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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 October 2015 (29.10.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/164765 A1

(51) International Patent Classification:
H04L 12/26 (2006.01)

(21) International Application Number:
PCT/US2015/027547

(22) International Filing Date:
24 April 2015 (24.04.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2113/CHE/2014 25 April 2014 (25.04.2014) IN

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W, Houston, Texas 77070 (US).

(72) Inventors: **CHETAN, Ambi**; Sy.No. 192, Whitefield Road, Mahadevapura Post, Bangalore 560048 (IN). **RAMAPRASAD, Allu**; Sy.No. 192, Whitefield Road, Mahadevapura Post, Bangalore 560048 (IN). **DEVARAJAN, Venkatavaradhan**; Sy.No. 192 Whitefield Post, Mahadevapura Post, Bangalore 560048 (IN).

(74) Agent: **BURROWS, Sarah E**; 3404 E Harmony Road, Fort Collins, Colorado 80528-9599 (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))*

Published:

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

WO 2015/164765 A1

(54) Title: FLOW SAMPLE

(57) Abstract: A network anomaly may be detected by comparing the network behavior of a packet to an expected network behavior. The network behavior may be determined using a packet sample of a packet matching a flow rule that includes a sampling rule.

FLOW SAMPLE

BACKGROUND

[0001] In networks using software defined networking (SDN), one or more network controllers may manage the control plane of network devices, such as switches, bridges and routers. The network controller may also manage the data plane of the switches by providing flow rules to the switches. The flow rules may have various attributes, such as match fields, meters, go-to instructions, and actions. A flow is a set of packets sharing common attributes. For example, a flow may be defined by layer 2 or link layer information, such as source or destination MAC address; layer 3 or network layer information, such as source or destination IP address; or other information such as frame type, class of service indicator, or frame control information. The match fields of a flow rule establish a corresponding flow by setting the attributes shared by packets of the flow. During operation, if a match field is met by a packet then the network device performs the action on the packet. Match fields may include various criteria, such as source or destination IP or MAC address, port numbers, transport protocol type, frame type, class of service indicators, or frame control information. Actions may include various operations that the switch can perform on packets, such as forwarding the packet to a specified port, dropping the packet, or forwarding the packet to the controller.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Certain examples are described in the following detailed description and in reference to the drawings, in which:

[0003] Figure 1 illustrates an example method of detecting a network anomaly;

[0004] Figure 2 illustrates an example network controller including an anomaly detector; and

[0005] Figure 3 illustrates an example network controller including a non-transitory computer readable medium storing instructions executable to identify a network anomaly.

DETAILED DESCRIPTION OF SPECIFIC EXAMPLES

[0006] Once a controller instantiates flow rules onto its network devices, the controller typically assumes that the desired flow behavior is followed in the network. For example, if an SDN application executed by the controller programs a particular network path, the controller may send a set of flow rules to the network devices to implement the path. Incorrectly programmed flow rules or unexpected behavior resulting from correctly programmed flow rules may result in various network anomalies. For example, a network anomaly might be an impediment preventing traffic from reaching its destination, such as a network loop. As another example, the network anomaly might be a leakage of quarantined communications off of a designated network path.

[0007] In an example deployment, a controller may install thousands of rules on network devices in a network. Each rule has a precedence value, and if a flow is found to match more than one rule, the rule with the highest precedence wins and the action corresponding to the winning rule is applied to the flow. A flow unexpectedly matching a rule with a higher precedence than the rule it was expected to match may result in a network anomaly.

[0008] The controller may receive flow counters from network devices. A flow counter may provide a count of the number of times a particular flow rule was matched by incoming packets. Such flow counters may provide insufficient information to identify a network anomaly or event to determine whether a network anomaly exists in the network.

[0009] Some aspects of the disclosed technology allow identification of network anomalies using flow rule sampling techniques. A flow rule may include a sampling rule indicating that sampling is enabled for flows matching the flow rule. Packet samples matching the sampling-enabled flow rule are transmitted to the network controller. The network controller may use the packet samples to identify unexpected network behavior of packet flows matching the flow rule.

[0010] Figure 1 illustrates an example method of identifying a network anomaly. For example, an SDN controller, such as an SDN controller implementing an OPENFLOW protocol, may perform the example method.

[0011] The method may include block 101. Block 101 may include the controller transmitting a flow rule to a network device. For example, the flow rule may be transmitted to an SDN-controlled network switch, such as a switch implementing an OPENFLOW protocol. The flow rule may include a sampling rule. The sampling rule may include sampling criteria indicating how packets matching the flow rule should be sampled. In some cases, the sampling rule may be an action of the flow rule. In other cases, the sampling rule may be an additional element of the flow rule. For example, the sampling rule may be contained in sampling related fields of the flow rule, such as a sampling enabled field that indicates whether or not sampling is enabled for the flow rule and a sampling criterion field that indicates how sampling will be performed on the flow matching the flow rule. For example, the sampling rule may instruct the network device to send a packet sample every *n* packets, where *n* is an integer. In other words, every *n*th packet that matches the flow rule is sampled and the sample is sent to the controller. As another example, the sampling rule may instruct the network device to send *n* packets after a time interval. For example, the sampling rule may instruct the network device to send *n* packets every *s* seconds.

[0012] In some implementations, block 101 may further include transmitting a second flow rule to a second network device, the second flow rule including a second sampling rule. A controller may transmit a set of flow rules to a set of network devices to implement a network policy. For example, a controller may transmit a set of flow rules to a corresponding set of network devices to implement a certain network path for packets from one client to another. Each flow rule of the set of flow rules may include a corresponding sampling rule. In some cases, the sampling rules may all have the same sampling criteria. In other cases, the sampling rules may have different sampling criteria.

[0013] The example method may further include block 102. Block 102 may include the controller obtaining a packet sample of a packet matching the flow rule. The packet sample may comply with the sampling rule included in the flow rule transmitted in block 101. For example, if a packet matches the flow

rule and meets the sampling criteria, the network device may return a packet sample to the controller. A packet sample may be the entire sampled packet, the header of the sampled packet, or other set of packet information, such as a designated subset of the header.

[0014] In some cases, the controller may obtain the packet sample over an SDN control channel. In some implementations, the controller may obtain the packet sample in a packet-in message used by the network device to send packets to the controller. For example, the packet sample may use the same packet-in message formatted used by the network device to upload packets that do not match any of the device's flow rules. In other implementations, the controller may obtain the packet sample in a different message type, such as in a sample-specific message format. For example, the packet sample message may include information identifying the flow rule, a timestamp, or other information.

[0015] The example method may further include block 103. Block 103 may include using the packet sample to identify the packet. In some cases, identifying the packet may include identifying a source or destination of the packet, identifying a packet type, or identifying a preceding or next hop in the packet's network path. The information from the packet sample, such as source address, destination address, and packet type may be used to identify the packet. In some implementation, identifying the packet may include identifying a flow to which the packet belongs. For example, the controller may use packet information from the packet sample to identify a flow for the packet from stored flow information.

[0016] The example method may further include block 104. Block 104 may include identifying a network behavior for the packet. The network behavior may be information regarding how the packet was treated by the network to which the network device belongs. In some cases, the network behavior may be the action of the flow rule including the sampling rule. For example, the network behavior may be an indication of where the packet was forwarded, quality of service treatment of the packet, or header rewriting. In other cases, the network behavior may be information regarding how the packet

was treated prior to arriving at the network device with the flow rule. For example, the network behavior may be information identifying which peer network device forwarded the packet to the network device having the flow rule.

[0017] The example method may further include block 105. Block 105 may include comparing the network behavior to an expected network behavior to detect a network anomaly. The expected network behavior may be an SDN treatment intended for the packet. In some cases, the expected network behavior may be determined by the controller using the identified packet to consult stored flow information. For example, the expected network behavior may be determined by using the identified packet to identify an expected flow rule that was expected to match the packet. The expected flow rule may be a flow rule programmed on the network device or a flow rule programmed on another network device. For example, if a flow rule *X* on network device *A* unexpectedly matches the packet, then device *A* may forward the packet to device *B* instead of the expected device *C*. In this case, block 105 may include identifying a flow rule on the expected device *C* that the packet was expected to match. The expected network behavior may be the action of the expected flow rule. For example, the expected network behavior may be an expected next hop, an expected network destination, or an expected network path.

[0018] A network anomaly may be detected if the network behavior identified in block 104 differs from the expected network behavior. In some cases, a network anomaly may be detected if the packet matches an unexpected flow rule. The unexpected flow rule may perform an unexpected action on the packet. For example, the packet's next hop may differ from the expected next hop, the packet's network destination may differ from the expected network destination, or the packet's network path may differ from the expected network path.

[0019] In some cases, if the network behavior is a network path, block 105 may include comparing the network path to an expected network path. In this case, the network anomaly may be a deviation from the expected network path. The deviation may be a network loop or packets from a client being forwarded off of a quarantined network path. For example, a packet may be

unexpectedly matched by a higher priority flow rule than expected as a result of unexpected matching of wildcard fields. This may cause the packet to be forwarded back to a network device it had already visited, creating a network loop. As another example, using OPENFLOW rules, a client may have been quarantined but if there is a flow based sample from that client seen elsewhere in the network, it could indicate some kind of an anomaly in the network. For example, a flow rule that was programmed may not have the right match attributes to uniquely identify a client, creating packet leaks.

[0020] In some implementations, block 105 may include failing to receive a packet sample from another flow rule on the network. In some cases, if in block 101, a set of flow rules was transmitted to a set of network devices, block 105 may include failing to receive an expected packet sample from a flow rule of the set of flow rules. Failing to receive an expected packet sample from a flow rule on a network device may be used by the controller to identify the location of the network anomaly. As an example, the controller may transmit flow rule *a* to device *A*, flow rule *b* to device *B*, and flow rule c to device *C* to implement a network path from client *x* to client *y*, where device *A* forwards packets from client *x* to device *B*, device *B* forwards the packets to device *C*, and device *C* forwards the packets to client *y*. In this example, if the controller receives packet samples from devices *A* and *B*, but fails to receive packet samples from device *C*, this may indicate that a network anomaly is being created by flow rule programming on device *B*.

[0021] In some cases, upon detecting a network anomaly, the controller may repeat all or a portion of blocks 101-105. For example, upon performing block 105, the controller may identify a set of one or more network devices as having flow rules that are creating a network anomaly. To identify which flow rule is creating the anomaly, the controller may perform block 101 and resend any previously sent flow rules to the set of network devices with the addition of flow sampling rules. The controller may then perform blocks 102-105 on packet samples received from the set of network devices to determine which flow rule is causing the network anomaly.

[0022] As another example, upon detecting a network anomaly, the controller may repeat block 101 by re-transmitting the flow rule previously transmitted in the first iteration of block 101. The retransmitted flow rule may include an updated sampling rule with different sampling criteria. For example, the updated sampling rule may result in more frequent packet samples to provide more data. The additional packet samples may be used in block 105 to more precisely characterize the network anomaly.

[0023] Figure 2 illustrates an example network controller 200 including an anomaly detector 203 to detect a network anomaly using a packet sample. For example, the network controller 200 may be an SDN controller, such as an OPENFLOW controller, able to connect to one or more SDN-controlled network devices, such as bridges, routers, or switches. The example network controller 200 may include a flow programmer 201, a network monitor 202, and an anomaly detector 203. In various implementations, these modules may be implemented as software executable by a processor and stored on a non-transitory computer readable medium, as hardware, such as application-specific integrated circuits (ASICs) or field-programmable gate arrays (FPGAs), or as a combination of software and hardware.

[0024] The example network controller 200 may include a flow programmer 201. The flow programmer 201 may transmit a plurality of flow rules to a set of network devices. The set of network devices may be one or more SDN-controlled network devices of a network. For example, the flow programmer 201 may include an OPENFLOW stack or other SDN module and may transmit the plurality of flow rules as described with block 101 of Figure 1. Accordingly, the plurality of flow rules may each include a corresponding sampling rule. In some cases, each corresponding sampling rule may have the same or different sampling criteria as the other sampling rules. For example, the corresponding sampling rule of a flow rule may instruct the network device to send *n* packet samples after a set time interval. As another example, the corresponding sampling rule of a flow rule may instruct the network device to send packet samples every *n* packets.

[0025] The example network controller 200 may also include a network monitor 202. The network monitor 202 may obtain a packet sample of a packet flow matching a flow rule of the plurality. For example, the network monitor may perform block 102 to obtain the packet sample. Additionally, the network monitor 202 may obtain packet samples from the entire set of network devices for packets meeting the sampling criteria of the programmed flow rules. As described with respect to block 102, the packet samples may include various data such as timestamps or flow identification information. In some cases, the packet samples may include packet headers. For example, the packet samples may include packet headers extracted from the packets or may include copies of the packets.

[0026] The example network controller 200 may also include an anomaly detector 203. The anomaly detector 203 may be configured to perform blocks 103-105 of Figure 1. For example, the anomaly detector 203 may be configured to use the packet sample to detect a network anomaly by identifying a network behavior of the packet flow using the packet sample. For example, the anomaly detector 203 may check a packet sample to determine an expected flow rule expected to match the corresponding sample. The expected flow rule may be used to determine an expected network behavior for the packet. The expected network behavior may be compared to the actual network behavior to identify a network anomaly.

[0027] Figure 3 illustrates an example network controller 300. In some implementations, the example network controller 300 may be an implementation of the example network controller 200 of Figure 2. The example network controller 300 may include a network interface 301 to connect to various SDN network devices. For example, the network interface 301 may be able to establish OPENFLOW control channel with a set of network devices.

[0028] The example network controller 300 may further include a non-transitory computer readable medium 303 storing instructions 304-307 executable by a processor 302 to identify a network anomaly. For example, the medium 303 may include random access memory (RAM), read only memory (ROM), flash memory, storage, or a combination thereof.

[0029] The instructions may include instruction set 304. Instruction set 304 may be executable by the processor 302 to transmit a set of flow rules to a plurality of network devices, the flow rules including corresponding sampling rules. For example, the instructions 304 may be executable by the processor 302 to transmit the flow rules to the network devices using the interface 301 as described with respect to block 101 of Figure 1. As described herein, in some cases a sampling rule transmitted to a network device may instruct the network device to send packet samples every *n* packets, where *n* is an integer. In other cases, a sampling rule transmitted to a network device may instruct the network device to send *n* packet samples after a time interval, where *n* is an integer. In some cases, different flow rules of the set may include different sampling rule parameters. For example, *n* may differ between different flow rules. As another example, some sampling rules may be based on time intervals and other sampling rules may be based on packet intervals. In other cases, the set of flow rules may share the same sampling rule parameters.

[0030] The instructions may also include instruction set 305. Instruction set 305 may be executable by the processor 302 to determine an expected network path for a packet flow corresponding to a subset of the set of flow rules expected to match the packet flow. For example, the instruction set 305 may be executable by the processor 302 to consult flow tables to determine an expected network path for the packet flow. For example, the expected network path may be determined as described with respect to block 105 of Figure 1.

[0031] The instructions may also include instruction set 306. Instruction set 306 may be executable by the processor 302 to obtain a packet sample of the packet flow from a network device of the plurality of network devices. For example, the instructions 306 may be executable by the processor 302 to obtain the packet sample via the network interface 301. In some implementations, the instructions 306 may be executable by the processor 302 to perform block 102 of Figure 1.

[0032] The instructions may also include instruction set 307. Instruction set 307 may be executable by the processor 302 to identify a network anomaly using the packet sample to determine that a flow rule outside the subset

matches the packet flow. For example, the flow rule outside the subset may be a flow rule programmed on a network device outside the expected network path. As another example, the flow rule outside the subset may be a flow rule programmed on a network device in the expected network path that has a higher priority than a flow rule of the subset. This higher-priority flow rule may have unexpectedly matched the packet corresponding to the packet sample, resulting in a network anomaly. This information may be used to identify a network anomaly such as a network loop and to identify which network devices are involved in the loop. For example, the processor 302 may execute instruction set 307 to perform blocks 104 and 105 of Figure 1.

[0033] In the foregoing description, numerous details are set forth to provide an understanding of the subject disclosed herein. However, implementations may be practiced without some or all of these details. Other implementations may include modifications and variations from the details discussed above. It is intended that the appended claims cover such modifications and variations.

CLAIMS

1. A method, comprising:

transmitting a flow rule to a network device, the flow rule including a sampling rule;

obtaining a packet sample of a packet matching the flow rule, the packet sample complying with the sampling rule;

using the packet sample to identify the packet;

identifying a network behavior for the packet; and

comparing the network behavior to an expected network behavior to detect a network anomaly.

2. The method of claim 1, wherein the sampling rule instructs the network device to send packet samples every *n* packets, where *n* is an integer.

3. The method of claim 1, wherein the sampling rule instructs the network device to send *n* packet samples after a time interval, where *n* is an integer.

4. The method of claim 1, wherein identifying the network behavior comprises identifying a network path of the packet and comparing the network behavior to the expected network behavior comprises comparing the network path to an expected network path.

5. The method of claim 1, wherein the network anomaly is a network loop.

6. The method of claim 1, further comprising transmitting a second flow rule to a second network device, the second flow rule including a second sampling rule; and wherein identifying the network anomaly comprises failing to receive a second packet sample of a second packet matching the second flow rule.

7. A network controller, comprising:

a flow programmer to transmit a plurality of flow rules to a set of network devices, each flow rule including a corresponding sampling rule;

a network monitor to obtain a packet sample of a packet flow matching a flow rule of the plurality;

an anomaly detector to use the packet sample to detect a network anomaly.

8. The network controller of claim 7, wherein the corresponding sampling rule of the flow rule of the plurality instructs the network device to send packet samples every *n* packets, where *n* is an integer.

9. The network controller of claim 7, wherein the corresponding sampling rule of the flow rule of the plurality instructs the network device to send *n* packet samples after a time interval, where *n* is an integer.

10. The network controller of claim 7, wherein the packet sample includes packet header information.

11. A non-transitory computer readable medium storing instructions executable by a processor to:

transmit a set of flow rules to a plurality of network devices, the flow rules including corresponding sampling rules;

determine an expected network path for a packet flow corresponding to a subset of the set of flow rules expected to match the packet flow;

obtain a packet sample of the packet flow from a network device of the plurality of network devices; and

identify a network anomaly using the packet sample to determine that a flow rule outside the subset matches the packet flow.

12. The non-transitory computer readable medium of claim 11, wherein a sampling rule transmitted to a network device instructs the network device to send packet samples every *n* packets, where *n* is an integer.

13. The non-transitory computer readable medium of claim 11, wherein a sampling rule transmitted to a network device instructs the network device to send *n* packet samples after a time interval, where *n* is an integer.

14. The non-transitory computer readable medium of claim 11, wherein a first flow rule of the set of flow rules includes different sampling rule parameters than a second flow rule of the set of flow rules.

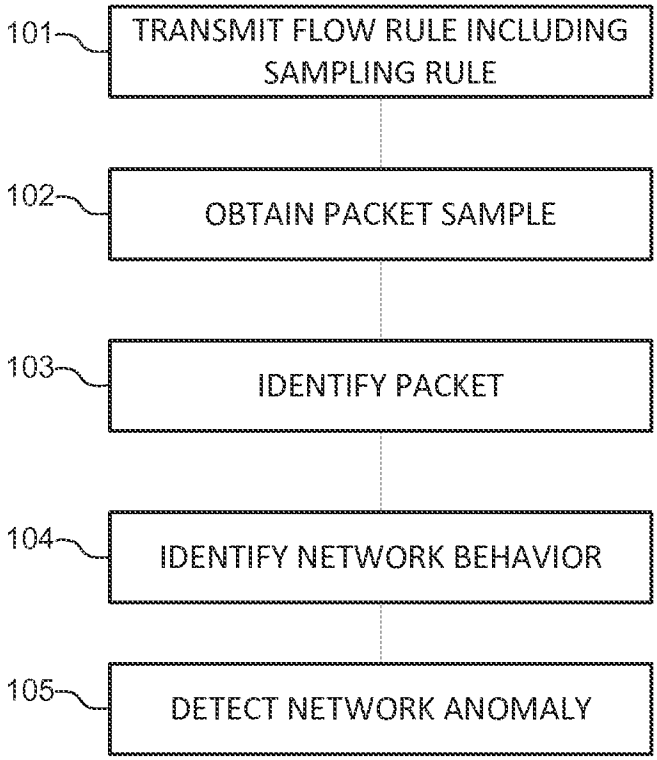
101
TRANSMIT FLOW RULE INCLUDING SAMPLING RULE
102
OBTAIN PACKET SAMPLE
103
IDENTIFY PACKET
104
IDENTIFY NETWORK BEHAVIOR
105
DETECT NETWORK ANOMALY

FIG. 1

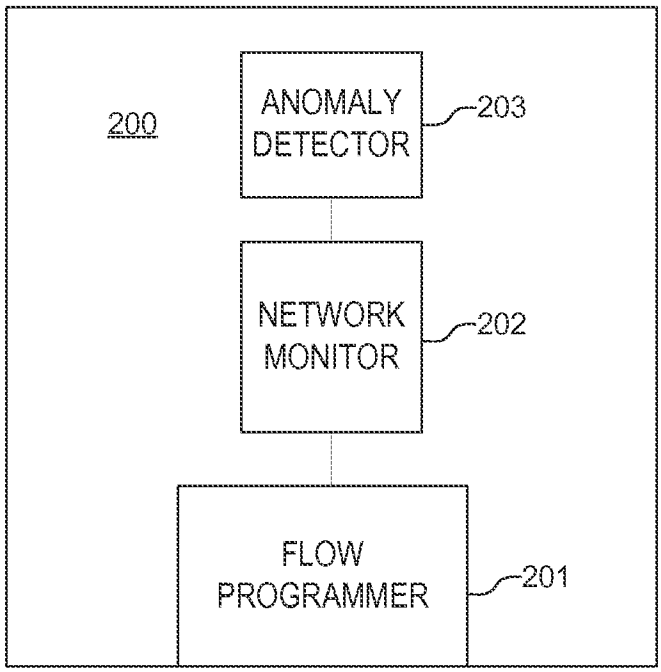
200
ANOMALY DETECTOR
203
NETWORK MONITOR
202
FLOW PROGRAMMER
201

FIG. 2

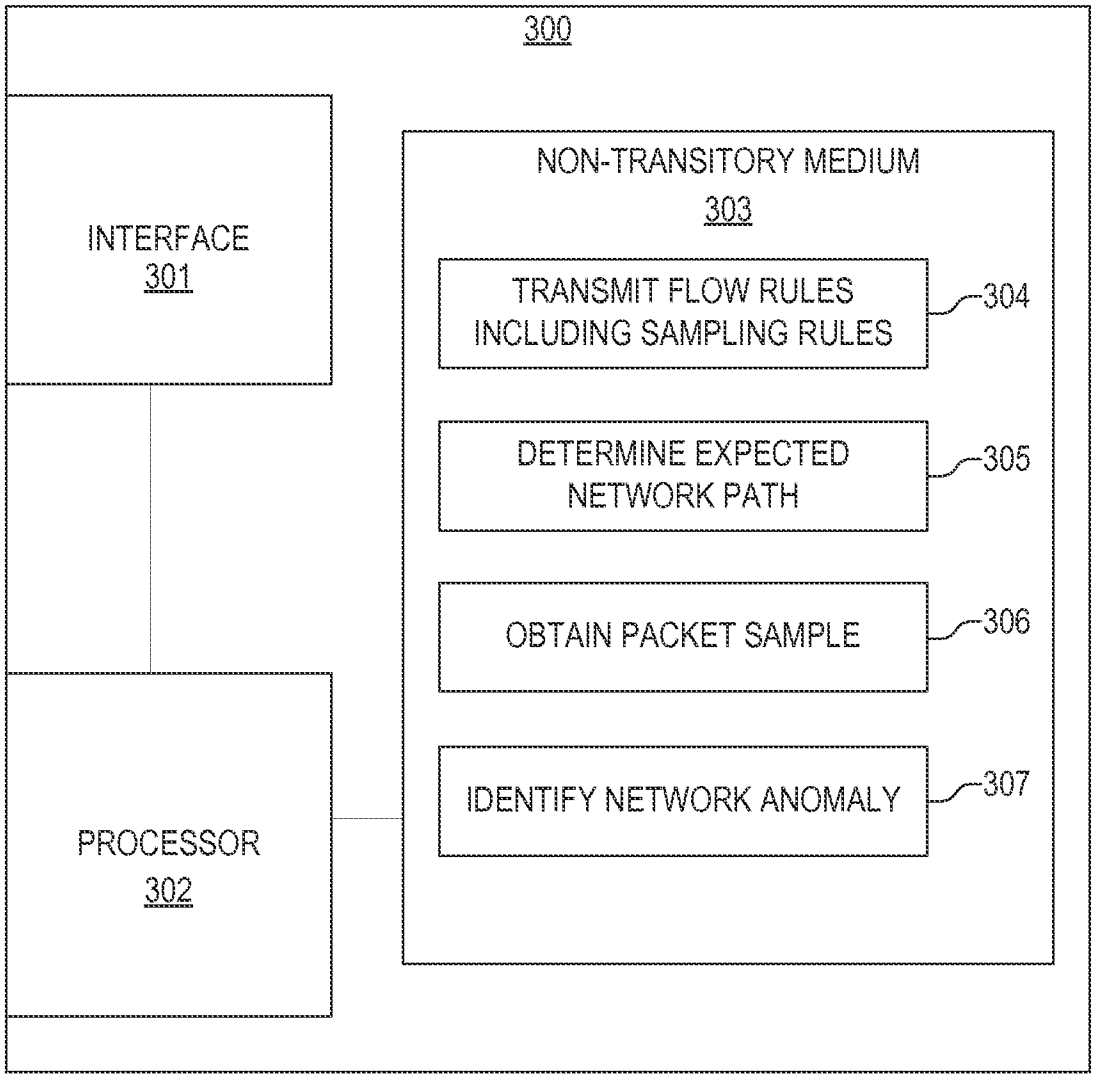
300
INTERFACE
301
PROCESSOR
302
NON-TRANSITORY MEDIUM
303
TRANSMIT FLOW RULES INCLUDING SAMPLING RULES
304
DETERMINE EXPECTED NETWORK PATH
305
OBTAIN PACKET SAMPLE
306
IDENTIFY NETWORK ANOMALY
307

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/027547

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26(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 12/26; G06F 11/30

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: packet, sample, sdn, anomaly

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	K. GIOTIS et al. `Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments.` Computer Networks, 07 April 2014, vol. 62, pp. 122-136. See pages 124-127 and figure 1.	1-14
Y	SAJAD SHIRALI-SHAHREZA et al. `Flexam: Flexible sampling extension for monitoring and security applications in openflow.` In: Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 16 August 2013, pp. 167-168. See page 168.	1-14
A	US 2009-0180393 A1 (NOBUYUKI NAKAMURA) 16 July 2009 See paragraphs [0042]-[0049], claims 1-11 and figure 2.	1-14
A	US 2008-0196100 A1 (SAJEEV MADHAVAN et al.) 14 August 2008 See abstract, paragraphs [0025]-[0040] and figures 2-3.	1-14
A	US 2007-0171824 A1 (NATALE RUELLO et al.) 26 July 2007 See abstract, claims 1-9 and figures 2-3B.	1-14

☐ 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
04 August 2015 (04.08.2015)	**05 August 2015 (05.08.2015)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea
Facsimile No. +82-42-472-7140

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/027547

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009-0180393 A1	16/07/2009	EP 2081321 A2	22/07/2009
		JP 2009-171194 A	30/07/2009
US 2008-0196100 A1	14/08/2008	US 8910275 B2	09/12/2014
US 2007-0171824 A1	26/07/2007	US 8018845 B2	13/09/2011