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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 August 2018 (02.08.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/137761 A1

(51) International Patent Classification:
H04L 12/721 (2013.01) *H04L 12/725* (2013.01)
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/EP2017/051479

(22) International Filing Date:
25 January 2017 (25.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **NEC LABORATORIES EUROPE GMBH** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors: **SIRACUSANO, Giuseppe**; Via Nicolò Piccinni 32, 00199 Roma (IT). **BIFULCO, Roberto**; Bergheimerstraße 38, 69115 Heidelberg (DE).

(74) Agent: **ULLRICH & NAUMANN**; Schneidmühlstraße 21, 69115 Heidelberg (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: EXPLICITLY ADDRESSED SERVICE FUNCTION CHAINING

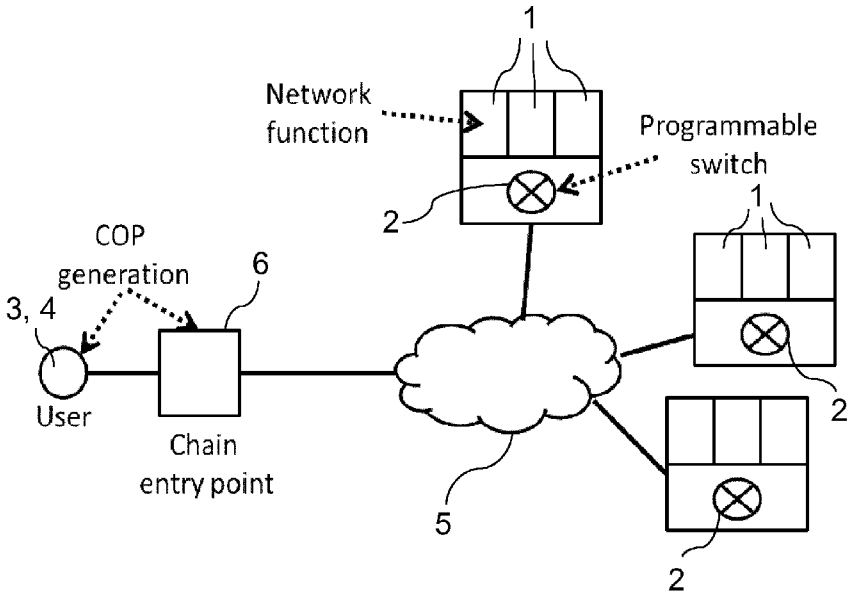

Fig. 1

(57) Abstract: A method for service function chaining in a network, comprises defining, for a flow of network packets sent from a source node (4) to a destination node, a chain of selected network service functions (1) to be traversed by the flow, wherein each of the selected network service functions (1) is attached or connected to a programmable switch (2) capable of operating as a packet forwarding element, generating a chain establishment packet that contains network identifier information about the selected network service functions (1) and that is configured as a regular network packet to be delivered to the destination node along a network path that includes the programmable switches (2) to which the selected network service functions (1) are attached or connected, wherein each of the programmable switches (2), upon receipt of the chain establishment packet and based on the network identifier information about the selected network service functions (1) contained in the chain establishment packet, performs installation of packet forwarding rules

WO 2018/137761 A1

[Continued on next page]

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))*

for the flow together with network address and port translation operations, and selects, on behalf of the respective attached or connected network service function (1), socket parameters to be used by the network service function (1) for processing the flow. Furthermore, the present invention relates to a network switch and a network addressable apparatus hosting a network service function.

EXPLICITLY ADDRESSED SERVICE FUNCTION CHAINING

The present invention relates to a method for service function chaining in a network. Furthermore, the present invention relates to a network switch as well as to a network addressable apparatus hosting a network service function.

Network operators deploy network functions to enforce their policies and to provide additional services on top of plain connectivity (for reference, see M. Honda et al.: “Is it still possible to extend TCP?”, in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (IMC '11), ACM, New York, NY, USA, 181-194).

Content caching, NAT, TCP optimization, video transcoding, HTTP header enrichment, are examples of such services. Despite their ubiquitous usage (as documented in Z. Wang, Z. Qian, Q. Xu, Z. Mao, and M. Zhang: “An untold story of middleboxes in cellular networks”, in *Proceedings of the ACM SIGCOMM 2011 conference* (SIGCOMM '11), ACM, New York, NY, USA, 374-385) network functions deployment is still performed by modifying the network topology. That is, network functions are hard-wired on the network traffic’s path. The inflexibility and complexity of this approach is not acceptable when network functions are implemented by means of software running in virtual machines, as envisioned in the case of Network Function Virtualization (NFV). In fact, hard-wiring would hinder the benefits brought by the possibility of dynamically deploying virtual network functions (VNFs) on general purpose servers.

Therefore, there is a growing interest on Service Function Chaining (SFC) systems, which enable the flexible deployment of network functions while guaranteeing their configurable and dynamic chaining.

In general, a SFC system assigns a network flow entering the managed network to a chain of functions, and steers the flow through the functions of such chain, according to the chain's functions ordering. A number of challenges arise when addressing the design of a SFC system. First, assigning a network flow to its chain requires network traffic classification, an operation that is critical for the system

scalability since it should be performed for all the handled traffic. Second, traffic forwarding should be performed according to the chain the traffic belongs to, instead of following the typical forwarding approach, e.g., based on IP routing. Third, network flows are usually bi-directional, that is, there is an upstream and a downstream direction and a network function, e.g., a firewall, may need to handle both of them. This requires performing a coordinated classification of upstream and downstream flows, and the enforcement of symmetric paths for the two directions. Finally, network functions may have dynamic and opaque behaviors that modify the network traffic in unknown ways, which may introduce a need for traffic reclassification or even make the traffic unclassifiable (for reference, see Zafar Ayyub Qazi et al.: “SIMPLE-fying middlebox policy enforcement using SDN”, in *SIGCOMM Comput. Commun. Rev.* 43, 4 (August 2013), 27-38).

To address these challenges, a number of SFC systems have been already proposed (for instance, in Seyed Kaveh Fayazbakhsh et al.: “Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags”, in *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation* (NSDI'14), USENIX Association, Berkeley, CA, USA, 533-546). However, they usually target green field or long term deployments. In fact, they require a number of changes either in the network hardware or in the network functions, or in both. In other cases, they require modifications to the network architecture. Ready to deploy solutions, which don't require such changes, may instead not handle all the aforementioned challenges. For example, some SFC systems are unable to deal with opaque network functions actions.

In view of the above it is an objective of the present invention to improve and further develop a method for service function chaining in a network, a network switch as well as a network addressable apparatus hosting a network service function in such a way that the above issues are overcome or at least partially alleviated.

In accordance with the invention, the aforementioned objective is accomplished by a method for service function chaining in a network, wherein the method comprises

defining, for a flow of network packets sent from a source node to a destination node, a chain of selected network service functions to be traversed by the flow, wherein each of the selected network service functions is attached or connected to a programmable switch capable of operating as a packet forwarding element,

generating a chain establishment packet that contains network identifier information about the selected network service functions and that is configured as a regular network packet to be delivered to the destination node along a network path that includes the programmable switches to which the selected network service functions are attached or connected,

wherein each of the programmable switches, upon receipt of the chain establishment packet and based on the network identifier information about the selected network service functions contained in the chain establishment packet, performs installation of packet forwarding rules for the flow together with network address and port translation operations, and selects, on behalf of the respective attached or connected network service function, socket parameters to be used by the network service function for processing the flow.

Furthermore, the above objective is accomplished by a network switch, comprising

network interfaces configured to receive and transmit packets of a network flow,

network service function interfaces configured to communicate with one or more attached or connected network service functions, and

a processing circuitry in communication with the network interfaces and the network service function interfaces, the service chain processing circuitry configured to:

read, from a chain establishment packet that is received via a network interface, network identifier information about network service functions of a chain of network service functions selected for the network flow, and

perform, based on the network identifier information about the selected network service functions contained in the chain establishment packet, installation of packet forwarding rules for the flow together with network address and port translation operations.

Still further, the above objective is accomplished by a network addressable apparatus hosting a network service function, the apparatus comprising

a hardware component on which the network service function is executed,

an operating system configured to manage the hardware component and a pool of port numbers, and

a network function program running on the operating system that is configured to provide the network function's operations, wherein the network function program is configured

to query the operating system to provide a socket for a new network flow, and

to receive and employ a socket for the new network flow that is provided with a port number selected by a delegated switch to which the network service function is attached are connected, instead of using a port number selected autonomously by the operating system.

According to the invention it has been recognized that a configurable and dynamic chaining of network service functions can be achieved by the inclusion of chain information in and only in a first chain establishment or opening packet. The present invention enables service function chaining with no core network infrastructure support and can therefore be used, e.g., on the Internet. Data plane is more lightweight and efficient since no tunneling or extra headers are added to the packets and only the first packet of the chain requires extra processing.

In the context of the present invention it is important to note that, generally, source routing is a well-known technique that allows a sender to specify the route that a packet should take through the network. Given its role in steering packets in a network, source routing has some similarities with the present invention. Essentially, there are two types of source routing possible, strict or loose source routing. The strict source routing lists the precise path the packet has to traverse through the network, while the loose source routing specifies a sequence of 'waypoint' addresses the packet has to traverse.

Differently from the present invention, source routing headers have to be added to every packet of the flow. This reduces the available space for the packet payload if

the header is applied by the node that generates the traffic, if the header is added by an intermediate node (proxy or classifier on path) the packets composing the flows need to be fragmented.

Furthermore, the source routing header is added at IP level, this information is not exposed by the OS socket and cannot be processed at application level.

In contrast, embodiment of the present invention add chaining information only to the first packet of a flow and adds such information in L4+ header, enabling the chaining of L4+ opaque functions over, e.g., a general purpose TCP/IP network. Furthermore, embodiments of the invention, which require only minimal modifications of the network functions, address also classification issues when packets traverse opaque functions. In these cases, packets can be assigned to their chains after processing by the function even if the function modifies packets' header.

According to an embodiment the chain establishment packet may be generated either by the source node (i.e. the entity that starts the communication) or by an on-path proxy.

According to an embodiment the chain establishment packet is configured to contain a list that includes network service function identifiers of the selected network service functions and an address of the destination node as a last entry of the list.

According to an embodiment the chain establishment packet may be configured to use indirection functions that map a network service function address and/or port numbers to an address and/or port numbers of the respective programmable switch to which the network service function is attached or connected.

According to an embodiment the chain establishment packet may be configured to include an additional identification element of the respective programmable switches.

According to an embodiment of the method comprises the steps of receiving, by a programmable switch, a chain establishment packet, reading from the chain establishment packet a network identifier of the next network service function in the chain of selected network service functions, and steering the flow towards the next network service function by installing appropriate packet forwarding rules for the flow.

Embodiment of the present invention address network service functions that, when processing network packets of a flow, modify the network packets' headers According to these embodiments such network service function may execute a network identifier selection delegation operation that is configured to delegate to the programmable switch to which the network service function is attached or connected a task of defining a delegation network address or port number the network service function will use when sending network packets in response to the reception of network packets of the flow.

Specifically, according to an embodiment, a programmable switch may generate either a delegation source address or port number or a delegation destination address or port number and, for the purpose of enabling usage, passing the generated address or port number to the respective network service function.

According to an embodiment a programmable switch may be pre-configured with a pool of reserved addresses or port numbers the respective network service function does not assign in any other case. In such case the programmable switch may select a delegation network address or port number from this pool of reserved addresses or port numbers.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end it is to be referred to the dependent patent claims on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the drawing on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the drawing, generally preferred

embodiments and further developments of the teaching will be explained. In the drawing

Fig. 1 is a schematic view illustrating service function chaining in a network in accordance with an embodiment of the present invention,

Fig. 2 is a schematic view illustrating a network identifier selection delegation operation in accordance with an embodiment of the present invention,

Fig. 3 is a schematic view illustrating service function chaining for a TCP flow in accordance with an embodiment of the present invention, using a shortened address/port notation,

Fig. 4 is a schematic view illustrating the embodiment of Fig. 3, using a more realistic address/port notation, and

Fig. 5 is a schematic view illustrating the structure of a network service function in accordance with an embodiment of the present.

Generally, a service function chain includes a sequence of network service functions (hereinafter sometimes briefly referred to as service functions or network functions, or simply as NFs) that are hosted by various network nodes. When a traffic flow is steered along a service chain, packets in the traffic flow are processed by the various service functions. These service functions may include typical network services such as content caching, firewall, network access translation (NAT), video transcoding, TCP optimization, deep packet inspection (DPI), etc. After processing a packet of a flow by applying a particular service function, the packet will be forwarded to the next service function in the chain.

Essentially, embodiments of the present invention described hereinafter in detail, relate to one or more of the following aspects:

1. Usage of explicitly addressed programmable switches to enforce traffic steering

2. Generation of a first packet of a new network flow to contain a list of network functions to be traversed
3. Configuration of NAPT operations in the programmable switches
4. Definition of a delegation function, which instructs programmable switches to define the network parameters a NF should be using for a given flow.

Fig. 1 illustrates, according to an embodiment, a system for performing resource efficient chaining of transparent and non-transparent (layer 4-7) service functions 1 without network support using programmable (software) switches 2. According to common deployment models, a chain of service functions 1 typically applies a sequence of service functions 1 to a traffic flow in a specific order. In the context of the present invention it is assumed that each of the service functions 1 is attached or connected to a programmable switch 2. These programmable switches 2, through which network traffic traverses, are capable of operating as packet forwarding elements.

According to the embodiment of Fig. 1, it is assumed that a flow of network packets is sent from user 3, who acts as a source node 4 starting the communication, to a destination node (not shown), e.g., via the Internet 5. For this flow, a chain of selected network service functions 1 to be traversed by the flow is defined. This definition can be made by the user 3 itself, it can be imposed merely by the network, or can be a composition of a user 3 selection and network demand.

Based on the selected network service functions 1, at first, either the user 3 itself or a chain entry point 6 generates a chain establishment or chain opening packet (hereinafter briefly denoted COP) that is delivered to those programmable switches 2 to which the selected network service functions 1 are connected. Generally, the entity that generates the COP can be any on-path proxy that intercepts flows entering the network.

At a logical level, the COP contains a list of the selected NFs that should be traversed by the flow. In practice, the COP contains a list of NFs' identifiers such

as a list of IP address/port number couples. The last entry of the list is always the final destination of the flow, for instance, a content provider's server.

The following notation will be used to express the content of a COP, according to an embodiment: COP (*src*, *dst*) [NF1,NF2,...], where '*dst*' is the destination included in the packet header and used by the routing system to define the next hop of the packet. '*src*' is the source value included in the packet's header. The list [NF1, NF2, ..] is the list of network functions to be used for the flow.

For simplicity and without loss of generality, in accordance with the embodiment described in connection with Fig. 1 it is assumed that the COP is generated by an on-path proxy 6. Upon reception of a new packet starting a flow from a client C, i.e. user 3, destined to a server S as destination node (i.e., packet (C,S)), and assuming that two network functions are included in the chain, the proxy 6 will generate a COP (C,NF1)[NF2,S].

Here, NF1, NF2 are addresses assigned to the switches 2 to which the network functions 1 are attached or connected. However, it is also possible to use an indirection function to map NF1 to a switch address, and therefore have different addresses between the network functions 1 and the switches 2 they are attached or connected to. In another case, the COP could be extended to introduce an additional identification element for the switches 2, such as COP (*src*, *dst*) [sw1:NF1,sw2:NF2,...]. In accordance with the embodiment of Fig. 1 the easier case of network functions 1 and switches 2 having the same assigned IP address when they are directly connected will be assumed, as it will ease standing of essential aspect of the invention.

The COP (C,NF1)[NF2,S] is a regular network packet for e.g., a TCP/IP network, and it is therefore delivered to NF1. It is pointed out once again that in this example NF1 is the address of a switch 2 connected to the NF1 function 1 (that has the same address). The switch 2 receives the packet and performs one of the following two actions, depending on whether the respective network function 1 does not change the packet headers (case 1) or does change the packet headers (case 2). The notation (src,dst) → forwardTo is used to express a switch

forwarding rule that causes “packets from src and destined to dst being sent on the switch port that goes towards forwardTo”:

In case 1, the switch 2 is configured to create a number of four forwarding rules as follows:

(C, NF1) →NF1
(NF1, C) →C
(NF1, NF2) → NF2
(NF2, NF1) → NF1

While the first two rules deal with the packets from/to the client C, the next two rules deal with packets to/from the next network function (or final destination). In this context is noted that the switch 2 reads from the COP(C,NF1)[NF2,S] the address of NF2 and therefore can generate all the rules as soon as the COP is received.

On the other hand, in case 2, i.e. when a network function 1 modifies the packet headers, the corresponding switch 2 cannot correlate packets entering the NF 1 with packets being sent back by the NF 1. Therefore, the switch 2 cannot correctly re-classify packets after the network function 1 to perform the steering towards the next service function 1 in the chain. In this case, as illustrated in Fig. 2, the network function 1, which here is assumed to be a L3+ service function, is configured to support a *network identifier selection delegation* operation. In essence, the function 1 delegates to the switch 2 the task of creating a network address which the function 1 will use when sending packets in the response to the reception of a given network flow.

For example, upon reception of COP(C,NF1)[NF2,S], as shown at 210 in Fig. 2 using a shortened notation, the switch 2 would generate the following rules:

(C, NF1) → NF1 + generate and include R in the packet
(NF1, C) →C
(R, NF2) → NF2 + rewrite R with NF1

(NF2, NF1) → NF1 + rewrite NF1 with R,

where R is a source or destination address generated by the switch 2 and passed to the function 1 in the context of the *network identifier selection delegation* operation, as shown at 220. That is, the network function 1 will use R either as source address, as shown at 230, or as destination address, as shown at 240, for packets that are generated as a reaction to the new received network flow. According to an embodiment, it may be provided that the address R is exchanged, and exists, only between the function 1 and the switch 2.

Upon receiving packets back from the network function 1, the switch 2 will be able, by detecting the assigned address R, to identify and reclassify the packets as belonging to a particular flow, and to apply the appropriate forwarding rule for the respective flow, as indicated at 250.

Referring to Figs. 3 and 4, these figures illustrate an embodiment where the flow initiated by the user 3 is a TCP flow. Both figures are almost identical, with the only difference that, while Fig. 3 uses a shortened, more general address/port notation for the packets, Fig. 4 uses a more realistic address/port notation.

In case of TCP flows, the COP can be the TCP SYN packet, whose payload can contain the list of network functions 1 to be traversed by the TCP flow. Once the packet arrives at a NF's switch 2, the switch 2 reads the SYN packet's payload to extract the next hop. Using this information, the switch 2 obtains a TCP SYN plus the NF list, as indicated 310/410.

Next, as indicated at 320/420, the switch 2 randomly selects a source port number ('L4 Rand port=23456') and associates this source port number to the TCP flow. In this case, the switch 2 has been configured in advance with a bucket of reserved ports that can be used during the port number selection and that the network function 1 does not assign in any other case.

Next, the switch 2 installs a rule to forward subsequent packets of the same TCP flow to the connected network function 1. Such rule performs a rewriting of the source TCP port of the flow, as indicated at 330/430.

In the illustrated embodiment the network function 1 is modified to use the source port of the received packet for the generation of any new packet that belongs to the same TCP flow. For instance, a web proxy that receives a connection from 1.2.3.4:23456, will open new TCP connection towards the next hop using a source port 23456, as indicated at 340/440.

At 350/450, once a packet sent by the network function 1 is received by the switch 2, the switch 2 will detect the assigned source port. Therefore, the switch 2 can identify the flow again. This will allow the switch 2 at changing, with a relevant forwarding rule, the destination of the flow to point to the next network function in the chain, as indicated at 360/460.

Referring now to Fig. 5, this figure schematically illustrates the structure of a network service function 1 in accordance with embodiments of the present invention.

The network function 1 is composed of multiple modules. A general operating system 7 is used to manage the hardware component 8 on which the function is executed. A network function program 9, running on the Operating System 7, provides the specific network function's operations.

To manage network communications in the operating system 7, a common abstraction is the *socket.* The socket is specified by a data structure that contains L3, L4 destination and source addresses and other pieces of information. When a Network Function Program 9 has to create a new communication channel with a different network node, it asks the Operating System 7 to provide a new socket.

The new socket is then provided with some pieces of information already filled by the operating system 7. For instance, the source L4 port value is usually extracted from a pool 10 of L4 port numbers that the operating system 7 manages.

According to an embodiment of the invention, the network functions 1 delegate to the programmable switches 2 the generation of relevant socket parameters to be used for a newly established network flow. More specifically, the management of a subset of the port numbers pool 10 is delegated to the switching element 2 to which the network function 1 is attached or connected. As a result, when a specific packet that contains a port number selected by the switch 2 is received by the Network Function Program 9, the program can request a new socket which will be provided with the port number selected by the switch 2, instead of using a port number selected autonomously by the operating system 7.

To summarize, embodiments of the present invention relate to one or more of the following aspects:

1. Generation, by a user or a chain entry point, a first packet (COP) and inclusion of chain information (e.g. a list of functions in the chain) in and only in this first chain establishment packet;
2. Delegation of the selection of a network function's relevant socket parameters to a switching element based on the chain establishment packet information, i.e. network functions and programmable switching are configured to delegate to the switches the generation of relevant socket parameters for the functions;
3. Processing, by the switches attached to the network functions, of the COP to read the list of functions, and perform accordingly NAPT operations and socket parameters selection.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. A method for service function chaining in a network,
the method comprising:

defining, for a flow of network packets sent from a source node (4) to a destination node, a chain of selected network service functions (1) to be traversed by the flow, wherein each of the selected network service functions (1) is attached or connected to a programmable switch (2) capable of operating as a packet forwarding element,

generating a chain establishment packet that contains network identifier information about the selected network service functions (1) and that is configured as a regular network packet to be delivered to the destination node along a network path that includes the programmable switches (2) to which the selected network service functions (1) are attached or connected,

wherein each of the programmable switches (2), upon receipt of the chain establishment packet and based on the network identifier information about the selected network service functions (1) contained in the chain establishment packet, performs installation of packet forwarding rules for the flow together with network address and port translation operations, and selects, on behalf of the respective attached or connected network service function (1), socket parameters to be used by the network service function (1) for processing the flow.

2. The method according to claim 1, wherein the chain establishment packet is generated either by the source node (4) or by an on-path proxy (6).

3. The method according to claim 1 or 2, wherein the chain establishment packet is configured to contain a list that includes network service function identifiers of the selected network service functions and an address of the destination node as a last entry of the list.

4. The method according to any of claims 1 to 3, wherein the chain establishment packet is configured to use indirection functions that map a network service function address to an address of the respective programmable switch (2) to which the network service function (1) is attached or connected.

5. The method according to any of claims 1 to 4, wherein the chain establishment packet is configured to include an additional identification element of the respective programmable switches (2).

6. The method according to any of claims 1 to 5, comprising:

receiving, by a programmable switch (2), a chain establishment packet,

reading from the chain establishment packet a network identifier of the next network service function (1) in the chain of selected network service functions (1), and

steering the flow towards the next network service function (1) by installing appropriate packet forwarding rules for the flow.

7. The method according to any of claims 1 to 6, comprising:

by a network service function (1) that, when processing network packets of a flow, modifies the network packets' headers, executing a network identifier selection delegation operation that is configured to delegate to the programmable switch (2) to which the network service function (1) is attached or connected a task of defining a delegation network address or port number the network service function (1) will use when sending network packets in response to the reception of network packets of the flow.

8. The method according to claim 7, further comprising:

by a programmable switch (2), generating either a delegation source address or port number or a delegation destination address or port number and, for the purpose of enabling usage, passing the generated address or port number to the respective network service function (1).

9. The method according to claim 7 or 8, comprising:

pre-configuring a programmable switch (2) with a pool of reserved addresses or port numbers the respective network service function (1) does not assign in any other case, and

by the programmable switch (2), selecting a delegation network address or port number from the pool of reserved addresses or port numbers.

10. A network switch, comprising:

network interfaces configured to receive and transmit packets of a network flow,

network service function interfaces configured to communicate with one or more attached or connected network service functions (3), and

a processing circuitry in communication with the network interfaces and the network service function interfaces, the service chain processing circuitry configured to:

read, from a chain establishment packet that is received via a network interface, network identifier information about network service functions (1) of a chain of network service functions (1) selected for the network flow, and

perform, based on the network identifier information about the selected network service functions (1) contained in the chain establishment packet, installation of packet forwarding rules for the flow together with network address and port translation operations.

11. The network switch according to claim 10, wherein the service chain processing circuitry is configured to:

select, on behalf of a respective attached or connected network service function (1), socket parameters to be used by the network service function (1) for processing a network flow.

12. The network switch according to claim 10 or 11, wherein the service chain processing circuitry is configured to:

read from a chain establishment packet a network identifier of a next network service function (1) in a chain of selected network service functions (1), and

steer the flow towards the next network service function (1) by installing appropriate packet forwarding rules for the flow.

13. The network switch according to any of claims 10 to 12, wherein the service chain processing circuitry is configured to:

determine that a network service function (1), when processing network packets of a flow, modifies the network packets' headers,

execute a network identifier selection delegation operation with the network service function (1), and

generate either a delegation source address or port number or a delegation destination address or port number and pass the generated delegation address or port number to the respective network service function (1).

14. The network switch according to claim 13, wherein the service chain processing circuitry is configured to:

use the generated delegation address or port number for identifying and/or reclassifying packets received from a network service function (1) as belonging to a particular network flow.

15. A network addressable apparatus hosting a network service function, the apparatus comprising:

a hardware component (8) on which the network service function (1) is executed,

an operating system (7) configured to manage the hardware component (8) and a pool (10) of port numbers, and

a network function program (9) running on the operating system (7) that is configured to provide the network function's (1) operations, wherein the network function program (9) is configured

to query the operating system (7) to provide a socket for a new network flow, and

to receive and employ a socket for the new network flow that is provided with a port number selected by a delegated switch (2) to which the network service function (1) is attached are connected, instead of using a port number selected autonomously by the operating system (7).

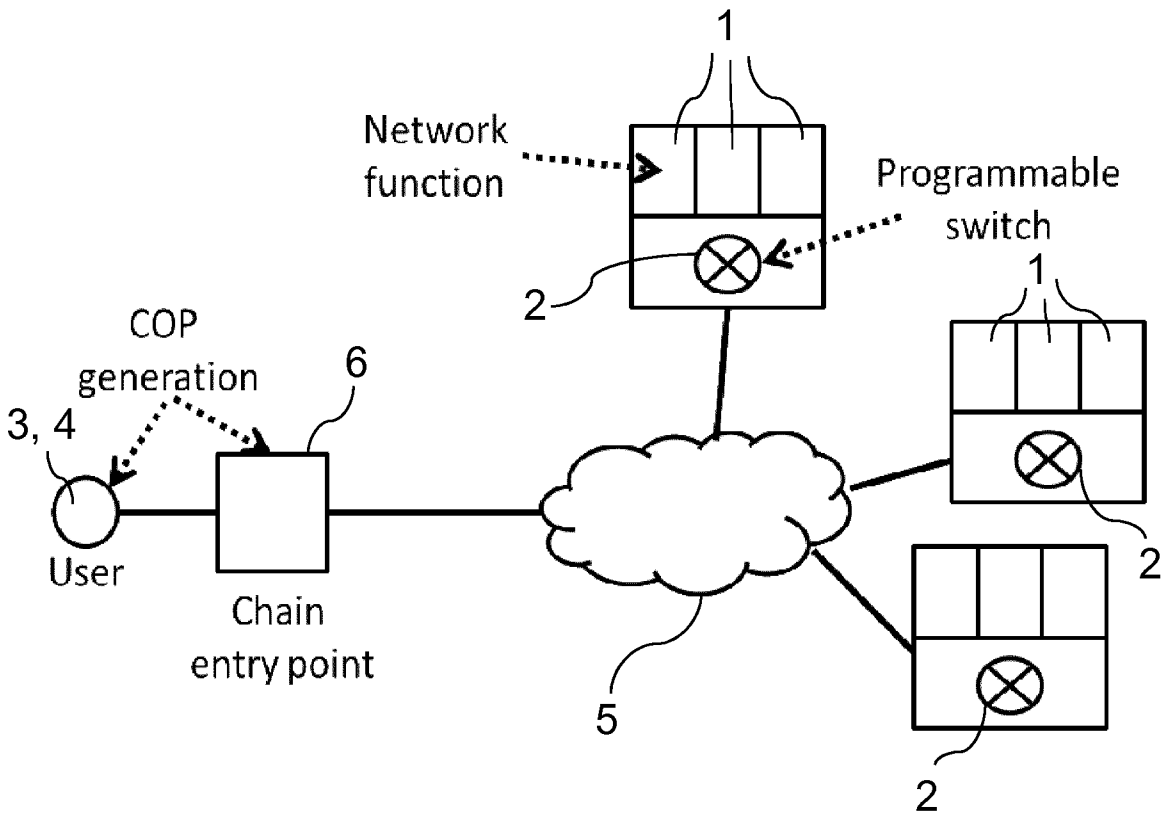
1
Network function
Programmable switch
1
2
COP generation
6
3, 4
User
Chain entry point
5
2
2

Fig. 1

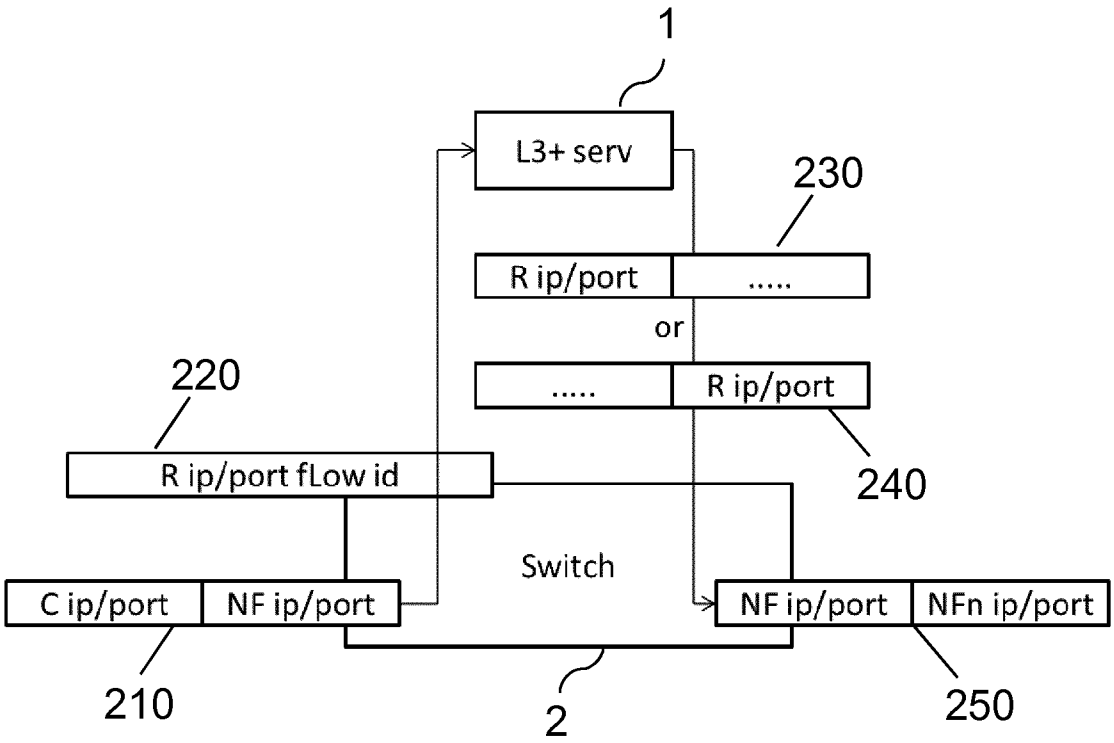
1
L3+ serv
230
R ip/port
.....
or
.....
R ip/port
220
R ip/port fLow id
240
Switch
C ip/port
NF ip/port
NF ip/port
NFn ip/port
210
2
250

Fig. 2

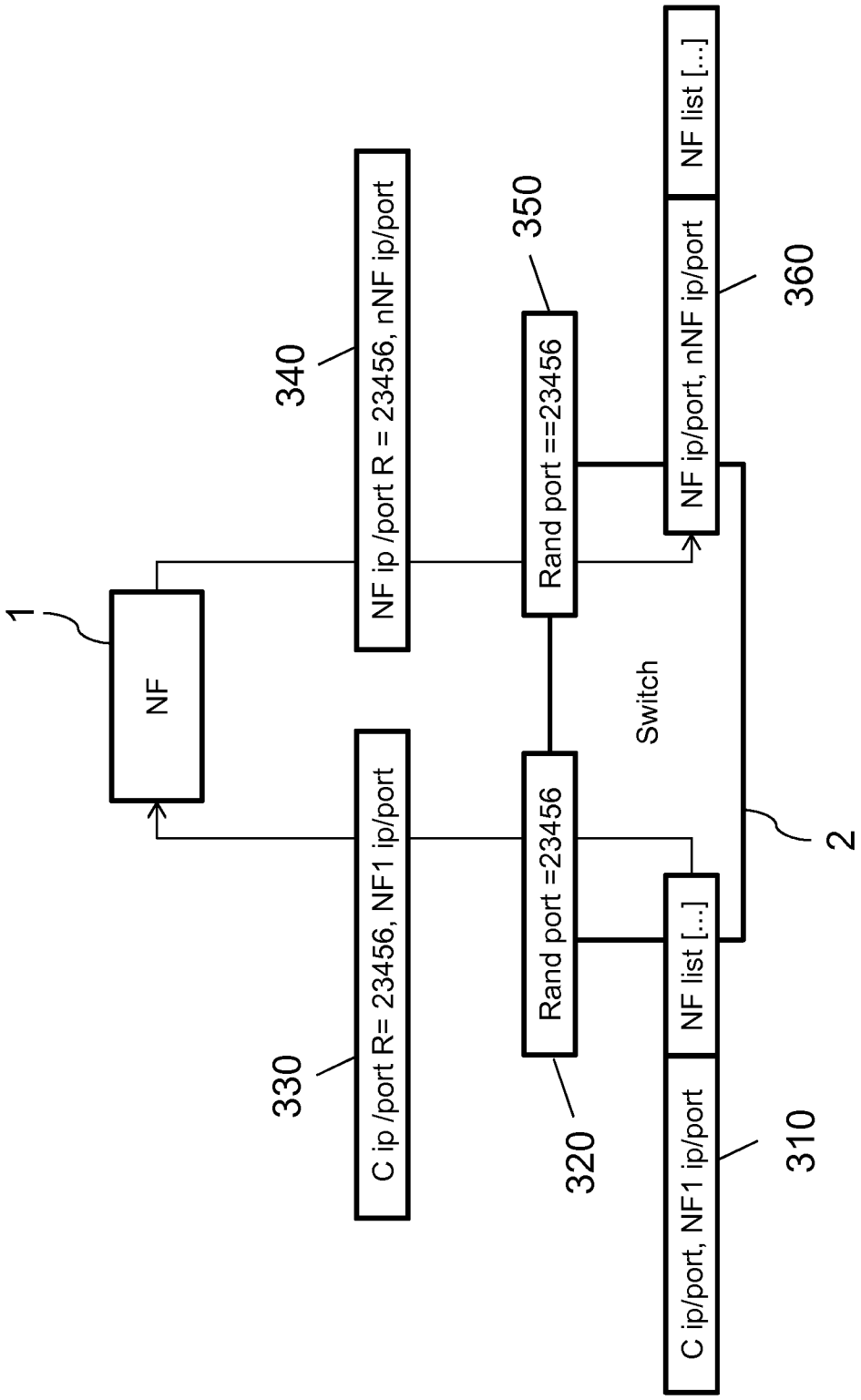
1
NF
340
NF ip /port R = 23456, nNF ip/port
330
C ip /port R= 23456, NF1 ip/port
350
Rand port ==23456
Rand port =23456
320
Switch
360
NF ip/port, nNF ip/port
NF list [...]
NF list [...]
C ip/port, NF1 ip/port
310
2

Fig. 3

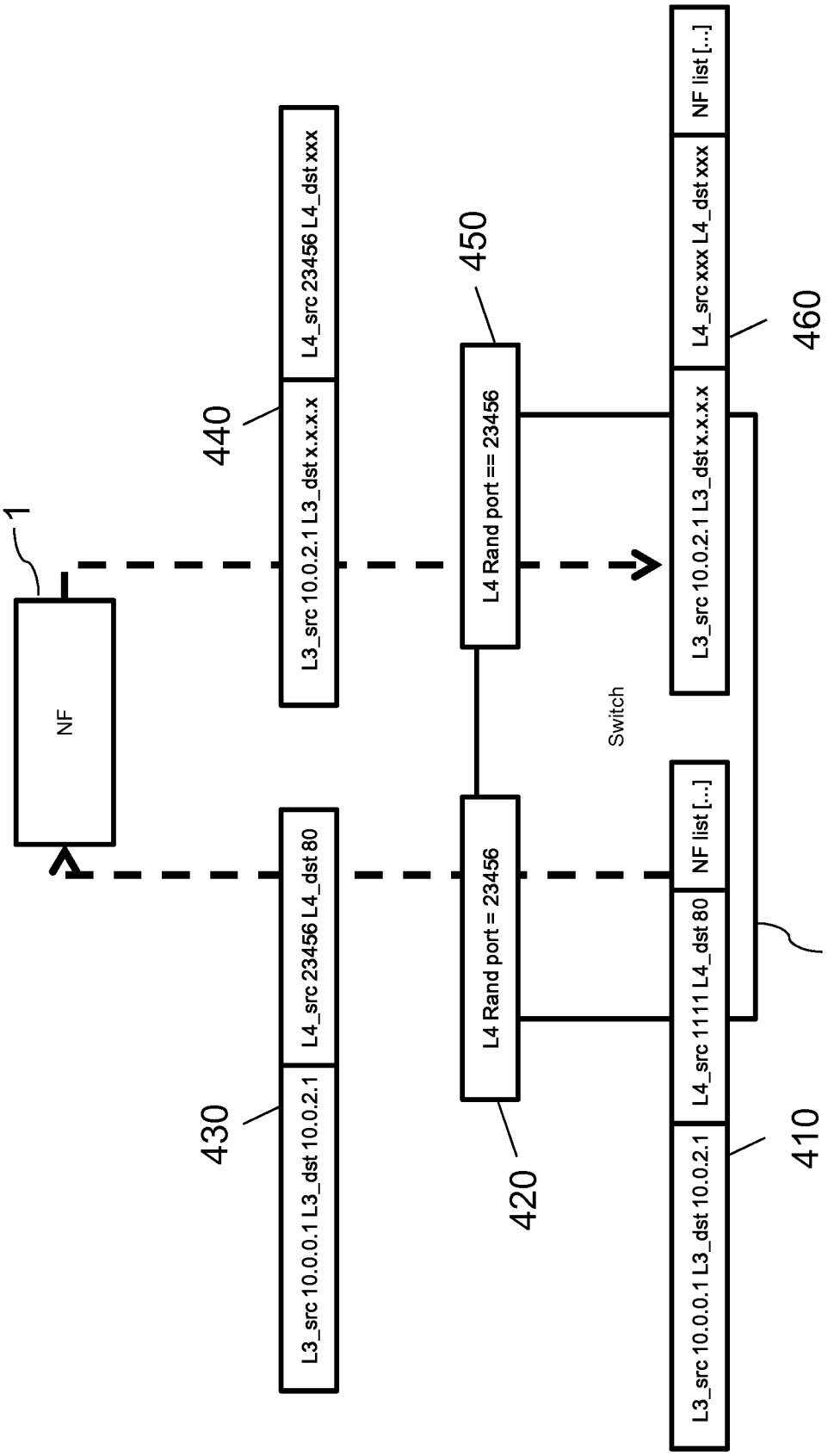
1
NF
440
L3_src 10.0.2.1 L3_dst x.x.x.x
L4_src 23456 L4_dst xxx
450
L4 Rand port == 23456
460
L3_src 10.0.2.1 L3_dst x.x.x.x
L4_src xxx L4_dst xxx
NF list [...]
Switch
430
L3_src 10.0.0.1 L3_dst 10.0.2.1
L4_src 23456 L4_dst 80
420
L4 Rand port = 23456
410
L3_src 10.0.0.1 L3_dst 10.0.2.1
L4_src 1111 L4_dst 80
NF list [...]
2

Fig. 4

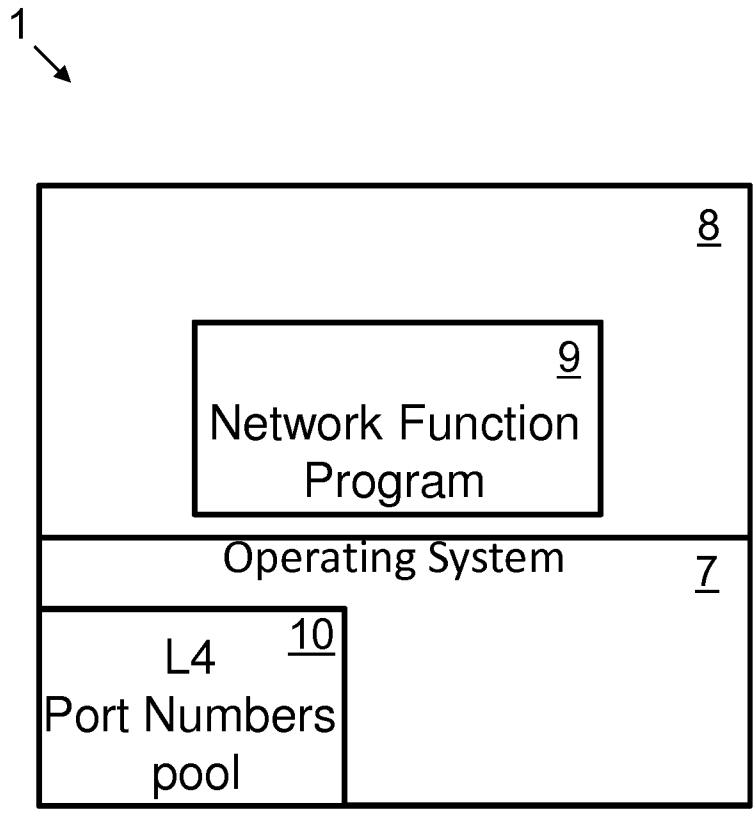
1
8
9
Network Function Program
Operating System
7
10
L4 Port Numbers pool

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/051479

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/721
ADD. H04L12/24 H04L12/725

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/326473 A1 (DUNBAR LINDA [US] ET AL) 12 November 2015 (2015-11-12)	1-14
A	figures 4-6, 9 paragraph [0025] - paragraph [0029] paragraph [0033] - paragraph [0034] paragraph [0038] paragraph [0041] - paragraph [0043] paragraph [0051] -----	15
X	US 6 912 590 B1 (LUNDBAECK ARNE [SE] ET AL) 28 June 2005 (2005-06-28)	15
A	figures 7, 8, 9A, 9B, 10 column 3, line 15 - line 18 column 5, line 15 - line 32 column 10, paragraph 62 - paragraph 67 column 11, line 1 - line 22 column 12, line 54 - line 58 -----	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
7 September 2017	14/09/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Badoi, Cornelia

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/051479

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015326473 A1	12-11-2015	NONE	
US 6912590 B1	28-06-2005	NONE	