scenario 1000 for systems and methods for graphically displaying messaging traffic. In step 1010, the operational scenario logs electronic communications. In some examples, the scenario could log only headers and other characteristics associated with the messages. At step 1020, the operational scenario parses the headers of the messages and compiles statistics associated with the logged

messages or message characteristics. It should be understood that in various example systems and methods that the statistics collection and/or aggregation system could also provide latitudinal and longitudinal information, or other information to assist in linking the statistics to a map. It should also be understood that the compilation of statistics can be performed by a messaging system, by a messaging filtering system, by a messaging client, or by any other suitable mechanisms by which statistics can be collected regarding the data traffic flow.

The operational scenario then generates a map based upon the compiled statistics, as shown by step 1030. In various example systems and methods, the map generation can include a location system for using the addresses provided by the statistics collection and/or aggregation system to locate the nodes identified by the statistical information, and thereby use this information to link the statistics to the map. At step 1040, the operational scenario overlays the map using the compiled statistics. It should be understood that the compilation of statistics can be performed by a messaging system, by a messaging filtering system, by a messaging client, or by any other suitable mechanisms by which statistics can be collected regarding the data traffic flow. The operational scenario then sends the generated map to for display to a user, as shown by step 1050.

The operational scenario then determines whether input from the user has been received in step 1060. If the operational scenario determines that input from the user has been received, the operational scenario instructs the map generation system to perform the action requested by the user. It should be understood that the action requested by the user can include, in various example systems an methods, zooming in on a location, zooming out from a location, zooming in on a traffic flow, zooming out on a traffic flow, separating traffic flows based upon the characteristics of individual data stream included

in the traffic flow, combining individual streams to show an overall traffic flow, among many others. The operational scenario then returns to generate a map (1030) and overlay compiled statistics onto the map (1040) and send the map for display to a user (1050), as shown by step 1070.

If the operational scenario determines that no input from the user has been received in step 1060, the operational scenario then determines whether an exit command has been received at step 1080. If no exit command has been received, the operation scenario waits until it is determined that an exit command has been received or that an input from the user has been received. Upon determining that an exit command has been received from the user, the operational scenario ends at step 1090.

FIG. 11 depicts an example of an graphical user interface window representation 1100 upon which a user can view and interact with systems and methods of this disclosure. The graphical user interface window representation 1100 can depict in one example a map of the United States, including traffic flowing through a messaging system that is configured to supply statistics to a map generator. The graphical user interface window representation 1100 of this example shows hypothetical messaging traffic flowing through a messaging system in Atlanta, GA. Moreover, the graphical user interface window representation 1100 can include some sort of notation indicating the level of traffic passing between the displayed nodes. In the example of graphical user interface window representation 1100, the level of traffic is indicated by the thickness of the line. However, it should be understood that there are other ways to depict the level of traffic. For example, among others, traffic level could be color coded using, for example, red, for high messaging traffic, green for average levels of traffic, and blue for low levels of traffic. It should be understood, however, that these are merely examples of ways to

indicate messaging traffic levels, and that there are myriad other ways to indicate messaging traffic levels, each of which is intended to be included within the scope of the present disclosure. It should be noted that including every node with which the messaging system communicates can be done, however, the display of such information can be too busy. Some examples of systems and methods of this disclosure can obviate this problem by, for example, depicting states on the map in a color coded manner, to indicate a level of traffic coming from the entire state, rather than a particular node located within that state.

FIG. 12 depicts another example of an graphical user interface window representation 1200 which a user can utilize to view and interact with systems and methods of this disclosure. The graphical user interface window representation 1200 can depict in one example a map showing a regional breakdown of traffic, including traffic flowing through a messaging system that is configured to supply statistics to a map generator. The graphical user interface window representation 1200 of this example shows hypothetical messaging traffic flowing through a messaging system in Atlanta, GA to points located within the southeastern United States. Moreover, the graphical user interface window representation 1200 can include some sort of notation indicating the level of traffic passing between the displayed nodes. In the example of graphical user interface window representation 1200, the level of traffic is indicated by the thickness of the line. However, it should be understood that there are other ways to depict the level of traffic. For example, among others, traffic level could be color coded using, for example, red, for high messaging traffic, green for average levels of traffic, and blue for low levels of traffic. It should be understood, however, that these are merely examples of ways to indicate messaging traffic levels, and that there are myriad other ways to indicate

messaging traffic levels, each of which is intended to be included within the scope of the present disclosure.

FIG. 13 depicts another example of an graphical user interface window representation 1300 which a user can utilize to view and interact with systems and methods of this disclosure. The graphical user interface window representation 1300 can depict in one example a map showing a regional breakdown of traffic, including traffic flowing through a messaging system that is configured to supply statistics to a map generator. The graphical user interface window representation 1300 of this example shows hypothetical messaging traffic flowing through a messaging system in Atlanta, GA to points located within the southeastern United States. Further, the graphical user interface window representation 1300 depicts characteristics of the traffic flowing between Raleigh, NC and Atlanta, GA. While traffic characteristics in this example show the types of traffic indicated as separated lines, in various other example systems and methods, the traffic could be color codes to represent the various types of traffic. Moreover, the graphical user interface window representation 1300 can include some sort of notation indicating the level of the traffic types passing between the displayed nodes. In the example of graphical user interface window representation 1300, the level of a traffic type is indicated by the thickness of the line. However, it should be understood that there are other ways to depict the level of a traffic type. For example, among others, traffic level could be color coded using, for example, red, for high messaging traffic, green for average levels of traffic, and blue for low levels of traffic. It should be understood, however, that these are merely examples of ways to indicate messaging traffic levels, and that there are myriad other ways to indicate messaging traffic levels, each of which is intended to be included within the scope of the present disclosure.

A number of embodiments of this disclosure have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention.

CLAIMS

1. A system configured to graphically display message traffic in a geographical context, the system comprising:

a communications interface configured to link the system with an electronic communication network;

a system data store configured to store statistical information related to electronic communications, data associated therewith, configuration data or combinations thereof;

a system processor in communication with the interface, the system data store and endpoints, the system processor comprising one or more processing elements, wherein the one or more processing elements are programmed or adapted to:

receive electronic communications having headers, the headers containing source and destination addresses;

parse the source and destination addresses associated with the electronic communications;

convert source and destination addresses into a geographical position;

assemble statistical information based upon at least the source and destination addresses of at least a sample of electronic communications received at the communications interface, and to store the statistical information in the system data store;

provide a graphical user interface component comprising a geographical information pane configured to display a geographical map to a user via a display device;

a map generator configured to generate the geographical map for use by the graphical user interface based upon user input, the map generator being further configured to overlay statistical information onto the geographical map to show an electronic traffic flow associated with the source and destination addresses of at least the sample of electronic communications.

2. The system of claim 1, wherein the graphical user interface component is further configured to receive input from the user and communicate the input to the map generator, the map generator being configured to generate a new map based upon the user input and send the new map to the graphical user interface component for display to the user.

3. The system of claim 2, wherein the input requests for the new map to focus on a particular portion of the geographical map.

4. The system of claim 3, wherein the input requests more information on a particular traffic flow displayed as part of the geographical map; wherein the map generator is further operable to provide more detailed focus upon a particular traffic flow based upon the user input.

5. The system of claim 4, wherein details about the particular traffic flow can be obtained by hovering over the traffic flow on a new map.

6. The system of claim 1, further comprising a message classification system configured to classify electronic communications and filter those electronic communications that violate at least one of a spam policy, a security policy, a virus policy, a compliance policy, an encryption policy, or combinations thereof.

7. The system of claim 6, wherein the statistical information assembled based upon the electronic communications includes statistics related to the classification of the electronic communications by the message classification system.

8. The system of claim 7, wherein the map generation further comprises separating the electronic traffic flow between two nodes into multiple flows, each flow characterizing a different classification of message.

9. The system of claim 8, wherein each of the multiple traffic flows is color coded according to the classification of traffic it represents.

10. The system of claim 8, wherein the input from the user includes a specific point of origination or destination to display.

11. The system of claim 8, wherein the display is accompanied by an audio depiction associated with the geographical map or traffic flows.

12. The system of claim 7, wherein the map generator is further operable to display message classification statistics when a user hovers a mouse pointer

representation over a particular traffic flow for which the message classification statistics are requested.

13. A computer implemented method for graphically displaying data traffic in a geographical context, comprising the steps of:

receiving a plurality of electronic communications, the electronic communications having source and destination addresses associated with the communications;

parsing the source and destination addresses associated with the electronic communications;

converting the source and destination addresses into a geographical position;

assembling statistical information based upon at least the source and destination addresses of at least a sample of electronic communications received at the communications interface;

storing the statistical information in the system data store;

generating a geographical map;

displaying the geographical map to a user; and

overlaying the geographical map with traffic information based upon the statistical information and geographical position associated with the statistical information.

14. The method of claim 13, further comprising the steps of:

receiving input from the user; and

adjusting the display based upon input from the user.

15. The method of claim 14, wherein adjusting the display comprises:

adjusting the boundaries of the geographical map based upon the input from the user;

displaying the adjusted geographical map to the user; and

overlaying the adjusted geographical map with traffic information based upon the statistical information and geographical position associate with the statistical information.

16. The method of claim 15, wherein adjusting the boundaries of the geographical map based upon the input from the user comprises zooming in on a selected portion of the map, the selected portion of the map being based upon the user input.

17. The method of claim 15, wherein adjusting the boundaries of the geographical map based upon input from the user comprises panning towards a selected portion of the geographical map, the selected portion of the map being based upon the user input.

18. The method of claim 14, wherein adjusting the display comprises zooming in on a selected traffic flow, the selected traffic flow comprising traffic between two nodes, and being based upon the user input.

19. The method of claim 18, wherein upon selection of a traffic flow, the selected traffic flow is separated into component parts, thereby enabling a user to review more detailed information about the selected traffic flow.

20. The method of claim 19, wherein a selected traffic flow comprises a plurality of traffic flow subsets related by a common component, and wherein the traffic flow subsets can be selected to reveal further subsets of traffic flow.

21. The method of claim 20, wherein the smallest level of granularity for selection is an individual electronic communication.

22. The method of claim 14, wherein the input from the user comprises hovering a mouse pointer representation over a selected traffic flow, and adjusting the display comprises displaying a dialog box representation showing statistics related to the selected traffic flow.

23. The method of claim 13, further comprising the step of receiving input from a user, wherein the generated map is based upon the input received from the user.

24. The method of claim 23, wherein the input received from the user specifies an internet protocol address, and the generated map and statistical information focuses on traffic involving the specified internet protocol address.

25. The method of claim 13, wherein the plurality of electronic communications comprise information collected from a plurality of sensors distributed on the Internet.

26. The method of claim 13, wherein the step of converting comprises using a location program to determine the physical location of an address.

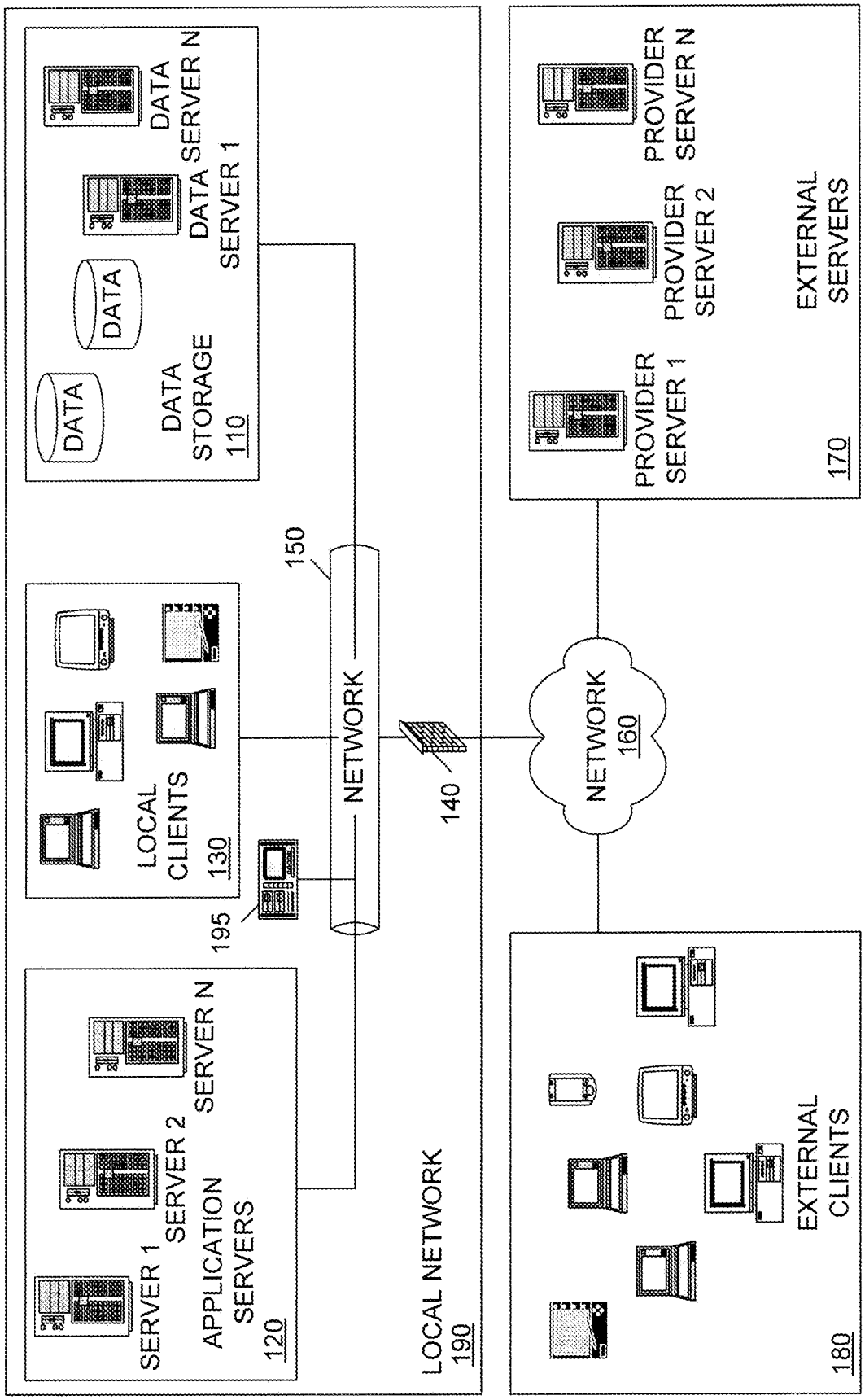
27. The method of claim 13, further comprising:

receiving input from the user comprising one or more geographical or internet protocol addresses; and

retrieving statistic associated with the one or more geographical or internet protocol addresses input by the user;

wherein the geographical map and the overlay are based upon the one or more geographical or internet protocol addresses received from the user.

FIG. 1


DATA
DATA
DATA
DATA SERVER N
DATA SERVER 1
DATA STORAGE 110
LOCAL CLIENTS 130
195
150
NETWORK
140
NETWORK 160
PROVIDER SERVER 1
PROVIDER SERVER 2
PROVIDER SERVER N
EXTERNAL SERVERS 170
SERVER 1
SERVER 2
SERVER N
APPLICATION SERVERS 120
LOCAL NETWORK 190
EXTERNAL CLIENTS 180

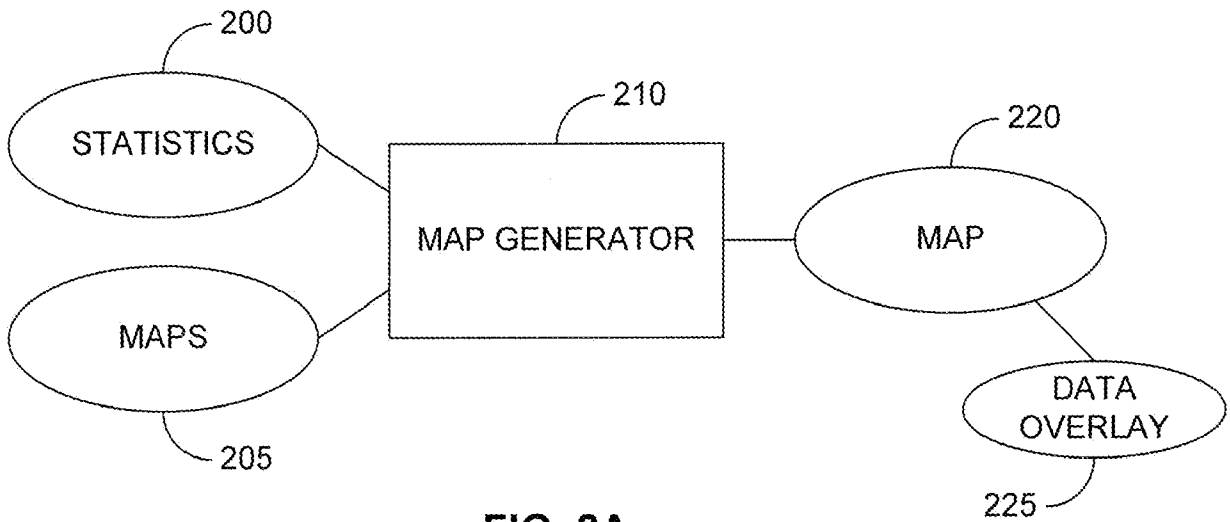

200
STATISTICS
210
MAP GENERATOR
220
MAP
MAPS
DATA
OVERLAY
205
225

FIG. 2A

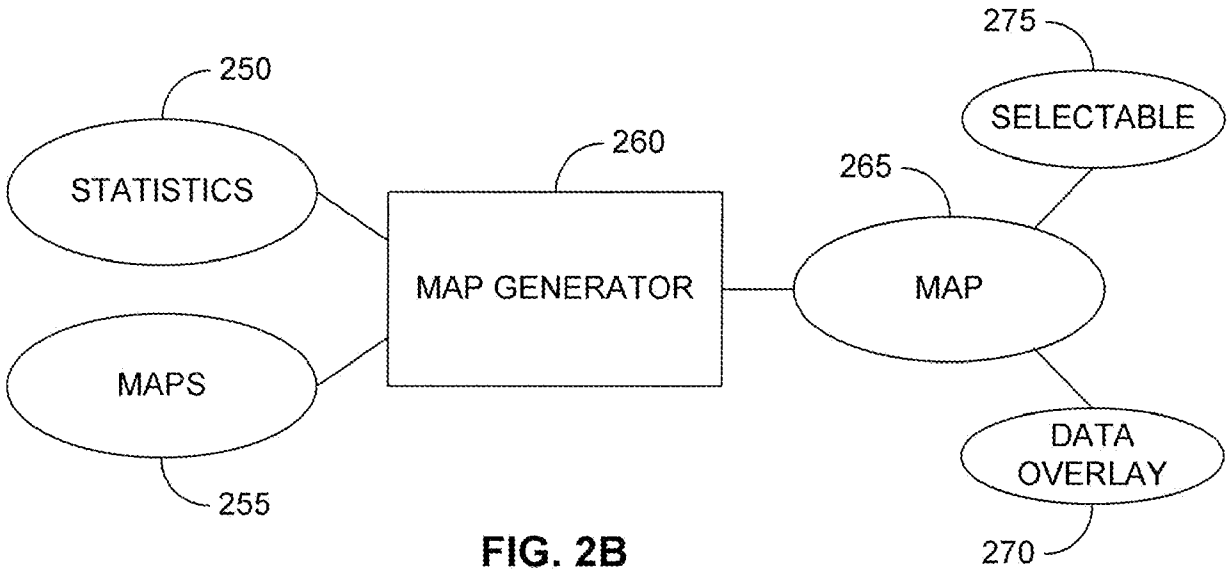

250
STATISTICS
MAPS
255
260
MAP GENERATOR
265
MAP
275
SELECTABLE
DATA
OVERLAY
270

FIG. 2B

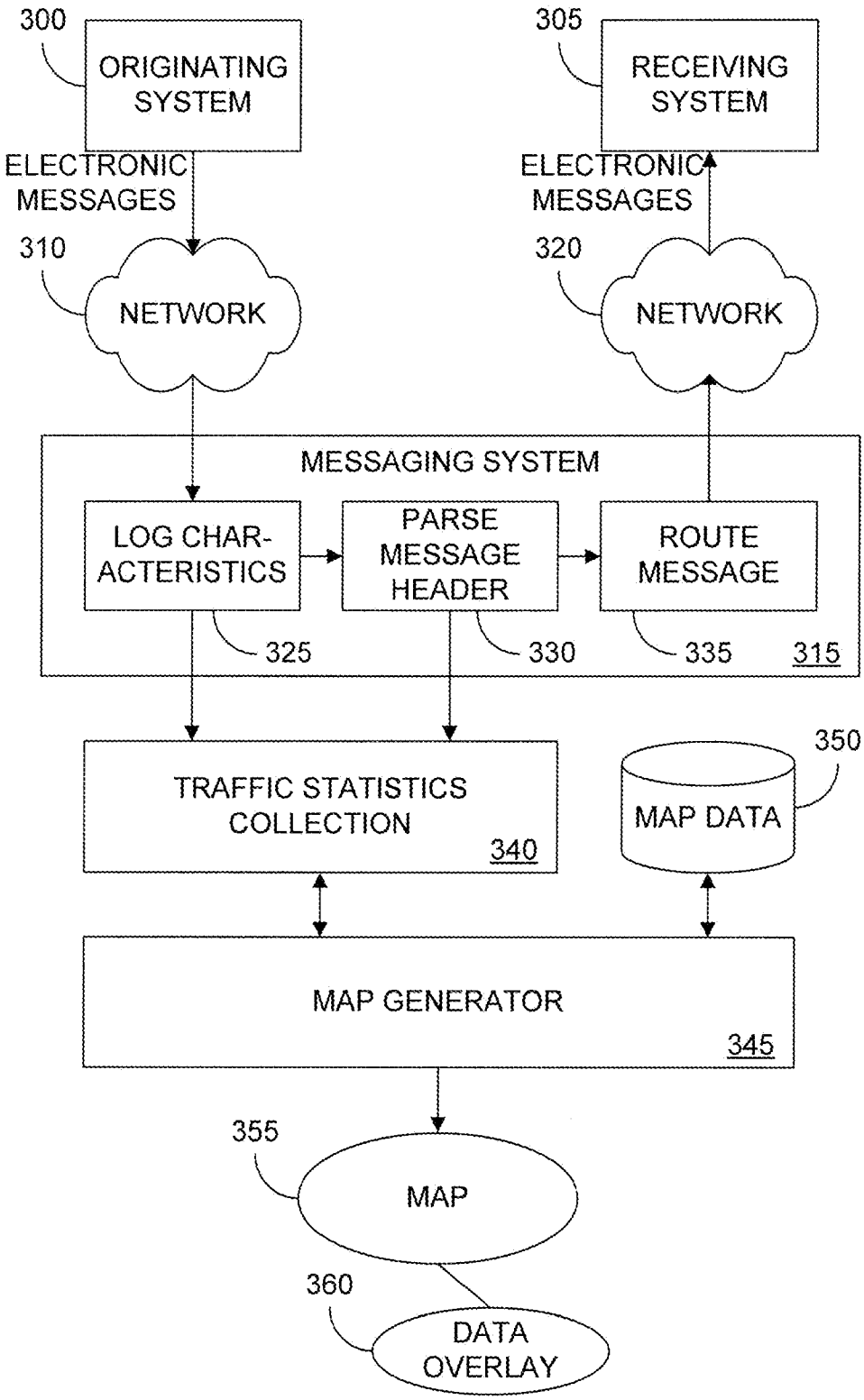

300
ORIGINATING SYSTEM
305
RECEIVING SYSTEM
ELECTRONIC MESSAGES
ELECTRONIC MESSAGES
310
NETWORK
320
NETWORK
MESSAGING SYSTEM
LOG CHAR-ACTERISTICS
PARSE MESSAGE HEADER
ROUTE MESSAGE
325
330
335
315
TRAFFIC STATISTICS COLLECTION
340
350
MAP DATA
MAP GENERATOR
345
355
MAP
360
DATA OVERLAY

FIG. 3

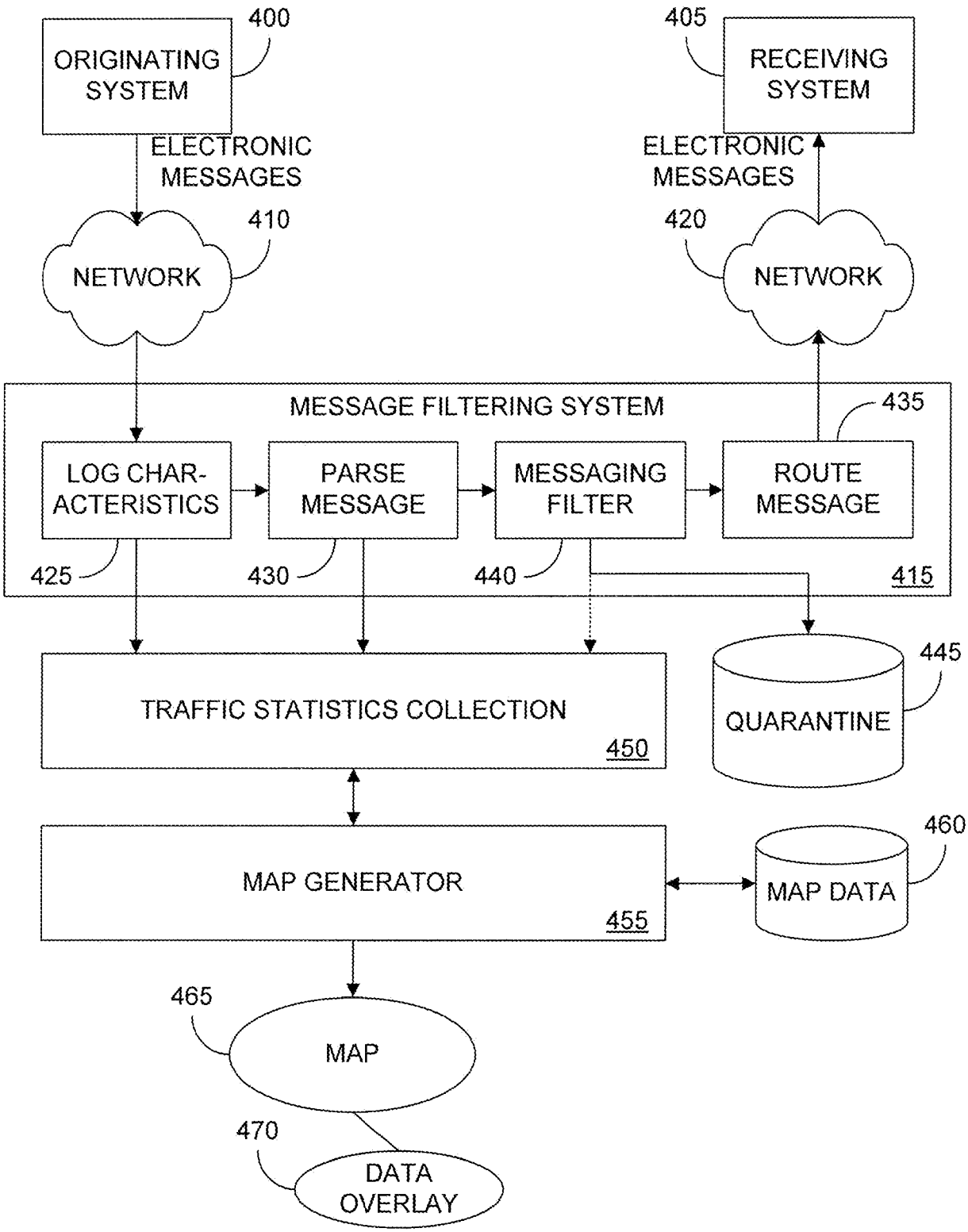

ORIGINATING SYSTEM
400
ELECTRONIC MESSAGES
NETWORK
410
405
RECEIVING SYSTEM
ELECTRONIC MESSAGES
420
NETWORK
MESSAGE FILTERING SYSTEM
435
LOG CHAR-ACTERISTICS
PARSE MESSAGE
MESSAGING FILTER
ROUTE MESSAGE
425
430
440
415
TRAFFIC STATISTICS COLLECTION
450
QUARANTINE
445
MAP GENERATOR
455
MAP DATA
460
465
MAP
470
DATA OVERLAY

FIG. 4

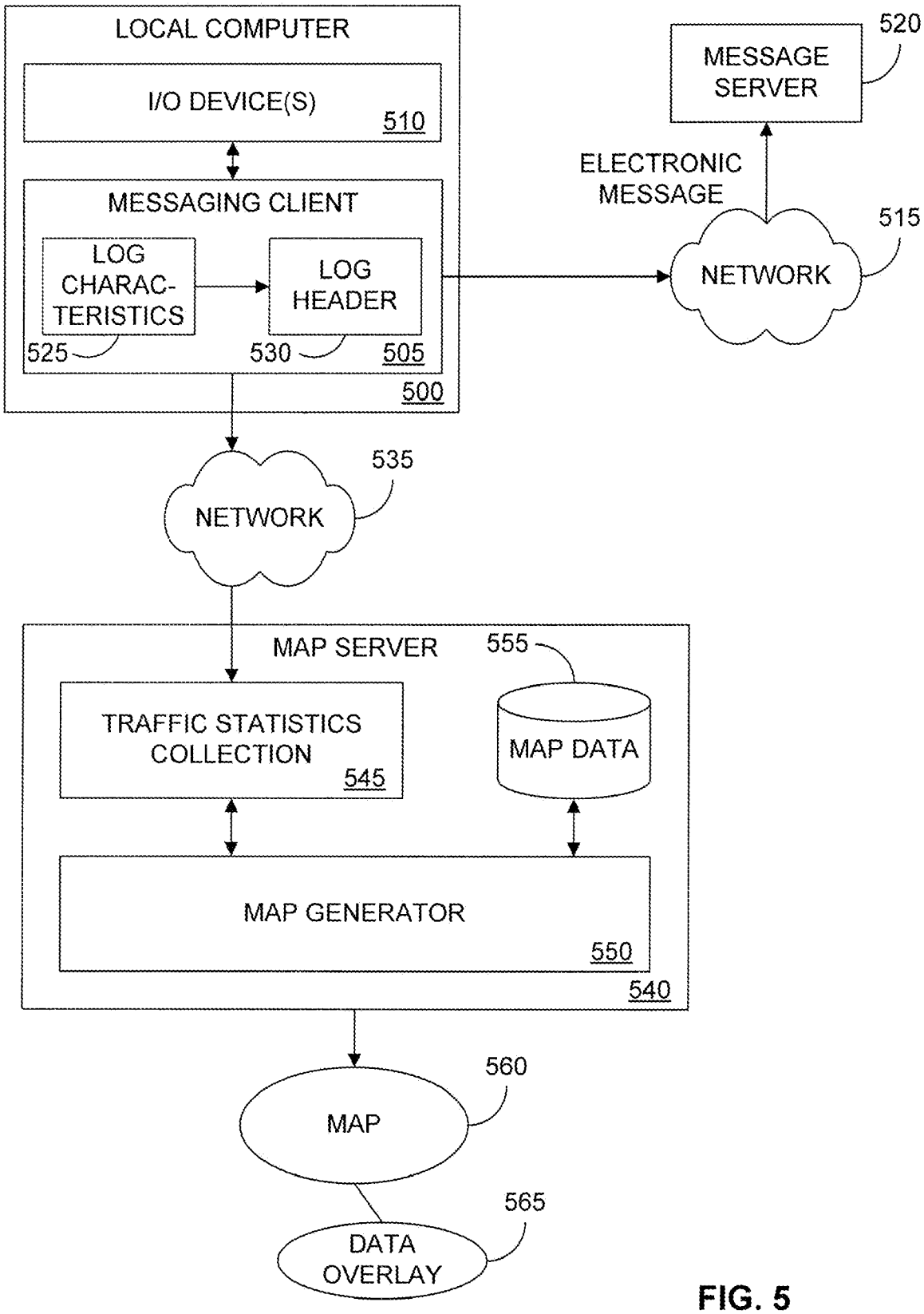

LOCAL COMPUTER
I/O DEVICE(S)
510
MESSAGING CLIENT
LOG CHARAC-TERISTICS
LOG HEADER
525
530
505
500
MESSAGE SERVER
520
ELECTRONIC MESSAGE
NETWORK
515
NETWORK
535
MAP SERVER
555
TRAFFIC STATISTICS COLLECTION
545
MAP DATA
MAP GENERATOR
550
540
MAP
560
DATA OVERLAY
565

FIG. 5

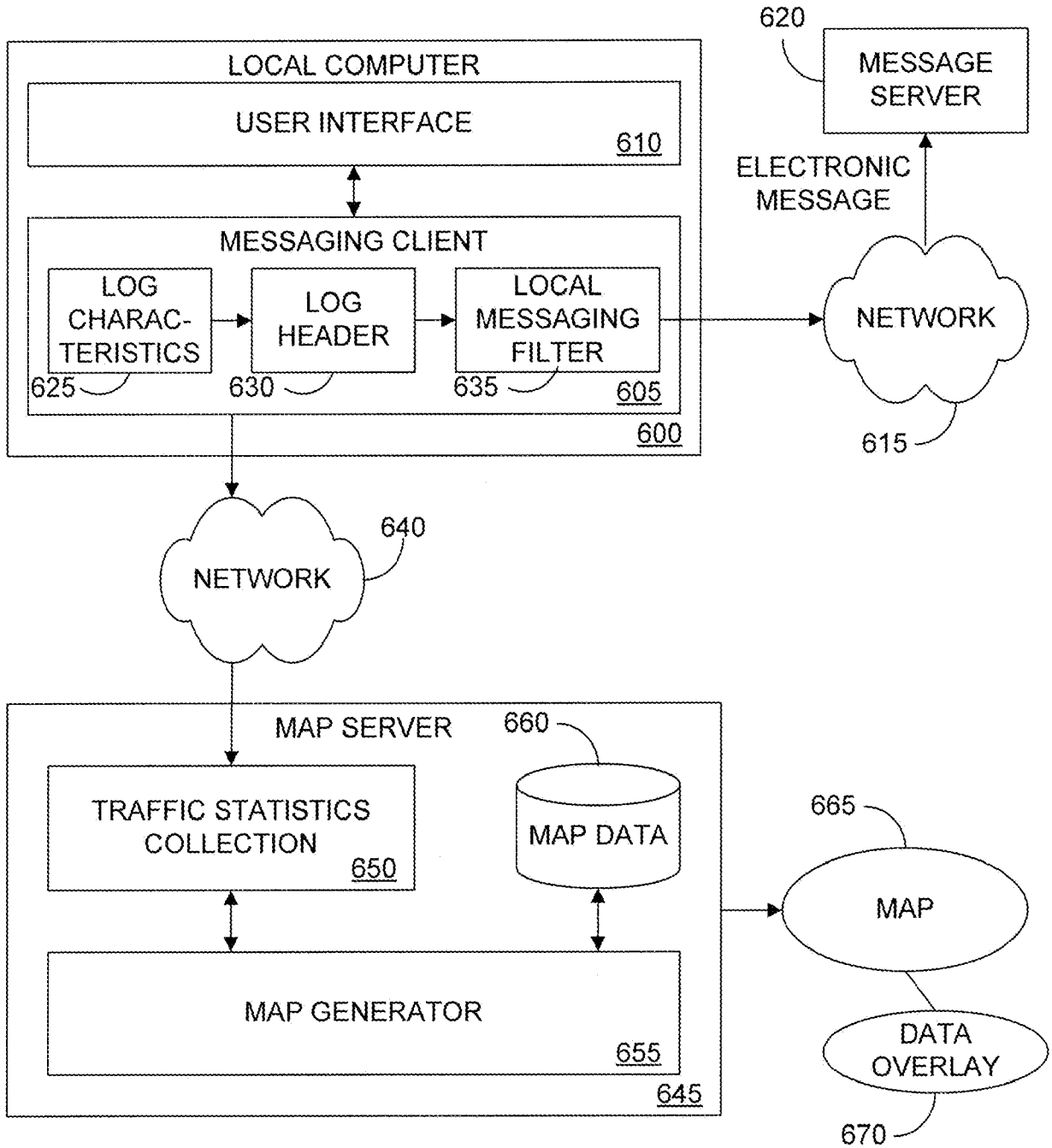

620
MESSAGE SERVER
LOCAL COMPUTER
USER INTERFACE
610
ELECTRONIC MESSAGE
MESSAGING CLIENT
LOG CHARAC-TERISTICS
LOG HEADER
LOCAL MESSAGING FILTER
NETWORK
625
630
635
605
600
615
640
NETWORK
MAP SERVER
660
TRAFFIC STATISTICS COLLECTION
650
MAP DATA
665
MAP
MAP GENERATOR
655
DATA OVERLAY
645
670

FIG. 6

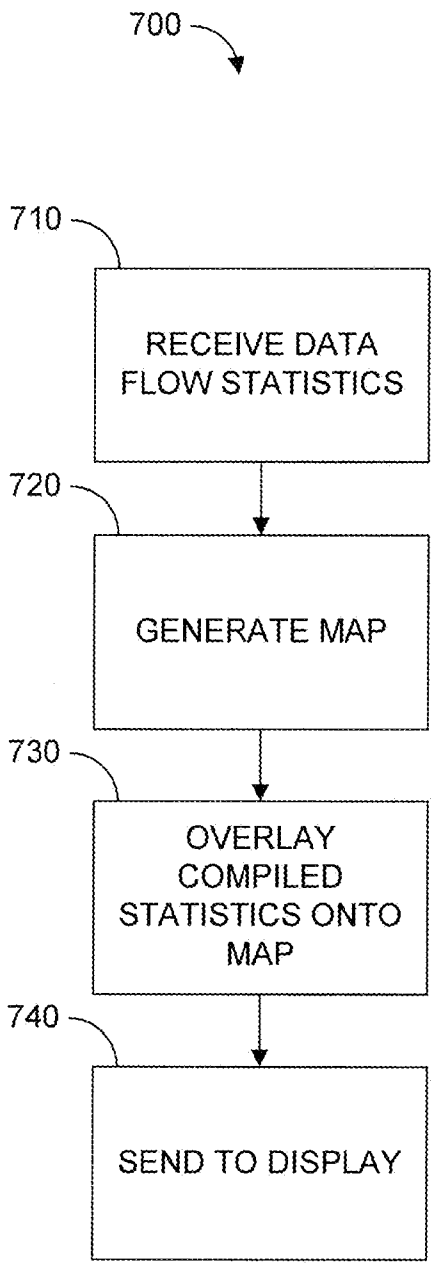

700
710
RECEIVE DATA FLOW STATISTICS
720
GENERATE MAP
730
OVERLAY COMPILED STATISTICS ONTO MAP
740
SEND TO DISPLAY

FIG. 7

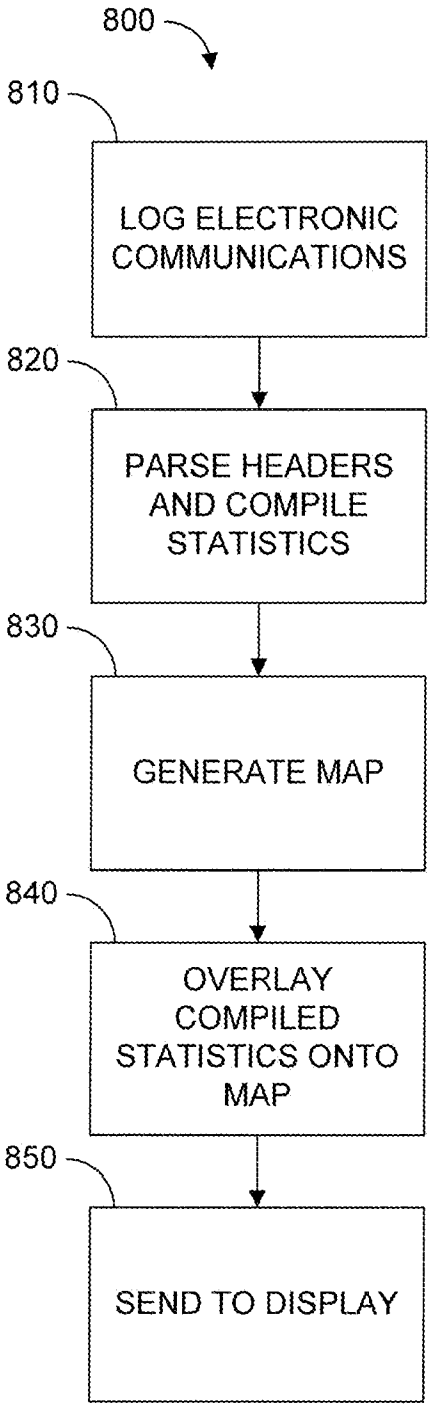

800
810
LOG ELECTRONIC COMMUNICATIONS
820
PARSE HEADERS AND COMPILE STATISTICS
830
GENERATE MAP
840
OVERLAY COMPILED STATISTICS ONTO MAP
850
SEND TO DISPLAY

FIG. 8

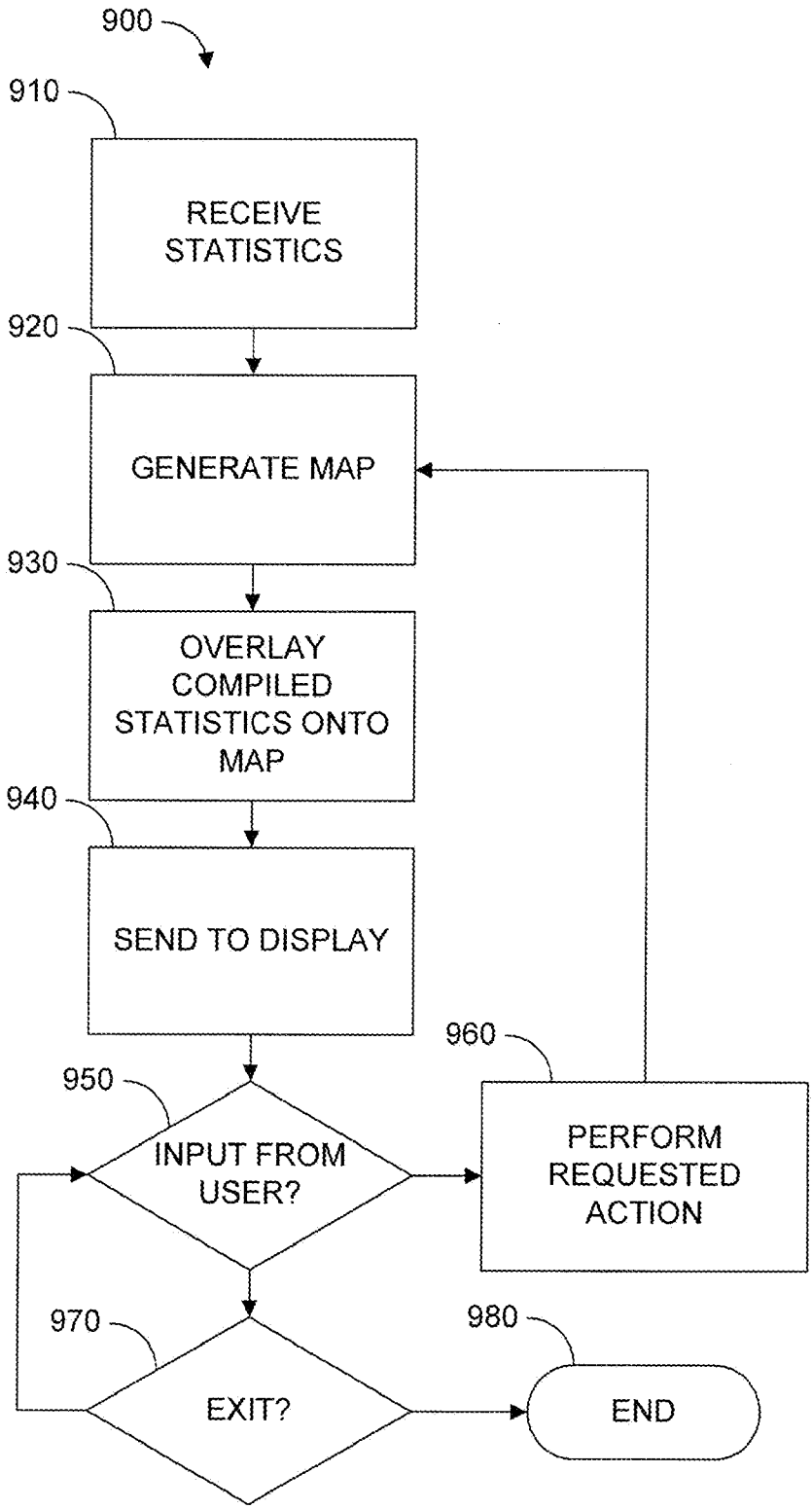

900
910
RECEIVE STATISTICS
920
GENERATE MAP
930
OVERLAY COMPILED STATISTICS ONTO MAP
940
SEND TO DISPLAY
950
INPUT FROM USER?
960
PERFORM REQUESTED ACTION
970
EXIT?
980
END

FIG. 9

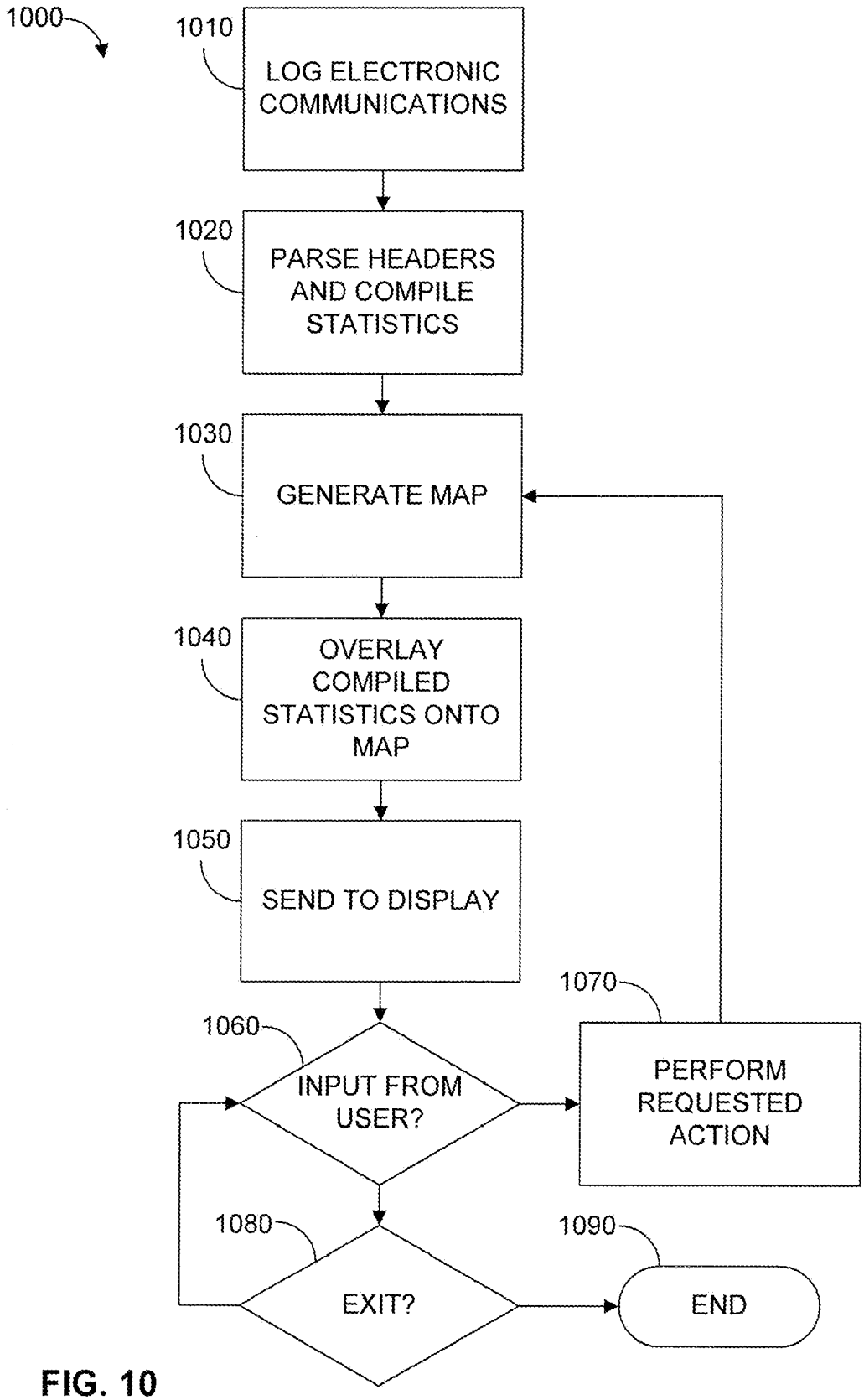

1000
1010
LOG ELECTRONIC COMMUNICATIONS
1020
PARSE HEADERS AND COMPILE STATISTICS
1030
GENERATE MAP
1040
OVERLAY COMPILED STATISTICS ONTO MAP
1050
SEND TO DISPLAY
1060
INPUT FROM USER?
1070
PERFORM REQUESTED ACTION
1080
EXIT?
1090
END

FIG. 10

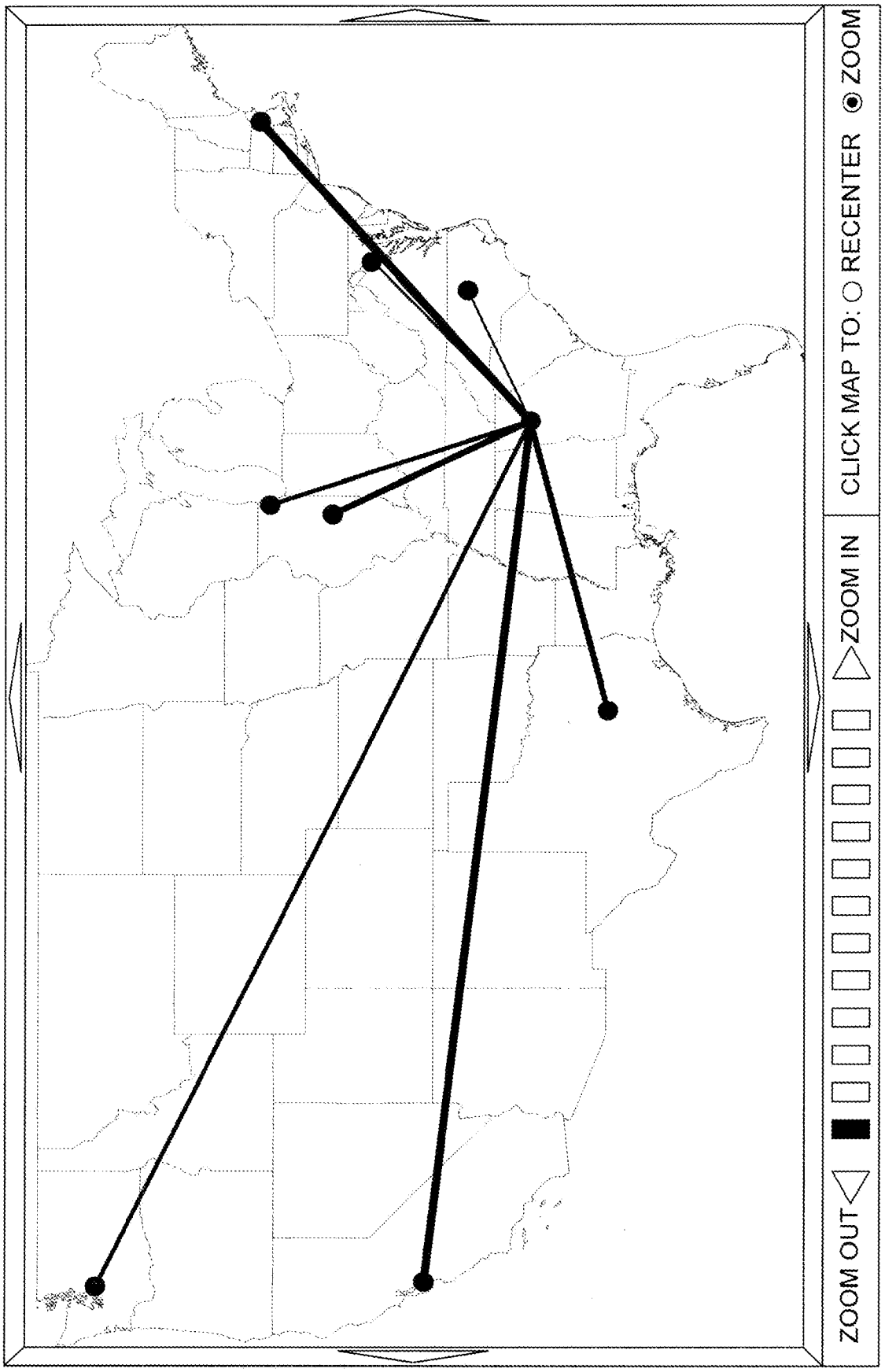


FIG. 11

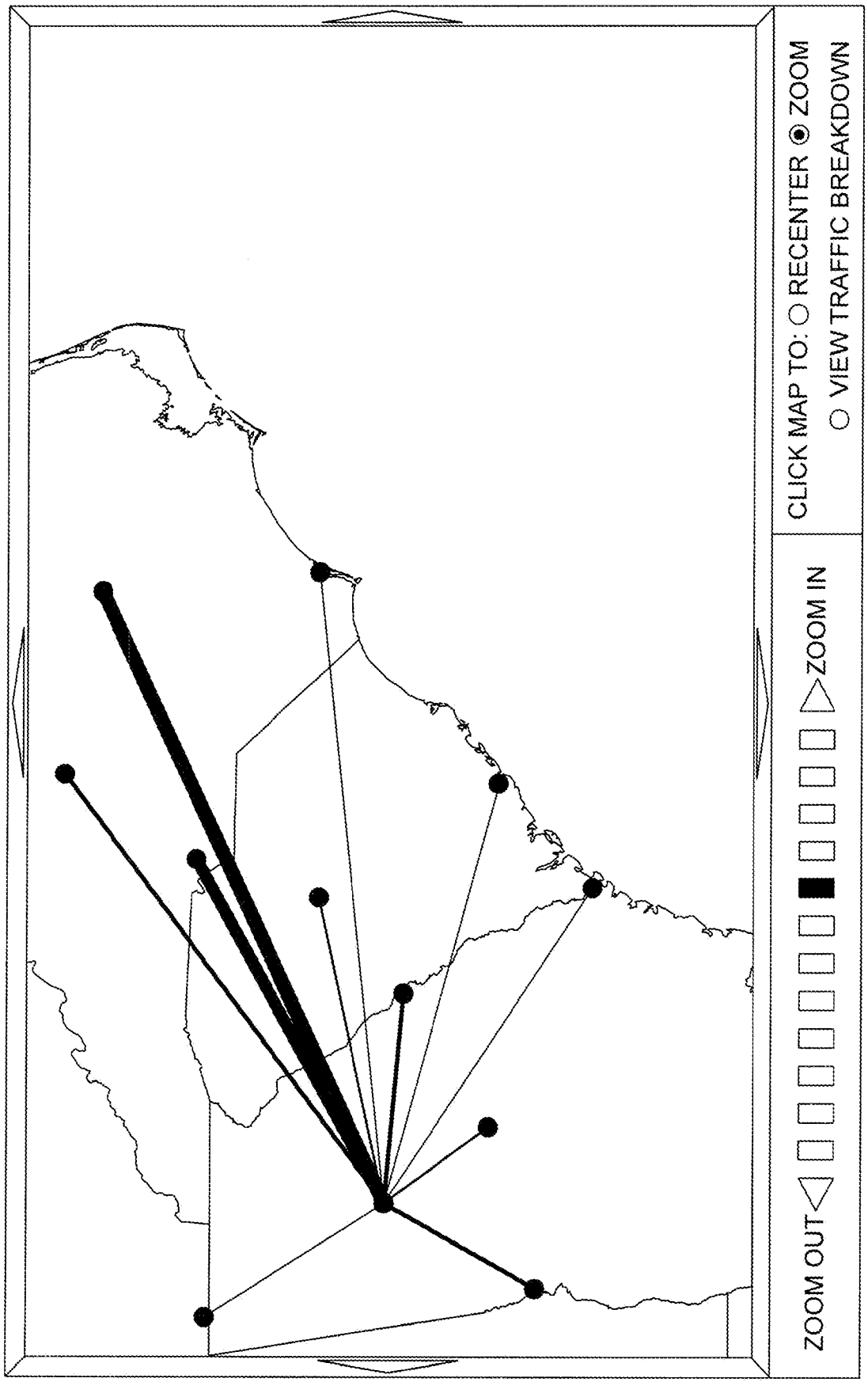

CLICK MAP TO: ○ RECENTER ◉ ZOOM
○ VIEW TRAFFIC BREAKDOWN
ZOOM OUT
ZOOM IN
1200

FIG. 12

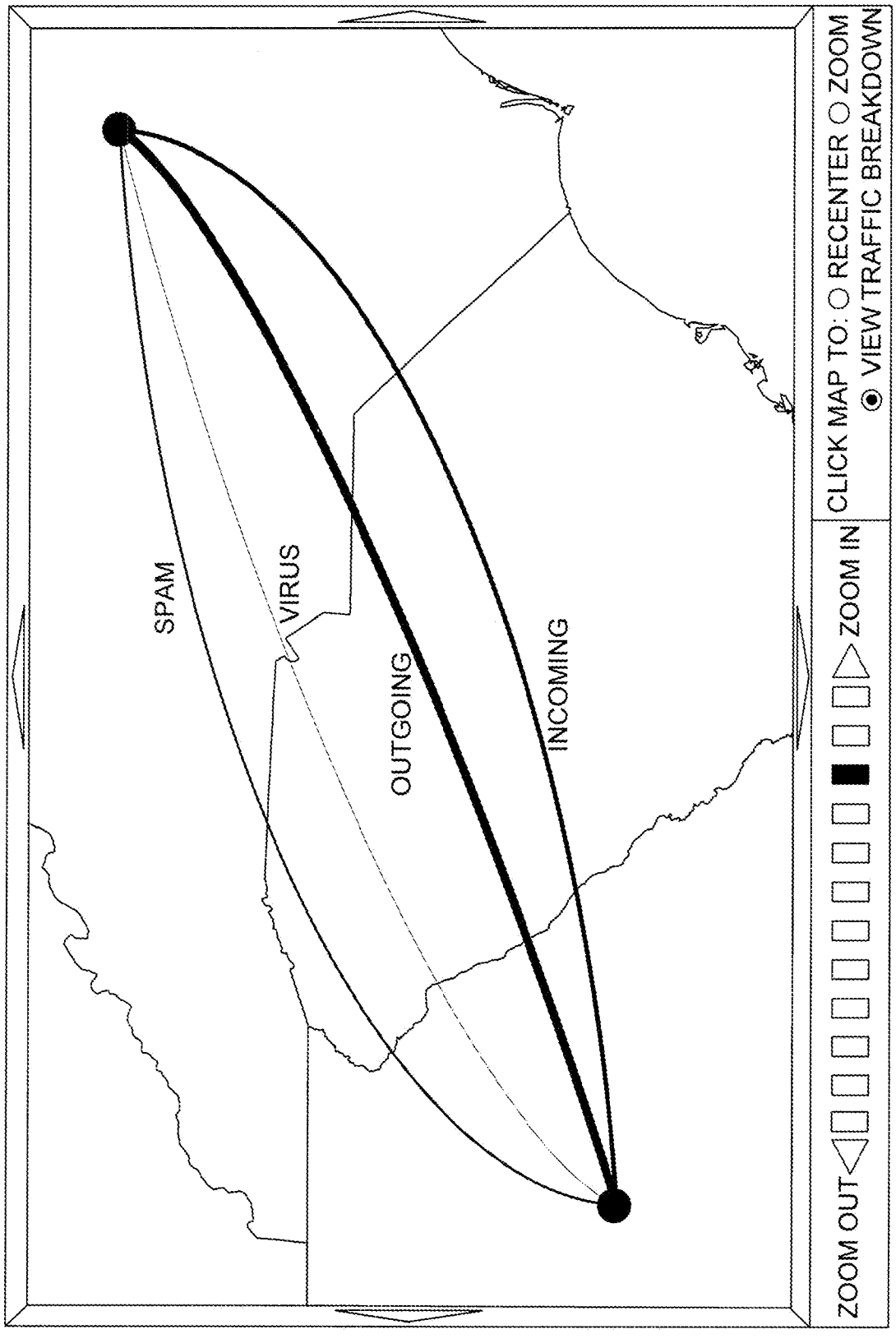

SPAM
VIRUS
OUTGOING
INCOMING
CLICK MAP TO: ○ RECENTER ○ ZOOM
◉ VIEW TRAFFIC BREAKDOWN
ZOOM OUT
ZOOM IN
1300

FIG. 13