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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 January 2018 (18.01.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/013521 A1

(51) International Patent Classification:
G06F 11/30 (2006.01) *G06F 21/55* (2013.01)
G06F 11/34 (2006.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US2017/041463

(22) International Filing Date:
11 July 2017 (11.07.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/211,968 15 July 2016 (15.07.2016) US

(71) Applicant: **A10 NETWORKS, INC.** [US/US]; 3 West Plumeria Drive, San Jose, California 95134 (US).

(72) Inventors: **JALAN, Rajkumar**; 3 West Plumeria Drive, San Jose, California 95134 (US). **SZETO, Ronald Wai Lun**; 3 West Plumeria Drive, San Jose, California 95134 (US). **SAMPAT, Rishi**; 3 West Plumeria Drive, San Jose, California 95134 (US). **LIN, Julia**; 3 West Plumeria Drive, San Jose, California 95134 (US).

(74) Agent: **KLINE, Keith E.**; Ampacc Law Group, LLP, 6100 219th St. S.W., Suite 580, Mountlake Terrace, Washington 98043 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: AUTOMATIC CAPTURE OF NETWORK DATA FOR A DETECTED ANOMALY

(57) Abstract: Methods and systems are provided for automatically capturing network data for a detected anomaly. In some examples, a network node establishes a baseline usage by applying at least one baselining rule to network traffic to generate baseline statistics, detects an anomaly usage by applying at least one anomaly rule to network traffic and generating an anomaly event, and captures network data according to an anomaly event by triggering at least one capturing rule to be applied to network traffic when an associated anomaly event is generated.

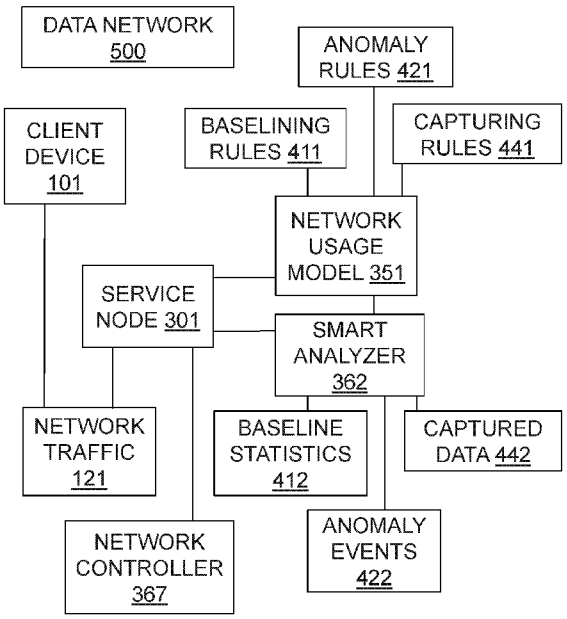

FIG. 1

WO 2018/013521 A1

[Continued on next page]

Declarations under Rule 4.17:

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

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

Published:

— *with international search report (Art. 21(3))*

AUTOMATIC CAPTURE OF NETWORK DATA FOR A DETECTED ANOMALY

BACKGROUND OF THE INVENTION

Cross-Reference to Related Applications

[0001] This application claims priority to U.S. Patent Application No. 15/211,968, filed July 15, 2016 incorporated by reference herein in its entirety.

Filed of the Invention

[0002] This invention relates generally to data network and more particularly to a network node automatically capturing network data during an anomaly.

Description of the Related Art

[0003] Both consumer computing and business computing are moving at a fast pace toward mobile computing and cloud computing. Data networks that support mobile computing and cloud computing needs are growing at accelerated rates. These data networks behave differently from prior data networks supporting mostly static computing environments such as desktops, offices, and server rooms. In a mobile computing environment, users do not stay in a place for a long time. They move from place to place in a matter of hours, minutes, or even seconds as the users may be in a driving vehicle or strolling on a street. In a cloud computing environment, enterprise or service servers are allocated in different data centers in different locations, perhaps in different cities or countries. The servers may be allocated on demand and may be brought to service in a matter of minutes. Therefore, in today's data networks, it is difficult, if not impossible, to predict where a user terminal is or where a server is for a network service session. The task for a network administrator to troubleshoot a data network is very difficult. Once a data network is put in place based on a current plan, a network administrator must oversee the usage of the data network and address any usage anomaly due to unexpected usage or failure of the network. Typically, a usage anomaly occurs when a service becomes popular, leading to excessive server access, or when a resource or facility fails causing traffic to be routed and congested. In the new mobile and cloud computing environments, the same usage showing a healthy functioning data network yesterday may lead to a congested server without any failure of data network. In part, the anomaly may be caused by changing locations of mobile users. In

part, it may be caused by changing of allocation of servers. In part, it may be caused by a combination of mobile users and server allocation. When an anomaly occurs, it is important for the network administrator to examine detailed data to determine the cause, so as to correct the configurations of the data network.

[0004] It should be apparent from the foregoing that there is a need to provide a smart analyzer to assist a network element to capture detailed network data during a network usage anomaly.

SUMMARY

[0005] This summary is provided to introduce a selection of concepts in a simplified form that are further described in the Detailed Description below. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

[0006] According to some embodiments, the present technology is directed to a network node for detecting and storing network usage anomalies, the network node storing instructions that when executed by at least one processor: establish a baseline usage by applying at least one baselining rule to network traffic to generate baseline statistics; detect an anomaly usage by applying at least one anomaly rule to network traffic and generating an anomaly event; and capture network data according to an anomaly event by triggering at least one capturing rule to be applied to network traffic when an associated anomaly event is generated.

[0007] According to other embodiments, the present technology is directed to a corresponding method for capturing network data during a network usage anomaly based on a network usage model,

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Embodiments are illustrated by way of example and not by limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

[0009] FIG. 1 illustrates an exemplary embodiment of a network node capturing network data during an anomaly event.

[0010] FIG. 2 illustrates an exemplary embodiment of a network node.

[0011] FIG. 3 illustrates an exemplary embodiment of establishing a baseline usage.

[0012] FIG. 4 illustrates an exemplary embodiment of detecting an anomaly usage.

[0013] FIG. 5 illustrates an exemplary embodiment of capturing network data according to an anomaly event.

DETAILED DESCRIPTION

[0014] The following detailed description includes references to the accompanying drawings, which form a part of the detailed description. The drawings show illustrations in accordance with example embodiments. These example embodiments, which are also referred to herein as "examples," are described in enough detail to enable those skilled in the art to practice the present subject matter. The embodiments can be combined, other embodiments can be utilized, or structural, logical, and electrical changes can be made without departing from the scope of what is claimed. The following detailed description is therefore not to be taken in a limiting sense, and the scope is defined by the appended claims and their equivalents.

[0015] FIG. 1 illustrates an exemplary embodiment of a network node capturing network data during an anomaly event. In the exemplary embodiment, service node 301 connects to data network 500 and receives network traffic 121. In some embodiments, network traffic 121 includes a plurality of network data transmitted by one or more network devices, such as client device 101. Service node 301 analyzes network traffic 121 according to a network usage model 351.

[0016] In exemplary embodiments, service node 301 includes a smart analyzer 362 to process network traffic 121 based on network usage model 351. Network usage model 351 may include at least one baselining rule 411, at least one anomaly rule 421, or at least one data capturing rule 441. In some embodiments, smart analyzer 362 processes baselining rules 411 and generates baseline statistics 412; processes anomaly rules 421 and generates at least one anomaly event 422; and processes capturing rules 441 to generate captured data 442. In further embodiments, smart analyzer 362 processes anomaly rules 421 together with baselining rules 411 and/or baseline statistics 412 to generate anomaly event 422. In some embodiments, smart analyzer 362 processes capturing rules 441 according to anomaly event 422 to generate captured data 442 for anomaly event 422.

[0017] In exemplary embodiments, service node 301 stores baseline statistics 412, anomaly event 422, and/or captured data 442 in a storage medium of service node 301. Service node 301 may send baseline statistics 412, anomaly event 422, and/or captured data 442 to network controller 367 computing device, which may be a network computer such as a network management system for storage or for further processing.

[0018] FIG. 2 illustrates an exemplary embodiment of a network node 510 or a network computer which can be a security gateway, a client device, a server device, or the like. Network node 510 may include a processor module 560, a network module 530, and a storage module 540. Processor module 560 may include at least one processor which may be a micro-processor, an Intel processor, an AMD processor, a MIPS processor, an ARM-based processor, a RISC processor, or any other type of processor. Processor module 560 may include at least one processor core embedded in a processor. Additionally, processor module 560 may include at least one embedded processor or embedded processing element in a Field Programmable Gate Array (FPGA), an Application Specific Integrated Circuit (ASIC), or Digital Signal Processor (DSP). In some embodiments, network module 530 includes a network interface such as Ethernet, optical network interface, a wireless network interface, T1 / T3 interface, a WAN or LAN interface. Furthermore, network module 530 may include a network processor. Storage module 540 may include RAM, DRAM, SRAM, SDRAM or memory utilized by processor module 560 or network module 530. Storage module 540 may store data utilized by processor module 560. In some embodiments, storage module 540 includes a hard disk drive, a solid state drive, an external disk, a DVD, a CD, or a readable external disk. Additionally, storage module 540 may store at least one computer programming instruction which when executed by processor module 560 or network module 530 implement at least one of the functionality of the present invention. Network node 510 may also include an input/output (I/O) module 570, which may include a keyboard, a keypad, a mouse, a gesture-based input sensor, a microphone, a physical or sensory input peripheral, a display, a speaker, or a physical or sensory output peripheral.

[0019] Returning to FIG. 1, in some embodiments, client device 101 is a network node, as illustrated in FIG. 2, connected to data network 500. Client device 101 can be a personal computer, a laptop computer, a tablet, a smartphone, a mobile phone, an Internet phone, a netbook, a home gateway, a broadband gateway, a network appliance, a set-top box, a media

server, a personal media play, a personal digital assistant, an access gateway, a networking switch, a server computer, a network storage computer, or any computing device comprising at least a network module and a processor module.

[0020] In exemplary embodiments, service node 301 is a network node and includes at least one of a functionality of a firewall, a SSL proxy gateway, a server load balancer (SLB), an application delivery controller (ADC), a threat protection system (TPS), a secure traffic manager, a legal interception gateway, a virtual private network (VPN) gateway, or a TCP proxy gateway. In another embodiment, service node 301 includes at least one of a functionality of a network switch, a network router, a security network appliance, a broadband gateway, a broadband remote access system, or a layer 2 or layer 3 network element.

[0021] In some embodiments, smart analyzer 362 includes a piece of software residing and executing in service node 301. In exemplary embodiments, smart analyzer 362 includes at least one of a processor module, a storage module, or a piece of hardware-based network processing module.

[0022] Data network 500 may include an Ethernet network, an ATM network, a cellular network, a wireless network, a Frame Relay network, an optical network, an IP network or any data communication network utilizing other physical layer, link layer capability or network layer to carry data packets. Additionally, data network 500 may include a corporate network, a data center network, the Internet, a service provider network, or a mobile operator network.

[0023] FIG. 3 illustrates an exemplary embodiment of establishing a baseline usage. In this embodiment, smart analyzer 362 processes network usage model 351, which includes baselining rules 411 to generate baseline statistics 412. In some embodiments, baselining rules 411 include criteria 415, which indicates a method to process network traffic 121 in order to generate statistic data for baseline statistics 412. Network traffic 121 may include data packets at link layer, such as Ethernet, WLAN, or VLAN; network layer, such as IP packets; session layer, such as TCP, UDP, IPSec, or SSL; or application layer, such as HTTP, FTP, telnet, network applications, or applications such as video streaming, music streaming, email, instant messaging, or photo upload. In various embodiments, criteria 415 includes a filter 419 which indicates at least one filter criteria for processing network traffic 121. Network traffic 121 satisfying filter 419 is processed to generate baseline statistics 412. In some embodiments, filter 419 includes a

network address such as an IP address, a source IP address, or a destination IP address. In the exemplary embodiment of FIG. 3, IP data packets of network traffic 121 having the specified network address in filter 419 are processed. In some embodiments, filter 419 includes a network interface or its identity, such as an Ethernet interface, a VLAN interface, a virtual interface, a virtual routing interface, a physical interface, or a port of a network module of the network node. Filter 419 can specify a content pattern such as a URL, a domain name, a cookie, or a file name of an application layer protocol such as HTTP or FTP. Filter 419 also can indicate a content signature such as a user identity, a universally unique identifier (UUID) of a smartphone, a device identity, or a mobile application identity.

[0024] In some embodiments, baselining rules 411 include a time duration 416 indicating a duration of time where the baselining rules 411 are to be applied to generate baseline statistics 412. For example, time duration 416 may include morning hours, 5am-8am, lunch hour, 12pm-2pm, evening, weekend, a day of a year, Feb 14, a range of days, June 1-August 15, day of a week, Monday morning, Friday evening, 12:15pm – 4:27pm today, or any duration of time or days. In exemplary embodiments, smart analyzer 362 is connected to a clock 365 and checks clock 365 against time duration 416 to start and stop applying baselining rules 411.

[0025] In various embodiments, baselining rules 411 include usage 418, indicating at least one quantitative counter to be calculated by smart analyzer 362 in order to generate baseline statistics 412. Usage 418 may indicate packet length, session count, bandwidth utilization, a rate, such as rate per second, rate per minute, rate per hour, rate per day, rate per millisecond, or other types. For example, combining usage 418, filter 419, and time duration 416, baselining rules 411 may specify to smart analyzer 362 to count packet lengths of IP packets over an interface where the destination IP address is in range 134.154.1.0 to 134.154.27.234, or to count HTTP session rate per minute during Christmas 2015 for domain names abc.com and google.com, or to count bandwidth usage of all interfaces on the gigabit Ethernet card in the last 24 hours.

[0026] In some embodiments, smart analyzer 362 processes baselining rules 411 and determines one or more counters accordingly. Moreover, smart analyzer 362 may generate one or more baseline statistics 412 based on the counters. In an exemplary embodiment, smart analyzer 362 calculates a minimum value, a maximum value, a mean value, or a median value of

the counters. In another embodiment, smart analyzer 362 calculates values based on a statistical model such as a standard deviation, a second moment, or a distribution, based on the counters. In further embodiments, smart analyzer 362 calculates these statistical values as baseline statistics 412. Furthermore, smart analyzer 362 stores baseline statistics 412 in a datastore or storage medium of service node 301.

[0027] FIG. 4 illustrates an exemplary embodiment of detecting an anomaly usage. In this embodiment, network usage model 351 includes anomaly rules 421 to help detect an anomaly usage indicated by anomaly event 422. In some embodiments, anomaly rules 421 include at least one criteria 425 and/or a time duration 426. Time duration 426 includes a period of time when anomaly rules 421 is to be applied. Time duration 426 may include, for example, morning hours, 8am-5pm, midnight, weekend, every weekday, Christmas, or any duration of time. In various embodiments, criteria 425 includes a filter 429, which may include at least one network address, piece of content, content signature, network interface, or other filter to be applied for anomaly rules 421. In exemplary embodiments, smart analyzer 362 connects to clock 365, and based on matching clock 365 and time duration 426, determines to apply anomaly rules 421 to network traffic 421. Smart analyzer 362 receives network traffic 421 and applies filter 429 of anomaly rules 421 to received network traffic 421. In some embodiments, anomaly rules 421 further includes usage 428, which indicates one or more means for smart analyzer 362 to count or calculate when processing network traffic 421. Usage 428 may indicate packet length, session count, bandwidth utilization, a rate, or other counting means. Upon determining at least one usage counter after applying usage 428, smart analyzer 362 applies criteria 425 to the at least one usage counters to determine if criteria 425 is satisfied. In various embodiments, criteria 425 indicates a deviation from a pre-determined metric to signal an anomaly. For example, criteria 425 may include calculation of a plurality of deviations from a plurality of metrics based on the usage counters in order to determine an anomaly. In some embodiments, criteria 425 is determined to be satisfied. Smart analyzer 362 generates an anomaly event 422 for the satisfied criteria 425. In various embodiments, usage 428 is associated to previously determined baseline statistics 412 as illustrated in this application. Smart analyzer 362 retrieves baseline statistics 412, from a storage medium or datastore, which may include statistical data such as minimum, maximum, mean, or median. Smart analyzer 362 uses baseline statistics 412 when applying criteria 425 with the usage counters. In some embodiments, criteria 425 includes spread 427,

which indicates a range of values when comparing calculated usage counters and baseline statistics 412. Criteria 425 may include a rule to compare whether a session rate usage counter, determined from usage 428, is larger than a spread 427 of 200% of a maximum session rate usage counter according to baseline statistics 412. If the rule is satisfied, criteria 425 indicates there is an anomaly. In another embodiment, criteria 425 includes a rule to be satisfied over a time duration, such as 3 seconds, 1 minute, 2 hours, or any other time duration in order to indicate an anomaly.

[0028] FIG. 5 illustrates an exemplary embodiment of capturing network data according to an anomaly event. In this embodiment, network usage model 351 includes capturing rules 441, which when applied, allows smart analyzer 362 to process network traffic 121 to generate captured data 442. In some embodiments, capturing rules 441 associate to anomaly event 422, which when generated, triggers capturing rules 441 to be applied. In exemplary embodiments, capturing rules 441 include a time duration 446 indicating a duration of time to capture data. Time duration 446 may include a start time, a stop time, 10 seconds, 500 milliseconds, 20 milliseconds, 2 hours, one day, every other hour, or any duration of time. In another embodiment, capturing rules 441 includes an action 445 indicating a data capturing action. For example, action 445 may indicate "capture packet trace", "trace session", "record user cookies and timestamp", "capture GET-REQUEST:URL", "record TCP:option fields" or other capturing action with an indication of data to be captured. Furthermore, in some embodiments, capturing rules 441 include a filter 449 to be applied to network traffic 121 when action 445 is used to capture data. Filter 449 may include a network address, a content pattern, an interface, a protocol, or other filter. Additionally, filter 449 may indicate a source IP address, a content pattern matching a file name, a virtual service IP address, and a protocol of HTTP.

[0029] In an exemplary embodiment, capturing rules 441 indicates an association to anomaly event 422, which indicates a high access rate of website internal.abcde.com; a time duration 446 of start time in one minute and a duration of one hour; an action 445 to capture session timestamps, source IP address, or user-id in cookies; a filter 449 to indicate virtual IP address corresponding to abcde.com, protocol of HTTP, or a content pattern matching "internal.abcde.com".

[0030] Smart analyzer 362, upon applying capturing rules 441 to network traffic 121, generates captured data 442. Smart analyzer 362 generates a data entry 444, according to action 445, to be stored in captured data 442. Data entry 444 may include a timestamp, a packet trace, a session trace of all content for the session, a network address, or a piece data captured according to action 445.

[0031] Smart analyzer 362 sends captured data 442 to network controller 367. In another embodiment, smart analyzer 362 sends anomaly event 422 to network controller 367. Network controller 367 processes anomaly event 422 and requests smart analyzer 362 to apply capturing rules 441 of network usage model 351. In some embodiments, network controller 367 sends network usage model 551 or capturing rules 441 to smart analyzer 362.

[0032] The invention can be used to detect and record security anomaly using a network usage model 351 including a combination of baselining rules 411, anomaly rules 421, and capturing rules 441. The following tables illustrate one or more security anomaly addressed using this invention.

[0033] Table 1. Mismatch IP and Layer 2 packet length Usage Model

Anomaly Rules

Filter: IP Packet Length does not match Ethernet packet length

Usage: Packet Count Rate per second (PPS)

Criteria: PPS > 100

Capturing Rules

Filter: IP Packet Length does not match Ethernet packet length

Time Duration: Start immediate, Duration 60 seconds

Action: Record Timestamp, Source IP Address, network interface id, IP packet length

[0034] Table 2. Fragmentation Attack Usage Model

Baselining Rules

Filter: IP Fragment Packet

Criteria: Fragment Length < 10 bytes

Usage: Packet count

Time Duration: 12:00am-12:00pm tomorrow

Anomaly Rules

Filter: IP Fragment Packet, Fragment Length < 10 bytes

Usage: Packet Count Rate per second (PPS)

Criteria: PPS > 100 * (maximum of baseline statistics / 24 hr)

Capturing Rules

Filter: IP Fragment Packet, Fragment length < 20 bytes

Time Duration: Start immediate, Duration 60 seconds

Action: Record Timestamp, IP packet trace

[0035] Table 3. LAND(Local Area Network Denial) Attack Usage Model

Baselining Rules

Filter: IP Packet

Criteria: Source port being the same as Destination port

Usage: Packet count

Time Duration: 12:00am-12:00pm tomorrow

Anomaly Rules

Filter: IP Packet, Source port being the same as Destination port

Usage: Packet Count Rate per second (PPS)

Criteria: PPS > 100 * (maximum of baseline statistics / 24 hr)

Capturing Rules

Filter: IP Packet, Source port being the same as Destination port

Time Duration: Start immediate, Duration 10 seconds

Action: Record Timestamp, IP packet header

[0036] Table 4. Slow Loris Attack Usage Model

Baselining Rules

Filter: TCP Packet, Virtual IP interface

Usage: Packet Length

Time Duration: 12:00am-12:00pm tomorrow

Anomaly Rules

Filter: TCP Packet, Virtual IP interface

Usage: Average Packet Length

Criteria: Average Packet Length < Average Baseline Statistics * 30%

Capturing Rules

Filter: TCP Packet, Virtual IP interface

Time Duration: Start in 1 second, duration 5 seconds

Action: Record Timestamp, IP packet header

[0037] The description of the present technology has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. Exemplary embodiments were chosen and described in order to best explain the principles of the present technology and its practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

[0038] Aspects of the present technology are described above with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by programming instructions. These

programming instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

CLAIMS

What is claimed is:

1. A computer-implemented method for capturing network data during a network usage anomaly based on a network usage model, comprising:

establishing a baseline usage by applying at least one baselining rule to network traffic to generate baseline statistics;

detecting an anomaly usage by applying at least one anomaly rule to network traffic and generating an anomaly event; and

capturing network data according to an anomaly event by triggering at least one capturing rule to be applied to network traffic when an associated anomaly event is generated.

2. The computer-implemented method of claim 1, wherein the at least one baselining rule comprises at least one of: a criteria indicating a method to process network traffic to generate baseline statistic data, a network usage indicating at least one quantitative counter to be calculated to generate the baseline statistics, and a time duration for applying the at least one baselining rule to generate the baseline statistics.
3. The computer-implemented method of claim 2, wherein the criteria indicating a method to process network traffic comprises at least one filter for processing network traffic.
4. The computer-implemented method of claim 3, wherein if the network traffic satisfies at least one filter, the network traffic is processed to generate the baseline statistics.
5. The computer-implemented method of claim 3, wherein the at least one filter comprises at least one of a network address, a network interface, a content pattern, and a content signature.
6. The computer-implemented method of claim 2, wherein the network usage indicating at

least one quantitative counter to be calculated to generate the baseline statistics comprises at least one of a packet length, a session count, a bandwidth utilization, and a session rate.

7. The computer-implemented method of claim 1, wherein the at least one anomaly rule comprises at least one of a criteria indicating an anomaly, a network usage indicating at least one quantitative counter to be calculated when processing network traffic, and a time duration indicating when the at least one anomaly rule is to be applied.

8. The computer-implemented method of claim 7, wherein the criteria indicating an anomaly includes at least one filter comprising at least one of a network address, a network interface, a content pattern, and a content signature.

9. The computer-implemented method of claim 7, wherein the network usage indicating at least one quantitative counter to be calculated when processing network traffic comprises at least one of a packet length, a session count, a bandwidth utilization, and a session rate.

10. The computer-implemented method of claim 7, wherein the generating an anomaly event comprises at least one of: satisfying an anomaly rule, determining if the criteria indicating an anomaly is satisfied when applied to the network usage indicating at least one quantitative counter to be calculated when processing network traffic, and determining if the criteria indicating an anomaly deviates from at least one pre-determined metric based on the network usage

11. The computer-implemented method of claim 1, wherein the at least one capturing rule comprises at least one of a time duration to capture data, a data capturing action, and a filter.

12. The computer-implemented method of claim 11, wherein captured network data

comprises at least one of a timestamp, a packet trace, a session trace of all content for a session, a network address, or data captured according to a data capturing action.

13. A network node for detecting and storing network usage anomalies, the network node storing instructions that when executed by at least one processor:

establish a baseline usage by applying at least one baselining rule to network traffic to generate baseline statistics;

detect an anomaly usage by applying at least one anomaly rule to network traffic and generating an anomaly event; and

capture network data according to an anomaly event by triggering at least one capturing rule to be applied to network traffic when an associated anomaly event is generated.

14. The network node of claim 13, wherein the at least one baselining rule comprises at least one of: a criteria indicating a method to process network traffic to generate the baseline statistic data, a network usage indicating at least one quantitative counter to be calculated to generate baseline statistics, and a time duration for applying the at least one baselining rule to generate baseline statistics.

15. The network node of claim 14, wherein the criteria indicating a method to process network traffic to generate the baseline statistic data comprises at least one filter for processing network traffic.

16. The network node of claim 15, wherein if the network traffic satisfies at least one filter, the network traffic is processed to generate the baseline statistics.

17. The network node of claim 15, wherein the at least one filter comprises at least one of a

network address, a network interface, a content pattern, and a content signature.

18. The network node of claim 14, wherein the network usage indicating at least one quantitative counter to be calculated to generate baseline statistics comprises at least one of a packet length, a session count, a bandwidth utilization, and a session rate.

19. The network node of claim 13, wherein the at least one anomaly rule comprises at least one of a criteria indicating an anomaly, a network usage indicating at least one quantitative counter to be calculated when processing network traffic, and a time duration indicating when the at least one anomaly rule is to be applied.

20. The network node of claim 19, wherein the criteria indicating an anomaly includes at least one filter comprising at least one of a network address, a network interface, a content pattern, and a content signature.

21. The network node of claim 19, wherein the network usage indicating at least one quantitative counter to be calculated when processing network traffic comprises at least one of a packet length, a session count, a bandwidth utilization, and a session rate.

22. The network node of claim 19, wherein the generating an anomaly event comprises at least one of: satisfying an anomaly rule, determining if the criteria indicating an anomaly is satisfied when applied to the network usage indicating at least one quantitative counter to be calculated when processing network traffic, and determining if the criteria indicating an anomaly deviates from at least one pre-determined metric based on the network usage.

23. The network node of claim 13, wherein the at least one capturing rule comprises at least one of a time duration to capture data, a data capturing action, and a filter.

24. The network node of claim 23, wherein captured network data comprises at least one of a timestamp, a packet trace, a session trace of all content for a session, a network address, or data captured according to a data capturing action.

25. A non-transitory computer-readable medium comprising computer readable code, which when executed by one or more processors, implements a method for capturing network data during a network usage anomaly based on a network usage model, comprising:

establishing a baseline usage by applying at least one baselining rule to network traffic to generate baseline statistics;

detecting an anomaly usage by applying at least one anomaly rule to network traffic and generating an anomaly event; and

capturing network data according to an anomaly event by triggering at least one capturing rule to be applied to network traffic when an associated anomaly event is generated.

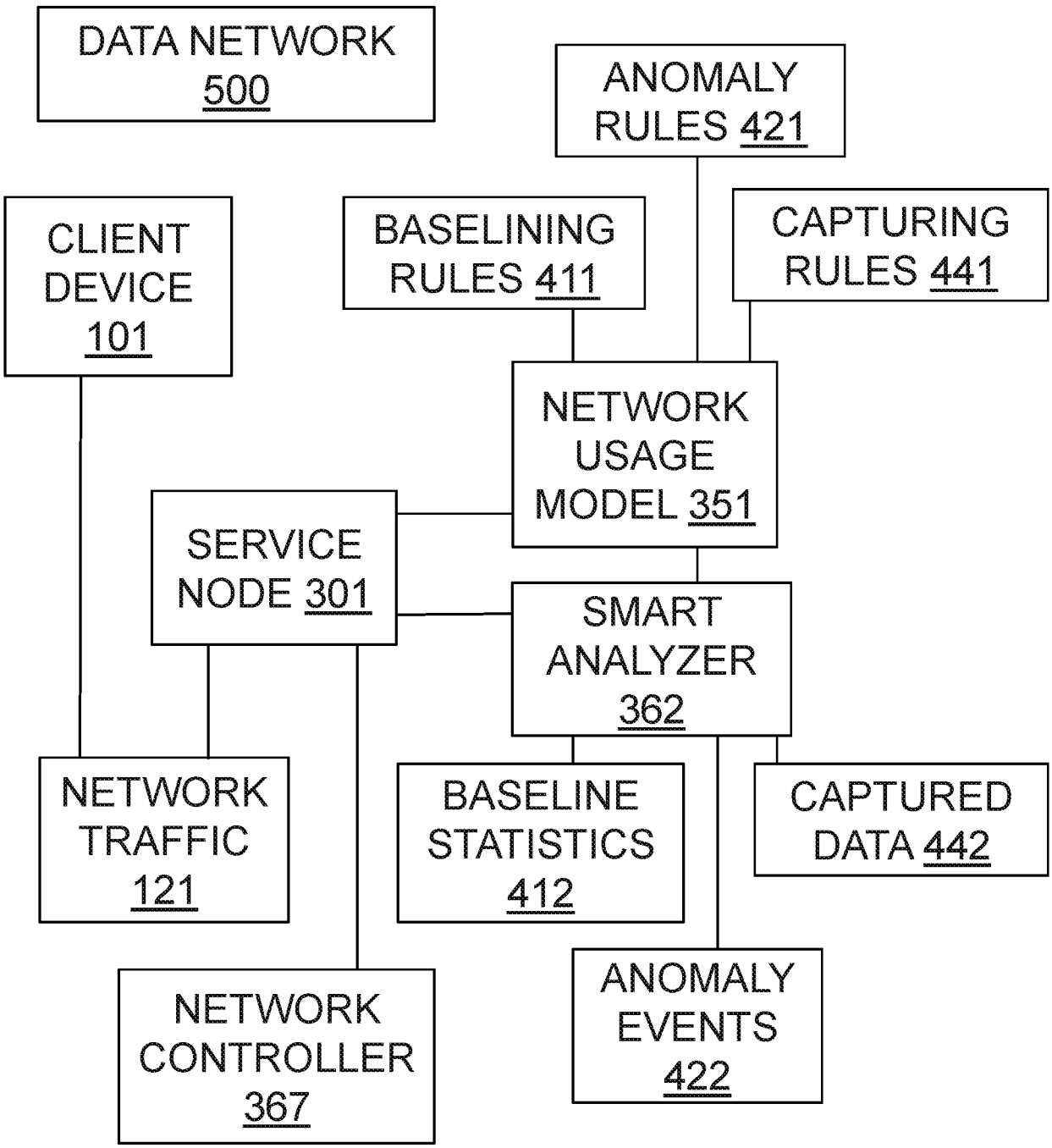
DATA NETWORK 500
ANOMALY RULES 421
CLIENT DEVICE 101
BASELINING RULES 411
CAPTURING RULES 441
NETWORK USAGE MODEL 351
SERVICE NODE 301
SMART ANALYZER 362
NETWORK TRAFFIC 121
BASELINE STATISTICS 412
CAPTURED DATA 442
NETWORK CONTROLLER 367
ANOMALY EVENTS 422

FIG. 1

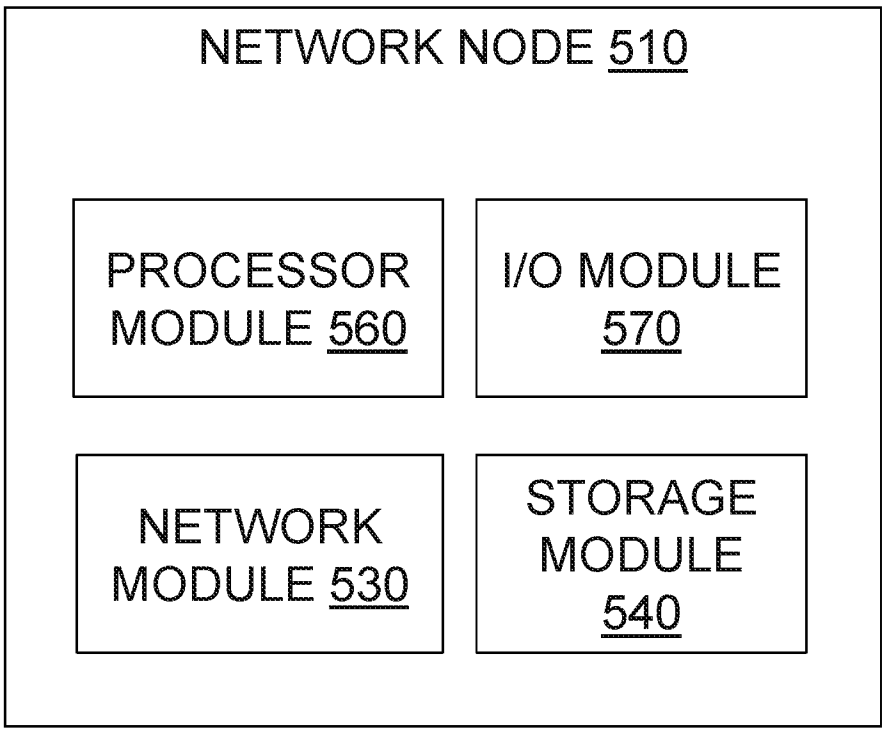
NETWORK NODE 510
PROCESSOR MODULE 560
I/O MODULE 570
NETWORK MODULE 530
STORAGE MODULE 540

FIG. 2

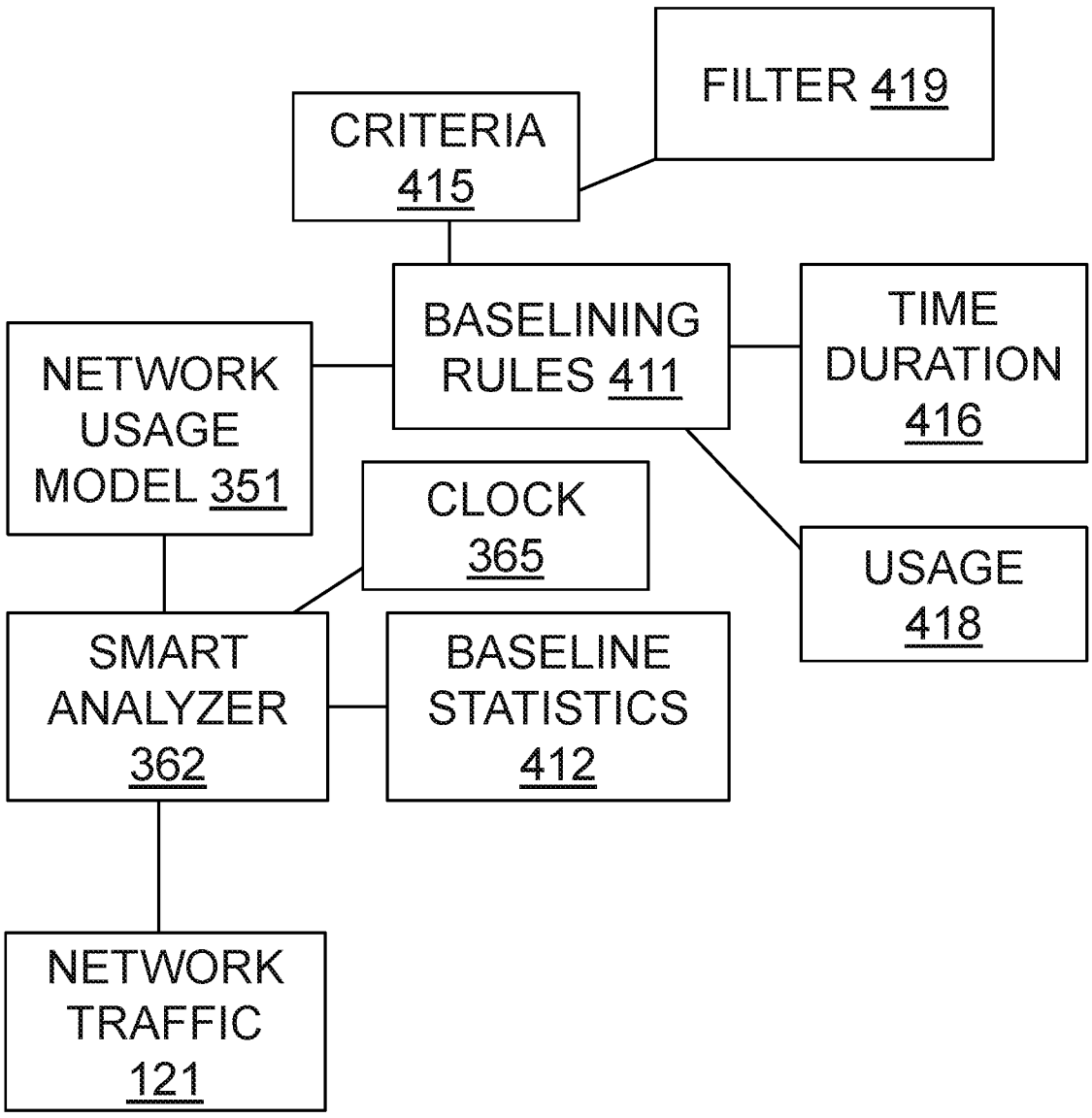
FILTER 419
CRITERIA 415
BASELINING RULES 411
TIME DURATION 416
NETWORK USAGE MODEL 351
CLOCK 365
USAGE 418
SMART ANALYZER 362
BASELINE STATISTICS 412
NETWORK TRAFFIC 121

FIG. 3

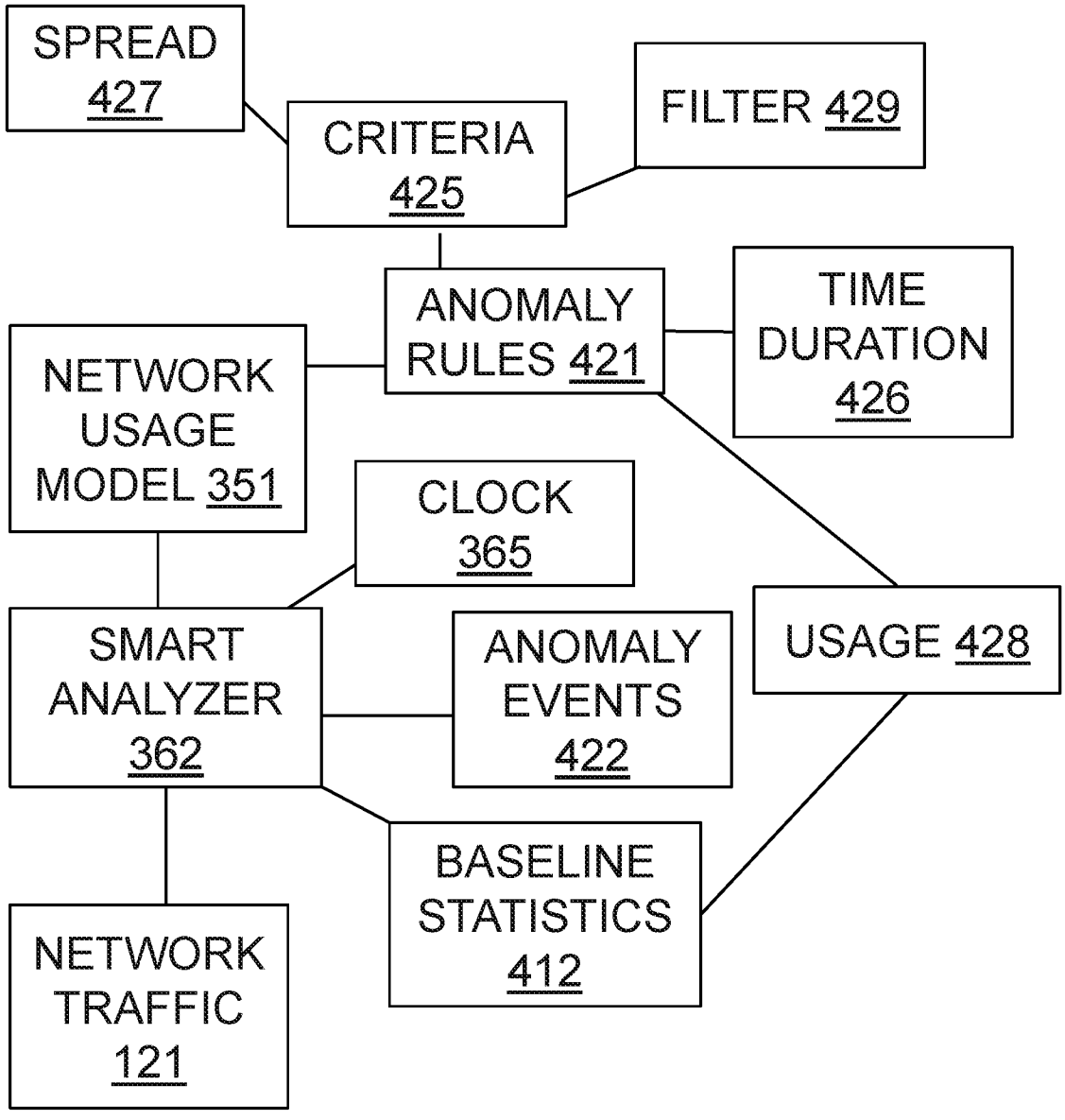
SPREAD 427
CRITERIA 425
FILTER 429
ANOMALY RULES 421
TIME DURATION 426
NETWORK USAGE MODEL 351
CLOCK 365
USAGE 428
SMART ANALYZER 362
ANOMALY EVENTS 422
BASELINE STATISTICS 412
NETWORK TRAFFIC 121

FIG. 4

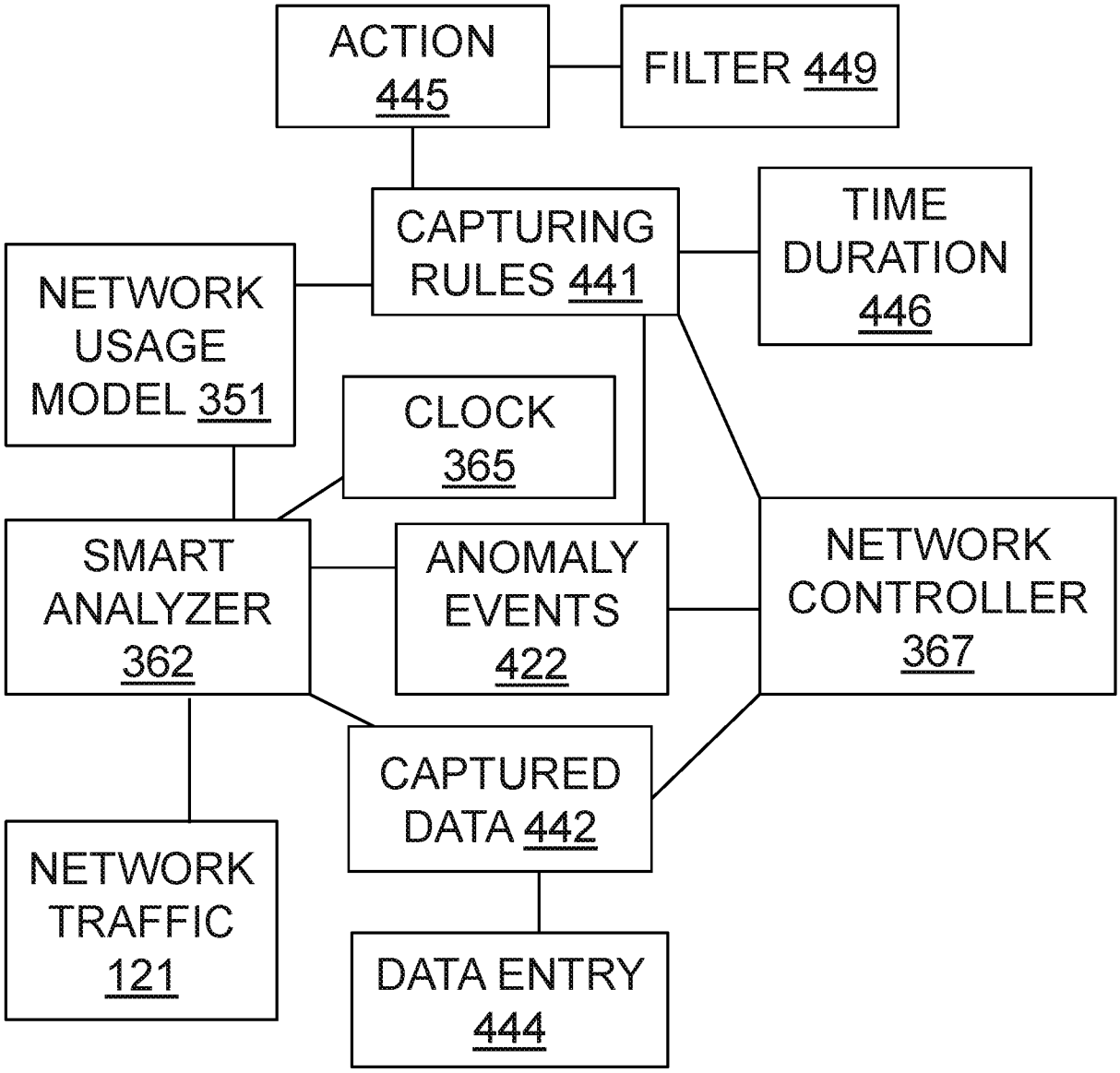
ACTION 445
FILTER 449
CAPTURING RULES 441
TIME DURATION 446
NETWORK USAGE MODEL 351
CLOCK 365
SMART ANALYZER 362
ANOMALY EVENTS 422
NETWORK CONTROLLER 367
CAPTURED DATA 442
NETWORK TRAFFIC 121
DATA ENTRY 444

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2017/041463

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 11/30; G06F 11/34; G06F 21/55; H04L 29/06 (2017.01)
CPC - G06F-011/07/09; H04L 63/14; H04L 63/1425; H04L 63/20 (2017.08)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 706/12.000; 707/728.000; 714/4.200; 714/20.000; 726/1.000 (keyword delimited)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7,593,936 B2 (HOOKS) 22 September 2009 (22.09.2009) entire document	1-5, 7, 8, 10, 11, 13-17, 19, 20, 22, 23, 25
---		---
Y		6, 9, 12, 18, 21, 24
Y	US 9,332,024 B1 (EMC CORPORATION) 03 May 2016 (03.05.2016) entire document	6, 9, 18, 21
Y	US 2006/0026678 A1 (ZAKAS) 02 February 2006 (02.02.2006) entire document	12, 24
A	US 9,258,217 B2 (DUFFIELD et al) 09 February 2016 (09.02.2016) entire document	1-25
A	US 8,984,331 B2 (QUINN) 17 March 2015 (17.03.2015) entire document	1-25
A	US 2007/0245420 A1 (YONG et al) 18 October 2007 (18.10.2007) entire document	1-25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2017	28 SEP 2017
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, VA 22313-1450 Facsimile No. 571-273-8300	Authorized officer Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774