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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2015 (05.02.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/017422 Al

(51) International Patent Classification:
H04L 12/801 (2013.01) *H04L 29/06* (2006.01)

(21) International Application Number:
PCT/US20 14/048644

(22) International Filing Date:
29 July 2014 (29.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/956,304 31 July 2013 (31.07.2013) US

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Mail Stop 50P7, Redwood Shores, CA 94065 (US).

(72) Inventors: **SPARKS, Robert, James;** 1613 Lake Crest Lane, Piano, TX 75023 (US). **CAMPBELL, Ben, Allen;** 204 Touchdown Drive, Irving, TX 75063 (US). **MCMURRY, Sam, Eric;** 2991 Greenfield Drive, Richardson, TX 75082 (US).

(74) Agent: **HUNT, Gregory, A.;** Jenkins, Wilson, Taylor & Hunt, P.A., Suite 1200, University Tower, 3100 Tower Boulevard, Durham, NC 27707 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind cf 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, LT, 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 cf regional protection available):* ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, 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).

Published:

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

(54) Title: METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR MITIGATING TRAFFIC STORMS

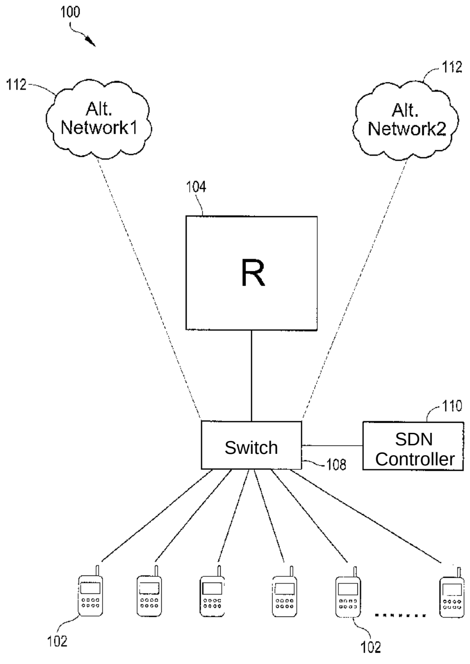

FIG. 1

(57) Abstract: Methods, systems, and computer readable media for mitigating traffic storms are provided herein. In some aspects, a system for mitigating traffic storms includes a traffic storm detector configured to detect an indication of a traffic storm. The system may also include a software defined network (SDN) controller configured to generate and send SDN commands to a controllable network entity for mitigating the traffic storm. In some aspects, a method for mitigating traffic storms includes detecting an indication of a traffic storm, wherein the traffic storm includes a burst of message traffic in a network. The method further includes sending one or more SDN commands to a controllable and/or controlled network entity to mitigate the traffic storm.

DESCRIPTION

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR MITIGATING TRAFFIC STORMS

PRIORITY CLAIM

This application claims the benefit of U.S. Patent Application Serial No. 13/956,304, filed July 31, 2013, the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The subject matter described herein relates to mitigating traffic storms. More particularly, the subject matter described herein relates to mitigating traffic storms via software defined network (SDN) commands communicated to controllable network entities.

BACKGROUND

A traffic storm is a flurry or burst of message traffic in a network, which may overwhelm network resources and/or cause the network to fail. One example of a traffic storm is when a large number of internet protocol (IP) phones attempt to simultaneously register with the network after a power outage. Another example of a traffic storm is when a software bug at a network registrar results in deregistration and simultaneous re-registration of mobile devices.

One strategy for mitigating the effects of a traffic storm is to statically provision firewalls to limit or throttle access to the overwhelmed and/or protected network resource. Another strategy is to statically provision or throttle traffic to the overwhelmed network resource. Using statically provisioned resources to handle traffic storms is undesirable because the protection devices themselves may be overwhelmed or inadequate to handle the traffic storm.

Accordingly, there exists a need for methods, systems, and computer readable media for dynamically mitigating traffic storms, using, for example, using software defined networks (SDNs) to provide flexible, scalable alternate resources when traffic storms are detected.

SUMMARY

The subject matter described herein includes methods, systems, and computer readable media for mitigating traffic storms. In some embodiments, a system for mitigating traffic storms includes a traffic storm detector configured to detect an indication of a traffic storm. The system may also include a software defined network (SDN) controller configured to generate and send SDN commands to a controllable network entity for mitigating the traffic storm.

In some embodiments, a method for mitigating traffic storms includes detecting an indication of a traffic storm, wherein the traffic storm includes a burst of message traffic in a network. The method further includes sending one or more SDN commands to a controllable and/or controlled network entity to mitigate the traffic storm.

In some embodiments, SDN commands communicated from an SDN controller can partition traffic based upon a class of traffic, an emergency indicator (e.g., an emergency attribute value pair (AVP) encoded within a payload of a message), a destination, an address, an IP prefix, an IP address, one or more QoS rules, or one or more policy rules.

The subject matter described herein may be implemented in software in combination with hardware and/or firmware. For example, the subject matter described herein may be implemented in software executed by one or more hardware processors. In one exemplary implementation, the subject matter described herein may be implemented using a non-transitory computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include disk memory devices, chip memory devices, programmable logic devices, and application specific integrated circuits. In addition, a computer readable medium that implements the subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

As used herein, the term "node" refers to an addressable entity in a network. A node may be all or a portion of a physical computing platform, such as a server with one or more hardware processor blades or a single processor blade that implements a function, such as a router, a switch, a home subscriber server (HSS), a mobility management entity (MME), a policy and charging rules function (PCRF), an application function (AF), a subscription profile repository (SPR), etc. A node may include one or more hardware processors and memory for executing and storing instructions for implementing the node's particular function. A node may also be a virtual entity implemented by one or more processor blades.

As used herein the term "controller" refers to all or a portion of a physical computing platform adapted to control one or more nodes and/or establish routing paths using one or more nodes via rules provided and/or stored therein. A controller may include one or more hardware processors and memory for executing and storing instructions and/or rules for implementing at a node using a communication protocol communicated via a port or logical interface. The controller may communicate with a client to instruct the client how and where to route packets. A controller may also control and/or establish one or more virtual entities implemented by one or more processor blades.

As used herein, the term "user device" describes subscriber or user equipment, such as a mobile handset, for communicating with one or more portions of a network. User devices may also include a computer, a pager, a smartphone, a phone, a wireless modem, a computing platform, a mobile handset, other subscriber devices and/or combinations thereof.

As used herein, the term "network", when referring to a home, visited, and/or an alternate network, includes any one of a 3G network, a 3G+ network, a GSM network, a 4G network, an LTE network, an evolved packet core (EPC) network, a 3rd Generation Partnership Project (3GPP) network, a GPRS core network, an IMS core, or other suitable type of network.

As used herein, the term "software defined network" or SDN refers to the physically decoupling of network control plane hardware from the data forwarding plane hardware such that an addressable node (e.g., a switch) can forward packets and a separate server (e.g., a SDN controller) can run the network control plane.

As used herein, the term "OpenFlow" describes a communication protocol defined according to OpenFlow version 1.2, available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1 .2.pdf, which gives access to the forwarding plane of a node (e.g., a network switch or router) over the network. As used herein an "OpenFlow controller" refers to a control device, including a hardware processor and memory, configured to communicate with one or more network components via the OpenFlow protocol.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the subject matter described herein will now be explained with reference to the accompanying drawings, of which:

Figures 1, 2A and 2B are network diagrams illustrating network components for mitigating traffic storms according to embodiments of the subject matter described herein; and

Figure 3 is a flow chart illustrating an exemplary process for mitigating traffic storms according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

In accordance with the subject matter disclosed herein, systems, methods, and computer readable media for mitigating traffic storms are provided. Notably, some embodiments of the present subject matter described herein may include establishing or creating alternate networks, such as software defined networks (SDNs), for managing traffic and preventing one or more network components from being flooded and/or overloaded with traffic. In some embodiments, traffic may be offloaded to one or more alternate resources until the overwhelmed network can recover and/or sustain the amount of traffic initially requested. In other embodiments, the traffic offloaded to alternate resources may be permanent.

In some embodiments, a stand-alone control device or SDN controller and/or a control device integrated with one or more existing network components may be configured to detect or receive an indication of a traffic storm, and instruct one or more controllable network entities to mitigate the storm by allocating additional resources and/or creating alternate resources for routing traffic thereto. Notably, methods systems, and computer readable media described herein may include mitigating traffic storms prior to the traffic reaching an ingress node, or edge device of a network. Thus, traffic may be dynamically re-routed to alternate resources before entering and/or overwhelming a destination network.

In some embodiments, subject matter described herein includes provision of a locally managed or operated control device or controller, configured to move network control out of proprietary network switches and/or routers. For example, the locally managed controller may include a SDN controller having computer readable medium stored thereon for executing instructions for pushing one or more SDN commands to one or more network components (e.g., switches or routers) via an interface, such as a SDN interface or an OpenFlow interface. The one or more network components may then route traffic to one or more alternate resources and/or create alternate resources as instructed by the controller.

Reference will now be made in detail to exemplary embodiments of the subject matter described herein, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

In Figure 1, a network, generally designated **100,** for mitigating traffic storms is provided. Network **100** may include a plurality of user devices **102.** In some embodiments, the plurality of user devices **102** are attempting to simultaneous register with a registration node **104.** In one embodiment, registration node **104** may include a SIP registrar. In some embodiments, hundreds, thousands, or even hundreds of thousands of user devices **102** may be simultaneously signaling registration node **104.** The large quantity (e.g., more than 100, more than 200, more than 500, more than 1,000, more than 2,000 subscriber devices) of user devices **102** attempting to simultaneous signal and/or otherwise register with node **104** may collectively form a traffic storm which would typically overwhelm node **104.** However, network **100** advantageously includes a controllable entity or switch **108** and a SDN controller **110** for mitigating the effects of the traffic storm.

Notably and in some embodiments, SDN controller **110** and switch **108** may be configured to dynamically create or establish alternative routing paths or SDNs for offloading some or all of the incoming traffic signaled via user devices **102.** In other embodiments, SDN controller **110** may instruct switch **108** to offload traffic to one or more alternate entities, such as a server, to delay, quiet, and/or stall some or all of the traffic before it can reach the intended registration node **104.** Traffic may be offloaded using the one or more alternate routing paths and/or SDNs to mitigate a storm. Notably, switch **108** may be instructed by SDN controller **110** to implement, create, and/or establish switching paths to alternate resources for mitigating the traffic storm prior to the storm overwhelming registration node **104.**

In some embodiments, SDN controller **110** may include a traffic storm detector configured to detect a traffic storm and send SDN commands to a controlled network entity, such as switch **108,** in response to detecting a storm. Although a switch is illustrated in Figure 1, the controlled network entity may also include a router, an access point (e.g. a WiFi access point), an ingress node, a signaling gateway, and/or any other addressable node that handles network traffic. Switch **108** may be configured to use routing rules to allow a portion of the traffic to reach registration node **104,** while offloading other portions to one or more alternate resources including alternate networks **112** and/or alternate resources. In some embodiments, traffic may be offloaded to such alternate resources permanently, or only until registration node **104** may handle the load.

Notably, SDN controller **110** and switch **108** may collectively be configured to dynamically create or establish alternate networks **112.** For illustration purposes only two alternate networks **112** are shown, however, only one or more than two alternate networks **112** may also be provided and are contemplated herein. Alternate networks **112** may include SDNs that are "virtual networks" until dynamically established and implemented to receive packets. Alternate networks **112** may be dynamically established as needed for dynamically re-routing traffic about the congested network node (e.g., registration node **104)** according to SDN commands communicated from SDN controller **110** at the onset of a traffic storm. Establishing SDNs is advantageous as it obviates a need to manually configure hardware, and allows network administrators to provision and/or program SDN controller **110** with instructions or routing rules for dealing with traffic, without requiring physical access to network-specific hardware devices.

In some embodiments, alternate networks **112** include dynamically created networks. In other aspects, alternate networks **112** include one or more pre-existing networks offered by an alternate carrier.

In some embodiments, SDN controller **110** may push one or more routing rules and/or SDN commands to switch **108** via a controller to switch interface. In some embodiments, the controller to switch interface includes an OpenFlow interface configured to communicate via OpenFlow protocol. In some embodiments, SDN controller **110** implements OpenFlow protocol for controlling one or more OpenFlow switches, routers, or nodes.

In some embodiments, SDN commands communicated via SDN controller **110** may be configured to partition traffic based upon a class of traffic, an emergency indicator (e.g., an emergency AVP encoded within a payload of a message), a destination, an address, an IP prefix, an IP address, one or more QoS rules, or one or more policy rules.

Figure 2A illustrates another example of mitigation of traffic storms in a network **200.** In Figure 2A, a policy and charging rules function (PCRF) **202** detects an indication of a traffic storm and communicates the indication to SDN controller **110.** PCRF **202** may include a traffic storm detector **204** configured to detect an indication of a traffic storm based upon policy requests or other data received from network entities, such as gateways, application servers, etc. In response to detecting the indication of a traffic storm, PCRF **202** may communicate the indication to SDN controller **110.**

SDN controller **110** may include a standalone node, or it may be integrated within one or other nodes, such as PCRF **202** (e.g., Figure 2B). In response to detection of the indication of the traffic storm, SDN controller **110** sends SDN commands to one or more network entities, such as a controllable data plane entity **206.** Data plane entity **206** may include a controllable entity adapted to mitigate the detected traffic storm by routing traffic to other alternate resources. In some embodiments, data plane entity **206** may include a switch, a router, or other node configured for handling network traffic. In one exemplary embodiment, SDN controller **110** may include an OpenFlow controller and the SDN commands may be OpenFlow commands for instructing data plane entity **206** to route traffic to alternate services **208.** For example, if the traffic storm indicates an unusually high volume of call attempts, the automated voice response servers instruct the callers to retry calls again at a later time.

Figure 2B illustrates another embodiment of a network or system for detecting and mitigating traffic storms according to aspects of the subject matter described herein. Referring to Figure 2B, network traffic storm detector **204** may include a standalone node and/or a node integrated within an ingress node, such as a border gateway (BGW) node **210.** In the illustrated example, traffic storm detector **204** is configured to detect an indication of a traffic storm caused by a burst or flurry of user equipment **212** (e.g., "UE" devices such as IP phones, computers, tablets, etc.) attempting to BGW **210** may be configured to communicate an indication of the traffic storm to PCRF **202.** SDN controller **110,** which in this example may be integrated within PCRF **202,** may issue SDN commands to BGW **210** for dynamically routing traffic to alternate services provided by one or more application servers (A/S) **214.**

Figure 3 is a flow chart illustrating an exemplary process for mitigating traffic storms according to an embodiment of the subject matter described herein. In block **302,** an indication of a traffic storm can be detected. The indication may include a flurry or burst of message traffic in a network. A traffic storm detector may include a standalone node, or it may be integrated with another node (e.g., a PCRF, an ingress node, and/or an SDN controller) for detecting the sudden burst of message traffic.

In block **304,** in response to detecting the indication of the traffic storm, one or more SDN commands can be communicated to a controllable network entity for mitigating the traffic storm. The controllable network entity may include a controlled switch, gateway, or addressable data plane entity configured to reroute traffic according to the SDN commands.

While the methods, systems, and computer readable media have been described herein in reference to specific embodiments, features, and illustrative embodiments, it will be appreciated that the utility of the subject matter is not thus limited, but rather extends to and encompasses numerous other variations, modifications and alternative embodiments, as will suggest themselves to those of ordinary skill in the field of the present subject matter, based on the disclosure herein.

Various combinations and sub-combinations of the structures and features described herein are contemplated and will be apparent to a skilled person having knowledge of this disclosure. Any of the various features and elements as disclosed herein may be combined with one or more other disclosed features and elements unless indicated to the contrary herein. Correspondingly, the subject matter as hereinafter claimed is intended to be broadly construed and interpreted, as including all such variations, modifications and alternative embodiments, within its scope and including equivalents of the claims. It is understood that various details of the presently disclosed subject matter may be changed without departing from the scope of the presently disclosed subject matter. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

CLAIMS

What is claimed is:

1. A method for mitigating traffic storms, the method comprising:

detecting an indication of a traffic storm, wherein the traffic storm includes a burst of message traffic in a network; and

in response to detection of the indication of the traffic storm, sending one or more software defined network (SDN) commands to a controlled network entity to mitigate the traffic storm.

2. The method of claim 1, wherein detecting an indication of a traffic storm occurs at an SDN controller.

3. The method of claim 2, wherein the SDN controller comprises an OpenFlow controller and wherein the controlled network entity comprises an OpenFlow compatible switch.

4. The method of claim 2, wherein the SDN controller includes a stand-alone node.

5. The method of claim 2, wherein the SDN controller is integrated within a policy and charging rules function (PCRF).

6. The method of any of the preceding claims, wherein the SDN commands instruct the controlled network entity to allocate additional resources to mitigate the traffic storm.

7. The method of any of claims 1 to 5, wherein the SDN commands instruct the controlled network entity to route traffic to alternate networks or service nodes.

8. The method of claim 7, wherein the alternate networks include one or more dynamically created networks.

9. The method of claim 7, wherein the alternate networks include one or more pre-existing networks offered by an alternate carrier.

10. The method of any of claims 1 to 5, wherein the SDN commands partition traffic based upon a class of traffic, an emergency indicator, a destination, an address, an IP prefix, an IP address, one or more QoS rules, or one or more policy rules.

11. The method of any of the preceding claims, wherein the traffic storm includes registration traffic following a service outage.

12. A system for mitigating traffic storms, the system comprising:

a traffic storm detector for detecting an indication of a traffic storm, wherein the traffic storm comprises a burst of message traffic in a network; and

a software defined network (SDN) controller configured to generate and send SDN commands to a controlled network entity to mitigate the traffic storm.

13. The system of claim 12, wherein the controlled network entity comprises an OpenFlow compatible switch.

14. The system of claim 12, wherein the SDN controller includes a stand-alone node.

15. The system of claim 12, wherein the SDN controller is integrated with a policy and charging rules function (PCRF).

16. The system of any of claims 12 to 15 wherein the SDN commands instruct the controlled network entity to allocate additional resources to mitigate the traffic storm.

17. The system of any of claims 12 to 15, wherein the SDN commands instruct the controlled network entity to route traffic to alternate networks or service nodes.

18. The system of claim 17, wherein the alternate networks include one or more dynamically created networks.

19. The system of claim 17, wherein the alternate networks include one or more pre-existing networks offered by an alternate carrier.

20. The system of any of claims 12 to 15, wherein the SDN commands partition traffic according to a class of traffic, an emergency indicator, a destination, an address, an IP prefix, an IP address, one or more QoS rules, or one or more policy rules.

21. The system of any of claims 12 to 20, wherein the traffic storm includes registration traffic following a service outage.

22. A non-transitory computer readable medium having stored thereon computer executable instructions embodied in a computer readable medium and when executed by a processor of a computer performs steps comprising:

detecting an indication of a traffic storm, wherein the traffic storm includes a burst of message traffic in a network; and in response to detection of the indication of the traffic storm, sending one or more software defined network (SDN) commands to a controlled network entity to mitigate the traffic storm.

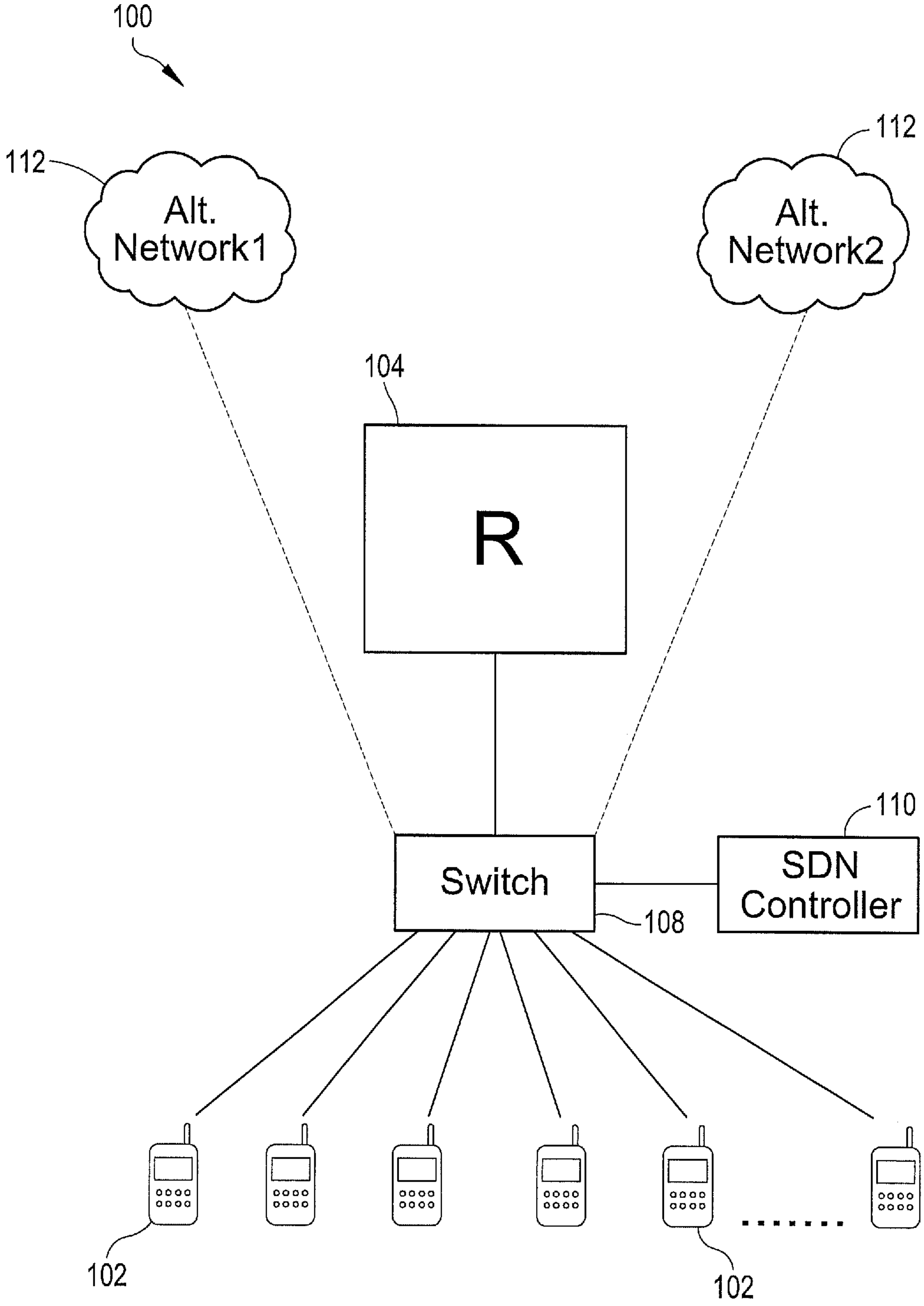
100
112
Alt.
Network1
112
Alt.
Network2
104
R
110
SDN
Controller
Switch
108
102
102

FIG. 1

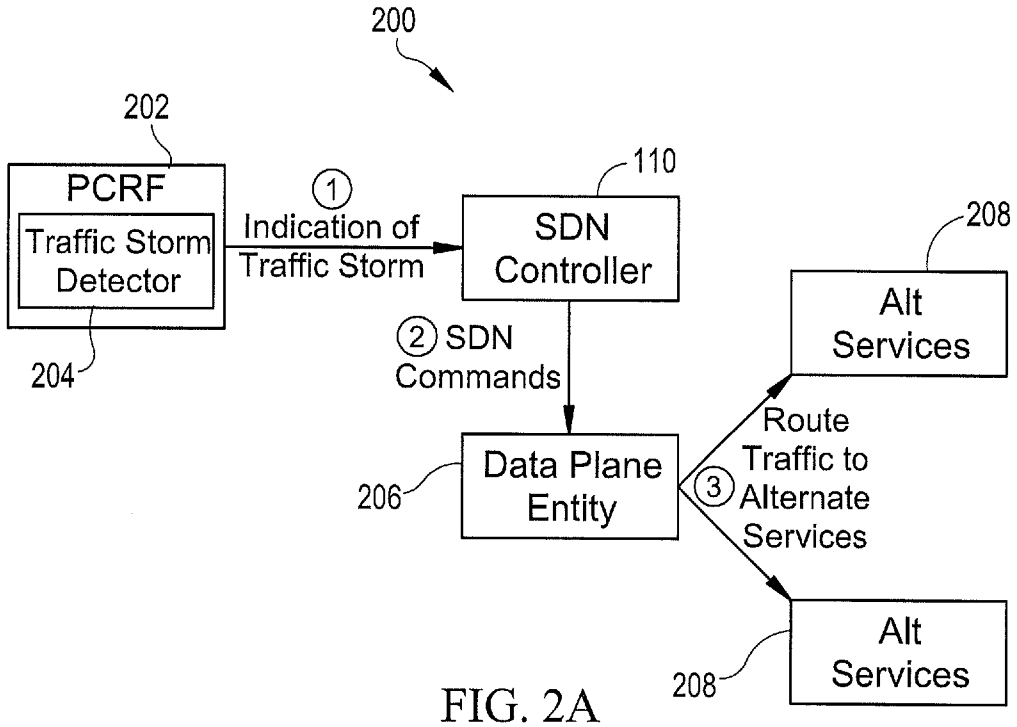
200
202
PCRF
Traffic Storm Detector
204
1 Indication of Traffic Storm
110
SDN Controller
2 SDN Commands
206
Data Plane Entity
3 Route Traffic to Alternate Services
208
Alt Services
208
Alt Services

FIG. 2A

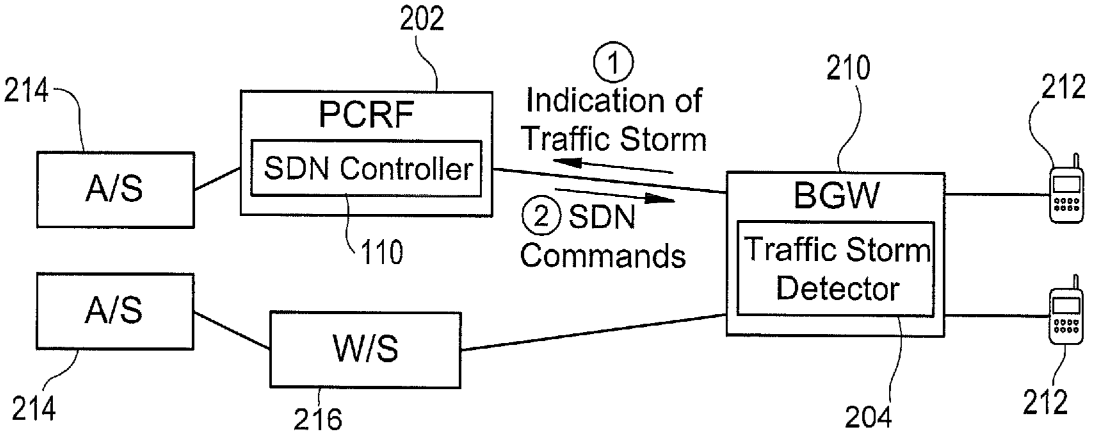
202
214
A/S
PCRF
SDN Controller
110
1 Indication of Traffic Storm
2 SDN Commands
210
BGW
Traffic Storm Detector
204
212
212
A/S
214
W/S
216

FIG. 2B

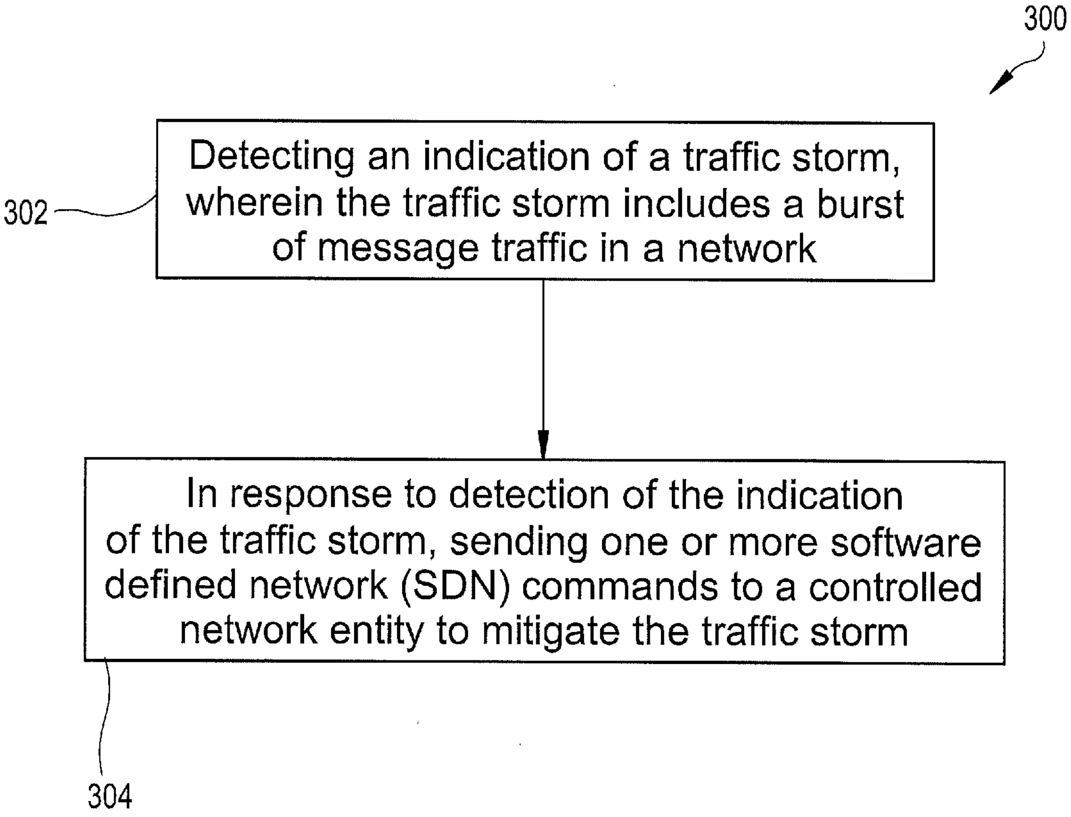
300
302
Detecting an indication of a traffic storm, wherein the traffic storm includes a burst of message traffic in a network
In response to detection of the indication of the traffic storm, sending one or more software defined network (SDN) commands to a controlled network entity to mitigate the traffic storm
304

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/048644

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/801 H04L29/06
ADD.

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

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

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

EPO-Internal , WPI Data, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/130264 Al (NEC EUROPE LTD [DE]; MIR FAISAL GHIAS [DE]; BRUNNER MARCUS [DE]; WINTE) 4 October 2012 (2012-10-04) abstract paragraph [0001] paragraph [0034] - paragraph [0041]; figure 3 -----	1-22
A	US 2011/090900 Al (JACKSON JAMES E [US] ET AL) 21 April 2011 (2011-04-21) abstract paragraph [0001] - paragraph [0008] paragraph [0025] - paragraph [0026] paragraph [0033] - paragraph [0034] figures 1,2 -----	1-22

-/- ·

☒ 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" documentwhich may throw doubts on priority claim(s) orwhich 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 9 October 2014	Date of mailing of the international search report 17/10/2014
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Poppe, Fabrice

2

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2014/048644

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2011/161575 Al (ERICSSON TELEFON AB L M [SE] ; KERN ANDRAS [HU] ; JOCHA DAVID [HU]) 29 December 2011 (2011-12-29) abstract page 1, line 13 - page 3, line 24 figures 1,2 -----	1-22
A	The Open Networking Foundation: "OpenFLow Switch Specification version 1.2" , , 5 December 2011 (2011-12-05) , XP55073743 , Retrieved from the Internet: URL:https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openf1ow/openf1ow-spec-vl.2.pdf [retrieved on 2013-07-31] the whole document -----	1-22

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/048644

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012130264 Al	04-10-2012	EP 2692096 Al	05-02-2014
		US 2014192646 Al	10-07-2014
		WO 2012130264 Al	04-10-2012
US 2011090900 Al	21-04-2011	US 2011090900 Al	21-04-2011
		US 2013077487 Al	28-03-2013
		US 2014250216 Al	04-09-2014
WO 2011161575 Al	29-12-2011	CN 102959910 A	06-03-2013
		EP 2586163 Al	01-05-2013
		US 2011317559 Al	29-12-2011
		WO 2011161575 Al	29-12-2011