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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 April 2017 (27.04.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/069792 A1

(51) International Patent Classification:
H04L 12/24 (2006.01) *H04L 29/12* (2006.01)

(21) International Application Number:
PCT/US2016/014728

(22) International Filing Date:
25 January 2016 (25.01.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
5685/CHE/2015 21 October 2015 (21.10.2015) IN

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) Inventor: **ELLAPPAN, Kumaresan**; Sy.No.192, Whitefield Road, Mahadevapura Post, 560048 Bangalore (IN).

(74) Agents: **LIOU, Lisa W.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop #79, Fort Collins, Colorado 80528 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *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))*

[Continued on next page]

(54) Title: DYNAMIC FAULT MANAGEMENT

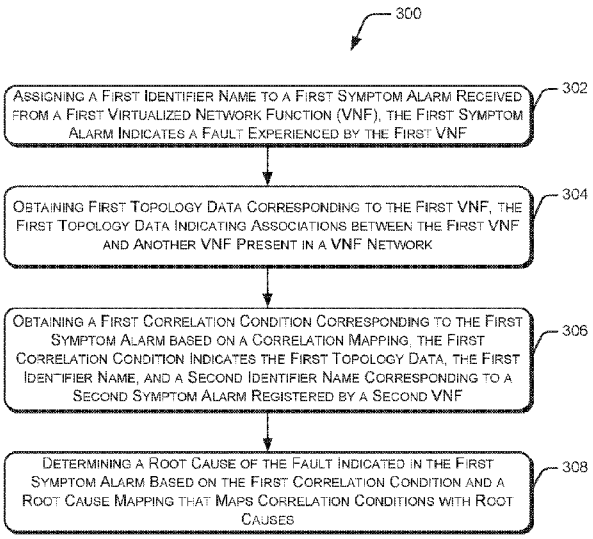


Figure 3

(57) Abstract: A method comprising assigning a first identifier name to a first symptom alarm received from a first virtualized network function (VNF). The first symptom alarm indicates a fault experienced by the first VNF. Further, first topology data corresponding to the first VNF is obtained. The first topology data indicates associations between the first VNF and another VNF present in a VNF network. Subsequently, a first correlation condition corresponding to the first symptom alarm is obtained based on a correlation mapping. The first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by a second VNF. Consequently, a root cause of the fault indicated in the first symptom alarm is determined based on the first correlation condition and a root cause mapping that maps correlation conditions with root causes.

WO 2017/069792 A1

Published:

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

DYNAMIC FAULT MANAGEMENT

BACKGROUND

[0001] Network Function Virtualization (NFV) is a network architecture that aims at using cloud based resources for providing telecommunication services. A NFV environment includes a plurality of virtualized network functions (VNFs) for performing functions of various network entities, such as load balancers, home location registers, and base stations. The VNFs are implemented as virtualized machines such that they can run on a range of industry standard server hardware for implementing the network functions. The VNFs may communicate with each other over the NFV environment for performing the network functions.

BRIEF DESCRIPTION OF DRAWINGS

[0002] The detailed description is described with reference to the accompanying figures. It should be noted that the description and figures are merely example of the present subject matter and are not meant to represent the subject matter itself.

[0003] Figure 1 illustrates a block diagram of a system for dynamic fault management, according to an example of the present subject matter.

[0004] Figure 2 illustrates various example components of a system for dynamic fault management in a network function virtualization environment, according to an example of the present subject matter.

[0005] Figure 3 illustrates an example method for dynamic fault management in a network function virtualization environment, according to an example of the present subject matter.

[0006] Figure 4 illustrates an example method for dynamic fault management in a network function virtualization environment, according to another example of the present subject matter.

[0007] Figure 5 illustrates an example network environment implementing a non-transitory computer readable medium for dynamic fault management in a network function virtualization environment, according to an example of the present subject matter.

DETAILED DESCRIPTION

[0008] Network Function Virtualization (NFV) environment is a cloud computing based network architecture implemented for virtualizing telecommunication network based services. Any NFV environment includes a plurality of virtualized network functions (VNFs) for performing various network functions, such as message routing, traffic analysis, and security measure implementation.

[0009] To efficiently implement and maintain the VNFs, a network provider may regularly monitor and analyze alarms raised by the VNFs implemented in the NFV environment. The alarms raised by the VNFs may indicate various events, such as fault events experienced by the VNFs which may be used to analyze health and performance of the VNFs. For instance, the alarm indicating fault events, such as network connectivity issue faced by the VNF may be used to determine network related issues. Such alarms received from different VNFs may be analyzed to determine a root cause of the fault events reported by the VNFs. The root cause may then be used to identify a solution for resolving the root cause.

[0010] Generally, determining the root cause and the solution includes correlating fault events faced by different VNFs using predefined correlation rules. These correlation rules are predefined at the time of installing the VNFs based on interconnections between different VNFs. Thus, in case of change in interconnections between different VNFs, the existing correlation rules may not work and new correlation rules may have to be defined. For instance, if a first VNF and a second VNF are directly connected by a link and the link goes down, then the first VNF and the second VNF may raise an alarm indicating loss of connection with

each other. In such a case a correlation rule may be defined to correlate alarms from the first VNF and the second VNF to identify the root cause in such faults as link down. If the first VNF and the second VNF are connected via a router and face network connectivity issues, the first VNF and the second VNF may raise an alarm indicating loss of connection with each other. In such a case, various correlation rules may have to be defined to identify whether the root cause is router malfunctioning or disruption of links between the router and the two VNFs.

[0011] Defining correlation rules each time network topology changes may be a hectic and tedious task, and may lead to extensive use of resources. Further, since a large number of VNFs are implemented in a network, such a customization of correlation rules may involve regular monitoring of the network topology to identify modifications in the topology, thus leading to further wastage of resources.

[0012] Approaches for dynamically managing faults experienced by virtualized network functions (VNFs) in a network function virtualization (NFV) environment are described. As per an example of the present subject matter, a dynamic correlation rule is defined that performs dynamic correlation between a plurality of symptom alarms for determining a root cause of a fault indicated in the symptom alarms. The dynamic correlation is performed based on a correlation condition associated with the symptom alarm. The correlation condition includes data, such as an identifier name that may be used for identifying another symptom alarm, registered in a symptom alarm directory, similar to the symptom alarm. Further, topology data may be used to determine if the VNFs raising the symptom alarms are associated. If the VNFs are associated, the correlation condition is ascertained to be true. The root cause mapped to the correlation condition is determined to be the root cause of the faults experienced by the VNFs. Thus, the same dynamic correlation rule can be used for managing faults in various networks irrespective of the network topology.

[0013] In operation, when a first VNF experiences a fault, say, loss of connectivity with a second VNF, the first VNF may raise an alarm. On receiving the alarm, it is initially determined whether the alarm is a symptom alarm, based on a symptom criterion. On determining the alarm to be a symptom alarm, say, a first symptom alarm, a first identifier name is assigned to the first symptom alarm.

[0014] Subsequently, first topology data corresponding to the first VNF is obtained and used to update the first symptom alarm. The first topology data indicates associations or links between the first VNF and other VNFs present in a VNF network. The first symptom alarm is then registered in a symptom alarm directory that lists a plurality of symptom alarms and corresponding VNFs from which the symptom alarms are received. Subsequently, a first correlation condition corresponding to the first symptom alarm is obtained using a predefined correlation mapping. The first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm that may be registered by a second VNF in the symptom alarm directory. For instance, the second VNF may also have raised an alarm indicating loss of connectivity with the first VNF.

[0015] Further, it is determined whether the second symptom alarm has been registered in the symptom alarm directory and whether the second VNF is associated with the first VNF. If the second symptom alarm has been registered and is associated with the first VNF, the correlation condition is ascertained to be true. The symptom alarms raised by the first VNF and the second VNF may thus be ascertained to be correlated. Further, a root cause of the fault is determined using the first correlation condition and a root cause mapping. A corrective action is then determined for resolving the root cause based on a predefined cause-action mapping.

[0016] The present subject matter thus facilitates in dynamically managing faults experienced by the VNFs in the NFV environment

irrespective of the network topology of the NFV environment. As previously described, correlation conditions are defined based on types of faults that the VNFs may experience. Using such correlation conditions for identifying correlated symptom alarms makes the correlation rules adaptable to various network types irrespective of the network topology. Further, since the correlation conditions use the identifier names for determining correlated symptom alarms, the same correlation conditions can be used even if the network topology is modified.

[0017] The present subject matter is further described with reference to Figures 1 to 5. It should be noted that the description and figures merely illustrate principles of the present subject matter. It is thus understood that various arrangements may be devised that, although not explicitly described or shown herein, encompass the principles of the present subject matter. Moreover, all statements herein reciting principles, aspects, and examples of the present subject matter, as well as specific examples thereof, are intended to encompass equivalents thereof.

[0018] Figure 1 illustrates a system 102, according to an example of the present subject matter. The system 102 may be implemented for dynamically managing faults experienced by virtualized network functions (VNFs) in a Network Function Virtualization (NFV) environment. In one example, the system 102 may be a virtual machine hosted in the NFV environment. In another example, the system 102 may be implemented in, for example, desktop computers, multiprocessor systems, personal digital assistants (PDAs), laptops, network computers, mainframe computers, and computing based devices in general.

[0019] The system 102 may include, for example, processor(s) 104, an alarm identification module 106 coupled to the processor 104, a symptom identification module 108 coupled to the processor 104, and a corrective action module 110 coupled to the processor 104.

[0020] In operation, the alarm identification module 106 may determine if an alarm received from a first VNF is a first symptom alarm. In

one example, the alarm indicates a fault experienced by the first VNF. On determining the alarm to be a symptom alarm, the alarm identification module 106 may assign a first identifier name to the first symptom alarm. The alarm identification module 106 may further obtain first topology data corresponding to the first VNF. In one example, the first topology data indicating associations between the first VNF and another VNF present in a VNF network, such as the NFV environment.

[0021] Further, the symptom identification module 108 identifies a root cause of the fault indicated in the symptom alarm. In one example, the symptom identification module 108 identifies the root cause based on a first correlation condition corresponding to the first symptom alarm and a root cause mapping. The root cause mapping maps correlation conditions with root causes that may have resulted in the fault. Further, the first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by a second VNF.

[0022] The corrective action module 110 then determines a corrective action for resolving the root cause based on a predefined cause-action mapping. In one example, the cause-action mapping maps the root causes and corrective actions.

[0023] Figure 2 illustrates various example components of the system 102, according to an example of the present subject matter. In one example, the system 102 is hosted in a NFV environment 200. The NFV environment 200 further includes a plurality of virtualized network functions (VNFs) 202-1, 202-2, 202-3,…., 202-n, hereinafter collectively referred to as the VNFs 202 and individually referred to as VNF 202, communicating with the system 102.

[0024] In one example, the NFV environment 200 is a cloud based network architecture implemented for virtualizing telecommunication network based services. A service provider hosting the NFV environment 200 may install one or more of a variety of computing devices (not shown

in the figure), such as a desktop computer, cloud servers, mainframe computers, workstation, a multiprocessor system, a network computer, and a server for hosting the VNFs 202 in the form of virtual machines. In one example, the VNFs 202 may be hosted in the NFV environment 200 for performing various network functions, such as domain name lookup service, content delivery service, customer premises equipment function, interactive voice response service, home location service for a mobile network, message routing, traffic analysis, and security measure implementation. The VNFs 202 may be hosted as network elements, such as switching elements, mobile network nodes, and firewalls in the NFV environment 200. Each of the VNFs 202 may thus be hosted as a self-contained platform having its own VNF components, such as processers, storage disks, and network interfaces for running its own operating system and applications.

[0025] The system 102 includes the processor(s) 104, interface(s) 204, memory 206, module(s) 208, and data 210. The interfaces 204 may include a variety of commercially available interfaces, for example, interfaces for peripheral device(s), such as data input output devices, referred to as I/O devices, interface cards, storage devices, and network devices.

[0026] The memory 206 may be communicatively coupled to the processor 104 and may include any non-transitory computer-readable medium known in the art including, for example, volatile memory, such as static random access memory (SRAM) and dynamic random access memory (DRAM), and/or non-volatile memory, such as read only memory (ROM), erasable programmable ROM, flash memories, hard disks, optical disks, and magnetic tapes.

[0027] The modules 208, amongst other things, include routines, programs, objects, components, and data structures, which perform particular tasks or implement particular abstract data types. The modules 208 may also be implemented as, signal processor(s), state machine(s),

logic circuitries, and/or any other device or component that manipulate signals based on operational instructions. Further, the modules 208 can be implemented by hardware, by computer-readable instructions executed by a processing unit, or by a combination thereof.

[0028] The module(s) 208 may include the alarm identification module 106, the symptom identification module 108, the corrective action module 110, and other modules 212. The other modules 212 may include programs or coded instructions that supplement applications and functions, for example, programs in an operating system of the system 102. Further, the data 210 may include topology data 214, symptom alarm directory 216, mappings 218, and other data 220.

[0029] As previously described, the present subject matter facilitates in dynamically managing faults experienced by the VNFs 202. In one example, the alarm identification module 106 may determine if an alarm received from a first VNF, say, the VNF 202-1 is a symptom alarm, say, a first symptom alarm. The alarm is generated by the first VNF 202-1 upon experiencing a fault, say, loss of network connectivity. The alarm may thus indicate the fault experienced by the first VNF 202-1. For instance, assuming that the first VNF 202-1 is connected to a second VNF 202-2 through a link and the link gets damaged, thus disrupting the network connectivity between the first VNF 202-1 and the second VNF 202-2. When the first VNF 202-1 now attempts to transmit data to the second VNF 202-2, it may receive a destination unreachability error. The first VNF 202-1 may thus raise an alarm indicating that a fault, i.e., destination unreachability has been experienced. The alarm may further include attributes, such as VNF type, fault type, and fault name. For instance, the alarm raised by the first VNF 202-1 may indicate that the fault was destination unreachable and was experienced by the first VNF 202-1 which is a node.

[0030] On receiving the alarm, the alarm identification module 106 may analyze the alarm using a symptom criterion to ascertain if the alarm

is the first symptom alarm. In one example, the symptom criterion may include filters that analyze the alarm based on the attribute associated with the alarm. An example of the symptom criterion is as follows:

Filter: Event.ObjectClass=="router"

&& Event.addtionalText contains "unreachable"

[0031] On determining the alarm to be the first symptom alarm, the alarm identification module 106 may assign an identifier name, say, a first identifier name to the first symptom alarm. An identifier name is a descriptive identification name that describes the fault faced by the VNF raising the symptom alarm. In one example, the identifier names are predefined by a user, such as a network operator at the time of implementing the VNF environment to allow a uniform naming of the symptom alarm recognizable by the system 102 and the VNFs 202. The predefined identifier names are saved in a database (not showing in the figure) associated with the system 102. In one example, the database may be external to the system 102. In another example, the database may be internal to the system 102. The alarm identification module 106 may access the database to obtain an appropriate identifier name for each symptom alarm and update the symptom alarm to tag the identifier name. For instance, in the previous example of the first VNF 202-1 raising the alarm for destination unreachability, the alarm identification module 106 may assign the identifier name as "DstUnreachable". In one example, the alarm identification module 106 may obtain the appropriate identifier name based on the predefined identifier name rules.

[0032] The alarm identification module 106 may further assign an active time window to the first symptom alarm. The active time window indicates a period for which the first symptom alarm remains active for being used for identifying a root cause of the fault experienced by the first VNF 202-1. Keeping the symptom alarms active for just the active time window helps in removing old symptom alarms, that may have already been resolved, or arbitrary symptom alarms that may have been

erroneously raised. In one example, the active time window are predefined by a user, such as the network operator at the time of implementing the VNF environment and saved in the database associated with the system 102. The alarm identification module 106 may access the database to obtain an appropriate active time window for each symptom alarm and update the symptom alarm to add the active time window. For instance, in the previous example of the first VNF 202-1 raising the alarm for destination unreachability, the alarm identification module 106 may assign the active time window of 60 seconds. In one example, the alarm identification module 106 may obtain an appropriate active time window based on predefined time window rules.

[0033] The alarm identification module 106 may further obtain first topology data corresponding to the first VNF 202-1. In one example, topology data indicates associations between different VNFs 200. For example, the first topology data may indicate associations between the first VNF 202-1 and another VNFs 202 present in the NFV environment 200. Examples of the associations include, but are not limited to, direct links, communicative couplings via direct links or other VNFs, and sub-assemblies. The topology data may be predefined by a user, such as the network operator at the time of implementing the VNF environment and saved in the database associated with the system 102. In one example, the alarm identification module 106 may raise a database query to obtain the topology data 214 from the database and save it in the topology data 214. Further, the topology data 214 may be updated from time to time to include all modifications made to the NFV environment 200. The alarm identification module 106 may further update the symptom alarm to include the first topology data.

[0034] The symptom identification module 108 may subsequently register the first symptom alarm in a symptom alarm directory 216. In one example, the symptom alarm directory 216 may be a working memory listing a plurality of symptom alarms received by the system 102 and

corresponding VNFs 202 raising the symptom alarms. Registering the symptom alarms in the symptom alarm directory 216 facilitates in searching correlated symptom alarms that have been previously raised by other VNFs 202 and maybe useful for finding a root cause of fault indicated in the correlated symptom alarms. As previously described, the symptom alarms are useful for identifying the root cause for only short time duration as absence of any correlated symptom alarm within a specific time duration may mean that the fault is local to a VNF and no common or root cause has to be thus identified. The symptom identification module 108 may thus periodically scan the symptom alarm directory 216 to identify inactive symptom alarms being registered in the symptom alarm directory 216 for a period greater than corresponding active time windows. The inactive symptom alarms so identified may then be removed from the symptom alarm directory 216 by the symptom identification module 108.

[0035] Upon registering the first symptom alarm in the symptom alarm directory 216, the symptom identification module 108 may obtain a first correlation condition corresponding to the first symptom alarm. Correlation conditions are predefined by the user for each symptom alarm that a VNF may raise during operation. A correlation condition indicates identifier name of the symptom alarm to which the correlation condition is mapped and another identifier name of another symptom alarm that has to be registered in the symptom alarm directory 216 for the correlation condition to be true. In one example, the other symptom alarm may also indicate a fault similar to the fault indicated by the first symptom alarm and may thus have a common root cause. The correlation condition may also include the topology data 214 provided in the symptom alarms to determine if the symptom alarms are related. An example of the symptom criterion is as follows:

DstUnreachable exists && SrcUnreachable exists &&
DstUnreachable.topology==SrcUnreachable.topology

[0036] In one example, the symptom identification module 108 may identify the first correlation condition based on a correlation mapping, saved in the mapping 218. The first correlation condition may include the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by the second VNF 202-2. Further, the symptom identification module 108 may analyze the first correlation condition to obtain the second identifier name. The symptom identification module 108 may further scan the symptom alarm directory 216 to detect if the second symptom alarm corresponding to the second identifier name has been registered by the second VNF 202-2 in the symptom alarm directory 216. In case the second symptom alarm has not been registered, the symptom identification module 108 may ascertain the correlation condition to be false and stop the process of finding the root cause of the fault. In such a case, the symptom alarm may remain registered in the symptom alarm directory 216 for the remaining time from the active window and may be used for correlation if the second VNF 202-2 raises the second symptom alarm during that time.

[0037] In case the second symptom alarm has been registered, the symptom identification module 108 may ascertain if the second VNF 202-2 is associated with the first VNF 202-1. The symptom identification module 108 may ascertain the association based on the first topology data and second topology data corresponding to the second VNF 202-2. As previously described, association may include, direct link, indirect link, and system-sub-system relation. For instance, the second VNF 202-2 may be directly connected to the first VNF 202-1 via a link. In another example, the second VNF 202-2 may be communicatively coupled to the first VNF 202-1 via another VNF. In another example, the second VNF 202-2 may be a sub-component of the first VNF 202-1 or vice-versa.

[0038] On determining the second VNF 202-2 to be associated with the first VNF 202-1, the symptom identification module 108 may determine the correlation condition to be true. The symptom alarms raised by the first

VNF 202-1 and the second VNF 202-1 may thus be ascertained to be correlated. The symptom identification module 108 may subsequently identify the root cause of the fault indicated in the first symptom alarm and the second symptom alarm. In one example, the symptom identification module 108 may use the first correlation condition and a root cause mapping to identify the root cause. The root cause mapping is a predefined mapping that maps correlation conditions with root causes that may have resulted in the fault. The root cause mapping is predefined by the user and saved in the mapping 218.

[0039] For instance, in the previous example of the first VNF 202-1 being connected to the second VNF 202-2 through a link that got damaged, the first symptom alarm and the second symptom alarm raised by the VNFs may be identified to be correlated. The root cause mapping in such a case may have a mapping between the first correlation condition and the root cause, i.e., link damaged.

[0040] The root cause is subsequently used by the corrective action module 110 to determine a corrective action for resolving the root cause. In one example, the corrective action module 110 may use the root cause and a predefined cause-action mapping to determine the corrective action. The cause-action mapping maps the root causes and corrective actions that may be taken to resolve the root cause. For instance, in the previous example, the root cause "link damaged" may be mapped to a corrective action "connect affected VNFs through another VNF". The cause-action mapping may be predefined by the user and saved in the mappings 218. In one example, if the root cause cannot be resolved by the system 102, the cause-action mapping may instruct the system 102 to forward the identified root cause to a system administrator for manual intervention.

[0041] Figures 3 and 4 illustrate example methods 300 and 400, respectively, for provisioning and monitoring virtualized network functions, in accordance with an example of the present subject matter. The order in which the methods are described is not intended to be construed as a

limitation, and any number of the described method blocks may be combined in any order to implement the aforementioned methods, or an alternative method. Furthermore, the methods 300 and 400 may be implemented by processing resource or computing device(s) through any suitable hardware, non-transitory machine readable instructions, or combination thereof.

[0042] It may also be understood that the methods 300 and 400 may be performed by virtualized computing systems, such as the system 102 hosted in a network function virtualization environment. Furthermore, the methods 300 and 400 may be executed based on instructions stored in a non-transitory computer readable medium, as will be readily understood. The non-transitory computer readable medium may include, for example, digital memories, magnetic storage media, such as one or more magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media.

[0043] Further, the methods 300 and 400 are described below with reference to the system 102 as described above, other suitable systems for the execution of these methods can be utilized. Additionally, implementation of these methods is not limited to such examples.

[0044] Referring to Figure 3, at block 302, a first identifier name is assigned to a first symptom alarm. In one example, an alarm received from a first virtualized network function (VNF) is initially analyzed to determine if the alarm is a symptom alarm. On determining, the alarm to be a symptom alarm, say, the first symptom alarm, a first identifier name is assigned to the first symptom alarm. The identifier name may be a user defined name that may allow the system 102 to identify the symptom alarms in a uniform way. For instance, the identifier name may help in identifying the symptom alarm in a symptom alarm directory. Further, the first symptom alarm indicates a fault experienced by the first VNF. For example, connection interruption may be a fault experienced by the first VNF and indicated to the system 102 through the first symptom alarm.

[0045] At block 304, first topology data corresponding to the first VNF is obtained. The first topology data indicates associations between the first VNF and another VNF present in a VNF network. In one example, the first topology data may be obtained from a database using a database query. The database may be maintained, for example, by a network provider having information about topology of a network. The topology data may be updated in form of an expression following any user specified format. For example, topology data for a VNF A may be "VNF A connected to VNF B". Further, the symptom alarm may be updated to include the first topology data.

[0046] At block 306, a first correlation condition corresponding to the first symptom alarm is obtained. In one example, the first correlation condition is obtained based on a correlation mapping. The first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by a second VNF. In one example, a correlation condition is a predefined condition that may be used to identify if the first and the second VNF are correlated.

[0047] At block 308, a root cause of the fault indicated in the first symptom alarm is determined. In one example, the root cause is determined based on the first correlation condition and a root cause mapping. The root cause mapping maps correlation conditions with root causes that may have resulted in the fault. The root cause mapping is a pre-defined mapping that may be defined by a user, for example, a network provider. Consequently, a corrective action may be determined for resolving the root cause based on a predefined cause-action mapping. Further, the corrective action is triggered for resolving the root cause.

[0048] Referring to Figure 4, at block 402, a determination is made to ascertain whether an alarm received from a first Virtual Network Function (VNF) is a symptom alarm, say, a first symptom alarm. A VNF may use alarms to indicate various events, such as task completion

events and fault events experienced by the VNFs. In one example, the alarm is determined to be the first symptom alarm based on a symptom criterion. The symptom criterion may include filters that analyze the alarm based on the attribute associated with the alarm. In said example, the first symptom alarm indicates a fault experienced by the first VNF.

[0049] At block 404, a first identifier name is assigned to the first symptom alarm. In an example, an identifier name is a descriptive identification name that describes the fault faced by the VNF raising the symptom alarm. In one example, the identifier names are predefined by a user and are saved in a database. Further, an active time window may be assigned to the first symptom alarm. The active time window indicates a period for which the first symptom alarm remains active for being used for identifying the root cause of the fault experienced by the first VNF.

[0050] At block 406, first topology data corresponding to the first VNF is obtained. The first topology data indicates associations between the first VNF and another VNF present in a VNF network. Further, the first symptom alarm is updated to include the topology data. The topology data may be updated in form of an expression following any user specified format. For example, topology data for a VNF A may be "VNF A connected to VNF B". Further, the symptom alarm may be updated to include the first topology data. In one example, the updated first symptom alarm having the first identifier name, the active time window, and the first topology data is further updated in the symptom alarm directory.

[0051] At block 408, a first correlation condition corresponding to the first symptom alarm is obtained. In one example, the first correlation condition is obtained based on a predefined correlation mapping. The first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm that may be registered by a second VNF in the symptom alarm directory.

[0052] At block 410, if the second VNF is associated with the first VNF is ascertained. In one example, the associations between first VNF and second VNF are ascertained based on the first topology data and second topology data. For instance, initially the second identifier name is identified based on the first correlation condition. It is subsequently detected if the second symptom alarm corresponding to the second identifier name has been registered by the second VNF in the symptom alarm directory. It is further ascertained if the second VNF is associated with the first VNF based on the first topology data and second topology data corresponding to the second VNF. Further, the correlation condition is evaluated as true upon ascertaining that the VNFs are associated.

[0053] At block 412, a root cause of the fault indicated in the first symptom alarm is determined. In one example, the root cause is determined based on the first correlation condition and a root cause mapping that maps correlation conditions with root causes. The root cause mapping may be predefined mapping generated by a user. In one example, the root cause mapping is stored in mapping modules.

[0054] At block 414, a corrective action for resolving the root cause is determined. In one example, the corrective action is determined based on a predefined cause-action mapping. Further, the corrective action is triggered for resolving the root cause. Subsequently, the symptom alarm directory is scanned periodically to identify inactive symptom alarms being registered in the symptom alarms directory for a period greater than corresponding active time window. Further, the inactive symptom alarms are removed from the symptom alarm directory.

[0055] Figure 5 illustrates an example network environment implementing a non-transitory computer readable medium for dynamic fault management, according to an example of the present disclosure. The system environment 500 may comprise at least a portion of a public networking environment or a private networking environment, or a combination thereof. In one implementation, the system environment 500

includes a processing resource 502 communicatively coupled to a computer readable medium 504 through a communication link 506.

[0056] For example, the processing resource 502 can include one or more processors of a computing device for dynamic fault management. The computer readable medium 504 can be, for example, an internal memory device of the computing device or an external memory device. In one implementation, the communication link 506 may be a direct communication link, such as any memory read/write interface. In another implementation, the communication link 506 may be an indirect communication link, such as a network interface. In such a case, the processing resource 502 can access the computer readable medium 504 through a network 508. The network 508 may be a single network or a combination of multiple networks and may use a variety of different communication protocols.

[0057] The processing resource 502 and the computer readable medium 504 may also be coupled to requested data sources 510 through the communication link 506, and/or to communication devices 512 over the network 508. The coupling with the requested data sources 510 enables in receiving the requested data in an offline environment, and the coupling with the communication devices 512 enables in receiving the requested data in an online environment.

[0058] In one implementation, the computer readable medium 504 includes a set of computer readable instructions, implementing an alarm identification module 514, a symptom identification module 516, and a corrective action module 518. The set of computer readable instructions can be accessed by the processing resource 502 through the communication link 506 and subsequently executed to process requested data communicated with the requested data sources 510 in order to facilitate dynamic fault management of a VNF network. When executed by the processing resource 502, the instructions of the alarm identification

module 514 may perform the functionalities described above in relation to the alarm identification module 106.

[0059] For example, the alarm identification module 514 may determine if an alarm received from a first VNF is a first symptom alarm. In one example, the alarm indicates a fault experienced by the first VNF. On determining the alarm to be a symptom alarm, say, the first symptom alarm, the alarm identification module 514 may assign a first identifier name and an active time window to the first symptom alarm. The first identifier name may allow the system to identify the symptom alarm in a symptom alarm directory. The active time window indicates a period for which the first symptom alarm remains active for being used for identifying the root cause of the fault. The alarm identification module 514 may further obtain first topology data corresponding to the first VNF. In one example, the first topology data indicates associations between the first VNF and another VNF present in a VNF network, such as the NFV environment.

[0060] Further, the symptom identification module 516 identifies a root cause of the fault indicated in the symptom alarm. In one example, the symptom identification module 516 may identify the root cause based on a first correlation condition corresponding to the first symptom alarm and a root cause mapping. The root cause mapping is a predefined map that maps correlation conditions with root causes that may result in the fault. For example, “connection interruption” may be a symptom and “link down” may be a root cause for the symptom. Further, the first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by a second VNF

[0061] The corrective action module 518 then determines a corrective action for resolving the root cause based on a predefined cause-action mapping. In one example, the cause-action mapping maps the root causes and corrective actions. For example, the root cause “link damaged” may be mapped to a corrective action “connect affected VNFs

through another VNF". Further the corrective action is triggered for resolving the root cause of the fault.

[0062] Although examples for the present disclosure have been described in language specific to structural features and/or methods, it should be understood that the appended claims are not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed and explained as examples of the present disclosure.

What is Claimed:

1. A method comprising:

assigning a first identifier name to a first symptom alarm received from a first virtualized network function (VNF), wherein the first symptom alarm indicates a fault experienced by the first VNF;

obtaining first topology data corresponding to the first VNF, the first topology data indicating associations between the first VNF and another VNF present in a VNF network;

obtaining a first correlation condition corresponding to the first symptom alarm based on a correlation mapping, wherein the first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by a second VNF; and

determining a root cause of the fault indicated in the first symptom alarm based on the first correlation condition and a root cause mapping that maps correlation conditions with root causes.

2. The method as claimed in claim 1, wherein the assigning the identifier name further comprising:

receiving an alarm from the first VNF;

determining if the alarm received from the first VNF is a symptom alarm based on a symptom criterion;

assigning an active time window to the first symptom alarm, wherein the active time window indicates a period for which the first symptom alarm remains active for being used for identifying the root cause; and

updating the first symptom alarm to include the first topology data.

3. The method as claimed in claim 1, wherein the method further comprising registering the first symptom alarm in symptom alarm directory listing a plurality of symptom alarms and corresponding VNFs.

4. The method as claimed in claim 3, wherein the determining the root cause further comprising:

identifying the second identifier name based on the first correlation condition;

detecting if the second symptom alarm corresponding to the second identifier name has been registered by the second VNF in the symptom alarm directory; and

ascertaining if the second VNF is associated with the first VNF based on the first topology data and second topology data corresponding to the second VNF.

5. The method as claimed in claim 3, wherein the method further comprising:

periodically scanning the symptom alarm directory to identify inactive symptom alarms being registered in the symptom alarm directory for a period greater than corresponding active time windows; and

removing the inactive symptom alarms from the symptom alarm directory.

6. The method as claimed in claim 1, wherein the method further comprising:

determining a corrective action for resolving the root cause based on a predefined cause-action mapping; and

triggering the corrective action for resolving the root cause.

7. A system comprising:

a processor;

an alarm identification module coupled to the processor to:

determine if an alarm received from a first virtualized network function (VNF) is a first symptom alarm, wherein the alarm indicates a fault experienced by the first VNF;

assign a first identifier name to the first symptom alarm; and

obtain first topology data corresponding to the first VNF, the first topology data indicating associations between the first VNF and another VNF present in a VNF network;

a symptom identification module coupled to the processor to:

identify a root cause of the fault indicated in the symptom alarm based on a first correlation condition corresponding to the first symptom alarm and a root cause mapping that maps correlation conditions with root causes, wherein the first correlation condition indicates the first topology data, the first identifier name, and a second identifier name corresponding to a second symptom alarm registered by a second VNF;

a corrective action module coupled to the processor to:

determine a corrective action for resolving the root cause based on a predefined cause-action mapping that maps root causes and corrective actions.

8. The system as claimed in claim 7, wherein the alarm identification module further is to:

receive the alarm from the first VNF;

assign an active time window to the first symptom alarm, wherein the active time window indicates a period for which the first symptom alarm remains active for being used for identifying the root cause; and

update the first symptom alarm to include the first topology data, first identifier name, and the active time window.

9. The system as claimed in claim 7, wherein the symptom identification module further is to:

register the first symptom alarm in symptom alarm directory listing a plurality of symptom alarms and corresponding VNFs;

obtain the first correlation condition corresponding to the first symptom alarm based on a correlation mapping;

identify the second identifier name based on the first correlation condition;

detect if the second symptom alarm corresponding to the second identifier name has been registered by the second VNF in the symptom alarm directory; and

ascertain if the second VNF is associated with the first VNF based on the first topology data and second topology data corresponding to the second VNF.

10. The system as claimed in claim 9, wherein the symptom identification module further is to

periodically scan the symptom alarm directory to identify inactive symptom alarms being registered in the symptom alarm directory for a period greater than corresponding active time windows; and

remove the inactive symptom alarms from the symptom alarm directory.

11. A non-transitory computer readable medium having a set of computer readable instructions that, when executed, cause a processor to:

obtain first topology data corresponding to a first virtualized network function (VNF) experiencing a fault, the first topology data indicating associations between the first VNF and another VNF present in a VNF network;

obtain a first correlation condition corresponding to a first symptom alarm registered by the first VNF based on a correlation mapping, wherein

the first correlation condition indicates the first topology data, a first identifier name corresponding to the first symptom alarm, and a second identifier name corresponding to a second symptom alarm registered by a second VNF;

determine a root cause of the fault indicated in the first symptom alarm based on the first correlation condition and a root cause mapping that maps correlation conditions with root causes; and

identify a corrective action for resolving the root cause based on a predefined cause-action mapping that maps the root causes and corrective actions.

12. The non-transitory computer readable medium of claim 11, wherein the computer readable instructions, when executed, further cause the processor to:

receive an alarm from the first VNF;

determine if the alarm received from the first VNF is a symptom alarm, wherein the alarm indicates the fault experienced by the first VNF;

assign the first identifier name to the first symptom alarm;

assign an active time window to the first symptom alarm, wherein the active time window indicates a period for which the first symptom alarm remains active for being used for identifying the root cause; and

update the first symptom alarm to include the first topology data.

13. The non-transitory computer readable medium of claim 11, wherein the computer readable instructions, when executed, further cause the processor to register the first symptom alarm in symptom alarm directory listing a plurality of symptom alarms and corresponding VNFs.

14. The non-transitory computer readable medium of claim 13, wherein the computer readable instructions, when executed, further cause the processor to:

identify the second identifier name based on the first correlation condition;

detect if the second symptom alarm corresponding to the second identifier name has been registered by the second VNF in the symptom alarm directory; and

ascertain if the second VNF is associated with the first VNF based on the first topology data and second topology data corresponding to the second VNF.

15. The non-transitory computer readable medium of claim 13, wherein the computer readable instructions, when executed, further cause the processor to:

periodically scan the symptom alarm directory to identify inactive symptom alarms being registered in the symptom alarm directory for a period greater than corresponding active time windows; and

remove the inactive symptom alarms from the symptom alarm directory.

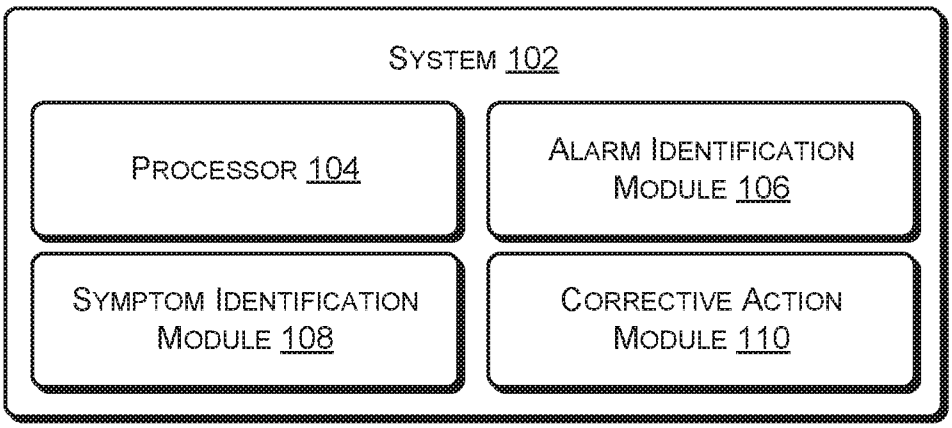

SYSTEM 102
PROCESSOR 104
ALARM IDENTIFICATION MODULE 106
SYMPTOM IDENTIFICATION MODULE 108
CORRECTIVE ACTION MODULE 110

Figure 1

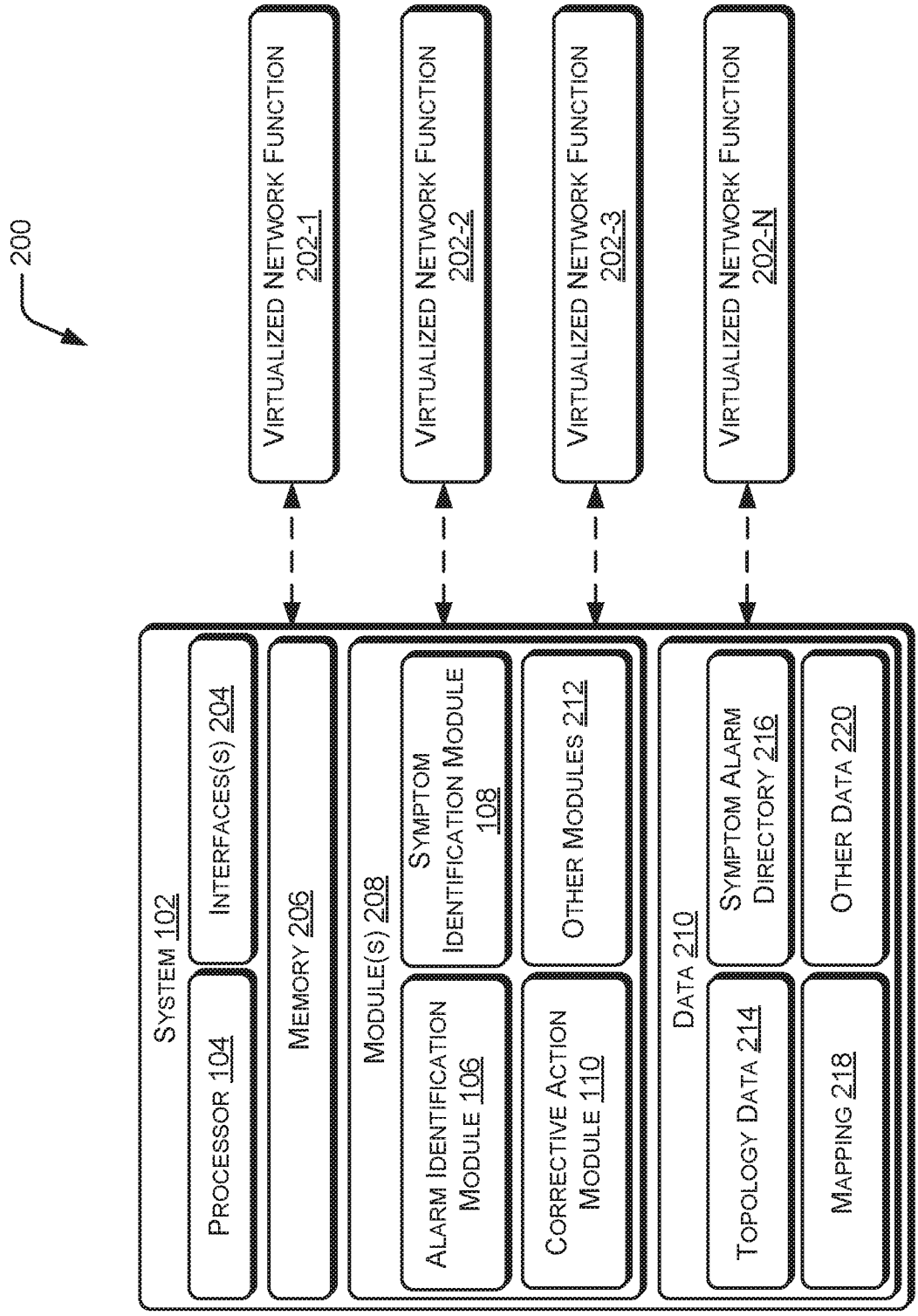

200
VIRTUALIZED NETWORK FUNCTION 202-1
VIRTUALIZED NETWORK FUNCTION 202-2
VIRTUALIZED NETWORK FUNCTION 202-3
VIRTUALIZED NETWORK FUNCTION 202-N
SYSTEM 102
PROCESSOR 104
INTERFACES(S) 204
MEMORY 206
MODULE(S) 208
ALARM IDENTIFICATION MODULE 106
SYMPTOM IDENTIFICATION MODULE 108
CORRECTIVE ACTION MODULE 110
OTHER MODULES 212
DATA 210
TOPOLOGY DATA 214
SYMPTOM ALARM DIRECTORY 216
MAPPING 218
OTHER DATA 220

Figure 2

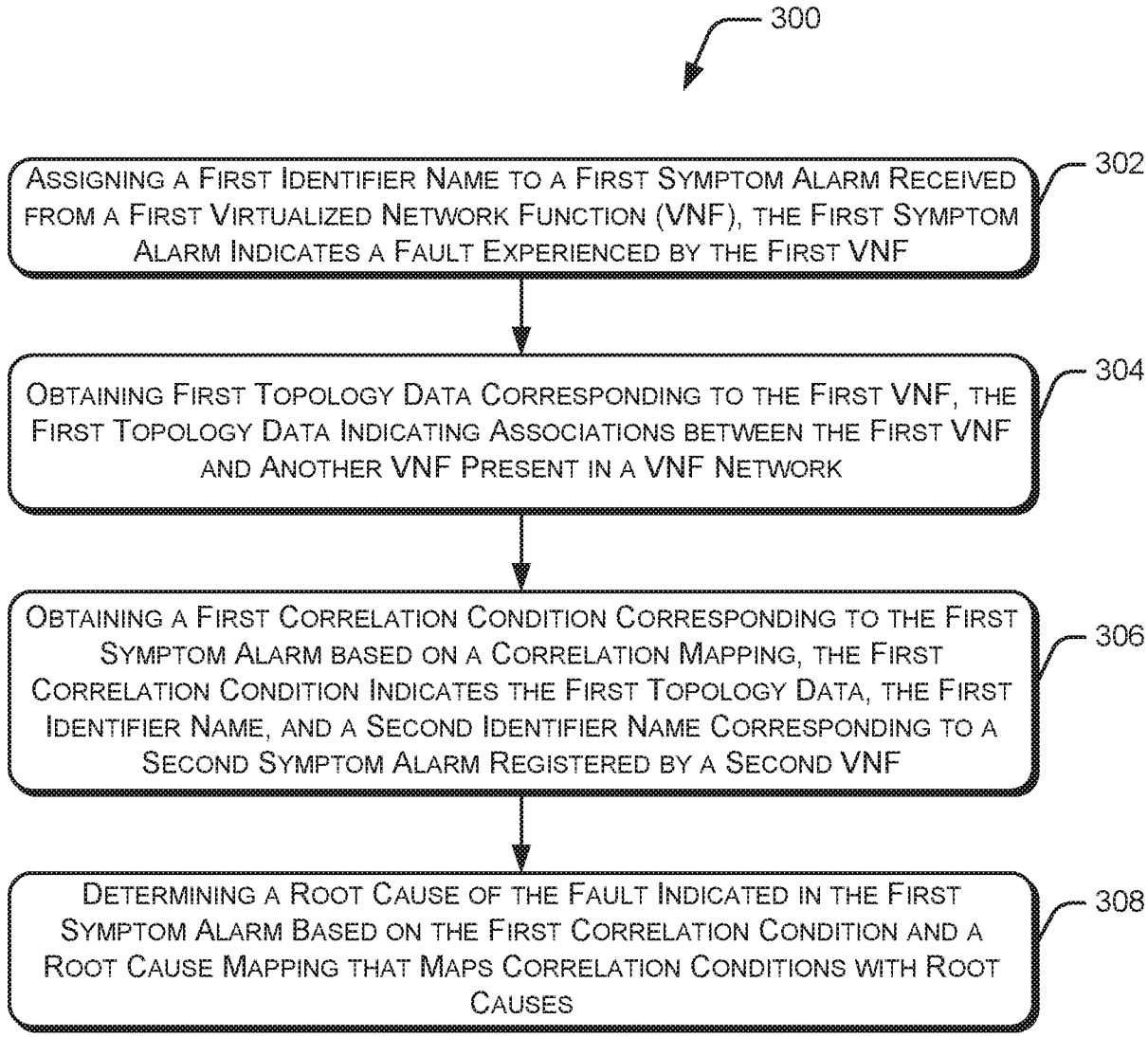

300
Assigning a First Identifier Name to a First Symptom Alarm Received from a First Virtualized Network Function (VNF), the First Symptom Alarm Indicates a Fault Experienced by the First VNF
302
Obtaining First Topology Data Corresponding to the First VNF, the First Topology Data Indicating Associations between the First VNF and Another VNF Present in a VNF Network
304
Obtaining a First Correlation Condition Corresponding to the First Symptom Alarm based on a Correlation Mapping, the First Correlation Condition Indicates the First Topology Data, the First Identifier Name, and a Second Identifier Name Corresponding to a Second Symptom Alarm Registered by a Second VNF
306
Determining a Root Cause of the Fault Indicated in the First Symptom Alarm Based on the First Correlation Condition and a Root Cause Mapping that Maps Correlation Conditions with Root Causes
308

Figure 3

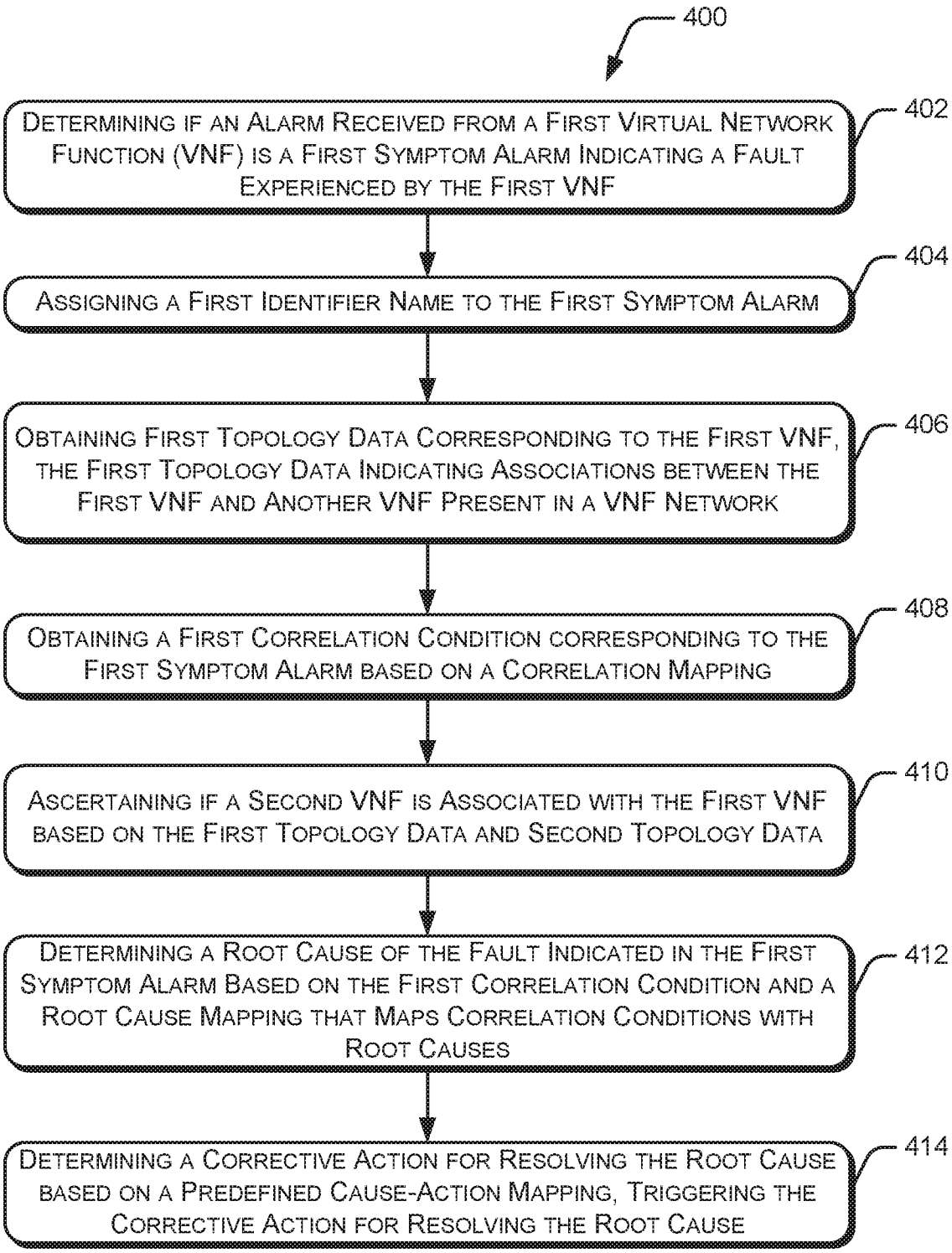

400
DETERMINING IF AN ALARM RECEIVED FROM A FIRST VIRTUAL NETWORK FUNCTION (VNF) IS A FIRST SYMPTOM ALARM INDICATING A FAULT EXPERIENCED BY THE FIRST VNF
402
ASSIGNING A FIRST IDENTIFIER NAME TO THE FIRST SYMPTOM ALARM
404
OBTAINING FIRST TOPOLOGY DATA CORRESPONDING TO THE FIRST VNF, THE FIRST TOPOLOGY DATA INDICATING ASSOCIATIONS BETWEEN THE FIRST VNF AND ANOTHER VNF PRESENT IN A VNF NETWORK
406
OBTAINING A FIRST CORRELATION CONDITION CORRESPONDING TO THE FIRST SYMPTOM ALARM BASED ON A CORRELATION MAPPING
408
ASCERTAINING IF A SECOND VNF IS ASSOCIATED WITH THE FIRST VNF BASED ON THE FIRST TOPOLOGY DATA AND SECOND TOPOLOGY DATA
410
DETERMINING A ROOT CAUSE OF THE FAULT INDICATED IN THE FIRST SYMPTOM ALARM BASED ON THE FIRST CORRELATION CONDITION AND A ROOT CAUSE MAPPING THAT MAPS CORRELATION CONDITIONS WITH ROOT CAUSES
412
DETERMINING A CORRECTIVE ACTION FOR RESOLVING THE ROOT CAUSE BASED ON A PREDEFINED CAUSE-ACTION MAPPING, TRIGGERING THE CORRECTIVE ACTION FOR RESOLVING THE ROOT CAUSE
414

Figure 4

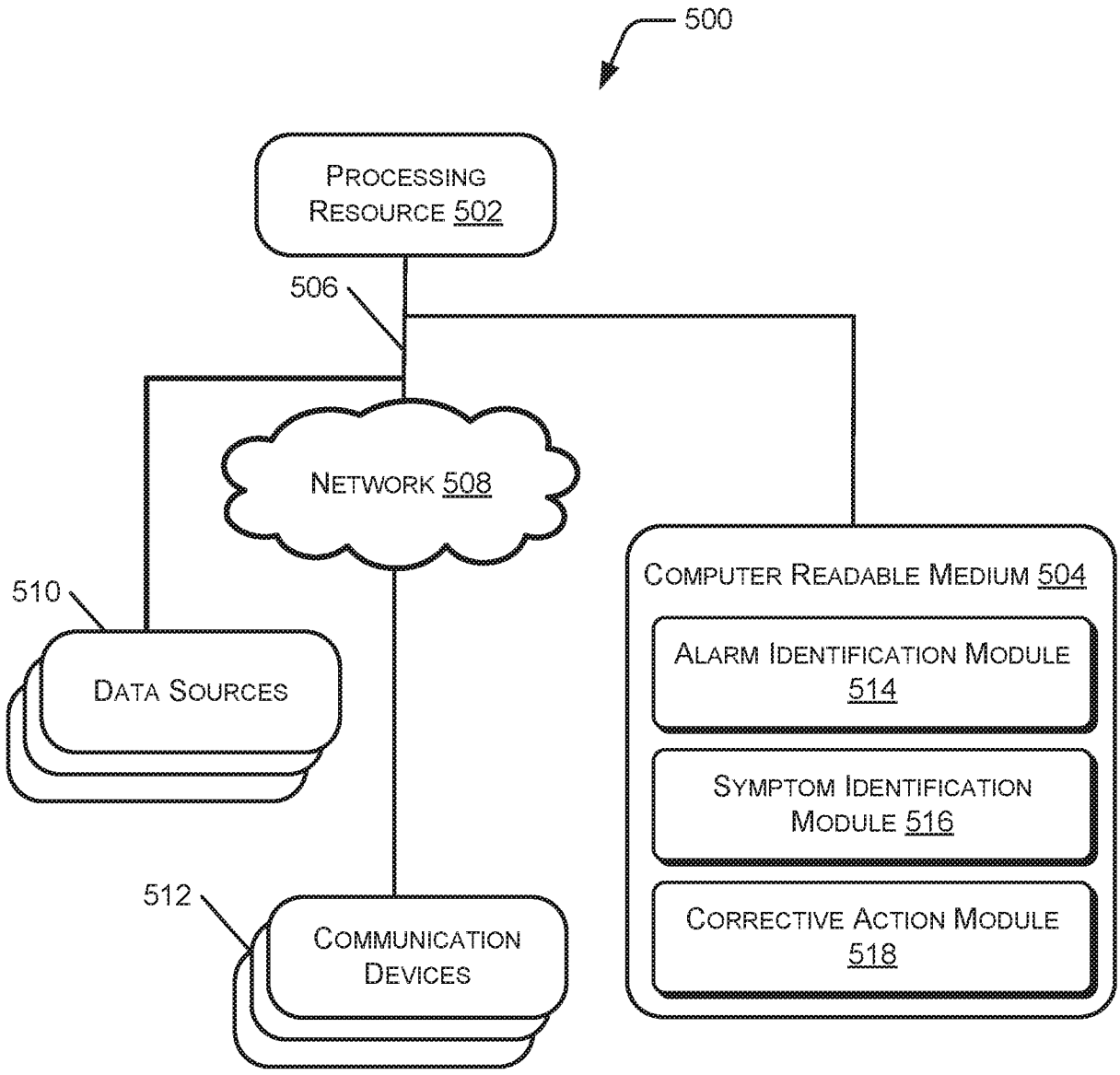

500
Processing Resource 502
506
Network 508
510
Data Sources
512
Communication Devices
Computer Readable Medium 504
Alarm Identification Module 514
Symptom Identification Module 516
Corrective Action Module 518

Figure 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/014728

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i, H04L 29/12(2006.01)i

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)
H04L 12/24; G06F 9/48; G06F 15/16; G06F 17/50; G06F 15/173; G06F 9/455; G06F 9/50; H04L 29/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: VNF(virtualized network function), symptom alarm, topology, correlation, root cause

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008-0114581 A1 (GIL MEIR et al.) 15 May 2008 See paragraphs [0059], [0136]; claims 1, 3, 14; and figure 1.	1-15
A	EP 2566103 A1 (ALCATEL LUCENT) 06 March 2013 See paragraphs [0013]-[0014]; and figure 6.	1-15
A	WO 2015-135611 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 17 September 2015 See paragraphs [0006], [0010]; and figure 2.	1-15
A	US 2001-0039577 A1 (SHARON BARKAI et al.) 08 November 2001 See paragraphs [0038]-[0039]; and figure 5.	1-15
A	US 2014-0229945 A1 (CONTEXTREAM LTD.) 14 August 2014 See paragraph [0112]; and figure 3.	1-15

☐ 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
29 June 2016 (29.06.2016)	**01 July 2016 (01.07.2016)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KIM, Seong Woo
Telephone No. +82-42-481-3348

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/014728

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0114581 A1	15/05/2008	US 2008-0114874 A1	15/05/2008
		US 8484336 B2	09/07/2013
		US 8583779 B2	12/11/2013
EP 2566103 A1	06/03/2013	None	
WO 2015-135611 A1	17/09/2015	None	
US 2001-0039577 A1	08/11/2001	AT 314765 T	15/01/2006
		AU 4931401 A	20/11/2001
		CA 2343370 A1	28/10/2001
		CA 2343370 C	14/10/2008
		DE 60116178 D1	02/02/2006
		DE 60116178 T2	20/07/2006
		EP 1150455 A2	31/10/2001
		EP 1150455 A3	10/12/2003
		EP 1150455 B1	28/12/2005
		IL 142783 A	20/08/2006
		IL 142783 D0	10/03/2002
		SG 101966 A1	27/02/2004
		US 6941362 B2	06/09/2005
		WO 01-86457 A1	15/11/2001
US 2014-0229945 A1	14/08/2014	EP 2957080 A1	23/12/2015
		WO 2014-125486 A1	21/08/2014