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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 June 2008 (05.06.2008)

PCT

(10) International Publication Number
WO 2008/067335 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2007/085677

(22) International Filing Date:
27 November 2007 (27.11.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/867,297 27 November 2006 (27.11.2006) US

(71) Applicant *(for all designated States except US)*: **SMOBILE SYSTEMS, INC.** [US/US]; 2020 Leonard Avenue, Columbus, OH 43220 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HU, Guoning** [CN/US]; 39535 Gallaudep Drive, Apt. 394, Fremont, CA 94538 (US). **VENUGOPAL, Deepak** [IN/US]; 222 Santa Fe Blvd., 2092, Irving, TX 75063 (US). **BHARDHWAJ, Shantanu** [IN/US]; 3954 Easton Square Place, Columbus, OH 43219 (US).

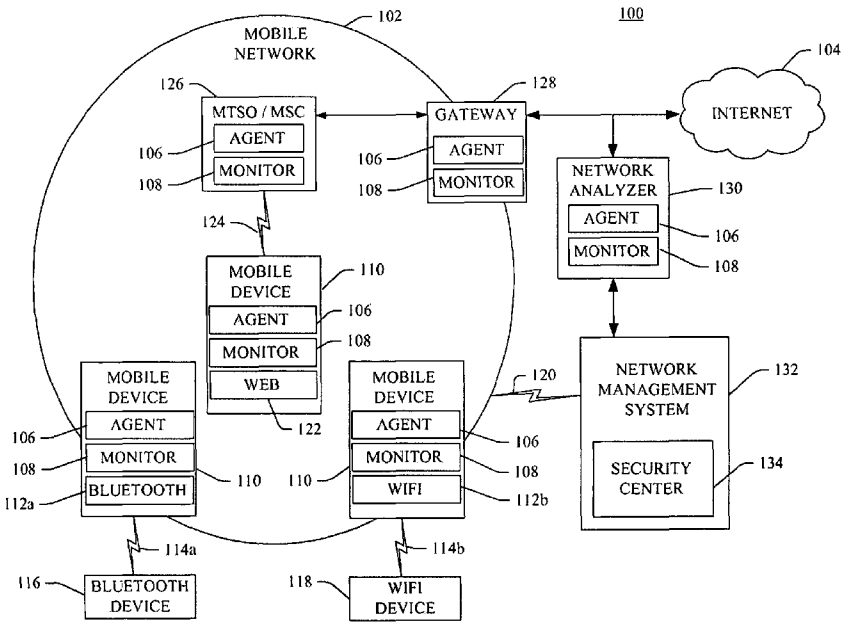
(74) Agent: **GORDON, Douglas, J.**; Thompson Hine Llp, P.o. Box 8801, Dayton, OH 45401-8801 (US).

(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, 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).

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

(54) Title: WIRELESS INTRUSION PREVENTION SYSTEM AND METHOD



(57) Abstract: A wireless intrusion prevention system and method to prevent, detect, and stop malware attacks is presented. The wireless intrusion prevention system monitors network communications for events characteristic of a malware attack, correlates a plurality of events to detect a malware attack, and performs mitigating actions to stop the malware attack.

WO 2008/067335 A2

WIRELESS INTRUSION PREVENTION SYSTEM AND METHOD

Inventors: Guoning Hu
Deepak Venugopal
Shantanu Bhardhwaj

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 60/867,297 entitled, "Wireless Intrusion Prevention System and Method", filed on November 27, 2006.

FIELD OF THE INVENTION

[0002] The present invention is related generally to a system and method for detecting, preventing, and stopping malware attacks on wireless networks.

BACKGROUND OF THE INVENTION

[0003] Mobile devices are potential targets for hackers and malware writers. As users increase the number of data applications on their mobile devices, the risk of malware being introduced into the mobile network and spread among mobile devices also increases. Malware tends to spread exponentially in a network, therefore it is important to stop malware early to prevent service disruption in significant portions of the network.

[0004] Typical malware detection applications scan a single computer to determine whether the computer is infected with malware and remove the offending malware when a malware signature is detected in a compromised application. Although post-infection cleaning can remove malware from a single computer, such cleaning is only effective for malware that has already been identified and recognized. Post-infection cleaning is not

capable of removing new or changing malware, and cannot prevent the infection from occurring.

[0005] Network techniques to prevent the spread of malware involve scanning network traffic for a malware signature at distinct points, called firewalls, to prevent malware from entering the network. However, this technique does not protect the network from malware that enters the network from points within the network itself. More robust network techniques involve placing a scanner within network elements, such as one or more of the routers that make up the data network. However, both of these network techniques are effective only for malware that has already been identified and recognized, not new or changing malware. Furthermore, such network techniques do not stop infections from happening in the first place.

[0006] Accordingly, there is a need for a system and method that can identify both new and old malware in the wireless network and prevent it from spreading to mobile phones. There is a need for a system that can detect, prevent, and stop malware attacks on wireless networks before the malware has a chance to spread and significantly disrupt service in a network.

SUMMARY OF THE INVENTION

[0007] The system and method for wireless intrusion prevention use information gathered within the entire mobile network to prevent, detect, and stop malicious attacks on a mobile network and assist in mitigating the spread of the malware. The system is especially effective with respect to specific types of attacks, namely mobile worm

attacks, battery draining attacks, and Denial of Service (DoS) attacks. However, the system and method are also applicable to other types of malware attacks and is therefore an important security component of an operator's mobile network. In an embodiment, the system includes three types of components: monitors, intelligent agents, and security centers. The system components operate on both network elements and mobile devices or handsets in mitigating malware attacks.

BRIEF DESCRIPTION OF THE FIGURES

[0008] The accompanying figures depict multiple embodiments of the system and method for detecting, preventing, and stopping malware attacks on wireless networks. A brief description of each figure is provided below. Elements with the same reference numbers in each figure indicate identical or functionally similar elements. Additionally, the left-most digit(s) of a reference number identifies the drawings in which the reference number first appears.

[0009] Fig. 1 depicts a block diagram of an exemplary deployment of monitors, agents, and a security center in accordance with an aspect of the subject matter described herein

[0010] Fig. 2 is flowchart illustrating an exemplary method for monitoring, detecting, and mitigating malicious communications in a mobile network in accordance with an aspect of the subject matter described herein.

[0011] Fig. 3 is flowchart illustrating an exemplary method for monitoring, detecting, and mitigating malware in a mobile network in accordance with an aspect of the subject matter described herein.

DETAILED DESCRIPTION

[0012] It should be noted that the invention is not limited in its application or use to the details of construction and arrangement of parts illustrated in the accompanying drawings and description. The illustrative embodiments of the invention may be implemented or incorporated in other embodiments, variations and modifications, and may be practiced or carried out in various ways. Furthermore, unless otherwise indicated, the terms and expressions employed herein have been chosen for the purpose of describing the illustrative embodiments of the present invention for the convenience of the reader and are not for the purpose of limiting the invention. In addition, as used herein, the term "exemplary" indicates a sample or example. It is not indicative of preference over other aspects or embodiments.

[0013] Referring now to Fig. 1, in an embodiment, the wireless intrusion prevention system **100** comprises monitors **108**, intelligent agents **106**, and at least one security center **134**. Each monitor **108** is associated with a network device **110**, **126**, **128**, **130**. Each monitor **108** is in communication with one or more intelligent agents **106** that communicate with the security center **134** portion of a network management system **132**. Communications with the security center **134** are generally performed via wireless communication **120**.

[0014] Network devices **110, 126, 128, 130** include mobile devices **110** or mobile devices **110**, network elements **126, 128** that serve as infrastructure components of the mobile network **102**, or network analyzers **130** used to independently monitor communications in the network. The term network element **126, 128** can be used interchangeably with the term network component **126, 128**, and can also include the network analyzers **130** in some contexts. The term mobile device **110** and handset **110** can also be used interchangeably, although mobile device **110** is generally used to encompass a wider array of wireless enabled devices, including but not limited to PDAs and laptop computers.

[0015] The mobile devices **110** may have wireless interfaces **112a, 112b** such as a Bluetooth interface **112a** for communicating via Bluetooth **114a** with another Bluetooth-equipped device **116**, or an 802.11x or Wi-Fi interface **112b** for communicating via Wi-Fi **114b** with another Wi-Fi-equipped device **118**. Internet enabled mobile devices **110** typically have network applications **122** such as a browser or web interface enabling them to send and receive data **124** from the Internet **104**.

The Monitor

[0016] Continuing to refer to Fig. 1, a monitor **108** is a component associated with a network device **110, 126, 128, 130** in the mobile network **102**. As used herein, the term component includes hardware, software, firmware, or any combination thereof. The device **110, 126, 128, 130** might be a mobile device **110** or a network element **126, 128, 130** in the mobile network **102**. The monitor **108** is communicatively connected to one or

multiple intelligent agents **106**. The monitor **108** is capable of performing the following functions:

- scanning the incoming and outgoing packets to detect malicious content or malware using heuristic rules;
- reporting detected malware to intelligent agents **106**;
- recording the activity of the network device **110**, **126**, **128**, **130**; and
- reporting the network device **110**, **126**, **128**, **130** activities upon requests from intelligent agents **106**.

[0017] By inspecting the incoming and outgoing data from a device **110**, **126**, **128**, **130**, monitors **108** acquire a significant amount of data. Some of the data may be duplicative with that collected by other monitors **108**. Scanning and reporting the same content from multiple devices **110**, **126**, **128**, **130** uses considerable network resources. However, such duplication increases the robustness of the wireless intrusion prevention system **100** since some attacks involve hiding or modifying of certain data. Also, some data is related to sensitive, private contents and is not monitored. Therefore, the client side (mobile device **110** side) monitors **108** and the network side monitors **108** may scan incoming and outgoing data differently.

[0018] For examples, monitors **108** on the client side may scan by performing any or all of the following functions:

- scanning the incoming and/or outgoing packets or files (data **124**) from the network application **122**, Wi-Fi connection **112b**, or a Bluetooth connection **112a**, where such scanning may be a deep scan, and include careful examination of individual contents using malware signatures and heuristic rules capable of identifying malicious programs or data;
- recording the time, the source (incoming packets) and destination (outgoing packets) address, and the size of the packets, where the format of the recorded data can be made consistent with the format used in the network **102** side monitoring; and
- monitoring and recording other activities upon requests from intelligent agents **106**.

[0019] Some representative malware scanning algorithms for mobile devices **110** include, but are not limited to, malware signature searches; hash signature searches as described in U.S. Patent Application 11/697,647 "Malware Detection System and Method for Mobile Platforms"; malware detection in headers and compressed parts of mobile messages as described in U.S. Patent Application 11/697,658 "Malware Detection System and Method for Compressed Data on Mobile Platforms"; malware modeling as described in U.S. Patent Application 11/697,642 "Malware Modeling Detection System and Method for Mobile Platforms"; malware modeling for limited access devices as described in U.S. Patent Application 11/697,664 "Malware Modeling Detection System and Method for Mobile Platforms"; and non-signature detection methods as described in U.S. Patent Application 11/697,668 "Non-Signature Malware Detection System and Method for Mobile Platforms".

[0020] Monitors **108** examine or scan communications among the elements of the mobile network **102**, including mobile devices **110**. In an embodiment, the monitors **108** on the network **102** side use the sFlow monitoring specifications (*see* RFC 3176, available online at www.ietf.org/rfc/rfc3176.txt and herein incorporated by reference) thereby gathering considerable envelope and routing information and relatively little or no content information. When scanning of content is permitted, representative malware algorithms for scanning on the network **102** side include, but are not limited to, malware signature searches; hash signature searches as described in U.S. Patent Application 11/697,647 "Malware Detection System and Method for Mobile Platforms"; and malware detection in headers and compressed parts of mobile messages as described in U.S. Patent Application 11/697,658 "Malware Detection System and Method for Compressed Data on Mobile Platforms".

The Intelligent Agent

[0021] An intelligent agent **106** receives information from one or several monitors **108**. Intelligent agents **106** can be located in both the mobile device **110** and the network **102**. In one embodiment, an intelligent agent **106** on a mobile device **110** is associated with a monitor **108** in the mobile device **110**. In another embodiment, an intelligent agent **106** on the network **102** is associated with multiple monitors **108** in distributed locations, for example in different cities. An intelligent agent **106** communicatively connects to the security center **134**. In alternative embodiments, an intelligent agent **106** is

communicatively connected to other intelligent agents **106**. In another embodiment, the functions of an intelligent agent **106** include:

- analyzing the information from monitors **108** to build up user, device, and network **102** activity profiles;
- detecting unusual mobile device **110** activities or network connections;
- reporting mobile device **110** activities to the security center **134** or other intelligent agents **108** upon request;
- reporting detected malicious attacks or malware to the security center **134**;
- reporting suspicious activities or programs to the security center **134** and requiring appropriate security actions;
- cleaning or blocking detected malicious programs or data; and,
- receiving updates from the security center **134** and informing the associated monitors **108**.

[0022] An intelligent agent **106** analyzes events reported from associated monitors **108** to determine if the events correlate to a characteristic of a malware attack. For example, an intelligent agent **106** reports a possible malicious attack if one or more mobile devices **110** receive multiple identical packets, a characteristic of a denial of service attack.

[0023] In an alternative embodiment, the functions of the intelligent agent **106** are performed by the security center **134**.

The Security Center

[0024] Security centers **134** are portions of network management systems **132** that monitor network **102** activities and control network **102** security with a comprehensive set of security tools. Security centers **134** receive information from intelligent agents **106** in both mobile devices **110** and from network elements **126, 128, 130** in the network **102**. One responsibility of each security center **134** is to integrate and analyze the information from distributed monitors **108** in the network **102**, e.g., information from both the network **102** traffic and mobile devices **110**, and use this information to protect the network **102** against any malicious attack. In one embodiment, the security centers **134** have a hierarchical architecture, e.g., one local security center **134** is responsible for a particular portion of the radio network, and reports up to one or more global security centers **134**. In this embodiment, a local security center **134** performs the following actions:

- integrate received information to build a profile for the activity of the locally monitored network **102**;
- detect malicious attacks and malware, including distinguishing normal network **102** activities from abnormal activities based on activity profile;
- send security warnings, instructions, or updates to intelligent agents **106**;
- generate security alarm to one or more of the global security centers **134**; and
- provide a user interference that allows human experts to monitor the network **102** activity, analyze suspicious programs, and verify security alarms.

[0025] In this embodiment, the global security center **134** is responsible for:

- coordinating local security centers **134**, integrating information from them and building a profile for the activity of the entire network **102**;
- detecting malicious attacks and malware that are missed by all the local security centers **134**;
- analyzing the detected malicious attacks and malware to determine the appropriate security actions or solutions and generating updates for local security centers **134** and intelligent agents **106**; and
- broadcasting security alarms and updates to local security centers **134**.

[0026] In an alternate embodiment, the security centers **134** have a flat architecture with overlapping regions of responsibility. The responsibilities of security centers **134** in a flat architecture can be distributed among different servers as is commonly known in the art of distributed systems.

[0027] In an alternative embodiment, the functions of the security center **134** are performed by the intelligent agent **106**. In an alternative embodiment, either or both the security center **134** and the intelligent agent **106** can be a mitigation agent triggering the mitigation actions to be performed on the network.

Example Applications of the Wireless Intrusion Prevention System

[0028] The wireless intrusion prevention system **100** is capable of identifying and neutralizing multiple types of malicious attacks on the mobile network **102**. Examples

listed below are meant to be illustrative and not to constrain the method and system to any specific embodiment.

[0029] Referring now to the flowchart of Fig. 2, a monitor **108** in a mobile device **110** or network element monitors **202** communications in the network **102** for identifying events characteristic of malicious communications to report to an intelligent agent **106**. A battery draining malware typically involves port scanning a mobile device from another site using a spoofed address. Therefore battery draining malware may result in a suspicious increase of local network traffic, e.g., increasing network traffic with decreasing average packet sizes, or increased distributed communication among mobile devices. An intelligent agent or security center detects **204** the battery draining malware attack based upon an analysis or correlation of network activity. In an embodiment, an agent **106** or security center **134** detects attack based upon the dynamics of network **102** activity when compared to the normal profiles of the network **102** activity. In another embodiment, the intelligent agent **106** or security center **134** compares activity levels to one or more predetermined thresholds. Such thresholds can be based upon historic data regarding network **102** activity. In yet another embodiment, normal activity can be determined based upon averages of historic network activity. Alternatively, the agent **106** or security center **134** can analyze the variation or percentage of change in network **102** activity over a specific time period to detect attacks.

[0030] In another embodiment, an intelligent agent **106** detects **204** the battery draining malware attack by noting a packet sent to an invalid handset address. In an embodiment,

a monitor on a trap handset **110**, also called a honeypot, that does not have any normal active communication by itself monitors **202** any packets directed to the trap handset **110** and reports the suspect activity. Similarly, an intelligent agent **106** or security center **134** detects **204** traffic directed towards mobile devices **110** that seldom have communications. Intelligent agents **106** report the detection to a security center **134** which analyzes **206** the results and determines whether a battery draining malware attack is occurring.

[0031] Once a battery draining malware attack is detected, intelligent agents in network elements perform appropriate actions to mitigate **208** the battery draining malware attack in the network. For example, on the network **102** side, intelligent agents **106** instruct **210** the network **102** to drop packets associated with the attack or provide information to the security system **134** of the network **102** operator. On the client side intelligent agents mitigate **212** the battery draining malware attack on the associated handsets. In an embodiment, intelligent agents instruct **216** mobile devices to ignore or filter the packets associated with the attack. If a mobile device **110** sending malicious communications is inside the service provider's network **102**, intelligent agents **106** disable **216** outbound communications on that mobile device **110**, or restrict **216** communications to stop the malicious activity without completely disabling the communications interfaces. For example, communications could be limited to allowing the mobile device **110** to reach network addresses associated with a service center **134** in order to download antivirus software.

[0032] Another kind of attack, a DoS attack, is designed to overwhelm the network and quickly consume its resources. DoS attacks are identified **204** in a similar manner as a battery draining malware by detecting **204** a significant increase of activities associated with a network device **110, 126, 128, 130** or communications with invalid or inactive mobile devices **110**. For example, under a DoS attack, the profile will show the an increase in volume of network traffic within a short time interval. This activity would indicate the likelihood of a DoS attack. Once a possible DoS attack is identified, the security center **134** can analyze **206** the detection results and determine **206** whether or not an attack is actually occurring by taking certain actions, e.g., intercepting the network traffic, and/or sending responses to the suspect source IP addresses and requiring feedback.

[0033] The DoS attack can be mitigated in a similar manner as a battery draining malware attack. In addition, a DoS attack can also be stopped by identifying the malicious sender. For this, IP traceback techniques can be adapted to detect spoofed addresses. Once the sender is identified, corresponding intelligent agents **106** instruct **210** the network to drop the packets associated with the attack. If the sender of the malicious communications is within the service provider's network **102**, intelligent agents **106** disable **216** outbound communications on that mobile device, or restrict **216** communications to stop the malicious activity.

[0034] Referring now to the flowchart of Fig. 3, a monitor in a mobile device scans **302** incoming programs on the mobile device for identifying characteristics of malware to

report **304** to an intelligent agent. Many existing worms can be detected by pre-defined signatures. However, worms that change as they spread or new worms whose signatures are not yet included in antivirus databases cannot be identified based upon signature. Therefore, in addition to the signature-based detection, the monitors, intelligent agents, and security centers cooperate to detect and identify mobile worm malware using heuristic rules that describe suspicious behaviors of worms, e.g., upon infecting one device malicious worms propagate to a different device using standard spreading mechanisms such as Bluetooth or MMS.

[0035] On the client side, a monitor in a mobile device scans **302** incoming programs. Once the monitor detects suspicious behaviors in incoming programs, the monitor **108** marks the program as suspicious and reports **304** the suspect program to the security center. The security center correlates **306** reports from distributed monitors. If a suspicious program is detected from many distributed monitors **108**, the security center concludes that the corresponding program is a spreading worm, performs **308** mitigating actions in the network **102** and instructs intelligent agents **106** to perform **312** mitigating actions in the mobile devices **110**.

[0036] In an embodiment, on the network side, intelligent agents **106** instruct **310** the network **102** to drop or delete the packets associated with the suspect program and provide information to the security system **134**of the network **102** operator. In another embodiment, on the client side, intelligent agents **106** instruct **316** mobile devices to ignore or filter the packets associated with the suspect program. If a mobile device **110**

sending the suspect program is inside the service provider's network **102**, intelligent agents disables **316** outbound communications on that mobile device. In another embodiment, the intelligent agent **106** restricts **316** communications to stop the spread of the suspect program without completely disabling the communications interfaces.

[0037] In another embodiment, the service center also instructs other network level security centers to take action to prevent the work from spreading. The suspicious program is also analyzed in the security centers by experts to determine whether or not the suspect program is truly malicious, and if it is not malicious the security center can reverse the protective measures taken by the intelligent agents.

CONCLUSION

[0038] The embodiments of the invention shown in the drawings and described above are exemplary of numerous embodiments that may be made within the scope of the appended claims. It is contemplated that numerous other configurations of the disclosed system and method for detecting, preventing, and stopping malware attacks on wireless networks may be created taking advantage of the disclosed approach. It is the applicant's intention that the scope of the patent issuing herefrom will be limited only by the scope of the appended claims.

What is claimed is:

1. A malware detection and mitigation system, comprising:

a plurality of monitors operably adapted to scan network communications for a plurality of events;

a detection agent operably adapted to communicate with at least one of said plurality of monitors, to correlate said plurality of said events to detect a malware attack, and to communicate an attack indication when said malware attack is detected; and

a mitigating agent operably adapted to communicate with said detection agent and to trigger a mitigating action in response to said attack indication.

2. The malware detection and mitigation system of claim 1, wherein said mitigating action comprises at least one mitigating action directed to a mobile device and at least one mitigating action directed to a network element.

3. The malware detection and mitigation system of claim 1, wherein said network communications are wireless network communications.

4. The malware detection and mitigation system of claim 1, wherein said malware attack is selected from the group consisting of a battery draining malware attack, a denial of service malware attack, and a mobile worm malware attack.

5. The malware detection and mitigation system of claim 1, wherein said plurality of events is correlated with a characteristic of said malware attack, said characteristic selected from the group consisting of an increase in network traffic to a network element, an increase in network traffic to a network element and a decrease in average packet size, a packet bound for an inactive mobile device, a packet bound for an invalid mobile devices, and a program sent to a plurality of mobile devices.

6. The malware detection and mitigation system of claim 1, wherein each of said plurality of monitors is operably adapted to run on a network element.

7. The malware detection and mitigation system of claim 6, wherein said network element is selected from the group consisting of a handset, a mobile device, a gateway, a traffic sniffer, a honeypot, a router, a switch, and a register.

8. The malware detection and mitigation system of claim 1, wherein said mitigating action is selected from the group consisting of reporting said malware attack, disabling said network communications, restricting said network communications, ignoring said network communications, performing a malware scan, and intercepting said network communications and forwarding to said security center.

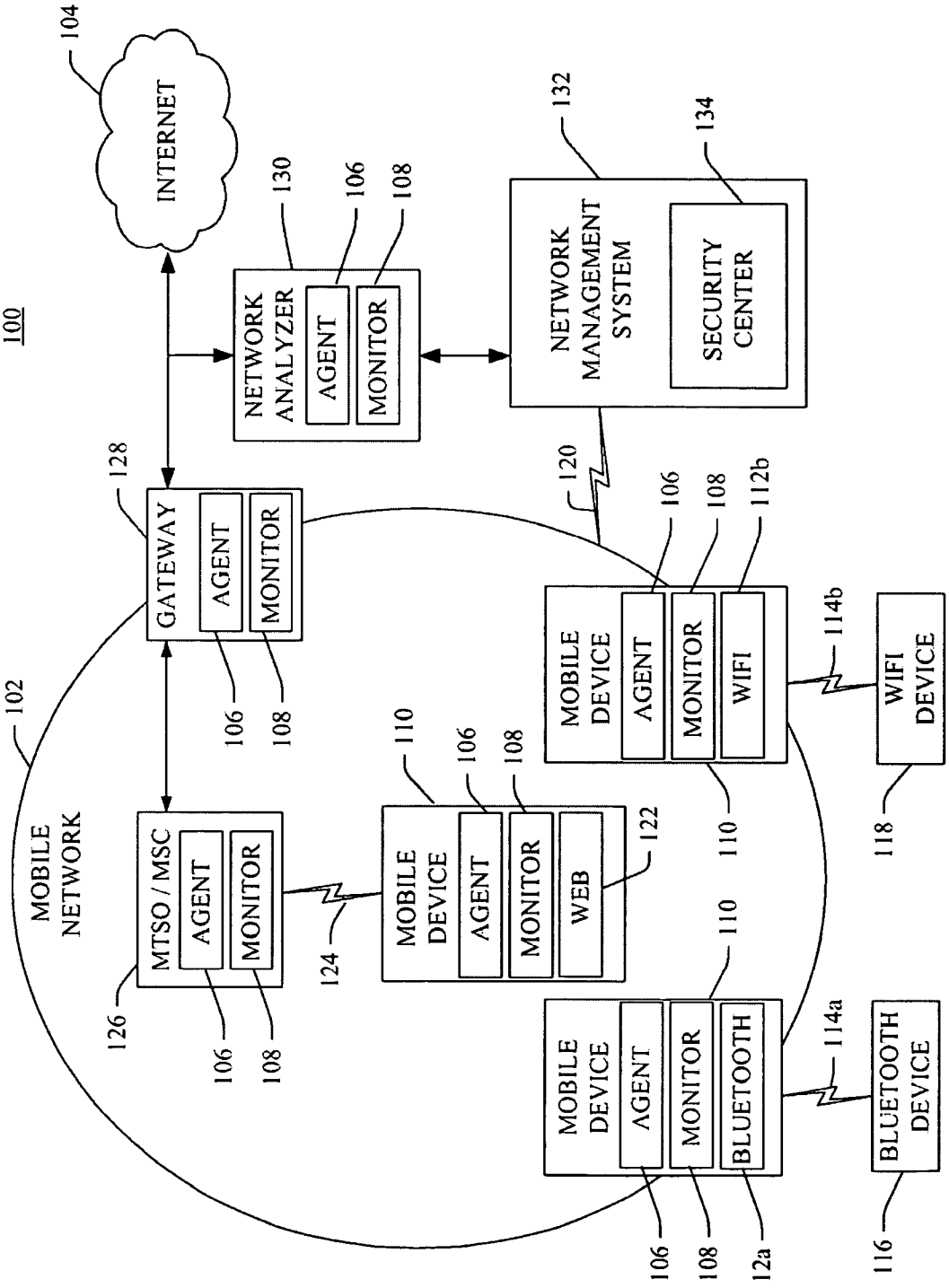

100
INTERNET
104
NETWORK ANALYZER
AGENT
MONITOR
130
106
108
NETWORK MANAGEMENT SYSTEM
SECURITY CENTER
132
134
120
GATEWAY
AGENT
MONITOR
128
MOBILE NETWORK
102
MTSO / MSC
AGENT
MONITOR
126
MOBILE DEVICE
AGENT
MONITOR
WEB
122
124
110
MOBILE DEVICE
AGENT
MONITOR
WIFI
112b
114b
WIFI DEVICE
118
MOBILE DEVICE
AGENT
MONITOR
BLUETOOTH
112a
114a
BLUETOOTH DEVICE
116

FIG. 1

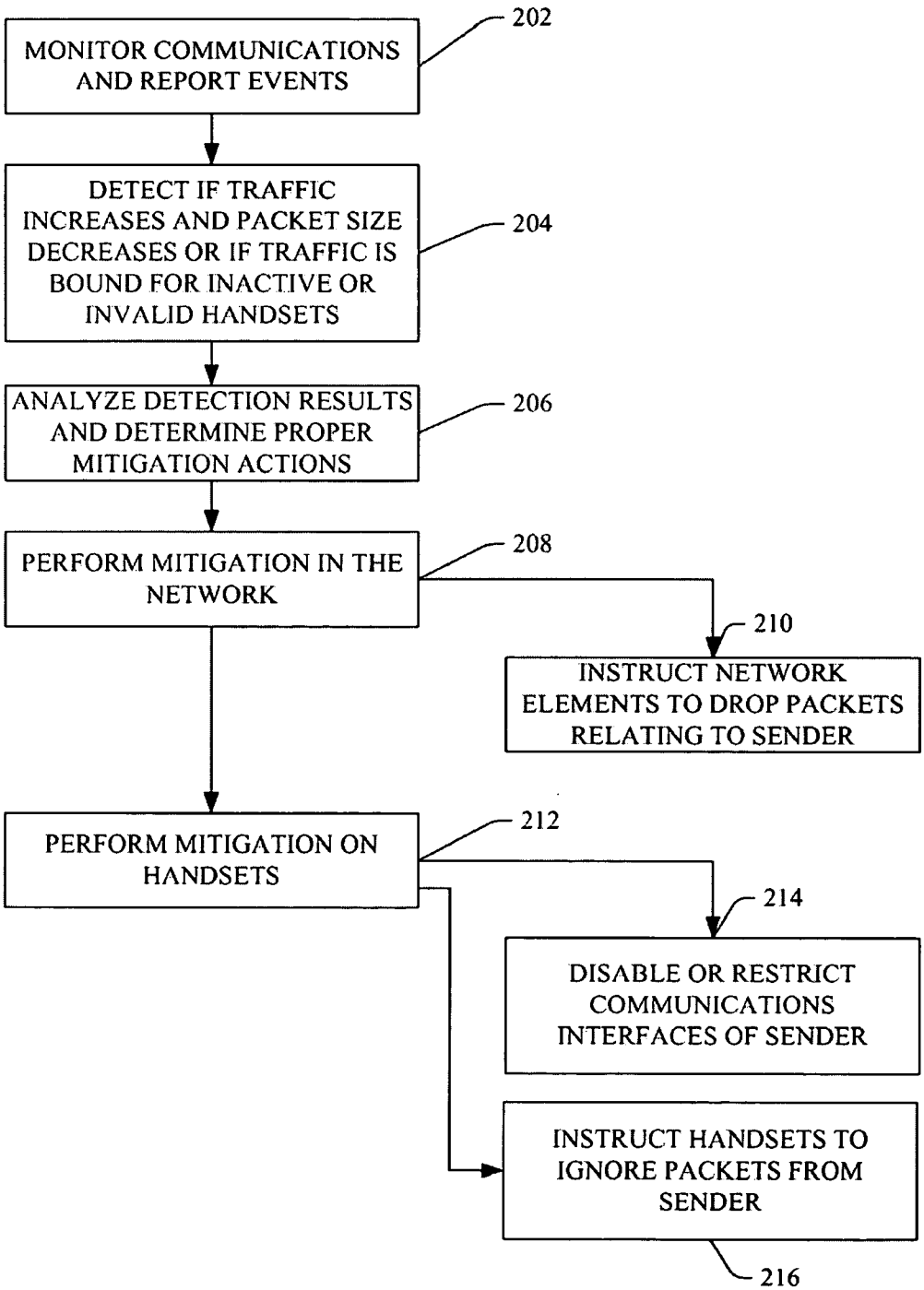

MONITOR COMMUNICATIONS AND REPORT EVENTS
202
DETECT IF TRAFFIC INCREASES AND PACKET SIZE DECREASES OR IF TRAFFIC IS BOUND FOR INACTIVE OR INVALID HANDSETS
204
ANALYZE DETECTION RESULTS AND DETERMINE PROPER MITIGATION ACTIONS
206
PERFORM MITIGATION IN THE NETWORK
208
210
INSTRUCT NETWORK ELEMENTS TO DROP PACKETS RELATING TO SENDER
PERFORM MITIGATION ON HANDSETS
212
214
DISABLE OR RESTRICT COMMUNICATIONS INTERFACES OF SENDER
INSTRUCT HANDSETS TO IGNORE PACKETS FROM SENDER
216

FIG. 2

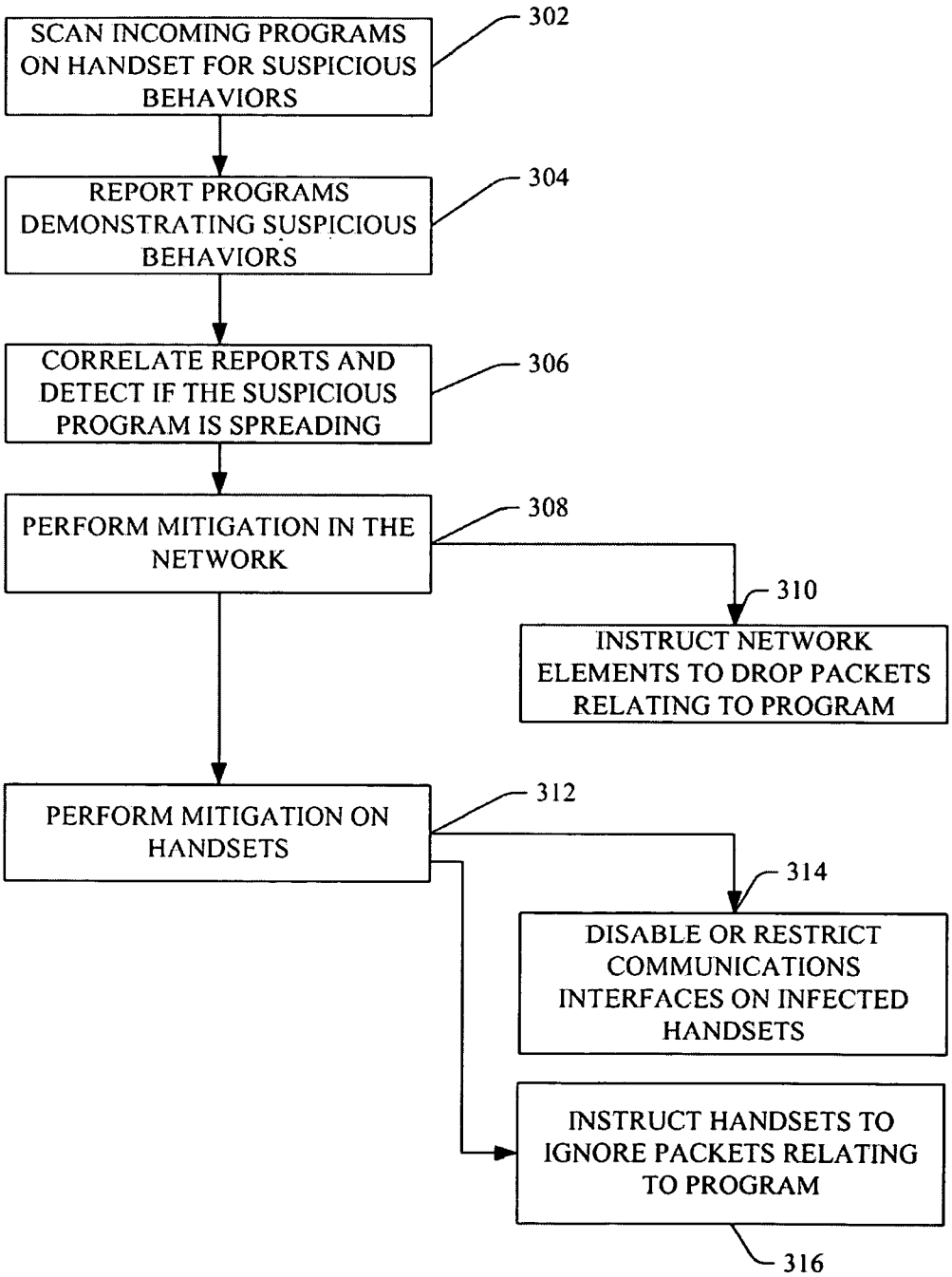

SCAN INCOMING PROGRAMS ON HANDSET FOR SUSPICIOUS BEHAVIORS
302
REPORT PROGRAMS DEMONSTRATING SUSPICIOUS BEHAVIORS
304
CORRELATE REPORTS AND DETECT IF THE SUSPICIOUS PROGRAM IS SPREADING
306
PERFORM MITIGATION IN THE NETWORK
308
310
INSTRUCT NETWORK ELEMENTS TO DROP PACKETS RELATING TO PROGRAM
PERFORM MITIGATION ON HANDSETS
312
314
DISABLE OR RESTRICT COMMUNICATIONS INTERFACES ON INFECTED HANDSETS
INSTRUCT HANDSETS TO IGNORE PACKETS RELATING TO PROGRAM
316

FIG. 3