



(43) International Publication Date  
14 September 2017 (14.09.2017)

- (51) **International Patent Classification:**  
*H04L 12/851* (2013.01) *H04L 12/26* (2006.01)
- (21) **International Application Number:**  
PCT/US2016/021314
- (22) **International Filing Date:**  
8 March 2016 (08.03.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).
- (72) **Inventors:** WACKERLY, Shaun; 8000 Foothills Blvd., Roseville, California 95747 (US). WAKUMOTO, Shaun; 8000 Foothills Blvd., Roseville, California 95747 (US). LAVIGNE, Bruce, E.; 8000 Foothills Blvd., Roseville, California 95747 (US).
- (74) **Agents:** PATEL, Milin, N. et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 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).

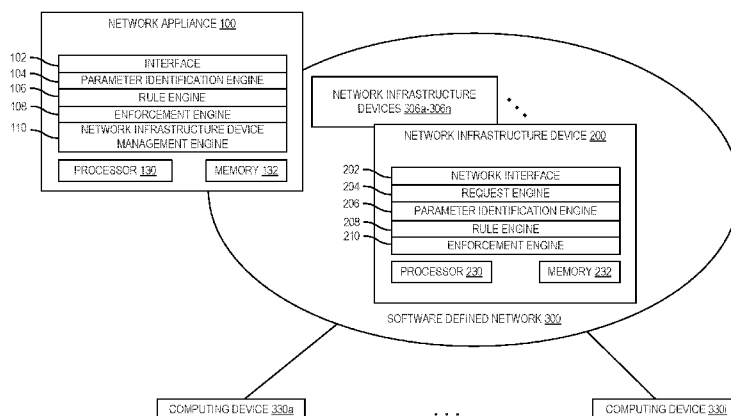
**Declarations under Rule 4.17:**

- 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))

**Published:**

- with international search report (Art. 21(3))

(54) **Title:** ACTION BASED ON ADVERTISEMENT INDICATOR IN NETWORK PACKET



**FIG. 3**

(57) **Abstract:** Examples disclosed herein relate to performing an action based on an advertisement indicator is present in a network packet. In one example, a network packet identified by a network infrastructure device as matching criteria associated with a pre-identified request is received. A parameter within the network packet is identified. A rule is used to determine whether the parameter indicates that an advertisement indicator is present in a flow associated with the network packet. An action is performed based on whether the advertisement indicator is present in the network packet.

## **ACTION BASED ON ADVERTISEMENT INDICATOR IN NETWORK PACKET**

### **BACKGROUND**

[0001] Computing networks can include multiple network devices such as routers, switches, hubs, servers, desktop computers, laptops, workstations, network printers, network scanners, etc. that are networked together across a local area network (LAN), wide area network (WAN), wireless networks, etc. Networks can include deep packet inspection devices, firewalls, etc. to detect unwanted activity acting on the computer network. Further, networks can be managed using a Software Defined Networking controller.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram of a network appliance capable of determining whether an advertisement indicator is present in a network packet, according to an example;

[0004] FIG. 2 is a block diagram of a network infrastructure device capable of performing an action based on an advertisement indicator, according to an example;

[0005] FIG. 3 is a block diagram of a network system including devices capable of performing actions on network packets based on an indication of advertisements, according to an example;

[0006] FIG. 4 is a flowchart of a method for performing an action based on an advertisement indicator, according to an example; and

[0007] FIG. 5 is a block diagram of a device capable of performing an action based on an advertisement indicator, according to an example.

#### **DETAILED DESCRIPTION**

[0008] Computing networks can include multiple network devices such as routers, switches, hubs, servers, desktop computers, laptops, workstations, network printers, network scanners, etc. that are networked together across a local area network (LAN), wide area network (WAN), wireless networks, etc.

[0009] Various entities add advertisements to websites to earn money. These advertisements may include malware or may be benign. In some examples, advertisements may consume processing power, energy, etc. from end user devices. For example, some advertisements include video or other rich content that consumes system resources and drain power and thus battery life. Moreover, blocking advertisements can make the network experience more enjoyable for users of end-user devices using the network. Further, a large portion of network traffic can be the result of advertisements. As such, reducing the amount of advertisements sent through a network would provide better bandwidth utilization for the network and/or owner of the network.

[0010] End users may install ad blocking technology on their devices. However, ad-blocking technology may still consume resources on the end-user device. Further, some devices may block ad-blocking technology. For example, a web browser may attempt to bypass the ad-blocking technology, an operating system may attempt to block or restrict installation/functionality of the ad-blocking technology, etc. Further, companies have embraced employees bringing their own

devices to work. Loading ad-blocking technology to client devices owned by the company will not stop network bandwidth consumption initiated by devices not owned by the company.

[0011] Accordingly, various approaches described herein relate to stopping or substituting advertisements at the network level instead of at the client level. The network itself can stop advertisements in an efficient manner, without need for an end-user to install any software. In one example, in an enterprise location or campus network, networks can be controlled by an administrator. The approaches described herein can facilitate an administrator's ability to reduce network bandwidth for downloading advertisements, enable focusing of advertisements to enterprise goals, monetizing the environment's network by replacing with paid content, etc.

[0012] FIG. 1 is a block diagram of a network appliance capable of determining whether an advertisement indicator is present in a network packet, according to an example. The network appliance 100 can include components that can be utilized to determine whether an advertisement indicator is present in a network packet. In one example, the network appliance 100 can include an interface 102, a parameter identification engine 104, a rule engine 106, and an enforcement engine 108. In other examples, such as in FIG. 3, the network appliance 100 can further include a network infrastructure device management engine 110, a processor 130, and/or memory 132. The network appliance 100 can be, for example, a server, a Software Defined Networking (SDN) controller, or other computing device capable of performing the features described herein.

[0013] FIG. 2 is a block diagram of a network infrastructure device capable of performing an action based on an advertisement indicator, according to an example. In some examples, network infrastructure devices can be used to forward network packets to the network appliance 100 if the network packets meet particular criteria. In one example, the network infrastructure device 200 can include a network interface 202, a request engine 204, a parameter identification engine 206, a rule engine 208, and an enforcement engine 210. In another

example, the network infrastructure device 200 can further include a processor 230 and/or memory 232. The network infrastructure device 200 can further include a processor 230 and/or memory 232. The network infrastructure devices 200 can include, for example, switches, routers, wireless access points, etc. capable of providing the functionality described herein.

[0014] FIG. 3 is a block diagram of a network system including devices capable of performing actions on network packets based on an indication of advertisements, according to an example. The networking system can include a software defined network (SDN) 300. The SDN 300 can include a number of network infrastructure devices 306a – 306n such as network infrastructure device 200. The SDN 300 can be used to provide communications capabilities between computing devices 330a – 330i. Though the software defined network 300 is shown between computing devices 330 in this example, communications may also travel through other network infrastructure devices that are both part of the software defined network 300 or part of other networks (e.g., via the Internet). The computing devices 330a – 330i can be implemented via a processing element, memory, and/or other components.

[0015] When a computing device 330a communicates with another computing device (e.g., computing device 330i), the communication can travel through the SDN 300. As such, traffic can pass through one or more network infrastructure devices 306, 200 in the SDN 300. In some examples, network infrastructure devices 306, 200, such as network infrastructure device 200, can be configured to inspect traffic and send packets that may be indicative of advertisements in a flow of traffic to the network appliance 100 for additional checking. As further described below, the network infrastructure device 200 may also perform some or all of the additional checking on the network infrastructure device 200.

[0016] When a packet goes through network infrastructure device 200, a network interface 202 can receive the packet. In some examples, the network interface 202 switches traffic between inputs and outputs using standard processing (e.g., a standard switch process based on source and destination

addresses of the packets). Traffic includes packetized data ("packets") formatted using multiple layers of protocol, e.g., the Transmission Control Protocol (TCP) Internet Protocol (IP) ("TCP/IP") model, Open Systems Interconnection (OSI) model, or the like. A packet generally includes a header and a payload. The header implements a layer of protocol. The payload includes data, which may be related to packet(s) at another layer of protocol.

[0017] In an example, the network interface 202 performs switching of the packets at a network access layer. The network access layer provides links between hosts over which packets are transmitted. The network access layer is sometimes referred to as layer 2, referring to layer 2 of the OSI model. The prevailing network access layer today includes the Ethernet family of protocols, although the network interface 202 can switch packets using other types of network access protocols. While the network interface 202 can switch traffic at the network access layer, the network interface 202 may also process packets at layers above the network access layer to implement various other functions (e.g., quality of service (QoS), such as at a network layer (e.g., IP or other OSI layer 3 protocol) and/or transport layer (e.g., TCP, User Datagram Protocol (UDP), or other OSI layer 4 protocol).

[0018] The network infrastructure device 200 can be configured to inspect packets to determine whether advertisement analysis should be performed by the network infrastructure device 200 and/or network appliance 100. In one example, the request engine 204 can be configured to look at network packets to identify network packets that represent requests that may provide useful information as to whether an advertisement is included in the packet and/or a flow of traffic associated with the request. One example of such a request is a domain name system (DNS) request. Other examples include Hypertext Transfer Protocol (HTTP) requests such as HTTP GET and CONNECT requests. As used herein, a GET request is a request for data from a specified resource. Further, as used herein, a CONNECT request is an approach to establish a tunnel to a remote end-point.

[0019] A network infrastructure device management engine 110 can be used to configure the network infrastructure device 200 to look for particular criteria in packets for further analysis. The network infrastructure device management engine 110 can communicate with the network infrastructure device 200 using various communications means, such as the OpenFlow communications protocol or other communication protocol that gives access to a forwarding plane of a network infrastructure device 306, 200. A rule insertion capability of the protocol can be used to configure implementation of matching functionality in the network infrastructure device 200.

[0020] In the example of DNS requests, the request engine 204 can inspect the packets for particular criteria that are associated with the pre-identified DNS requests. For example, the request engine 204 can be configured to match against particular header fields. In one example, if the header field `eth_type` = IPv4, `ip_proto` = UDP, and `udp_dst` = 53, the packet can be determined to be relevant to advertisement analysis. As such, the packet (or copy) can be forwarded, through the network interface 202, to the network appliance 100 for further analysis. The analysis may include whether the domain name in the packet is on a list that is recognized as being related to advertisements.

[0021] In the example of HTTP requests, a single website may contain references to other websites which serve valid content or advertisements. However, the distinction between valid content and advertisement may be apparent based upon a full or partial URL/URI of the requested resource, rather than merely the domain name. Thus, in one example, the request engine 204 can inspect the packets for particular criteria related to pre-identified requests that provide sufficient information about the requested resource. For example, the request engine 204 may match against header fields that indicate `eth_type` = IPv4, `ip_proto` = TCP, `tcp_dst` = (80 or 8080), and `http_request_method` = (GET or CONNECT), which can indicate that the packet is relevant to advertisements. As with the DNS request case, the network interface 202 can forward the identified packets (or copies) to the network appliance 100. Moreover, in some examples,

the network appliance 100 may be capable of making the request on behalf of the requestor and fetching the resource (e.g., advertisement) to inspect the resource.

[0022] The interface 102 of the network appliance 100 can receive communications from the network interface 202. In one example, the network appliance 100 can be a SDN controller and the SDN can also be controlled using the network appliance. Further, the network appliance 100 may use the interface 102 to communicate with the network infrastructure devices 306, 200. In some examples, the interface 102 may act on a control plane while data communications travel through a data plane. In other examples, the network interface 202 may send communications to the network appliance 100 using another protocol and the data plane. The network appliance 100 can receive at interface 102, the network packet that was identified by the network infrastructure device 200 as matching the criteria associated with the pre-identified request (e.g., DNS request, GET request, CONNECT request, etc.).

[0023] The parameter identification engine 104 can be used to identify a parameter in the network packet that can be used to determine whether there is an indication of association of the network packet and an advertisement. In one example, the packet is a DNS request. In this example, the parameter is a domain name. In other examples, the packet can be either a GET request or a CONNECT request. In these examples, the parameter is a URI or URL. These parameters can be found in headers. Moreover, the parameter identification engine 104 can base the parameter identification on what type of network packet is received. In some examples, the parameter identification engine 104 can compare the same header fields used by the network infrastructure device 200 to determine the type of packet. In other examples, the network infrastructure device 200 may add a communication (e.g., encapsulate the packet and send additional information using another protocol) to the network packet.

[0024] Rule engine 106 can be used to determine whether the parameter indicates that an advertisement indicator is present in a flow associated with the network packet based on a rule. The rule can be, for example, a comparison of

the parameter with a list, pattern matching the parameter against one or more patterns, etc.

[0025] In one example, the network packet is a DNS request. In this example, the parameter includes a domain name. The domain name can be compared to a list that includes domain names that are known or assumed to serve advertisements. If the domain name is on the list, an advertisement indicator is present indicating that an advertisement is likely in the flow.

[0026] In another example, the network packet is an HTTP request such as a GET request or CONNECT request. In this example, the parameter can be a URI. The URI may be absolute (e.g., a full URL including a host value (e.g., [hostvalue]/folder/advertisement.html)) or may be relative (e.g., /folder/advertisement.html). The URI can be compared to a URI pattern indicative of advertisements. Patterns that can be matched can be in the form of regular expressions, lists, Bloom tables, hashing and comparison to a list, etc. In some examples, machine learning can be used on lists of URIs with structures indicative of advertisements to determine the criteria used in the pattern matching. As such, an advertisement indicator can be determined to be present if the URI is matched with a URI pattern indicative of advertisements. Other examples of structures indicative of advertisements can include [\*/ads, /banners, /clickonme, etc. In some examples, URI structures and/or domain names can come from services or available lists.

[0027] The enforcement engine 108 can perform actions based on whether an advertisement indicator is present in the network packet. In one example, the action can include a response to a requestor of the request (e.g., computing device 330a). In another example, where the network packet is a DNS request, a response to a domain name found to be associated with advertisements can be a response indicating that the domain name was not found. In other examples, the response can indicate an Internet Protocol (IP) address for a substitute advertisement server, for example, a server controlled by an administrator of the SDN 300. Further, in some examples, the response can indicate that the

response is from a DNS server. The network appliance 100 may be provided the capability of assuming the identity of the DNS server (e.g., by being provided identification data of the DNS server) and/or advertisement server. With the above approaches, the network appliance 100 can respond to a request that includes an indicator that advertisements are present by denying the request and pretending that the host/resource is not available or responding with a substitute.

[0028] In some examples, the server can be an approved advertisement server. The approved advertisement server can be in the SDN 300 or outside of the SDN 300. Further, the approved advertisement server may include advertisements located in structures that mimic advertisements on known advertisement servers. To implement this, known advertisement servers can be crawled and replacement content for the ads be used on the approved advertisement server. In some examples, the replacement ad may be blank or smaller in size compared to the original advertisement. In other examples, the replacement ad may be based on an advertisement purchased by another or associated with a company owning the SDN 300. For example, in the case of a campus network or establishment such as a hotel or coffee shop, the advertisements may be sold to area shops or may be used to promote the establishment (e.g., provide sales promotions or advertise additional features).

[0029] In other examples, if an advertisement indicator indicating that an advertisement is present in the flow is not present, the request can be re-inserted to the network and destined for the DNS server. As noted, this can be implemented using OpenFlow or other control protocol. To avoid re-inspecting the same DNS request multiple times (e.g., as it crosses multiple controlled network infrastructure devices 306, 200), various approaches can be used. In one example, the matching criteria for the network infrastructure devices 200 can include the ingress port and push a separate rule for each edge port on the network. As such, non-edge network infrastructure devices need not implement the functionality. In another example, when the response to the DNS request is re-inserted (e.g., in the case of a non-match), it is not re-inserted into the network infrastructure device 200 that forwarded the packet to the network appliance 100.

Rather, the DNS request would be re-inserted into the network infrastructure device 200, 306 that is nearest to the known location of the DNS server.

[0030] In one example, the request is an HTTP request. In this example, the action can include substituting web content for a resource associated with the URI. This can occur, in one example, by responding with the content expected (e.g., the network appliance 100 may include default blank resources of each type (e.g., image, video, flash, etc.) and respond with blank content. This can also be implemented by providing a reference to the content. For example, if the requested URI matched a pattern, then a response would be issued by the network appliance 100 and inserted into the network as if it came from the intended HTTP recipient. The response can include, for example, a HTTP 302 response, which is an approach to perform URL redirection. The 302 response can invite the computing device 330a to perform another request to the URL input in the 302 response. In another example, the action can include denying the HTTP request and inserting an HTTP 404 “not found” response.

[0031] In one example, the network appliance 100 can fetch the resource requested from the host. The network appliance 100 can then inspect the fetched resource. In one example, the resource can be inspected to determine whether it includes an advertisement based on content. In another example, the resource can be inspected to determine a size of the resource (e.g., an image, video, other rich content, etc.). Using the size information, the network appliance 100 can determine a substitute for the advertisement (e.g., a same or similar viewable sized substitute advertisement, blank resource, etc.).

[0032] In some examples, to avoid re-inspection, if the requested URI did not match, the request could be re-inserted to the SDN 300 and destined for the HTTP recipient. This, too, may be accomplished via OpenFlow or another similar control protocol. Moreover, a replacement URL and/or domain may be included on a whitelist of allowed requests.

[0033] The network infrastructure device management engine 110 can be used to push rules to network infrastructure devices 200, 306. The rules can include

instructions for the network infrastructure device to check for whitelisted and/or blacklisted criteria. Matches for blacklisted criteria can lead to an advertisement indicator that an unwanted advertisement is present and can have corresponding pre-determined responses stored on the network infrastructure device 200. Matches for whitelisted criteria can similarly lead to an advertisement indicator that an approved advertisement may be present or an indicator that an unwanted advertisement is not present. This whitelisted advertisement indicator can lead to processing the packet normally without sending to the network appliance 100 or intercepting the packet and sending a response in its place.

[0034] The network infrastructure device management engine 110 can determine these rules from input such as new web advertisement data and advertisements commonly used on the SDN 300. In one example, when a domain name or particular URI is used the network appliance 100 can track the usage. This way, more common advertisement indicators can be made into rules for network infrastructure devices 200, 306. Moreover, the lists, rules, and criteria for both the network appliance and the network infrastructure devices 200, 306 can be updated. In one example, when usage hits a threshold, the network infrastructure device rule can be updated and sent to the network infrastructure devices 200, 306, which can implement the rules.

[0035] In some examples, the approaches for DNS requests and HTTP requests can be used in conjunction. At a first stage, DNS requests are processed. This way content from domain names known to serve advertisements can be stopped or substituted. In some examples, the list of domain names can include domain names that are well known ad servers (where all or most content can be assumed to be advertisements). Other websites that serve both non-advertisement content and advertisement content can be addressed by the second stage. The second stage looks at the HTTP request to determine whether the structure of a URI indicates an advertisement. With this approach, the number of HTTP requests to check is reduced because requests related to DNS requests that were responded to with “not found” are not formed.

[0036] In one example, the network infrastructure device 200 can receive, at network interface 202, a network packet. The request engine 204 can determine that the packet is associated with one of the pre-determined request types described. The parameter identification engine 206 of the network infrastructure device 200 can identify a parameter from the network packet based on the association with the pre-determined request type (e.g., a DNS request may yield a domain name parameter, a GET or CONNECT request may yield a URI).

[0037] The rule engine 208 can implement rules received from the network appliance 100 or other device. Rules can be used to check whether the parameter matches criteria that leads to a particular advertisement indicator. As used herein, an “advertisement indicator” is a gauge of whether an advertisement is likely present based on criteria. Advertisement indicators can be linked to particular actions to take. The enforcement engine 210 can perform that action.

[0038] In one example, a rule can provide criteria that, when matched by the parameter, yields an advertisement indicator that is blacklisted (e.g., a domain name in a DNS request is known to be associated with serving advertisements). A denial or substitute response action can be taken.

[0039] In another example, a rule can provide criteria that, when matched by the parameter, yields an advertisement indicator that is whitelisted (e.g., an approved domain name, a URI structure that indicates an approved advertisement is present, etc.). The action for such an advertisement indicator could be that request can be processed normally. In some examples, substitute domain names/URIs may include fingerprints (e.g., “approved server host name” or “/approvedadvertisements”) that can be used to indicate that advertisements or substitutions are approved.

[0040] In other examples, a rule can indicate that if other criteria are not matched, further processing is to be taken. As such, the enforcement engine 210 can take an action to forward the network packet to the network appliance 100 (e.g., a SDN controller). This approach can be used because the network

appliance 100 may have more resources and processing capability than a network infrastructure device 200, thus matching abilities may be limited.

[0041] The engines 104, 106, 108, 110, 204, 206, 208, 210 include hardware and/or combinations of hardware and programming to perform functions provided herein. Moreover, the modules (not shown) can include programming functions and/or combinations of programming functions to be executed by hardware as provided herein. When discussing the engines and modules, it is noted that functionality attributed to an engine can also be attributed to the corresponding module and vice versa. Moreover, functionality attributed to a particular module and/or engine may also be implemented using another module and/or engine.

[0042] A processor 130, 230, such as a central processing unit (CPU) or a microprocessor suitable for retrieval and execution of instructions and/or electronic circuits can be configured to perform the functionality of some or any of the engines 104, 106, 108, 110, 204, 206, 208, 210 described herein. In certain scenarios, instructions and/or other information, such as criteria and/or enforcement actions, can be included in memory 132, 232 or other memory. Moreover, in certain examples, some components can be utilized to implement functionality of other components described herein. Input/output devices such as communication devices like network communication devices or wireless devices can also be considered devices capable of using the input/output interfaces.

[0043] The SDN 300 can use wired communications, wireless communications, or combinations thereof. Further, the SDN 300 may be part of another communication network that can include multiple sub communication networks such as data networks, wireless networks, telephony networks, etc. Such networks can include, for example, a public data network such as the Internet, local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), cable networks, fiber optic networks, combinations thereof, or the like. In certain examples, wireless networks may include cellular networks,

satellite communications, wireless LANs, etc. Various communications structures and infrastructure can be utilized to implement the communication network(s).

[0044] By way of example, the computing devices 330a – 330i communicate with each other and other components with access to the communication network via a communication protocol or multiple protocols. A protocol can be a set of rules that defines how nodes of the communication network interact with other nodes. Further, communications between network nodes can be implemented by exchanging discrete packets of data or sending messages. Packets can include header information associated with a protocol (e.g., information on the location of the network node(s) to contact) as well as payload information.

[0045] In some examples, some or all of the engines 104, 106, 108, 110, 204, 206, 208, 210 can be implemented using various technologies, for example, a programmable switch ASIC and/or other resources (e.g., TCAM, hashes, counters, etc.). In an example, the implementation to match criteria can be based on at least one Bloom filter. A Bloom filter can be used to test whether an element (e.g., a character, string of characters, a byte pattern from packet(s)) is a member of a set (e.g., interesting byte patterns indicative of advertisements). In another example, the criteria can be based on a regular expression filter. A regular expression filter searches for byte patterns in the packets using regular expressions.

[0046] Though GET and CONNECT requests are called out in the description, inspection can also be performed on other packets, for example, each HTTPS packet. When the HTTPS connection is set up, a Secure Sockets Layer (SSL) proxy technique can be used to set up the network appliance 100 as a man-in-the-middle for communications of the flow. The network appliance 100 may further include some of the functionality of the network infrastructure device 200 in this example.

[0047] FIG. 4 is a flowchart of a method for performing an action based on an advertisement indicator, according to an example. FIG. 5 is a block diagram of a device capable of performing an action based on an advertisement indicator,

according to an example. The SDN controller 500 includes, for example, a processing element 510, and a machine-readable storage medium 520 including instructions 522, 524, 526, 528 for performing an action based on an advertisement indicator. SDN controller 500 may be implemented using, for example, a server, a workstation, or any other computing device capable of performing the tasks described herein.

[0048] Processing element 510 may include, one or multiple central processing unit (CPU), one or multiple semiconductor-based microprocessor, one or multiple graphics processing unit (GPU), other hardware devices suitable for retrieval and execution of instructions stored in machine-readable storage medium 520, or combinations thereof. The processing element 510 can be a physical device. Moreover, in one example, the processing element 510 may include multiple cores on a chip, include multiple cores across multiple chips, or combinations thereof. Processing element 510 may fetch, decode, and execute instructions 522, 524, 526, 528 to implement identification of advertisement indicators and actions to perform in response. As an alternative or in addition to retrieving and executing instructions, processing element 510 may include at least one integrated circuit (IC), other control logic, other electronic circuits, or combinations thereof that include a number of electronic components for performing the functionality of instructions 522, 524, 526, 528. For example, the processing element 510 can include a programmable packet processor, which may also include TCAMs, hashes, counters, etc.

[0049] Machine-readable storage medium 520 may be any electronic, magnetic, optical, or other physical storage device that contains or stores executable instructions. Thus, machine-readable storage medium may be, for example, Random Access Memory (RAM), an Electrically Erasable Programmable Read-Only Memory (EEPROM), a storage drive, a Compact Disc Read Only Memory (CD-ROM), and the like. As such, the machine-readable storage medium can be non-transitory. As described in detail herein, machine-readable storage medium 520 may be encoded with a series of

executable instructions for performing an action based on an advertisement indicator.

[0050] At 402, the interface instructions 522 can be executed by processing element 510 to receive a network packet identified by a network infrastructure device as matching criteria associated with a pre-identified request such as a DNS request, a GET request, or a CONNECT request. At 404, parameter identification instructions 524 can be executed to identify a parameter in the network packet. As noted above, the identification can be based on determining the type of network packet and looking for particular content (e.g., a domain name for a DNS request, a URI for a HTTP GET or CONNECT request, etc.).

[0051] At 406, parameter indication instructions 526 can be executed by the processing element 510 to determine whether an advertisement indicator is present in the network packet. More than one advertisement indicator can be searched for. One or more of the advertisement indicators can correspond to actions to be taken.

[0052] At 408, action instructions 528 can be executed by the processing element 510 to perform an action based on whether a particular advertisement indicator (e.g., based on a matched domain name, matched URI, etc.) is present in the network packet. In one example, the action can include providing a response to a source device of the network packet as described above.

[0053] In another example, the SDN controller 500 may perform an action to determine a new rule to implement at the network infrastructure device(s) controlled by the SDN controller 500. As noted above, a new rule can be based on analytics of advertisement content on the network and/or based on updated lists of advertisement servers and/or URI structures. Action instructions 528 can be implemented to send the network infrastructure device(s) the rule(s). As noted above, the rule(s) can include another action to perform locally on the network infrastructure device based on the advertisement indicator. For example, if a sufficient number of DNS requests come for a newly seen ADSERVER1, a rule for a default action to take can be updated on the network infrastructure devices.

## CLAIMS

### What is claimed is:

1. A network appliance comprising:  
an interface to receive a network packet identified by a network infrastructure device as matching criteria associated with a pre-identified request;  
a parameter identification engine to identify a parameter in the network packet;  
a rule engine to determine whether the parameter indicates that an advertisement indicator is present in a flow associated with the network packet based on a rule; and  
an enforcement engine to perform an action based on whether the advertisement indicator is present in the network packet.
2. The network appliance of claim 1,  
wherein the network packet is a domain name system (DNS) request and the parameter includes a domain name,  
wherein the rule compares the domain name to a list that includes domain names known to serve advertisements, and  
wherein the advertisement indicator is present if the domain name is on the list.
3. The network appliance of claim 2,  
wherein the action includes a response to a requestor of the pre-identified request, and  
wherein the response indicates that the response is from a DNS server.
4. The network appliance of claim 1,  
wherein the network packet includes a Uniform Resource Identifier (URI),  
wherein the parameter includes the URI, and  
wherein the advertisement indicator is present if the URI is matched with a URI pattern indicative of advertisements.

5. The network appliance of claim 4, wherein the request is a GET request or a CONNECT request.
6. The network appliance of claim 4, wherein the action includes substituting web content for a resource associated with the URI.
7. The network appliance of claim 1, further comprising:  
a network infrastructure device management engine to determine a network infrastructure device rule based on the rule,  
wherein the action includes sending the network infrastructure device rule to the network infrastructure device, and  
wherein the network infrastructure device rule includes another action to perform locally on the network infrastructure device based on the advertisement indicator.
8. The network appliance of claim 1, wherein the action includes denying the pre-identified request for the network packet and responding to a requestor of the network packet with an indication that a resource for the pre-identified request is unavailable.
9. A non-transitory machine-readable storage medium storing instructions that, if executed by a physical processing element of a software defined networking (SDN) controller, cause the SDN controller to:  
receive a network packet identified by a network infrastructure device as matching criteria associated with a pre-identified request;  
identify a parameter in the network packet;  
determine whether an advertisement indicator is present based on the parameter and a rule; and  
perform an action based on whether the advertisement indicator is present in the network packet,  
wherein the action includes providing a response to a source device of the network packet.

10. The non-transitory machine-readable storage medium of claim 9, further comprising instructions that, if executed by the physical processing element, cause the SDN controller to:

determine a network infrastructure device rule based on the rule,  
wherein the action further includes sending the network infrastructure device rule to the network infrastructure device, and

wherein the network infrastructure device rule includes another action to perform locally on the network infrastructure device based on the advertisement indicator.

11. The non-transitory machine-readable storage medium of claim 9, further comprising instructions that, if executed by the physical processing element, cause the SDN controller to:

compare the parameter to a list of known domain names known to serve advertisements,

wherein the parameter includes a domain name and the network packet is a domain name system (DNS) request, and

wherein the advertisement indicator is present if the domain name is on the list.

12. The non-transitory machine-readable storage medium of claim 9, further comprising instructions that, if executed by the physical processing element, cause the SDN controller to:

identify a Uniform Resource Identifier (URI) in the network packet,

wherein the parameter includes the URI;

determine that the advertisement indicator is present if the URI is matched with a URI pattern indicative of advertising.

13. A network infrastructure device comprising:

a network interface to receive a network packet;

a request engine to determine that the network packet is associated with a pre-determined request type;

a parameter identification engine to identify a parameter from the network packet based on the association with the pre-determined request type;

a rule engine to determine whether the parameter indicates that an advertisement indicator is present in a flow associated with the network packet based on a rule; and

an enforcement engine to perform an action on the network packet according to the advertisement indicator.

14. The network infrastructure device of claim 13, wherein the network packet is a domain name system (DNS) request and the parameter includes a domain name, the rule engine further to:

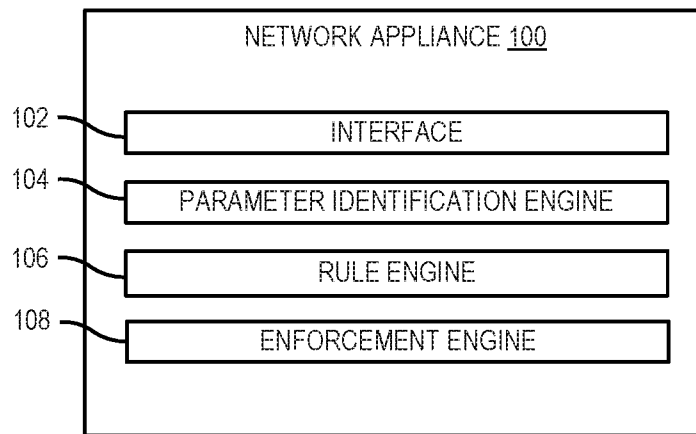
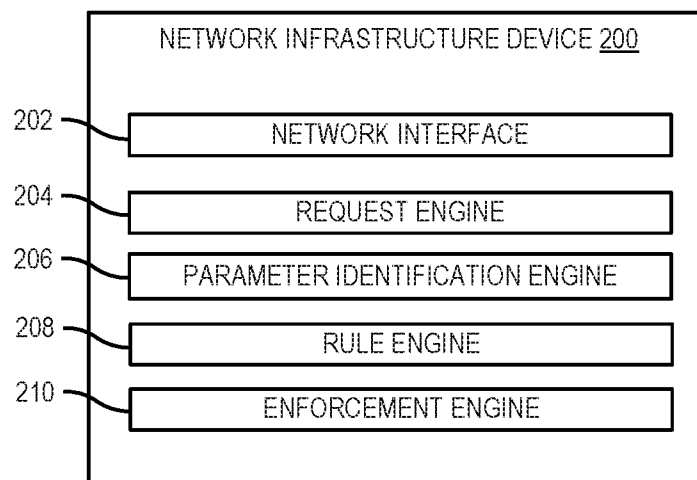
compare the domain name to a first list of allowed domain names and

compare the domain name to a second list of known domain names known to serve advertisements,

wherein when the domain name does not match the first list and the second list, the action includes forwarding the network packet to a software defined networking controller for further processing.

15. The network infrastructure device of claim 13, wherein the network packet includes a Uniform Resource Identifier (URI), wherein the parameter includes the URI, and wherein the advertisement indicator is present if the URI is matched with a URI pattern indicative of advertisements.

1/3

**FIG. 1****FIG. 2**

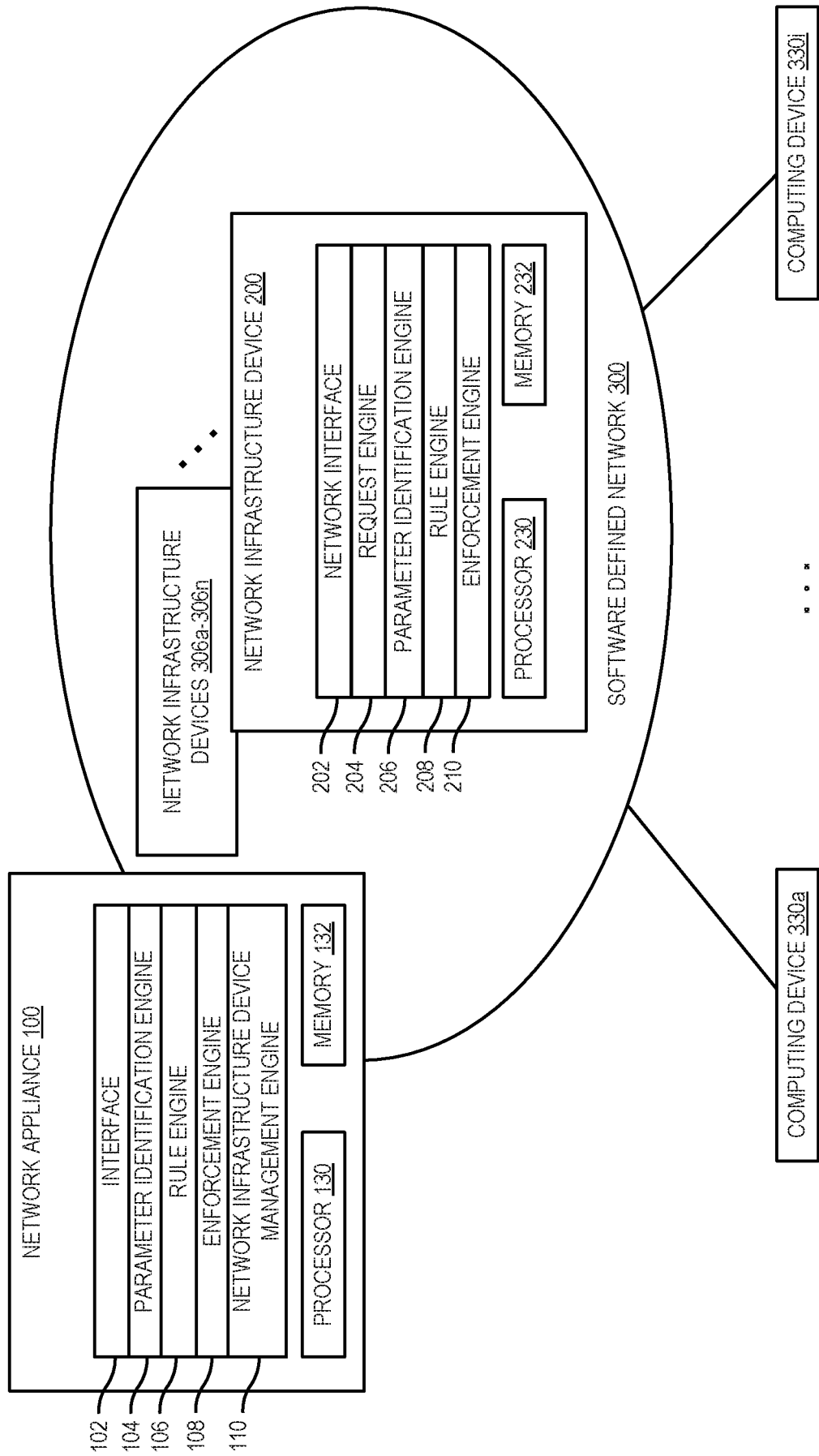
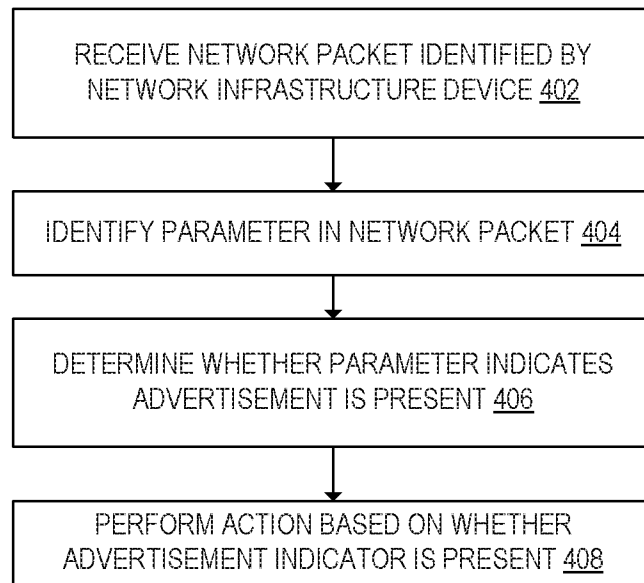
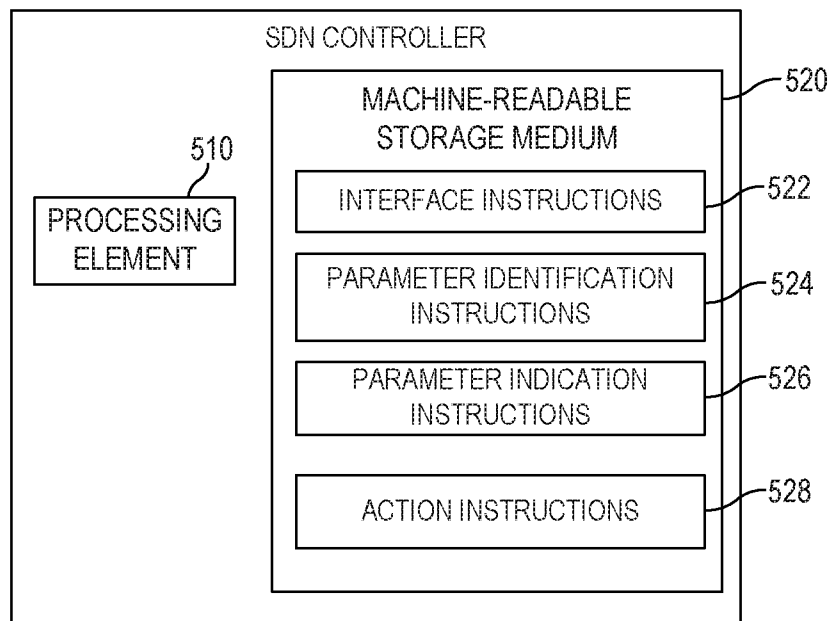


FIG. 3

3/3

400**FIG. 4**

500

**FIG. 5**

**A. CLASSIFICATION OF SUBJECT MATTER****H04L 12/851(2013.01)i, 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 12/851; G06Q 30/02; G06Q 10/06; G06F 17/30; H04L 29/06; H04L 12/26

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) &amp; Keywords: network appliance, matching, identify, parameter, advertisement, indicator, action

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2008-0133518 A1 (HARSH KAPOOR et al.) 05 June 2008 See paragraphs [0015], [0045], [0153]-[0158], [0166], [0210]; and claim 1; and figure 2.	1-15
Y	US 2015-0170072 A1 (AD-VANTAGE NETWORKS, INC.) 18 June 2015 See paragraphs [0009]-[0012], [0042], [0046], [0057], [0126]; claim 1; and figure 4.	1-15
Y	WO 2012-152813 A1 (TELEFONICA, S.A.) 15 November 2012 See page 7; lines 10-12, page 18; lines 23-24; and figure 1.	5
A	US 2015-0172300 A1 (HOPLITE INDUSTRIES, INC.) 18 June 2015 See paragraphs [0025], [0039]-[0044], [0049], [0065]-[0066]; and figures 1-2.	1-15
A	US 2012-0221386 A1 (OREN NETZER et al.) 30 August 2012 See paragraphs [0017]-[0025]; and figure 1.	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

"&amp;" document member of the same patent family

Date of the actual completion of the international search

24 November 2016 (24.11.2016)

Date of mailing of the international search report

**01 December 2016 (01.12.2016)**

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

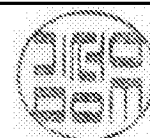
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

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/US2016/021314**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0133518 A1	05/06/2008	AU 2001-91227 A1 AU 2006-265624 A1 AU 2006-265624 B2 CA 2423475 A1 CA 2614328 A1 CA 2614328 C CN 1518694 A CN 1518694 C EP 1381937 A2 EP 1898822 A2 EP 1960867 A2 EP 2432188 A1 EP 2432188 B1 EP 2442525 A1 JP 2004-524598 A JP 2009-504201 A KR 10-2004-0005824 A US 2002-0059424 A1 US 2002-0165947 A1 US 2006-0010207 A1 US 2006-0143499 A1 US 2007-0006215 A1 US 2007-0016183 A1 US 2007-0192863 A1 US 2008-0133517 A1 US 2008-0134330 A1 US 2008-0162390 A1 US 2008-0229415 A1 US 2008-0262990 A1 US 2008-0262991 A1 US 2010-0042565 A1 US 7836443 B2 US 7979368 B2 US 8010469 B2 US 8046465 B2 US 8080009 B2 US 8402540 B2 US 8512333 B2 WO 02-027469 A3 WO 02-27469 A2 WO 2007-005830 A2 WO 2007-070838 A2	08/04/2002 11/01/2007 17/11/2011 04/04/2002 11/01/2007 19/04/2016 04/08/2004 16/05/2007 21/01/2004 19/03/2008 27/08/2008 21/03/2012 20/04/2016 18/04/2012 12/08/2004 05/02/2009 16/01/2004 16/05/2002 07/11/2002 12/01/2006 29/06/2006 04/01/2007 18/01/2007 16/08/2007 05/06/2008 05/06/2008 03/07/2008 18/09/2008 23/10/2008 23/10/2008 18/02/2010 16/11/2010 12/07/2011 30/08/2011 25/10/2011 20/12/2011 19/03/2013 20/08/2013 06/11/2003 04/04/2002 11/01/2007 21/06/2007
US 2015-0170072 A1	18/06/2015	WO 2015-013459 A1	29/01/2015
WO 2012-152813 A1	15/11/2012	AR 086341 A1 EP 2708004 A1 ES 2401900 A2 ES 2401900 B1	04/12/2013 19/03/2014 25/04/2013 05/03/2014

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2016/021314**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		ES 2401900 R1	30/07/2013
US 2015-0172300 A1	18/06/2015	None	
US 2012-0221386 A1	30/08/2012	CN 102713959 A	03/10/2012
		EP 2499607 A1	19/09/2012
		JP 2013-510359 A	21/03/2013
		JP 5780658 B2	16/09/2015
		WO 2011-055370 A1	12/05/2011