UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

GRADIENT ENTERPRISES, INC.,

Plaintiff,

vs.

SKYPE TECHNOLOGIES S.A. and SKYPE, INC.,

Defendants.

FIRST AMENDED COMPLAINT AND JURY DEMAND

Civil Action No.: 10-CV-6712L

Plaintiff, Gradient Enterprises, Inc. ("Gradient" or "plaintiff"), for its first amended complaint against the defendants, Skype Technologies, S.A. ("Technologies") and Skype, Inc. ("Skype") (collectively referred to as "the defendants"), alleges as follows:

PRELIMINARY STATEMENT

1. This is an action brought by Gradient against the defendants for infringement of United States Patent No. 7,669,207 ("the '207 patent"), in violation of the United States Patent Laws 35 U.S.C. § 1 *et seq.*

THE PARTIES

2. Gradient is, and at all times hereinafter mentioned was, a corporation organized and existing under the laws of the State of New York, with its principal place of business located in Rochester, New York.

3. Upon information and belief, Technologies is, and at all times hereinafter mentioned was, a company organized and existing under the laws of the Grand Duchy of Luxembourg.

4. Upon information and belief, Technologies conducts business within the United

States of America and the State of New York, including the Western District of New York.

5. Upon information and belief, defendant Skype is, and at all times hereinafter mentioned was, a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located in San Jose, California.

6. Upon information and belief, Skype conducts business within the United States of America and the State of New York, including the Western District of New York.

JURISDICTION AND VENUE

7. This Court has exclusive jurisdiction over the subject matter of the complaint pursuant to 35 U.S.C. §§ 271 *et seq.* and 28 U.S.C. §§ 1331 and 1338(a).

8. Venue is proper pursuant to 28 U.S.C. § 1400(b).

9. Upon information and belief, each of the defendants has sufficient contacts with the United States District Court for the Western District of New York to support the exercise of personal jurisdiction and the preservation of venue within this District.

U.S. PATENT NO. 7,669,207

10. On February 23, 2010, the '207 patent entitled "Method for Detecting, Reporting and Responding to Network Node-Level Events and a System Thereof" was issued by the United States Patent and Trademark Office (a copy of the '207 patent is attached hereto as **Exhibit "1"**).

11. Gradient is the lawful owner of and owns all right, title, and interest to the '207 patent and has the sole and exclusive right to exclude others from making, using, selling and offering for sale any and all systems, computer-readable media and methods covered by the '207 patent.

12. The '207 patent relates to a method, computer-readable medium and system for detecting, reporting and responding to network events in any environment which requires a

control structure where a distributed architecture is appropriate to the application scale. (Col. 7, lines 4-15).

13. The '207 patent includes three independent claims and thirty-six dependent claims.

14. Independent claim 1 of the '207 patent is directed to:

> A method for detecting, reporting, and responding to network node-level occurrences on a network-wide level, wherein the method comprises:
>
> providing a plurality of mobile agents, each of the mobile agents hosted by one of a plurality of nodes in the network which each detect for one or more events;
>
> designating one of the mobile agents hosted at one of the nodes as a controlling mobile agent;
>
> designating another one of the mobile agents hosted at another one of the nodes as the controlling mobile agent when the mobile agent previously designated as the controlling mobile agent is unavailable;
>
> communicating network event information associated with an event detected at one or more of the nodes in the network to the controlling mobile agent; and
>
> disseminating from the controlling mobile agent information describing the detected event to one or more other nodes.

15. Independent claim 14 of the '207 patent is directed to:

> A computer-readable medium having stored thereon instructions for detecting, reporting and responding to network node-level occurrences on a network-wide level, which when executed by at least one processor, causes the processor to perform:
>
> providing a plurality of mobile agents, each of the mobile agents is hosted by one of a plurality of nodes in a network which each detect for one or more events;
>
> designating one of the mobile agents hosted at one of the nodes as a controlling mobile agent;
>
> designating another one of the mobile agents hosted at another one of the nodes as the controlling mobile agent when the one of the mobile agents previously

designated as the controlling mobile agent is unavailable;

communicating network event information associated with an event detected at one or more of the nodes in the network to the controlling mobile agent; and

disseminating from the controlling mobile agent information describing the detected event to one or more other nodes.

16. Independent claim 27 of the '207 patent is directed to:

A system for detecting, reporting and responding to network node-level occurrences on a network-wide level, wherein the system comprises:

a plurality of mobile agents, each of the mobile agents is hosted by one of a plurality of nodes in a network which each detect for one or more events;

a designation system that designates one of the mobile agents hosted at one of the nodes as a controlling mobile agent and designates another one of the mobile agents hosted at another one of the nodes as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is unavailable;

an event detection system that communicates network event information associated with an event detected at one or more of the nodes in the network to the controlling mobile agent; and

a reporting system that disseminates from the controlling mobile agent information describing the detected event to one or more other nodes.

17. Dependent claims 2-13, 15-26 and 28-39 in the '207 patent depend either directly or indirectly from independent claims 1, 14 and 27 in the '207 patent, respectively, and are directed to additional aspects of the inventions set forth therein.

THE SKYPE SYSTEM

18. Upon information and belief, Defendants manufacture, use, sell and offer to sell in the United States a peer-to-peer Voice over Internet Protocol ("VoIP") communication system, which includes, but is not limited to, Skype software versions 5.0.0.152, 0.97.0.6, and similar

versions ("the Skype Software").

19. Upon information and belief, the Skype Software includes, *inter alia*: 1) peer-to-peer VoIP service, video communications, file transfer and chat facility between users of Skype Software; 2) "Add a Contact" feature, 3) "Edit Your Profile" and "Change Your Picture" features,; 4) Skype status designation feature; and 5) a feature that launches Skype Software (collectively, "the Skype Features").

20. Upon information and belief, Defendants connect users of the Skype Software ("Skype users") and control the execution, realization and performance of the Skype Features using the Skype Software and network systems, portals, servers, devices and channels ("the Skype Network").

21. Upon information and belief, the peer-to-peer VoIP service and video communications provided by the Skype Network allow a Skype user to establish a connection with another Skype user listed in a contacts list to allow for voice, video communication, chat and/or file transfer.

22. Upon information and belief, the "Add a Contact" feature in the Skype Software is configured for allowing a Skype user to provide a person's name, email address, phone number and/or Skype name to search for another Skype user using the Skype Network.

23. Upon information and belief, "Edit Your Profile" and "Change Your Picture" features provided in the Skype Software allow a Skype user to enter or update his or her personal information, including, but not limited to, first and/or last name, picture, telephone number, e-mail address, geographic location, website address, gender, birth date, language, and/or a description about himself or herself, wherein the Skype Network communicates the entered or updated personal information to the Skype users that are listed in his or her contacts list.

24. Upon information and belief, the Skype status designation feature provided by the Skype Software allows a Skype user to update his or her availability on the Skype Network by selecting an appropriate status designation icon, such as "Online" (green icon), "Away" (yellow icon), and "Do Not Disturb" (red icon), wherein the Skype Network communicates his or her availability on the Skype Network to the Skype users in his or her contacts list.

25. Upon information and belief, after launching of the Skype Software, the features of the Skype Software are made available to a user upon entry of a valid "Skype Name" and "Password" in data fields provided in a start-up window; upon entry of a valid "Skype Name" and "Password" in the start-up window, the Skype Network updates the Skype status designation for the Skype users in his or her contacts list and the Skype Software displays the appropriate status designation icon.

26. Under its "Terms of Service" requirements and as consideration for the services which defendants provide without charge, defendants charge for various other services associated with the use of its peer-to-peer communication system for which the Skype users are required to establish a Skype User Account, also referred to by Skype as "Skype Credit."

27. Under its "End User License Agreement" and as consideration for the services which defendants provide without charge, defendants require their users to allow the Skype Software to utilize the processor and bandwidth of the Skype user's computer or other applicable device to facilitate communications between users of the Skype Software so that their computers become part of the Skype Network.

DEFENDANTS' INFRINGEMENT OF THE '207 PATENT

28. Upon information and belief, the Skype Network provides a method and system that detects, reports, and responds to node-level occurrences on a network-wide level.

29. Upon information and belief, a node-level occurrence in the Skype Network the initiation of one or more of the Skype Features, such as, but not limited to: (1) selecting a Skype user listed in a contacts list in order to establish a connection with the selected Skype user to communicate by voice and/or video; (2) selecting the "Add a Contact" feature to search for another Skype user; (3) selecting the "Edit Your Profile" or "Change Your Picture" feature to allow a Skype user to enter or update his or her personal information, such as, but not limited to, first and/or last name, picture, telephone number, e-mail address, geographic location, website address, gender, birth date, language, and/or a description about himself or herself; (4) displaying the available Skype status designation icons; or (5) loading the Skype Software to display a start-up window that provides data fields to allow for the entry of a "Skype Name" and "Password."

30. Upon information and belief, the Skype Network includes a plurality of mobile agents in the form of copies of the Skype Software, wherein each copy of the Skype Software is hosted by one or more of a plurality of nodes ("Skype Client"), such as a personal computer or other applicable device in the Skype Network which each detect for one or more events.

31. Upon information and belief, one or more events in the Skype Network include the use of one or more of the Skype Features, including, but not limited to: (1) the initiation of voice and/or video communication with a Skype user listed in a contact list by clicking on a "Call" or "Video Call" button in Skype Client; (2) the initiation of a Skype user search by entering a person's name, email address, phone number and/or Skype name in one or more data fields provided in Skype Client; (3) entering or updating personal information of a Skype user by selecting the "Edit Your Profile" or "Change Your Picture" features, such as uploading a digital photograph to Skype Network using Skype Client; (4) updating the status designation with an appropriate icon using the Skype status designation feature, such as, for example, a yellow icon

indicating that the Skype user is "Away;" or (5) entry of a valid "Skype Name" and "Password" in the start-up window of Skype Client.

32. Upon information and belief, Skype Network includes a designation system that designates one of the Skype Clients as a controlling Skype Client ("Supernode") so long as it is available; when the designated Supernode is no longer available for use, Skype Network designates another Skype Client as a Supernode.

33. Upon information and belief, the Skype Software includes an event detection system at one or more of the nodes that communicates network event information associated with the use of one or more of the Skype Features detected at one or more of the nodes in the Skype Network to the Supernode.

34. Upon information and belief, network event information in the Skype Network includes, but is not limited to: (1) the name and/or other information associated with the Skype user that was selected for voice and/or video communication using Skype Client; (2) the person's name, email address, phone number and/or Skype name that was entered in the one or more data fields provided in Skype Client during the Skype user search; (3) the entered or updated personal information provided using the "Edit Your Profile" or "Change Your Picture" features; (4) the status designation that was updated using the Skype status designation feature; or (5) the name and/or other information associated with the one or more Skype users that are in the list of contacts of the Skype user that provided the valid "Skype Name" and "Password."

35. Upon information and belief, the Skype Network includes a reporting system that disseminates from the Supernode information describing the detected event to one or more other nodes in the Skype Network.

36. Upon information and belief, the Skype Software is stored on a computer readable

medium, such as, but not limited to, a memory included in at least one server that is owned, controlled, possessed, managed, operated or enlisted by defendants, and the Skype Software is sold, offered for sale, and made available to third-parties through the Internet for download on to a memory included in a computing device owned, controlled, possessed, managed, or operated by such third-parties, wherein the computing device includes a processor capable of processing instructions.

37. Upon information and belief, Skype Software is included or otherwise made available on televisions, personal computers, notebook computers, tablets and mobile handheld devices, such as mobile phones, tablets or mobile gaming devices, as an executable application, firmware and/or as a mobile application.

38. Upon information and belief, the defendants knew or should have known about the '207 patent as it (1) has been a matter of public record since February 23, 2010, (2) addresses the important concept of controlling mobile agents or supernodes, (3) would have been identified as part of the due diligence process leading up to the discontinued public offering undertaken by Skype in 2010 and/or the eventual sale of a controlling interest in Skype to Microsoft, Inc. in 2011 and (4) should have been identified by the defendants or Microsoft, Inc as part of their ongoing effort to identify and, possibly, acquire intellectual property in the computer technology and Internet sectors.

39. Defendants were also put on notice of the "207 patent and the plaintiff's infringement claims as a result of the significant media attention given to the filing of the Complaint on December 21, 2010 and, in particular, the articles which appeared on various Internet news sites and reported (erroneously) that the plaintiff's action was commenced in response to the extensive outage and disruption in the Skype Network which occurred on

December 22 and 23, 2010.

40. Defendants were also put on notice of the '207 patent and their infringement thereof as of the date of service of the originally filed Complaint, on January 14, 2011 and April 14, 2011.

41. Furthermore, the defendants were put on notice of the '207 patent and their infringement thereof no later than April 10, 2012, with their receipt of a letter from plaintiff's counsel, dated April 9, 2012, advising them of the patent and the plaintiff's infringement claims.

AS AND FOR A FIRST CAUSE OF ACTION, PLAINTIFF ALLEGES AS FOLLOWS:

Direct Infringement (35 U.S.C. § 271(a))

42. Gradient repeats and re-alleges the allegations of paragraphs "1" through "41" as if more fully set forth herein.

A. Independent Claim No. 1

43. In violation of 35 U.S.C. § 271, defendants have directly infringed, either literally or under the doctrine of equivalents, and continue to directly infringe, claim 1 of the '207 patent by making, using, selling and/or offering for sale within the United States a method for detecting, reporting and responding to network node-level occurrences on a network-wide level, wherein the node-level occurrences are initiated by of one or more of the Skype Features; in particular, the method (1) provides a plurality of mobile agents in the form of a plurality of Skype Clients, wherein each Skype Client is hosted by one or more of a plurality of nodes (e.g., personal computers) in the Skype Network which each detect for one or more events, such as the use of one or more of the Skype Features; (2) designates one of the Skype Clients hosted at one of the nodes as a Supernode; (3) designates another Skype Client hosted at another one of the nodes as

the Supernode when the previously designated Supernode is unavailable; (4)communicates network event information associated with the use of one or more of the Skype Features detected at one or more of the nodes in the Skype Network to the Supernode; and (5) disseminates from the Supernode information describing the detected event to one or more of the other nodes in the Skype Network.

B. Independent Claim No. 14

44. In violation of 35 U.S.C. § 271, upon information and belief, defendants have directly infringed, either literally or under the doctrine of equivalents, and continue to directly infringe, claim 14 of the '207 patent by making, using, selling and/or offering for sale within the United States a computer-readable medium having stored thereon instructions for detecting, reporting and responding to network node-level occurrences on a network-wide level, wherein the node-level occurrences are initiated by of one or more of the Skype Features; in particular, when the instructions are executed by at least one processor, causes the processor to perform: (1) providing a plurality of mobile agents in the form of a plurality of Skype Clients, wherein each Skype Client is hosted by one or more of a plurality of nodes (e.g., personal computers) in the Skype Network which each detect for one or more events, such as the use of one or more of the Skype Features; (2) designating one of the Skype Clients hosted at one of the nodes as a Supernode; (3) designating another Skype Client hosted at another one of the nodes as the Supernode when the previously designated Supernode is unavailable; (4) communicating network event information associated with the use of one or more of the Skype Features detected at one or more of the nodes in the Skype Network to the Supernode; and (5) disseminating from the Supernode information describing the detected event to one or more of the other nodes in the Skype Network.

C. Independent Claim No. 27

45. In violation of 35 U.S.C. § 271, upon information and belief, defendants have directly infringed, either literally or under the doctrine of equivalents, and continue to directly infringe, claim 27 of the '207 patent by making, using, selling and/or offering for sale within the United States a system for detecting, reporting and responding to network node-level occurrences on a network-wide level, wherein the node-level occurrences are initiated by of one or more of Skype Features; in particular, the system comprises: (1) a plurality of mobile agents in the form of a plurality of Skype Clients, wherein each Skype Client is hosted by one or more of a plurality of nodes (e.g., personal computers) in the Skype Network which each detect for one or more events, such as the use of one or more of the Skype Features; (2) a designation system that designates one of the Skype Clients hosted at one of the nodes as a Supernode and designates another one of the Skype Clients hosted at another one of the nodes as the Supernode when the previously designated Supernode is unavailable; (3) an event detection system that communicates network event information associated with the use of one or more of the Skype Features detected at one or more of the nodes in the Skype Network to the Supernode; and (4) a reporting system that disseminates from the Supernode information describing the detected event to one or more of the other nodes in the Skype Network.

D. Dependent Claims

46. In violation of 35 U.S.C. § 271, upon information and belief, defendants have directly infringed, either literally or under the doctrine of equivalents, and continue to directly infringe, dependent claims 2-13, 15-26 and 27-39 of the '207 patent by making, using, selling and/or offering for sale within the United States the method, computer-readable medium, and system set forth therein.

47. Defendants continue to make, use, sell, and offer to sell systems, computer-readable media and methods that infringe the '207 patent.

48. Gradient has been, and continues to be, damaged as a result of the defendants' infringement within the Western District of New York and elsewhere.

49. Said acts of infringement are willful and deliberate. At a minimum, the defendants have acted recklessly and in disregard of the plaintiff's rights since they first became aware of the '207 patent, as set forth above.

50. As a result of the foregoing, Gradient has been damaged in an amount to be determined by the trier of fact in accordance with 35 U.S.C. § 284.

AS AND FOR A SECOND CAUSE OF ACTION, PLAINTIFF ALLEGES AS FOLLOWS;

Inducement (35 U.S.C. § 271(b))

51. Gradient repeats and re-alleges the allegations of paragraphs "1" through "50" as if more fully set forth herein.

52. Upon information and belief, the defendants have knowingly induced, and continue to knowingly induce, others to infringe claims 1-39 of the '207 patent in violation of 35 U.S.C. § 271 by taking active steps with specific intent to encourage and facilitate direct infringement by others, such as by manufacturers, distributors and others in the chain of distribution selling or offering to sell televisions, personal computers, notebook computers, tablets and mobile handheld devices, such as mobile phones, mobile gaming devices including the Skype Software that provide access to the Skype Network and/or by their customers using the Skype Network, with knowledge of the distributors' and customers' infringement.

53. For example, the defendants have entered into commercial arrangements with

television manufacturers like Sony®, Panasonic® and Samsung® whereby these manufactures have installed, embedded or otherwise incorporated the Skype Software into their televisions, as each of them markets, promotes and advertises the availability of Skype's peer-to-peer VoIP communication system as an additional feature of their televisions and, in the case of Panasonic®, the remote control unit actually features a "Skype Button."

54. Defendants have encouraged and facilitated direct infringement by manufacturers, distributors and others in the chain of distribution and their customers, and others in the chain of distribution, by contracting for the distribution of the Skype Software, by marketing, promoting, and advertising the Skype Software and features on television commercials, and by creating and publishing instructions on using the Skype Software and Skype Features.

55. The installation, embedding, or incorporation of the Skype Software by manufacturers, distributors and others in the chain of distribution selling or offering to sell televisions, personal computers, notebook computers, tablets and mobile handheld devices, such as mobile phones, mobile gaming devices including the defendants' Skype Software which, in turn, provides access to the Skype Network by their customers using the Skype Network, constitutes direct infringement of the '207 patent.

56. Defendants knowingly continue to make, use, sell, and offer to sell systems, computer-readable media and methods that infringe the '207 patent as set forth herein.

57. Gradient has been, and continues to be, damaged as a result of the defendants' infringement within the Western District of New York and elsewhere.

58. Said acts of infringement are willful and deliberate. At a minimum, the defendants have acted recklessly and in disregard of the plaintiff's rights since they first became aware of the '207 patent, as set forth above.

59. As a result of the foregoing, Gradient has been damaged in an amount to be determined by the trier of fact in accordance with 35 U.S.C. § 284.

AS AND FOR A THIRD CAUSE OF ACTION, PLAINTIFF ALLEGES AS FOLLOWS:

Contributory Infringement (35 U.S.C. § 271 (c))

60. Gradient repeats and re-alleges paragraphs "1" through "59" as if more fully set forth herein.

61. Upon information and belief, the defendants with knowledge of the '207 patent have contributorily infringed, and continue to contributorily infringe, the '207 patent in violation of 35 U.S.C. § 271 by selling and/or offering to sell within the United States Skype Software, and facilitating the sale or offer for sale of Skype Software by manufacturers, distributors and others in the chain of distribution, and, in turn, the downloading and use of Skype Software by their customers, through Skype Network.

62. This sale, offer for sale, and use of Skype Network by defendants, its manufacturers, distributors and others in the chain of distribution, and, in turn, their customers, embodies a material part of the infringing systems, computer-readable media and methods described in the '207 patent.

63. The Skype Features are specially made or specially adapted for use in infringement of the '207 patent, and are not staple articles suitable for a commercially significant non-infringing use.

64. The installation, embedding, or incorporation of the Skype Software by manufacturers, distributors and others in the chain of distribution selling or offering to sell televisions, personal computers, notebook computers, tablets and mobile handheld devices, such

as mobile phones, mobile gaming devices including the defendants' Skype Software which, in turn, provides access to the Skype Network by their customers using the Skype Network, constitutes direct infringement of the '207 patent

65. Defendants knowingly continue to make, use, sell, and offer to sell systems, computer-readable media and methods that infringe the '207 patent as set forth herein.

66. Gradient has been, and continues to be, damaged as a result of the defendants' infringement within the Western District of New York and elsewhere.

67. Said acts of infringement are willful and deliberate. At a minimum, the defendants have acted recklessly and in disregard of the plaintiff's rights since they first became aware of the '207 patent, as set forth above.

68. As a result of the foregoing, Gradient has been damaged in an amount to be determined by the trier of fact in accordance with 35 U.S.C. § 284.

AS AND FOR A FOURTH CAUSE OF ACTION, PLAINTIFF ALLEGES AS FOLLOWS:

Injunction (35 U.S.C. § 283)

69. Gradient repeats and re-alleges paragraphs "1" through "68" as if more fully set forth herein.

70. As provided above, the defendants have made, used, sold and/or offered to sell systems, computer-readable media and methods which infringe the '207 patent and continue to do so in violation of Gradient's rights, for which there is no adequate remedy at law.

71. Unless the defendants are permanently enjoined from making, using, selling and/or offering to sell such systems and methods, Gradient will suffer irreparable harm.

72. As a result of the foregoing, Gradient is entitled to a permanent injunction, in

accordance with 35 U.S.C. § 283, enjoining and restraining the defendants from making, using, selling or offering to sell any system, computer readable medium or method which infringes upon one or more claims of the '207 patent.

AS AND FOR A FIFTH CAUSE OF ACTION, PLAINTIFF ALLEGES AS FOLLOWS:

Declaratory Judgment

73. Gradient repeats and re-alleges paragraphs "1" through "72" as if more fully set forth herein.

74. Gradient is entitled to a judgment, declaring that the defendants have infringed, and continue to infringe one or more claims of the '207 patent and further declaring their respective rights and responsibilities of the parties.

WHEREFORE, the plaintiff, Gradient Enterprises, Inc., requests judgment as follows:

A. Declaring that the one or more claims of United States Patent No. 7,669,207 have been infringed by one or more of the defendants and/or by third parties to whose infringement the defendants have contributed and/or by third parties whose infringement has been induced by the defendants;

B. Granting a permanent injunction, restraining and enjoining defendants, their officers, directors, agents, servants, employees, and all others in privity, concert or participation with them or on their behalf, from further acts of patent infringement, including the manufacture, use, sale and/or offering for sale infringing systems, computer-readable media and methods;

C. Granting an accounting for damages adequate to compensate plaintiff for infringement of the '207 patent, such damages to be trebled to the extent allowed by law due to the willful and deliberate character of the infringement;

D. Awarding to plaintiff all compensatory damages suffered as a result of the defendants' actions;

E. Awarding to the plaintiff its attorneys' fees and costs;

F. Further declaring the respective rights and responsibilities of the parties; and

G. Awarding the plaintiff such other and further relief as to this Court may seem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, Gradient Enterprises, Inc. hereby requests a trial by jury on all issues so triable.

DATED: April 11, 2012
Rochester, New York

WOODS OVIATT GILMAN LLP

By: _____

Donald W. O'Brien, Jr., Esq.
Dennis B. Danella, Esq.
Attorneys for Plaintiff
700 Crossroads Building
2 State Street
Rochester, New York 14614
585.987.2800

EXHIBIT 1

US007669207B2

(12) **United States Patent**
Johnson

(10) **Patent No.: US 7,669,207 B2**
(45) **Date of Patent: Feb. 23, 2010**

(54) **METHOD FOR DETECTING, REPORTING AND RESPONDING TO NETWORK NODE-LEVEL EVENTS AND A SYSTEM THEREOF**

(75) Inventor: **Kristaps Johnson**, Rochester, NY (US)

(73) Assignee: **Gradient Enterprises, Inc.**, Rochester, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 187 days.

(21) Appl. No.: **10/882,833**

(22) Filed: **Jul. 1, 2004**

(65) **Prior Publication Data**

US 2005/0015435 A1 Jan. 20, 2005

Related U.S. Application Data

(60) Provisional application No. 60/488,190, filed on Jul. 17, 2003.

(51) **Int. Cl.**
G06F 13/00 (2006.01)

(52) **U.S. Cl.** **719/318**; 709/202; 709/224

(58) **Field of Classification Search** 709/202, 709/224, 238; 719/318
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,832,208	A *	11/1998	Chen et al.	726/24
6,035,423	A	3/2000	Hodges et al.	
6,269,400	B1 *	7/2001	Douglas et al.	709/224
6,269,456	B1	7/2001	Hodges et al.	
6,336,139	B1	1/2002	Feridun et al.	
7,082,604	B2 *	7/2006	Schneiderman	718/100
7,096,264	B2 *	8/2006	Bonney et al.	709/224
2002/0013910	A1	1/2002	Edery et al.	
2002/0116639	A1 *	8/2002	Chefalas et al.	713/201
2002/0147974	A1	10/2002	Wookey	
2002/0188887	A1	12/2002	Largman et al.	
2003/0023866	A1	1/2003	Hinchliffe et al.	
2004/0064499	A1 *	4/2004	Kasravi	709/202

FOREIGN PATENT DOCUMENTS

WO	WO 00/70458	11/2000
WO	WO 01/93531 A2	12/2001
WO	WO 02/17599 A2	2/2002

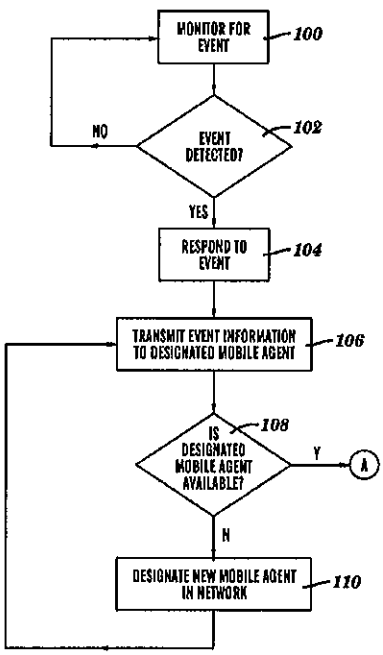
* cited by examiner

Primary Examiner—Andy Ho
(74) *Attorney, Agent, or Firm*—Nixon Peabody LLP

(57) **ABSTRACT**

A system for detecting, reporting and responding to network node-level occurrences on a network-wide level includes one or more first mobile agents, each of the one or more first mobile agents is hosted by one of a plurality of nodes in the network. An event detection system communicates network event information associated with an event detected at one or more of the nodes in the network to the one or more first mobile agents, and a reporting system disseminates from the one or more first mobile agents information describing the detected event to one or more other nodes.

39 Claims, 3 Drawing Sheets



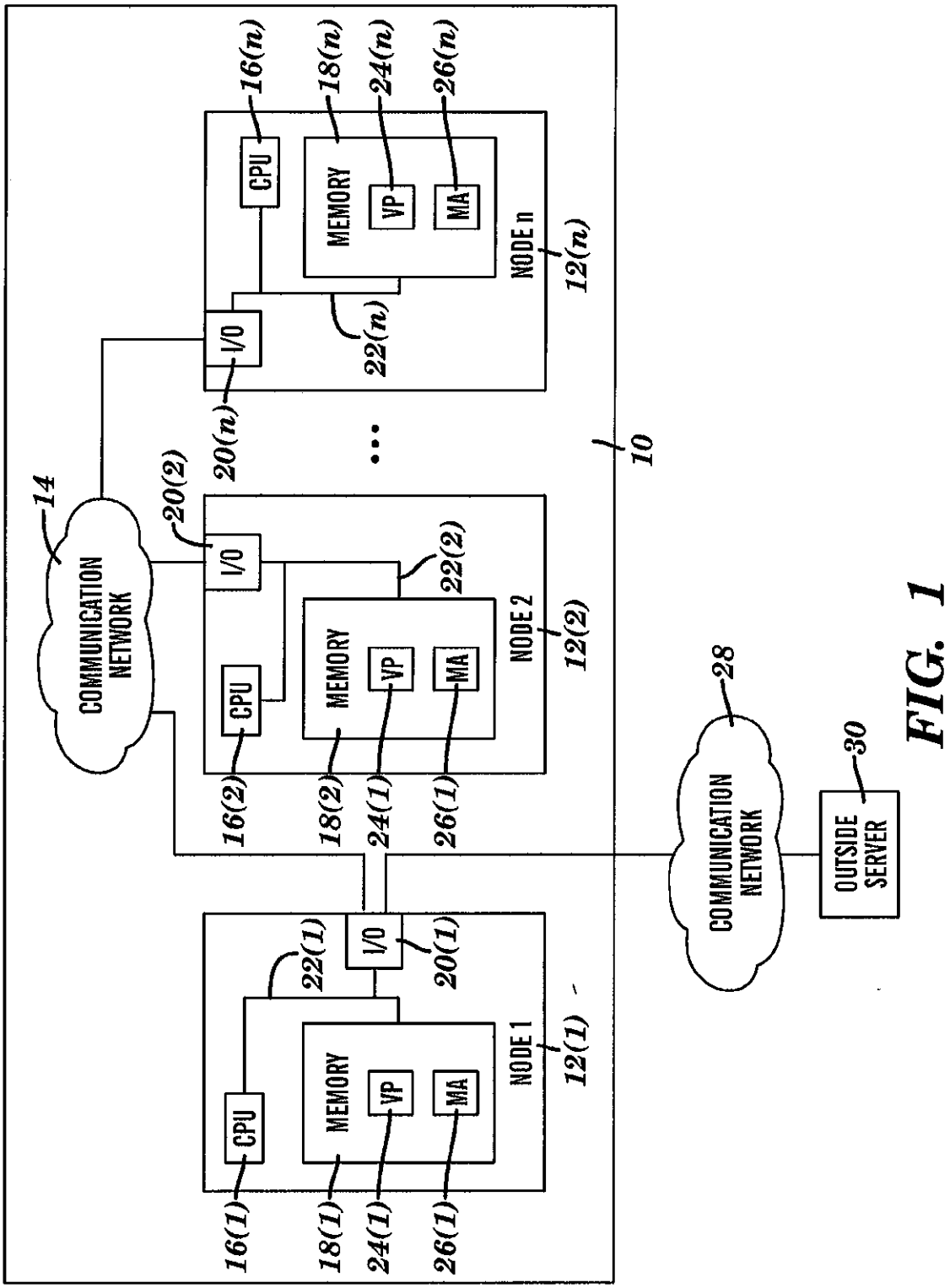

10
14
COMMUNICATION NETWORK
NODE n
12(n)
CPU
MEMORY
VP
MA
I/O
16(n)
18(n)
24(n)
26(n)
22(n)
20(n)
NODE 2
12(2)
16(2)
18(2)
24(1)
26(1)
22(2)
20(2)
NODE 1
12(1)
16(1)
18(1)
22(1)
20(1)
28
COMMUNICATION NETWORK
30
OUTSIDE SERVER

FIG. 1

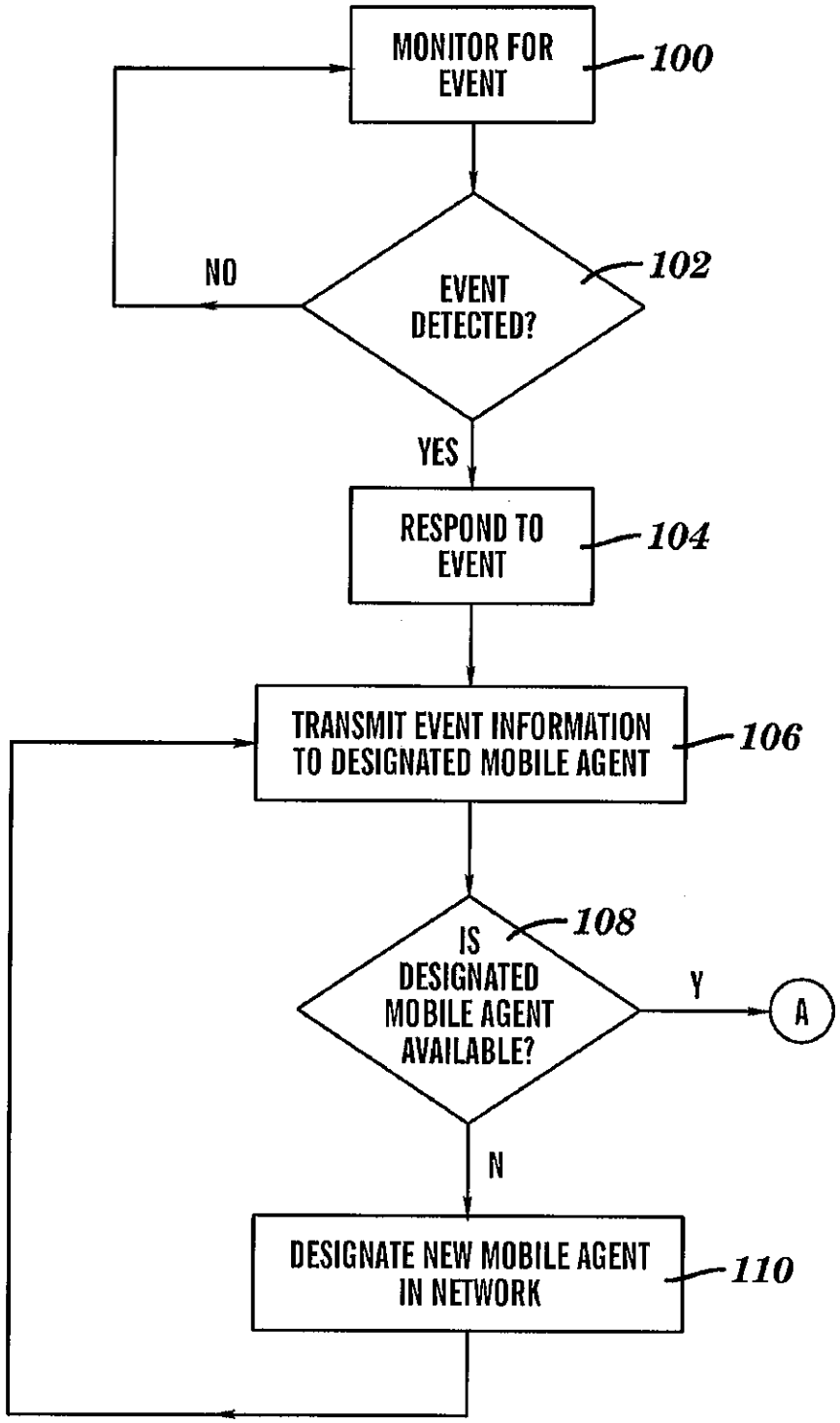

MONITOR FOR EVENT
100
EVENT DETECTED?
102
NO
YES
RESPOND TO EVENT
104
TRANSMIT EVENT INFORMATION TO DESIGNATED MOBILE AGENT
106
IS DESIGNATED MOBILE AGENT AVAILABLE?
108
Y
A
N
DESIGNATE NEW MOBILE AGENT IN NETWORK
110

FIG. 2

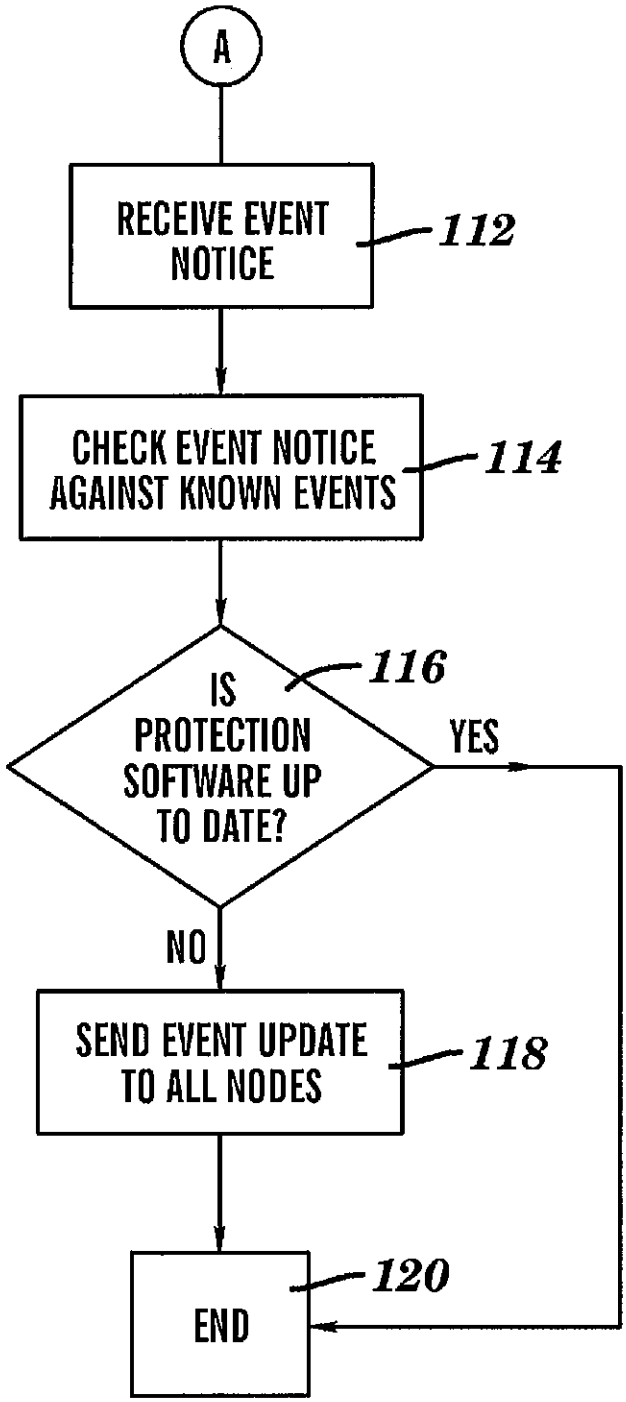

A
RECEIVE EVENT NOTICE
112
CHECK EVENT NOTICE AGAINST KNOWN EVENTS
114
IS PROTECTION SOFTWARE UP TO DATE?
116
YES
NO
SEND EVENT UPDATE TO ALL NODES
118
END
120

FIG. 3

METHOD FOR DETECTING, REPORTING AND RESPONDING TO NETWORK NODE-LEVEL EVENTS AND A SYSTEM THEREOF

This application claims the benefit of U.S. Provisional Patent Application Ser. No. 60/488,190 filed Jul. 17, 2003 which is hereby incorporated by reference in its entirety.

FIELD OF THE INVENTION

This invention relates generally to network communications and, more particularly, to a method and system for providing information associated with network events, such as a viral or unauthorized access attack, to a mobile agent hosted by one of a plurality of network nodes, which in turn reports the network event to client modules operating on the other nodes in the network for addressing the network event accordingly.

BACKGROUND

Current network security systems are primarily insular. These detection systems, such as virus scanners and intrusion detection systems, lack the capability to collaborate events to the controlled network. In other words, they lack the capability and inherent architecture to address attacks from a group perspective. Insular systems could thus be considered passive from a network perspective, as action taken on events has only the scope of network nodes, not the network as a whole. Furthermore, "distributed" defense systems use static, centralized sources of control which has several drawbacks. The foremost drawback is network failure. If a controller, such as a server, fails, the entire network security system is left without control. If the sever is compromised, a malicious entity may gain control of an entire system. Additionally, network conditions, such as segmentation and fragmentation, could lead to entire portions of the network not having access to the static server or the ability to adapt.

SUMMARY

A system for detecting, reporting and responding to network node-level occurrences on a network-wide level in accordance with embodiments of the present invention includes one or more first mobile agents, each of the one or more first mobile agents is hosted by one of a plurality of nodes in the network. An event detection system communicates network event information associated with an event detected at one or more of the nodes in the network to the one or more first mobile agents, and a reporting system disseminates from the one or more first mobile agents information describing the detected event to one or more other nodes.

A method and a program storage device readable by a machine and tangibly embodying a program of instructions executable by the machine for detecting, reporting and responding to network node-level occurrences on a network-wide level in accordance with embodiments of the present invention include providing one or more first mobile agents, each of the one or more first mobile agents is hosted by one of a plurality of nodes in the network, communicating network event information associated with an event detected at one or more of the nodes in the network to the one or more first mobile agents, and disseminating from the one or more first mobile agents information describing the detected event to one or more other nodes.

The present invention addresses the above-noted problems in current systems by distributing control of a network throughout the nodes of the network, such as computer systems and other programmable machines, themselves with a mobile agent. The mobile agent is "hosted" by one of the network nodes, but can be dispatched from node to node and is not restricted to any particular node. As a result, control of the system in a network is non-central and mobile. This, among other properties, ensures that the system is fault tolerant, meaning that the system remains on-line whenever there is an available host for the mobile agent. Fault tolerance guarantees that a system functions regardless of any node's status on the network. Even if every node is disabled, the present invention enables the system to restore itself to a protected state. Additionally, the present invention allows for adaptation to fragmented networks and allows data gathered in individual partitions to be merged when the network reforms. Thus, if a node is functioning as the host for the mobile agent at any given time and is rendered unavailable, one or more of the other nodes in the network can assume the responsibility for hosting the mobile agent since all of the nodes have a copy of the mobile agent. Determining which node will host the mobile agent can be accomplished using a variety of techniques, such as voting schemes, artificial intelligence, and/or other processing resource management techniques.

Another benefit of the present invention is that the invention may distribute and control software along with network events. New attack patterns and forms of transmission change daily, and current systems utilizing out-dated protection software often leads to a compromised system. The present invention addresses these problems by coupling real-time network communication with self-updating facilities. This real-time communication serves to disseminate third-party updates to the entire network, ensuring that all clients have the same underlying degree of protection.

With the present invention, there is no inherent limit or defined boundary for the minimum or maximum number of nodes that may be protected. When the network reaches a certain size which can be established by an operator of the network, with the present invention the network may have two distinct mobile agents. Similarly, there is no restriction on the type of node or nodes within a network. The nodes within the network may be of heterogeneous types, such as Microsoft Windows, Unix/Linux, Apple Macintosh, etc.

A further benefit of the present invention is that the system is non-invasive with respect to existing security protocols and established frameworks. The present invention can monitor its processes for effective operation and adapts itself to changing environments, i.e., network topology and/or size, as appropriate. Changed configurations are immediately propagated to nodes in the network as required.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a system for detecting and reporting network node-level occurrences and responding on a network-wide level in accordance with embodiments of the present invention;

FIG. **2** is a flow chart of a method for detecting and reporting an attack to a node in a system in accordance with embodiments of the present invention; and

FIG. **3** is a flow chart of a method for responding to an attack on a node in a system in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

A system **10** for detecting and reporting network node-level occurrences, such as viral attacks or unauthorized access, and responding on a network-wide level, such as defending a computer network against a viral attack, in accordance with embodiments of the present invention is illustrated in FIG. **1**. The system **10** includes a plurality of nodes **12(1)-12(*n*)** coupled together by a communication network **14**, each of the nodes **12(1)-12(*n*)** has one of a plurality of mobile agents **26(1)-26(*n*)** although the system **10** can comprise other numbers and types of components in other configurations. The present invention provides a number of advantages, including providing real-time, active protection of a computer network to enable a secure, efficient and fault tolerant system.

Referring more specifically to FIG. **1**, in these embodiments each of the nodes **12(1)-12(*n*)** has one of a plurality of central processing unit (CPU) or processor **16(1)-16(*n*)**, one of a plurality of memories **18(1)-18(*n*)**, and one of a plurality of input/output interface devices **20(1)-20(*n*)** which are coupled together in each of the nodes **12(1)-12(*n*)** by one of a plurality of buses **22(1)-22(*n*)** or other link, although each of the nodes **12(1)-12(*n*)** can comprise other numbers and types of components in other configurations and each of the nodes **12(1)-12(*n*)** can comprises other types of systems and devices.

Each of the processors **16(1)-16(*n*)** can execute a program of stored instructions for one or more aspects of the present invention as described herein, including the methods described herein with reference to FIGS. **2-3**. Each of the memories **18(1)-18(*n*)** can store some or all of these programmed instructions for one or more aspects of the present invention for execution by one or more of the processors **16(1)-16(*n*)**, although some or all of these programmed instructions which can include data could be stored and/or executed elsewhere. A variety of different types of memory storage devices, such as a random access memory (RAM) or a read only memory (ROM) in the system or a floppy disk, hard disk, CD ROM, or other computer readable medium which is read from and/or written to by a magnetic, optical, or other reading and/or writing system that is coupled to the processor, can be used for each of the memories **18(1)-18(*n*)** to store the programmed instructions described herein, as well as other information.

Each of the memories **18(1)-18(*n*)** also includes one of a plurality of virus protection modules **24(1)-24(*n*)** and one of a plurality of mobile agent modules or mobile agents **26(1)-26(*n*)**, although the memories **18(1)-18(*n*)** can stored other numbers and types of modules with programmed instructions for carrying out these and/or other processes. For example, in other embodiments one or more of the nodes **12(1)-12(*n*)** may not have one or more of the virus protection modules **24(1)-24(*n*)** and/or one or more of the mobile agents **26(1)-26(*n*)**.

Each of the virus protection modules **24(1)-24(*n*)** comprises programmed instructions stored in each of the memories **18(1)-18(*n*)** for execution by each of the processors **16(1)-16(*n*)** to recognize, notify and defend each of the nodes **12(1)-12(*n*)** from an attack, such as an attack from a virus, although each of the virus protection modules **24(1)-24(*n*)** can comprise other numbers and types of complement technologies. By way of example only, a virus protection module may comprise the Norton Antivirus program. Since the operation of virus protection modules are well known to those of ordinary skill in the art, they will not be described in greater detail herein.

The mobile agents **26(1)-26(*n*)** are dynamically loaded by the nodes **12(1)-12(*n*)** on the system **10** at the first startup of each of the nodes **12(1)-12(*n*)**, although the mobile agents **26(1)-26(*n*)** can be loaded at other times, such as when a failure occurs in the one of the nodes **12(1)-12(*n*)** which is hosting the controlling one of the mobile agents **26(1)-26(*n*)**. Each of the mobile agents **26(1)-26(*n*)** comprises programmed instructions stored in each of the memories **18(1)-18(*n*)** for execution by each of the processors **16(1)-16(*n*)** to provide real-time, active protection of a computer system or network **10**.

More specifically, each of the mobile agents **26(1)-26(*n*)** comprises programmed instructions which include data tables containing the state of the system **10**, although each of the mobile agents **26(1)-26(*n*)** can comprise other types of programmed instructions including other data. The state of the system **10** comprises information required by the virus protection modules **24(1)-24(*n*)** to enact defensive measures, as well as administrative and ancillary information required for the functions of each of the nodes **12(1)-12(*n*)**. For example, the information about the state of the system **10** may comprises data, such as a virus identifier and/or virus name, and metadata, such as a list of which of the nodes **12(1)-12(*n*)** is/are available for hosting a controlling one of the mobile agents **26(1)-26(*n*)**.

The state of the system **10** is maintained on all of the nodes **12(1)-12(*n*)** within a mobile-agent controlled sector so that each of the nodes **12(1)-12(*n*)** has the system state varies (in its synchrony) within a deterministic threshold as the other nodes **12(1)-12(*n*)**, although lesser numbers of the nodes **12(1)-12(*n*)** could be maintained. In these embodiments, there is one mobile-agent sector for the system **10** which controls nodes **12(1)-12(*n*)**, although system **10** can have other numbers of mobile agent controlled sectors. A rigorous system of acknowledgement and logging in the system **10** between the nodes **12(1)-12(*n*)** ensures that all transmitted data is effectively received, even in the event of a failure of the controlling one or more of the mobile agents **26(1)-26(*n*)** on the nodes **12(1)-12(*n*)**.

One or more of the nodes **12(1)-12(*n*)** may be hosting a controlling one or more of the mobile agents **26(1)-26(*n*)** and the other remaining nodes in the nodes **12(1)-12(*n*)** will have non-controlling mobile agents from the remaining ones of the mobile agents **26(1)-26(*n*)**. The non-controlling mobile agents from the remaining ones of the mobile agents **26(1)-26(*n*)**, also known as client modules, are each used to interact with and control the one or more virus protection modules **24(1)-24(*n*)** which are located in the same nodes **12(1)-12(*n*)** as each non-controlling mobile agent. Although in these embodiments one node in the nodes **12(1)-12(*n*)** hosts only one controlling mobile agent from the mobile agents **26(1)-26(*n*)**, the one node can host other numbers of controlling mobile agents. If the one node in the nodes **12(1)-12(*n*)** with the controlling one of the mobile agents **26(1)-26(*n*)** is shut down, another one of remaining nodes in the nodes **12(1)-12(*n*)** can host a controlling mobile agent module from the remaining mobile agents **26(1)-26(*n*)**. Only the nodes **12(1)-12(*n*)** in the system **10** can be used to host a controlling one or ones of the mobile agents **26(1)-26(*n*)**.

The controlling one of the mobile agents **26(1)-26(*n*)** is not restricted to any particular one of the nodes **12(1)-12(*n*)**. This promotes fault tolerance ensuring that a system **10** remains on-line whenever there is an available one of the nodes **12(1)-12(*n*)** to host a controlling one of the mobile agents **26(1)-26**

(*n*). This also promotes an additional level of security because it is more difficult to locate which of the mobile agents **26(1)-26(*n*)** is controlling.

Referring back to FIG. **1**, the input/output interface devices **20(1)-20(*n*)** are used to operatively couple and communicate between each of the nodes **12(1)-12(*n*)** via the communications network **14** and also with other systems and devices, such as with for example an outside server **30** via a communication network **28**. A variety of communication systems and/or methods can be used for each of the communication networks **14** and **28** to operatively couple and communicate between the nodes **12(1)-12(*n*)** and between one or of the nodes **12(1)-12(*n*)** and other systems and devices, such as the outside server **30**, such as wireless communication technology, a direct connection, a local area network, a wide area network, the world wide web, and modems and phone lines each having their own communications protocols.

The operation of the system **10** in accordance with embodiments of the present invention will now be described with reference to FIGS. **2-3**. In step **100**, the virus protection modules **24(1)-24(*n*)** in each of the nodes **12(1)-12(*n*)** monitor for an event, such as an attack on one of the nodes **12(1)** or an update. By way of example only, an attack may come from the outside server **30** during a communication between the node **12(1)** and the outside server **30** via the communication network **28**. The update may also comprise information about an update to one of the virus protection modules **24(1)-24(*n*)** or another module or modules or may comprise new data. To obtain updates, the controlling one of the mobile agents **26(1)-26(*n*)** in one of the nodes **12(1)-12(*n*)** may continually poll outside sources to look for new information and then disseminate this information to the other nodes **12(1)-12(*n*)**, although other manners for obtaining the updates can be used. In step **102**, if based on the monitoring, an event is not detected by the virus protection modules **24(1)-24(*n*)** at any of the nodes **12(1)-12(*n*)**, then the No branch is taken back to step **100**. In step **102**, if based on the monitoring, an event is detected by the virus protection modules **24(1)-24(*n*)** at one of the nodes **12(1)-12(*n*)**, then the Yes branch is taken to step **104**.

In step **104**, the one of the nodes **12(1)-12(*n*)** which detected the event, responds to the event. By way of example only, if the event is an attack, the one of the nodes **12(1)-12(*n*)** defends itself from the attack using the virus protection modules **24(1)-24(*n*)** at the attacked one of the nodes **12(1)-12(*n*)** and/or may implement new virus protection instructions. If the event is an update, then the one of the nodes **12(1)-12(*n*)** with the controlling one of the mobile agents **26(1)-26(*n*)** may obtain the update. In step **106**, the one of the nodes **12(1)-12(*n*)** which detected the event, transmits hash about the event, such as an identifier and ancillary data which the other nodes **12(1)-12(*n*)** with the virus protection modules **24(1)-24(*n*)** can use to determine the appropriate course of action, e.g. how to protect against a new virus, to the node in the nodes **12(1)-12(*n*)** which is currently hosting the controlling mobile agent in the mobile agents **26(1)-26(*n*)**.

In step **108**, the one of the nodes **12(1)-12(*n*)** which detected the event determines if the node in the nodes **12(1)-12(*n*)** which is currently hosting the controlling mobile agent is available. If the node in the nodes **12(1)-12(*n*)** which is currently hosting the controlling mobile agent is available, then the Yes branch is taken to step **112** in FIG. **3**. Referring back to FIG. **2**, if the node in the nodes **12(1)-12(*n*)** which is currently hosting the controlling mobile agent is not available, then the No branch is taken to step **110**.

In step **110**, another node in the nodes **12(1)-12(*n*)** is selected to host the controlling one of the remaining available mobile agents in the mobile agents **26(1)-26(*n*)** and then returns to step **106**. Determining which of the nodes **12(1)-12(*n*)** will host the controlling mobile agent from the mobile agents **26(1)-26(*n*)** can be accomplished using a variety of techniques, such as voting schemes, artificial intelligence, and/or other processing resource management techniques.

For example, a weighted voting protocol, i.e., a communication theory for nodes **12(1)-12(*n*)** to unanimously vote on an event, to elect the controlling one of the mobile agents **26(1)-26(*n*)** may be used, although other selection schemes may be used such as artificial intelligence. In this example, the event is a determination of which of the nodes **12(1)-12(*n*)** will host a controlling mobile agent. Voting protocols ensure that if failures occur while a voting session takes place, a node in the nodes **12(1)-12(*n*)** which has failed will not be elected.

When a new node in the nodes **12(1)-12(*n*)** is selected to host the controlling mobile agent, the other nodes **12(1)-12(*n*)** in the system **10** are notified of the new node in the nodes **12(1)-12(*n*)** which is hosting the controlling mobile agent. With the notification, the remaining nodes in the nodes **12(1)-12(*n*)** with the non-controlling or client modules know which node in the nodes **12(1)-12(*n*)** with the controlling mobile agent to send and receive data, such as information about a detected attack.

Referring to FIG. **3**, in step **112** the node in the nodes **12(1)-12(*n*)** which is hosting the controlling mobile agent from the mobile agents **26(1)-26(*n*)** receives information about the event from the node in the nodes **12(1)-12(*n*)** which was attacked. In step **114**, the controlling mobile agent in the hosting node checks the information received about the event against stored data about other events.

In step **116**, the controlling mobile agent in the hosting node determines if the virus protection modules **24(1)-24(*n*)** for the nodes **12(1)-12(*n*)** are up to date with respect to the detected event. If the information received about the detected event is already known at each of the nodes **12(1)-12(*n*)**, then the Yes branch is taken to step **120** where the process with respect to this particular event ends while the system **10** continues to monitor for the next event as set forth in step **100**. If the information received about the detected event is not already known at each of the nodes **12(1)-12(*n*)**, then the No branch is taken to step **118**.

In step **118**, the one of the nodes **12(1)-12(*n*)** which is hosting the controlling mobile agent transmits information about the detected event to the other nodes **12(1)-12(*n*)** which are not hosting the controlling mobile agent and those nodes can update their data. For example, the other nodes **12(1)-12(*n*)** which are not hosting the controlling mobile agent may update the virus protection modules **24(1)-24(*n*)** based on the transmitted information about the detected event. In these embodiments, the nodes **12(1)-12(*n*)** use Message digest ("MD") and Keyed-Hashing Message Authentication ("HMAC") for checking hash received about a particular event against stored data in the nodes **12(1)-12(*n*)**, although other techniques for checking data can be used. The information which is transmitted from the one of the nodes **12(1)-12(*n*)** which is hosting the controlling mobile agent may be encrypted before being sent out on the system **10** to the other nodes which have client modules. Encryption falls into symmetric and asymmetric authentication. Symmetric keys follow the standard for most encryption measures, where a message is encrypted and decrypted using the same key. Asymmetric measures are usually public/private key systems, where hosts have both a private key (for decrypting messages) and a public key (which other hosts use to encrypt messages), although other methods may be used. In step **120**,

the process with respect to this particular detected event ends, while the system **10** continues to monitor for the next event as set forth in step **100**.

While the present invention has been described above utilizing complement technology, such as virus detection software, for example, one of ordinary skill in the art in the computer science, network resource management, and distributed network arts will appreciate that the systems and processes disclosed herein may be applied in a number of other network environments utilizing a variety of other complement technologies for detecting, reporting and responding to network events besides virus detection systems, such as any environment which requires a control structure where a distributed architecture is appropriate to the application scale.

Having thus described the basic concept of the invention, it will be rather apparent to those skilled in the art that the foregoing detailed disclosure is intended to be presented by way of example only, and is not limiting. Various alterations, improvements, and modifications will occur and are intended to those skilled in the art, though not expressly stated herein. These alterations, improvements, and modifications are intended to be suggested hereby, and are within the spirit and scope of the invention. Further, the recited order of elements, steps or sequences, or the use of numbers, letters, or other designations therefor, is not intended to limit the claimed processes to any order except as may be explicitly specified in the claims. Accordingly, the invention is limited only by the following claims and equivalents thereto.

What is claimed is:

1. A method for detecting, reporting and responding to network node-level occurrences on a network-wide level, the method comprising:

providing a plurality of mobile agents, each of the mobile agents is hosted by one of a plurality of nodes in a network which each detect for one or more events;

designating one of the mobile agents hosted at one of the nodes as a controlling mobile agent;

designating another one of the mobile agents hosted at another one of the nodes as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is unavailable;

communicating network event information associated with an event detected at one or more of the nodes in the network to the controlling mobile agent; and

disseminating from the controlling mobile agent information describing the detected event to one or more other nodes.

2. The method as set forth in claim **1** wherein the designating another one of the mobile agents as the controlling mobile agent further comprises:

determining which one of the nodes is best suited to host the controlling mobile agent; and

selecting the one of the nodes to host the controlling mobile agent based on the determining.

3. The method as set forth in claim **2** further comprising utilizing at least one of a voting and an artificial intelligence algorithm to perform the determining which one of the nodes is best suited to host the controlling mobile agent.

4. The method as set forth in claim **1** wherein the disseminating from the controlling mobile agent further comprises disseminating the information describing the detected event to each of the nodes.

5. The method as set forth in claim **1** further comprising notifying one or more of the nodes that another one of the mobile agents is designated as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is determined to be unavailable.

6. The method as set forth in claim **1** wherein the designating another one of the mobile agents as the controlling mobile agent further comprising determining when the one of the mobile agents previously designated as the controlling mobile agent is unavailable.

7. The method as set forth in claim **1** wherein each of the one or more nodes that receives the disseminated information describing the detected event uses the information to protect the node.

8. The method as set forth in claim **1** further comprising protecting each of the one or more other nodes against a network-based attack associated with the detected event using the information describing the detected event.

9. The method as set forth in claim **1**, wherein the one of the nodes hosting the controlling mobile agent is selected based upon information about a state of the network, the information comprising metadata including a list of available nodes for hosting the controlling mobile agent.

10. The method as set forth in claim **1** further comprising designating mobile agents other than the controlling mobile agent as non-controlling mobile agents.

11. The method as set forth in claim **1**, wherein the controlling mobile agent is configured to continually poll one or more outside sources for new information prior to the disseminating.

12. The method as set forth in claim **1**, wherein the communicating comprises transmitting a hash to the controlling mobile agent.

13. The method as set forth in claim **1**, wherein the controlling mobile agent is configured to determine if a virus protection module is up to date with respect to the detected event.

14. A computer-readable medium having stored thereon instructions for detecting, reporting and responding to network node-level occurrences on a network-wide level, which when executed by at least one processor, causes the processor to perform:

providing a plurality of mobile agents, each of the mobile agents is hosted by one of a plurality of nodes in a network which each detect for one or more events;

designating one of the mobile agents hosted at one of the nodes as a controlling mobile agent;

designating another one of the mobile agents hosted at another one of the nodes as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is unavailable;

communicating network event information associated with an event detected at one or more of the nodes in the network to the controlling mobile agent; and

disseminating from the controlling mobile agent information describing the detected event to one or more other nodes.

15. The medium as set forth in claim **14** wherein the designating another one of the mobile agents as the controlling mobile agent further comprises:

determining which one of the nodes is best suited to host the controlling mobile agent; and

selecting the one of the nodes to host the controlling mobile agent based on the determining.

16. The medium as set forth in claim **15** further comprising utilizing at least one of a voting and an artificial intelligence algorithm to perform the determining which one of the nodes is best suited to host the controlling mobile agent.

17. The medium as set forth in claim 14 wherein the disseminating from the controlling mobile agent further comprises disseminating the information describing the detected event to each of the nodes.

18. The medium as set forth in claim 14 further comprising notifying one or more of the nodes that another one of the mobile agents is designated as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is determined to be unavailable.

19. The medium as set forth in claim 14 wherein the designating another one of the mobile agents as the controlling mobile agent further comprising determining when the one of the mobile agents previously designated as the controlling mobile agent is unavailable.

20. The medium as set forth in claim 19 wherein each of the one or more nodes that receives the disseminated information describing the detected event uses the information to protect the node.

21. The medium as set forth in claim 14 further comprising protecting each of the one or more other nodes against a network-based attack associated with the detected event using the information describing the detected event.

22. The medium as set forth in claim 14, wherein the one of the nodes hosting the controlling mobile agent is selected based upon information about a state of the network, the information comprising metadata including a list of available nodes for hosting the controlling mobile agent.

23. The medium as set forth in claim 14 further comprising designating mobile agents other than the controlling mobile agent as non-controlling mobile agents.

24. The medium as set forth in claim 14, wherein the controlling mobile agent is configured to continually poll one or more outside sources for new information prior to the disseminating.

25. The medium as set forth in claim 14, wherein the communicating comprises transmitting a hash to the controlling mobile agent.

26. The medium as set forth in claim 14, wherein the controlling mobile agent is configured to determine if a virus protection module is up to date with respect to the detected event.

27. A system for detecting, reporting and responding to network node-level occurrences on a network-wide level, the system comprising:

a plurality of mobile agents, each of the mobile agents is hosted by one of a plurality of nodes in a network which each detect for one or more events;

a designation system that designates one of the mobile agents hosted at one of the nodes as a controlling mobile agent and designates another one of the mobile agents hosted at another one of the nodes as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is unavailable;

an event detection system that communicates network event information associated with an event detected at one or more of the nodes in the network to the controlling mobile agent; and

a reporting system that disseminates from the controlling mobile agent information describing the detected event to one or more other nodes.

28. The system as set forth in claim 27 wherein the designation system determines which one of the nodes is best suited to host the controlling mobile agent and selects the one of the nodes to host the controlling mobile agent based on the determination.

29. The system as set forth in claim 28 wherein the designation system utilizes at least one of a voting and an artificial intelligence algorithm to determine which one or more of the nodes is best suited to host the controlling mobile agent.

30. The system as set forth in claim 27 wherein the reporting system disseminates information describing the detected event to each of the nodes.

31. The system as set forth in claim 27 wherein the reporting system notifies one or more of the nodes that another one of the mobile agents is designated as the controlling mobile agent when the one of the mobile agents previously designated as the controlling mobile agent is determined to be unavailable.

32. The system as set forth in claim 27 wherein the designation system determines when the one of the mobile agents previously designated as the controlling mobile agent is unavailable.

33. The system as set forth in claim 27 wherein the second system responds to the detected event using the network event information to protect the node each of the one or more nodes that receives the disseminated information describing the detected event uses the information to protect the node.

34. The system as set forth in claim 27 wherein each of the one or more nodes comprises a first system that protects the nodes against a network-based attack associated with the detected event using the information describing the detected event.

35. The system as set forth in claim 27, wherein the one of the nodes hosting the controlling mobile agent is selected based upon information about a state of the network, the information comprising metadata including a list of available nodes for hosting the controlling mobile agent.

36. The system as set forth in claim 27 wherein the designation system designates mobile agents other than the controlling mobile agent as non-controlling mobile agents.

37. The system as set forth in claim 27, wherein the controlling mobile agent is configured to continually poll one or more outside sources for new information for the reporting system to disseminate.

38. The system as set forth in claim 27, wherein the communicated network event information comprises a hash transmitted to the controlling mobile agent.

39. The system as set forth in claim 27, wherein the controlling mobile agent is configured to determine if a virus protection module is up to date with respect to the detected event.

* * * * *