



(51) International Patent Classification:

H04L 12/24 (2006.01) *H04L 29/06* (2006.01)
G06F 9/50 (2006.01)

(21) International Application Number:

PCT/US2017/023199

(22) International Filing Date:

20 March 2017 (20.03.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicants: **NOKIA TECHNOLOGIES OY** [FI/FI];
Karaportti 3, 02610 Espoo (FI). **ALCATEL-LUCENT
USA INC.** [US/US]; 600-700 Mountain Avenue, Murray
Hill, New Jersey 07974 (US).

(72) Inventors: **KAHN, Colin**; 69 Forest Way, Morris Plains,
New Jersey 07950 (US). **NIEMELA, Tuomas**; Vatu-
niemenkatu 14 A4, 00210 Helsinki (FI).

(74) Agent: **SINCELL, Mark W.**; Davidson Sheehan LLP,
8834 North Capital of Texas Hwy., Suite 100, Austin, Texas
78759 (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, 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.

(54) Title: DISTRIBUTED NETWORK POLICY DECISION MAKING

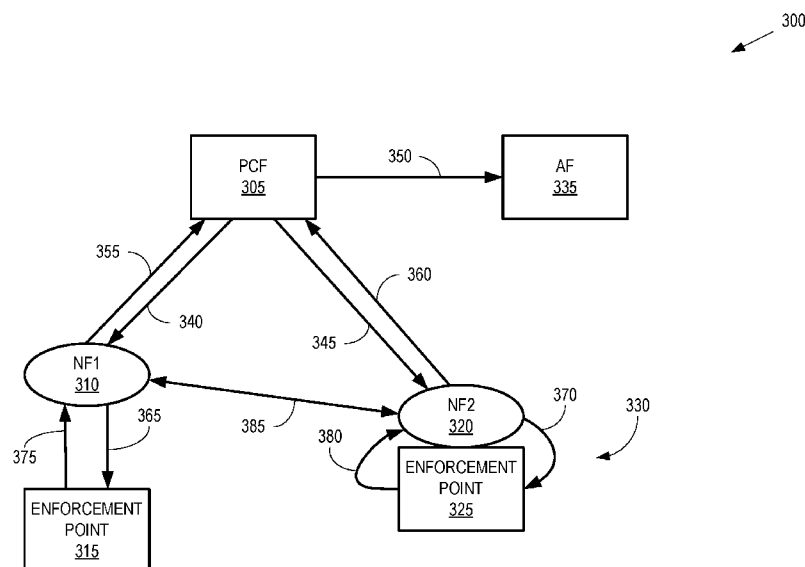


FIG. 3

(57) Abstract: A first network function in a communication system receives a policy that defines a rule to be enforced for users of the communication system in response to a set of conditions being satisfied. The first network function evaluates a first subset of the set of conditions and provides, in response to the first subset of the set of conditions being satisfied, information to configure a second network function to evaluate a partial policy decision that indicates that the rule is to be enforced in response to a second subset of the set of conditions being satisfied. The second network function evaluates the second subset of the set of conditions and provides information to configure an enforcement point to enforce the rule in response to the second subset of the set of conditions being satisfied.



(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).

Published:

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

DISTRIBUTED NETWORK POLICY DECISION MAKING

BACKGROUND

[0001] Operators of modern communication systems, including wired and wireless networks, control how services are provided to users by establishing service policies that are enforced by the network.

5 For example, operators of wireless communication systems typically enforce a policy of providing wireless connectivity to users that have a valid subscription or a positive balance on a prepaid plan. For another example, operators can enforce a policy of providing wireless connectivity at a quality-of-service (QoS) level to users that have signed up for the QoS level. For yet another example, a policy can be used to control charging a user for wireless connectivity according to a charging plan selected
10 by the user. The policy also requires that the wireless communication system deny wireless connectivity to users that do not possess a valid subscription or to users that have a negative or zero balance on their prepaid plan. Similarly, the policy ensures that QoS and charging are applied consistently with the user's subscription. Policies can also be applied to control other activities in the network.

15 [0002] Conventional 4G networks include a policy and charging rules function (PCRF) that determines policy rules in the network. The PCRF can aggregate information (such as event triggers) received from other entities in the network and then make policy decisions based on the received information. Operators typically provide policies to the PCRF in the form of a set of conditions in logical expressions that are evaluated based on the information available at the PCRF. For example,
20 a policy can be represented as:

IF (condition1 AND condition2) then Rule1

The PCRF evaluates "condition1 AND condition2" based on the available information, typically in response to receiving an event trigger that indicates a change in information used to evaluate one of the conditions. If the expression evaluates to "true," the PCRF propagates Rule1 to an enforcement
25 function such as a policy charging and enforcement function (PCEF). The PCEF then has responsibility for enforcing Rule1, e.g., denying wireless connectivity to users that do not possess a valid subscription or a positive balance on a prepaid plan.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The present disclosure may be better understood, and its numerous features and advantages
30 made apparent to those skilled in the art by referencing the accompanying drawings. The use of the same reference symbols in different drawings indicates similar or identical items.

[0004] FIG. 1 is a block diagram of a communication system according to some embodiments.

[0005] FIG. 2 is a block diagram illustrating a path for provisioning partial policy decisions in a hierarchy of network functions according to some embodiments.

[0006] FIG. 3 is a block diagram of a communication system that illustrates message flows used for distributed policy decision-making according to some embodiments.

[0007] FIG. 4 is a flow diagram of a method of performing distributed policy decision-making according to some embodiments.

5 [0008] FIG. 5 is a block diagram of a network function virtualization (NFV) architecture according to some embodiments.

DETAILED DESCRIPTION

[0009] Centralized policy decision-making, e.g., in a PCRF, is an effective way for operators to define conditions under which a small set of rules are triggered. For example, quality-of-service (QoS) rules and charging rules can be defined and evaluated in the PCRF. However, centralized policy decision-making is not efficient because it requires propagating all event triggers and all information that can be used to evaluate the conditions specified in policies to a single point in the network. The rules generated by the PCRF based on the policies and conditions must then be propagated back out to the PCEF entities distributed throughout the network. Moreover, centralized policy decision-making is not scalable to networks that use large numbers of policies to govern rules such as mobility rules, reliability rules, quality-of-service (QoS) rules, charging rules, session service continuity rules, rules governing selection of network slices in a network function virtualization (NFV) network, access selection rules, traffic steering rules, high availability rules, tracing rules, local breakout rules, data network access rules, connection/session termination rules, and the like. The problem of scalability is exacerbated by the large numbers of inputs used to evaluate the conditions. Furthermore, the high latency required to transmit network information and event triggers to the PCRF and then propagate the rules back to the PCEF slows down the PCRF's responses to changes in network conditions.

[0010] The advantages of centralized policy decision-making are combined with the efficiency, scalability, and low latencies of a distributed network that includes a hierarchy of network functions by selectively evaluating different subsets of conditions for each policy at different network functions. Rules specified by the policies are propagated to an enforcement function based on successful evaluation of the different subsets of conditions at the different network functions. Some embodiments of the hierarchy of network functions include a policy control function and one or more lower-level network functions such as an access management function and a session management function. In distributed policy decision making, a policy to enforce a rule based on a set of conditions is provisioned to the policy control function. A plurality of subsets of the set of conditions are associated with a corresponding plurality of the network functions. For example, a first subset of the set of conditions can be associated with the policy control function and a second subset of the set of conditions can be associated with a lower-level network function. The policy control function selectively provides a partial policy decision to the lower-level network function based on an evaluation of the first subset of the set of conditions. For example, if the first subset evaluates to "true," the policy control function provides (or provides information enabling) a partial policy decision that configures the

lower-level network function to evaluate the second subset. The lower-level network function selectively provides the rule to an enforcement function based on an evaluation of the second subset of the set of conditions. For example, the lower-level network function provides the rule to the enforcement function if the second subset evaluates to "true."

5 [0011] Distributing the decision-making to network functions at different levels in the hierarchy allows network functions to independently evaluate policies based on event triggers received at the network function (which are referred to herein as local event triggers) without having to inform or consult with higher-level network functions. For example, local event triggers associated with first and second subsets of a set of conditions can be provided to the corresponding network functions. If the higher-
10 level network function has provided (or enabled) a partial policy decision to the lower-level network function in response to the first subset of the set of conditions having a "true" evaluation, the lower-level network function can evaluate the partial policy decision based on local event triggers without communicating with the higher-level network function. In some embodiments, the network functions are able to subscribe to receive event triggers from other network functions. In some embodiments,
15 the partial policies are provisioned on the policy control function and lower-level network functions prior to the partial policies being activated by a higher-level network function. The higher-level network function can then send a trigger to the lower-level network function to activate or deactivate evaluation of the conditions that have been pre-provisioned in the lower-level network function.

[0012] FIG. 1 is a block diagram of a communication system 100 according to some embodiments.
20 The communication system 100 provides wireless connectivity to one or more user equipment 105 over an air interface 110 with a base station 115 implemented in a radio access network (RAN) 120 that implements a radio access technology and provides interconnection between the user equipment 105 and a core network. As used herein, the term "base station" can be used to refer to eNodeBs, gNodeBs, macrocells, base station routers, access points, microcells picocells, femtocells, and the
25 like. The user equipment 105 can include devices that are owned or operated by users, such as cell phones, smart phones, tablet computers, laptop computers desktop computers, and the like, as well as autonomous devices that are not necessarily owned or operated by a user. For example, the user equipment 105 can also include physical devices such appliances, vehicles, buildings, and other items that are embedded with electronics, software, sensors, actuators, and network connectivity that enable
30 the devices to collect and exchange data over the Internet. The physical devices can be referred to as the Internet-of-Things (IoT). Furthermore, some embodiments of the communication system 100 are able to provide wired connectivity to the user equipment 105.

[0013] From a policy perspective the communication system 100 is implemented using a hierarchy of network functions. The network functions include a policy control function (PCF) 125 that is configured
35 on the basis of policies that are provisioned by operators or other sources. In the illustrated embodiment, the PCF 125 is the highest-level network function in the hierarchy. The network functions also include lower-level network functions such as an access management function (AMF) 130 that is configured to manage access of devices such as the user equipment 105 to the communication system 100, a session management function (SMF) 135 that manages sessions

established between the communication system 100 and the user equipment 105, and a user plane function (UPF) 140 that manages routing of packets in the communication system 100 and enforces policy-based rules, as discussed herein. Some embodiments of the communication system 100 also implement other network functions, which are generally indicated by the network function (NF) 145.

5 Furthermore, some embodiments of the communication system 100 include additional levels of network functions in the hierarchy.

[0014] Operation of the communication system 100 is governed, at least in part, by policies provisioned by operators of the communication system 100. As used herein, the term “policy” refers to rules that are enforced dependent upon results of evaluating a set of conditions on the basis of input
10 information. A first example of a policy can be represented as:

IF (condition1 AND condition2) then Rule1

The first example policy specifies that Rule1 is propagated to an enforcement point (such as UPF 140) if condition1 evaluates to “true” on the basis of the input information used to determine the value of condition1 and condition2 evaluates to “true” on the basis of the input information used to determine
15 the value of condition2. A second example of a policy can be represented as:

IF (subscriber==Gold AND location==Acme_Enterprise) then set Max_DL_Rate=50Mbps,

The second example policy specifies that an enforcement point (such as UPF 140) is instructed to permit a maximum downlink data rate of 50 megabits per second (Mbps) to a session with the user equipment 105 if the corresponding subscriber has a GOLD subscription and the user equipment is
20 located on the premises of the Acme Enterprise.

[0015] The hierarchy of network functions is configured to perform distributed policy decision-making by configuring the different network functions to evaluate different subsets of conditions specified by various policies. Operators provision policies to the highest-level network function in the communication system, which in the illustrated embodiment is the PCF 125. Each of the network
25 functions 125, 130, 135, 145 are configured to evaluate subsets of the conditions of the policies. Thus, the provisioned policies include information indicating the network functions that are to evaluate the subsets of the conditions in the policies. For example, the first example policy can include information indicating that condition1 is to be evaluated at the PCF 125 and condition2 is to be evaluated at the SMF 135. For another example, the second example policy can include information
30 indicating that the “subscriber” condition is to be evaluated at the PCF 125 and the “location” condition is to be evaluated at the AMF 130.

[0016] Higher-level network functions evaluate a first subset of the conditions in a policy and then selectively provide partial policy decisions to lower-level network functions based upon the evaluation of the subset. Partial policy decisions include a second subset of the conditions (mutually exclusive to
35 the first subset) that are to be evaluated at the lower-level network function to determine whether to enforce a rule indicated by the original policy. For example, the PCF 125 can evaluate condition1 in

the first example policy. The PCF 125 does not take any action as long as condition1 evaluates to "false." However, when condition1 evaluates to "true," the PCF 125 provides a partial policy decision including condition2 to the SMF 135. The partial policy decision can be represented as:

IF (condition2) then Rule1

5 The SMF 135 selectively provides Rule1 to the UPF 140 based on evaluations of condition2. For example, Rule1 is not provided to the UPF 140 as long as condition2 evaluates to "false." The SMF 135 only provides Rule1 to the UPF 140 for enforcement in response to condition2 evaluating to "true." If condition1 subsequently changes from "true" to "false," the PCF 125 can remove or deactivate the partial policy decision previously promulgated to the SMF 135. The SMF 135 can then remove or
10 disable Rule1 from UPF 140 if Rule1 was previously installed as a result of condition2 evaluating to "true."

[0017] In some embodiments, the policies and corresponding partial policy decisions are pre-provisioned to the relevant network functions. For example, the first example policy with condition1 can be pre-provisioned to the PCF 125 and the corresponding partial policy decision with condition2
15 can be pre-provisioned to the SMF 135 prior to evaluation of condition1 by the PCF 125. The PCF 125 subsequently evaluates condition1 and, if condition1 evaluates to "true," the PCF 125 provides information such as a trigger or token that enables evaluation of the pre-provisioned partial policy decision by the SMF 135.

[0018] Conditions are evaluated at the network functions on the basis of information received by the
20 network functions and in response to corresponding event triggers received by the network functions. Some embodiments of the PCF 125 receive information or event triggers related to network analytics, application functions, user data management, user data records, subscriber profile records, online/off-line charging systems, and the like. Some embodiments of the AMF 130 receive information or event triggers related to mobility events. Some embodiments of the SMF 135 receive information or event
25 triggers related to user plane events. Some embodiments of the RAN 120 receive information or event triggers related to RAN congestion. Some embodiments of the other network functions 145 receive information or event triggers related to proprietary functions.

[0019] The subsets of conditions that are evaluated in the partial policy decisions provided to different network functions can therefore be matched to the information or event triggers that are available at
30 the corresponding network functions, thereby reducing latency and network traffic that would have been needed to convey this information to a central decision-making point. For example, information and event triggers associated with subscriber profile records are available at the PCF 125 and information and event triggers associated with a location of the user equipment 105 are available at the SMF 135. The PCF 125 is therefore configured to evaluate conditions related to subscriber profile
35 event triggers, such as the "subscriber" condition in the second example policy, and the SMF 135 is configured to evaluate conditions related to user plane event triggers, such as the "location" condition

in the second example policy. The partial policy decision implemented in the SMF 135 can be represented as:

IF (location==Acme_Enterprise) then set Max_DL_Rate=50Mbps,

Once the PCF 125 has determined that the subscriber has a Gold subscription and enabled the SMF 135 to evaluate the partial policy decision, the SMF 135 is able to independently determine the maximum downlink rate dependent upon the location of the user equipment 105 without needing any further communication with the PCF 125.

[0020] FIG. 2 is a block diagram illustrating a path 200 for provisioning partial policy decisions in a hierarchy of network functions according to some embodiments. The path 200 is implemented in some embodiments of the communication system shown in FIG 1. The path 200 includes a PCF 205, a first network function 210, and a second network function 215. Some embodiments of the path 200 also include additional network functions (not shown in FIG 2) at different levels in the hierarchy of network functions.

[0021] Policies are provisioned to the PCF 205 and the policies can be operator supplied or provisioned. Some embodiments of the PCF 205 are able to automatically or dynamically modify policies based on higher-level inputs, which can include semi-static inputs such as changes in subscriber data. The PCF 205 can also modify policies based on instructions received from a network function virtualization (NFV) Management and Orchestration function, such as the one illustrated in FIG. 5. The PCF 205 evaluates a first subset of the conditions defined or specified by the policy and then selectively provides partial policy decisions (or information enabling pre-provisioned partial policy decisions) to the first (lower-level) network function 210 based on the evaluation of the first subset. Some embodiments of the PCF 205 cache the results of the evaluation of the first subset.

[0022] The partial policy decisions provided to the network function 210 include a second subset of the conditions in the policy. In response to receiving the partial policy decisions (or enabling information), the first network function 210 can evaluate one or more conditions indicated in the partial policy decision. If the conditions evaluate to "true," the first network function 210 provides information identifying a rule to be enforced by the network function 215. Alternatively, if there are additional network functions in the hierarchy that are configured to evaluate other subsets of the conditions in the policies, the first network function 210 can provide additional partial policy decisions (or information enabling additional pre-provisioned partial policy decisions) to the next network function in the hierarchy. Some embodiments of the network function 210 cache the results of the evaluation of the second subset.

[0023] The first network function 210 evaluates the second subset of the conditions defined by the policies in response to receiving local event triggers. Examples of local event triggers that can be evaluated by a first network function 210 such as the SMF 130 shown in FIG. 1 are provided in the following table that is derived from Table 6.2 from 3GPP Technical Specification (TS) 23.203, which is incorporated herein by reference in its entirety:

Events trigger	Description
PLMN change	The UE has moved to another operator's domain.
QoS change	The QoS of the flow has changed
Mobility Anchor Change	The UPF acting as a mobility anchor has changed
Resource modification request	A request for resource modification has been received by the SMF
Routing information change	The IP flow mobility routing information has changed (IFOM/NB-IFOM)
Loss/recovery of transmission resources	The transmission resources are no longer usable/again usable
Location change (serving cell)	The serving cell of the UE has changed
Location change (serving area)	The serving area of the UE has changed
Location change (serving CN node)	The serving core network node of the UE has changed
Change of UE presence in Presence Reporting Area	The UE is entering/leaving a Presence Reporting Area
Out of credit	Credit is no longer available
UE IP address change	A UE IP address has been allocated/released
Access Network Charging Correlation Information	Access Network Charging Correlation Information has been assigned
Usage Threshold	Session or the Monitoring-key specific resources consumed by a UE reached the threshold
Start of application traffic detection and Stop of application traffic detection	The start or the stop of application traffic has been detected
Access Network Information report	Access information as specified in the Access Network Information Recording part of a PCC rule
Credit management session failure	Transit/permanent failure as specified by the OCS
Addition/removal of an access to a PDU session	An access is added or removed

Change of usability of an access	An access becomes unusable or usable again
----------------------------------	--

[0024] The network functions 205, 210 that evaluate subsets of conditions specified by a policy or a partial policy decision can reevaluate the corresponding subset in response to receiving new information or subsequent event triggers. The network functions 205, 210 can compare the new evaluations of the subsets to the cached results to determine whether the evaluation of the condition has changed. If so, the network functions 205, 210 can provide updated information to the downstream network functions. For example, if the first subset of conditions initially evaluated to “true” and a subsequent evaluation of the first subset evaluated to “false,” the network function 205 can disable the partial policy decision including the second subset at the network function 210. For another example, if the second subset of conditions initially evaluated to “true” and a subsequent evaluation of the second subset evaluated to “false,” the network function 210 can disable enforcement of the corresponding rule at the network function 215.

[0025] FIG. 3 is a block diagram of a communication system 300 that illustrates message flows used for distributed policy decision-making according to some embodiments. The communication system 300 includes a PCF 305, a first network function 310, a first enforcement point 315, a second network function 320, and a second enforcement point 325. In the illustrated embodiment, the second network function 320 and the second enforcement point 325 are integrated into a single entity 330. The communication system 300 is used to implement some embodiments of the communication system 100. For example, the PCF 305 corresponds to the PCF 125, the first network function 310 corresponds to the AMF 135, the first enforcement point 315 corresponds to the UPF 140, and the entity 330 corresponds to the SMF 130 shown in FIG. 1. The communication system 300 also includes an application function 335 that provides application services to users of the communication system 300.

[0026] Policy decisions are typically made less frequently than the occurrence of event triggers and so the distributed policy decision-making scheme avoids sending event information to central policy decision locations such as the PCF 305. Policy decisions are made more frequently than policy changes (e.g., policy changes applied by operators) and many policy decisions are made in response to local event triggers detected by the network functions 310, 320. Furthermore, events that occur at the network functions 310, 320 primarily affect local rules that are enforced by the corresponding enforcement points 315, 325. Distributed policy decision-making therefore devolves decision-making authority to the lowest possible level of the network function hierarchy.

[0027] In the illustrated embodiment, the PCF 305 makes policy decisions on the basis of subsets of the conditions in the corresponding policies, as discussed herein. In response to these decisions, the PCF 305 can provide (as indicated by arrows 340, 345) partial policy decisions to the network functions 310, 320. The policy decisions taken by the PCF 305 are expected to occur relatively infrequently. The PCF 305 can also provide (as indicated by the arrow 350) event notifications to the application function 335. The event notifications 350 are expected to occur relatively infrequently. The

network functions 310, 320 also provide event notifications to the PCF 305, as indicated by arrows 355, 360. The event notifications 355, 360 are expected to occur relatively infrequently.

[0028] The network functions 310, 320 selectively propagate rules to the corresponding enforcement points 315, 325, as indicated by the arrows 365, 370. The network functions 310, 320 are expected to make partial policy decisions relatively frequently, *e.g.*, more frequently than the PCF 305 makes policy decisions. The volume of messages transmitted between the network functions 310, 320 and the corresponding enforcement points 315, 325 is therefore expected to be significantly smaller than the volume of messages transmitted between the PCF 305 and the network functions 310, 320.

[0029] The enforcement points 315, 325 detect events and transmit event notifications to the corresponding network functions 310, 320, as indicated by the arrow 375, 380. The number of events detected by the enforcement points 315, 325 is expected to be larger than the number of events detected by the network functions 310, 320, which in turn is expected to be larger than the number of events detected by the PCF 305. The volume of messages transmitted from the enforcement points 315, 325 to the corresponding network functions 310, 320 is therefore expected to be larger than the volume of messages transmitted from the network functions 310, 320 to the PCF 305 and the volume of messages transmitted from the PCF 305 to the application function 335.

[0030] In a conventional communication system that implements centralized policy decision-making, all of the policy decisions would be made at the PCF 305. All of the event notifications would therefore have to be conveyed to the PCF 305 and all of the information configuring rules at the enforcement points 315, 325 would have to be generated at the PCF 305 and transmitted to the enforcement points 315, 325 via the network functions 310, 320. Distributed policy decision-making reduces or eliminates the need to transmit a large portion of these messages. Consequently, distributed policy decision-making reduces the number of messages flowing through the communication system 300 by orders of magnitude relative to centralized policy decision-making.

[0031] Some embodiments of the communication system 300 support a subscription/registration procedure that allows entities to subscribe to receive event notifications from each other. For example, the network function 310 can subscribe to receive event notifications from the network function 320, which then provides the event notifications to the network function 310, as indicated by the double-headed arrow 385. The subscription/registration procedure can facilitate more dynamic distributed decision-making in the communication system 300 and further reduces the volume of messages that are conveyed to the PCF 305 by allowing the network functions 310, 322 acquire relevant event notifications directly from each other.

[0032] FIG. 4 is a flow diagram of a method 400 of performing distributed policy decision-making according to some embodiments. The method 400 is implemented in some embodiments of the communication system 100 shown in FIG. 1, the PCF 205 and network functions 210, 215 shown in FIG. 2, and the communication system 300 shown in FIG. 3.

[0033] At block 405, a (first) high-level network function, such as a PCF, receives a policy that defines a rule to be selectively enforced dependent upon evaluation of a set of conditions. The policy also includes information indicating subsets of the set of conditions that are to be evaluated at different network functions. For example, the policy can include information indicating that a first subset is to be
5 evaluated at the first network function and a second subset is to be evaluated at a (second) lower-level network function, such as an AMF, SMF, or other function.

[0034] At block 410, the first network function receives an event trigger that triggers evaluation of the first subset of conditions. For example, if the high-level network function is a PCF, the event trigger can include information indicating a change in subscriber's subscription status.

10 [0035] At decision block 415, the first network function determines whether the first subset of conditions is satisfied in response to receiving the event trigger. The first subset of conditions can be evaluated based on information that is provided to the first network function. If the first subset of conditions is not satisfied, *e.g.*, if the first subset evaluates to "false," the method 400 flows to block 410 and awaits the next event trigger. If the first subset of conditions is satisfied, *e.g.*, if the first
15 subset evaluates to "true," the method 400 flows to block 420. If the first subset of conditions subsequently changes from evaluating to "true" to "false" based on a subsequent event trigger in block 410, then the first network function can provide information disabling the partial policy decision at the second network function. In some embodiments, the first subset can be an empty set, in which case the method 400 flows directly to block 420.

20 [0036] At block 420, the first network function enables a partial policy decision in a second network function. Some embodiments of the first network function enable the partial policy decision by providing the partial policy decision to the second network function. In other embodiments, partial policy decisions are pre-provisioned to the second network function, *e.g.*, on the basis of the information included in the policy that identifies the second network function as the network function
25 that should evaluate the partial policy decision. The first network function can then enable the partial policy decision in the second network function by providing a trigger or token that enables the partial policy decision. If information disabling the partial policy decision is received at block 420 from a higher network function, such as the first network function, the partial policy decision in the second network function is disabled.

30 [0037] At block 425, the second network function receives a local event trigger. For example, if the second network function is an AMF, the local event trigger can be a mobility event trigger. For another example, if the second network function is an SMF, the local event trigger can be a user plane event trigger.

[0038] At decision block 430, the second network function determines whether the second subset of
35 conditions are satisfied. The second subset of conditions can be evaluated based on locally available information such as mobility information that is locally available to an AMF and user plane information that is locally available to an SMF. If the second subset of conditions is not satisfied, *e.g.*, if the

second subset evaluates to "false," the method 400 flows to block 425 and awaits a subsequent local event trigger. If the second subset of conditions is satisfied, *e.g.*, if the second subset evaluates to "true," the method flows to block 435.

[0039] At block 435, the second network function provides the rule specified by the policy to an enforcement function, which is then responsible for enforcing the rule for users of the communication system.

[0040] FIG. 5 is a block diagram of an NFV architecture 500 according to some embodiments. The NFV architecture 500 is used to implement some embodiments of the communication system 100 shown in FIG. 1, the PCF 205 and network functions 210, 215 shown in FIG. 2, the communication system 300 shown in FIG. 3, and the method 400 shown in FIG. 4.

[0041] The NFV architecture 500 includes hardware resources 501 including computing hardware 502, storage hardware 503, and network hardware 504. A virtualization layer 505 provides an abstract representation of the hardware resources 501. The abstract representation supported by the virtualization layer 505 can be managed using a virtualized infrastructure manager 510, which is part of the NFV management and orchestration (M&O) module 515. Some embodiments of the manager 510 are configured to collect and forward performance measurements and events that may occur in the NFV architecture 500. For example, performance measurements and events can be forwarded to an orchestrator (ORCH) 517 implemented in the NFV M&O module 515. The hardware resources 501 and the virtualization layer 505 are used to implement virtual resources 520 including virtual computing 521, virtual storage 522, and virtual networking resources 523.

[0042] Virtual networking functions (VNF1, VNF2, VNF3) run over the NFV infrastructure (*e.g.*, the hardware resources 501) and utilize the virtual resources 520. For example the virtual networking functions (VNF1, VNF2, VNF3) may be implemented using virtual machines supported by the virtual computing resources 521, virtual memory supported by the virtual storage resources 522, or virtual networks supported by the virtual network resources 523. Element management systems (EMS1, EMS2, EMS3) are responsible for managing the corresponding virtual networking functions (VNF1, VNF2, VNF3). For example, the element management systems (EMS1, EMS2, EMS3) may be responsible for fault and performance management. In some embodiments, each of the virtual networking functions (VNF1, VNF2, VNF3) is controlled by a corresponding VNF manager 525 that exchanges information and coordinates actions with the manager 510 or the orchestrator 517.

[0043] The NFV architecture 500 includes an operation support system (OSS)/business support system (BSS) 530. The OSS/BSS 530 deals with network management including fault management using the OSS functionality. The OSS/BSS 530 also deals with customer and product management using the BSS functionality. Some embodiments of the NFV architecture 500 use a set of descriptors 535 for storing descriptions of services, virtual network functions, or infrastructure supported by the NFV architecture 500. Information in the descriptors 535 may be updated or modified by the NFV M&O 515.

[0044] The NFV architecture 500 is configurable to support one or more network slices 540, which are logical instantiations of independent networks. Each of the network slices 540 can be configured to support different network functions such as the network functions 125, 130, 135, 140, 145 shown in FIG. 1, the network functions 205, 210, 215 shown in FIG. 2, and the network functions 305, 310, 315, 320, 325, 330, 335 shown in FIG. 3. One or more of the network slices 540 can therefore be configured to implement some embodiments of the method 400 shown in FIG. 4.

[0045] Some embodiments of distributed policy decision-making discussed herein are used to modify conventional wireless communication systems, such as the communication systems disclosed in 3GPP Technical Specification (TS) 23.501, which is incorporated herein by reference in its entirety, 3GPP TS 23.203, which is incorporated herein by reference in its entirety, and 3GPP Technical Report (TR) 23.799, which is incorporated herein by reference in its entirety.

[0046] The policy framework for policy decisions and enforcement consists of a PCF with interfaces to the SMF (N7), AMF (N15) and through the AMF to the UE via N1. Policy decisions may be triggered by event reporting from AMPEF, PCEFs, NEF AF, OCS and other sources such as Network Data Analytics and the UDR.

[0047] In this architecture, the PCF may provide the following policies to the UE:

- Non-Seamless Off-load Policy
- SSC Mode Selection Policy (SSCMSP)
- DNN Selection Policy
- Access Network Selection Policy
- Network Slice Selection Policy (NSSP)

These policies are evaluated in the UE, taking into consideration attributes that are locally available such as application requirements, available accesses, UE location, time of day, access link quality and subscriber preference. A policy decision is made in the UE by assessing these attributes against one or more conditions according to operator preferences as reflected in the policies. When appropriate conditions are met, a rule is triggered that results in an action by the UE that may include selection of a new slice, selection of a different access, routing of traffic to a different access, establishment of a new PDU session, and selection of an SSC mode for a PDU session. Due to the overhead and timelines of sending event triggers over the air, it is without question that these policies must be evaluated locally and a decision made in the UE rather than in a centrally located policy function that gathers event triggers, formulates a policy decision and promulgates the decision to the UE.

[0048] In the EPC, the scope of dynamic policy control has been primarily for QoS, Charging and Traffic Steering. However, TS23.501 and TR23.799 section 8, mention 5G policies that cover additional areas including:

- Access and Mobility Management related policies pertinent to the AMF
- RAT Frequency Selection Priority (RFRP)
- Network slice change policy (based on NSSAI reception)
- AMF / CCNF change policy
- 5 • SMF Selection Policy
- UE Mobility Restriction Policy
- Network Policies to determine mobility patterns
- Network Policy for MO only mode and UE reachability
- UPF selection policies

10 It is also stipulated in TS23.501 that “the policy control framework does not preclude potential extensions in phase 2 for policy control in multiple administrative areas.” This may entail further expansion of policy to include domains outside of the 3PPP network, and support of additional areas of policy control such as ultra-reliability, security and multi-connectivity.

[0049] The increased scope of policy calls into question the approach used in the EPC for dynamic
15 policies, where event triggers are sent to a centralized network function (the PCRF) that makes decisions and promulgates policy rules to enforcement points. When the information necessary to make a policy decision is available locally in a network function, this signalling to the PCRF is in many cases unnecessary since the network function itself could evaluate the policy were it available to it.

[0050] A more scalable solution calls for extending the model used with the UE whereby some policy
20 decisions may be delegated to allow other core network functions, besides the PCF to evaluate policies, formulate decisions and trigger rules when local events dictate, while keeping the PCF as the coordinator of Policy. This eliminates much of the event notification and policy signalling to and from the PCF.

[0051] The methodology to extend the policy control architecture to support this is shown in the figure
25 below. A hierarchical structure is proposed. The PCF may evaluate policies and make decisions using information available to it, for example from a Network Data Analytics platform (NWDA), the UDM and AFs requesting service. The PCF also controls the evaluation of decisions delegated to the SMF and AMF. When indicted by the PCF, the SMF may evaluate local policies for QoS and charging triggered by user plane events and SM signalling. Similarly, the AMF when activated by the PCF may
30 autonomously evaluate aspects of Access and Mobility policies using its local information, and trigger enforcement of resulting rules within the AMF.

[0052] To support this more efficient structure the following requirements are proposed:

- The PCF shall be able to delegate policy decisions to other network functions.
 - The PCF shall be able to authorize policy evaluation in the AMF and SMF. This allows the PCF to control the policy decisions made by a NF and coordinate policy decision making between NFs.
 - The PCF shall be able to send policies to the AMF and SMF. This allows the PCF to deliver policies to the NF when only local events and information is needed for evaluation.
 - The AMF and SMF shall be able to evaluate delegated policies as triggered or authorised by the PCF based on local events and information locally available and autonomously trigger a rule that is enforced locally in the AMF, the SMF, or in a UPF associated with an SMF.
- This is intended to allow the PCF to use a “token” to trigger a provisioned policy on the AMF and SMF, and the sending of delegated policy conditions from the PCF to the SMF and AMF
- The PCF shall be able to query a NF to determine the current state of policies (e.g.: that a rule has been triggered and is in force at the PCEF).
- Network functions evaluating delegated policy shall support event notification to subscribing functions. Note the PCF and the NEF are functions that will likely need to subscribe to some event notifications.

[0053] The policy framework shall provide the relevant parts of the PCC framework as specified in TS 23.203 and TS 23.501, including:

- a. Policy Control Function (PCF) shall support interfaces to the Policy and Charging Enforcement Function (PCEF), Network Exposure Function (NEF), the Application Function (AF), and the Online Charging System (OCS).
- b. The PCF shall be able to evaluate operator policies that are triggered by events received from the PCEF, NEF, the AF, and the OCS.
- c. The PCF shall provide Rules for application and service data flow detection, gating, QoS and flow based charging to the PCEF.
- d. The Policy Framework shall be able to manage the Packet Filter Descriptions (PFDs) in the PCEF by the 3rd party AS via the NEF and PFDF.
- e. The Policy Framework shall support to negotiate the background data transfer policy with the 3rd party AS via the NEF.

f. The PCF shall implement a Front End to access subscription information relevant for policy decisions in a User Data Repository (UDR) including dynamic profile updates pushed by the UDR.

g. Traffic Steering Control for steering traffic for the services on the DN side of the N6 reference point,

h. The PCF shall be able to take input from Network Data Analytics (NWDA) into consideration for policies on assignment of network resources and for traffic steering policies.

Note: The existing PCC framework is applicable to PDU sessions of IP Type only.

Note: How the PCC framework applies to PDU sessions other than IP Type is FFS. Also, where IP-CAN is used, may need to update per 5G terminology.

[0054] Additionally, the policy framework shall provide following functionality for the access and mobility enforcement:

a. Policy Control Function (PCF) shall support the interface to the Access and Mobility Policy Enforcement Function (AMPEF).

b. The PCF shall be able to provide Access and Mobility Management related policies to the AMPEF.

c. The PCF shall be able to evaluate operator policies that are triggered by events received from the AMPEF.

Note: How to enforce the access and mobility policy when interfacing with PCF is FFS.

Note: The list above covers the high level requirements that are addressed in the document so far. Additional requirements are to be added when the related information is agreed. Mapping of PCEF and AMPEF into 5G CN entities are FFS.

[0055] The policy control framework shall support the following requirements to extend policy decisions to network functions, while keeping the PCF as the coordinator of Policy. This eliminates unnecessary event notification and signalling to and from the PCF. The role of the functions impacted in phase 1 are shown in the figure A.1-1

a. The PCF shall be able to delegate policy decisions to other network functions.

a. The PCF shall be able to authorize policy evaluation in the AMF and SMF. This allows the PCF to control the policy decisions made by a NF and coordinate policy decision making between NFs.

- b. The PCF shall be able to send policies to the AMF and SMF. This allows the PCF to deliver policies to the NF when only local events and information is needed for evaluation.
- c. The AMF and SMF shall be able to evaluate delegated policies as triggered or authorised by the PCF based on local events and information locally available and autonomously trigger a rule that is enforced locally in the AMF, the SMF, or in a UPF associated with an SMF.
- b. The PCF shall be able to query a NF to determine the current state of policies (e.g., that a rule has been triggered and is in force at the PCEF).
- c. Network functions evaluating delegated policy shall support event notification to subscribing functions. Note the PCF and the NEF are functions that will likely need to subscribe to some event notifications.

[0056] In some embodiments, certain aspects of the techniques described above may be implemented by one or more processors of a processing system executing software. The software comprises one or more sets of executable instructions stored or otherwise tangibly embodied on a non-transitory computer readable storage medium. The software can include the instructions and certain data that, when executed by the one or more processors, manipulate the one or more processors to perform one or more aspects of the techniques described above. The non-transitory computer readable storage medium can include, for example, a magnetic or optical disk storage device, solid state storage devices such as Flash memory, a cache, random access memory (RAM) or other non-volatile memory device or devices, and the like. The executable instructions stored on the non-transitory computer readable storage medium may be in source code, assembly language code, object code, or other instruction format that is interpreted or otherwise executable by one or more processors.

[0057] A computer readable storage medium may include any storage medium, or combination of storage media, accessible by a computer system during use to provide instructions and/or data to the computer system. Such storage media can include, but is not limited to, optical media (e.g., compact disc (CD), digital versatile disc (DVD), Blu-Ray disc), magnetic media (e.g., floppy disc, magnetic tape, or magnetic hard drive), volatile memory (e.g., random access memory (RAM) or cache), non-volatile memory (e.g., read-only memory (ROM) or Flash memory), or microelectromechanical systems (MEMS)-based storage media. The computer readable storage medium may be embedded in the computing system (e.g., system RAM or ROM), fixedly attached to the computing system (e.g., a magnetic hard drive), removably attached to the computing system (e.g., an optical disc or Universal Serial Bus (USB)-based Flash memory), or coupled to the computer system via a wired or wireless network (e.g., network accessible storage (NAS)).

[0058] Note that not all of the activities or elements described above in the general description are required, that a portion of a specific activity or device may not be required, and that one or more

further activities may be performed, or elements included, in addition to those described. Still further, the order in which activities are listed are not necessarily the order in which they are performed. Also, the concepts have been described with reference to specific embodiments. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the present disclosure as set forth in the claims below. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of the present disclosure.

[0059] Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits, advantages, solutions to problems, and any feature(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential feature of any or all the claims. Moreover, the particular embodiments disclosed above are illustrative only, as the disclosed subject matter may be modified and practiced in different but equivalent manners apparent to those skilled in the art having the benefit of the teachings herein. No limitations are intended to the details of construction or design herein shown, other than as described in the claims below. It is therefore evident that the particular embodiments disclosed above may be altered or modified and all such variations are considered within the scope of the disclosed subject matter. Accordingly, the protection sought herein is as set forth in the claims below.

WHAT IS CLAIMED IS:

1. A method comprising:
 - receiving, at a first network function in a communication system, a policy that defines a rule to be enforced for users of the communication system in response to a set of conditions being satisfied;
 - 5 evaluating, at the first network function, a first subset of the set of conditions; and
 - providing, from the first network function and in response to the first subset of the set of conditions being satisfied, information to configure a second network function to evaluate a partial policy decision that indicates that the rule is to be enforced in response to a second subset of the set of conditions being satisfied.
- 10 2. The method of claim 1, wherein the rule to be enforced comprises at least one of a mobility rule, a reliability rule, a quality-of-service (QoS) rule, a charging rule, a session service continuity rule, a rule governing selection of network slices in a network function virtualization (NFV) network, an access selection rule, a traffic steering rule, a high availability rule, a tracing rule, a local breakout rule, a data network access rule, or a connection/session termination rule.
- 15 3. The method of claim 1, wherein providing the information to configure the second network function comprises providing information defining the partial policy decision and the second subset of the set of conditions.
4. The method of claim 1, wherein information defining the partial policy decision and the second subset of the set of conditions is pre-provisioned to the second network function, and wherein
- 20 providing information to configure the second network function comprises providing a token that enables evaluation of the pre-provisioned partial policy decision.
5. The method of claim 1, further comprising:
 - providing, from the first network function and in response to the first subset of the set of
 - conditions not being satisfied, information to disable evaluation of the partial policy
 - 25 decision at the second network function.
6. The method of claim 1, further comprising:
 - receiving a first event trigger at the first network function, and
 - wherein evaluating the first subset comprises evaluating the first subset in response to
 - receiving the first event trigger at the first network function.
- 30 7. The method of claim 6, wherein providing the information to configure the second network function comprises providing information to configure the second network function to evaluate the partial policy decision in response to the second network function receiving a second event trigger.

8. The method of claim 7, further comprising:

receiving a third event trigger at the first network function,
evaluating the first subset in response to receiving the third event trigger; and
reconfiguring the second network function to not evaluate the partial policy decision in
5 response to the second subset of the set of conditions not being satisfied.

9. The method of claim 1, further comprising:

subscribing, at the first network function, to receive event triggers from at least one of the
second network function or a third network function.

10. The method of claim 1, wherein the first subset is an empty set.

10 11. A method comprising:

receiving, at a first network function in a communication system, information enabling a partial
policy decision that defines a rule to be enforced for users of the communication
system in response to a first subset of a set of conditions being satisfied, wherein the
information is received from a second network function in response to a second
15 subset of the set of conditions being satisfied;

evaluating, at the first network function, the first subset of the set of conditions; and
providing, from the first network function, information to configure an enforcement point to
enforce the rule in response to the first subset of the set of conditions being satisfied.

12. The method of claim 11, wherein the rule to be enforced comprises at least one of a mobility rule,
20 a reliability rule, a quality-of-service (QoS) rule, a charging rule, a session service continuity rule, a rule
governing selection of network slices in a network function virtualization (NFV) network, an access
selection rule, an access selection rule a traffic steering rule, a high availability rule, a tracing rule, a
local breakout rule, a data network access rule, or a connection/session termination rule.

13. The method of claim 11, wherein receiving the information enabling the partial policy decision
25 comprises receiving information defining the partial policy decision and the first subset of the set of
conditions.

14. The method of claim 11, further comprising:

receiving information defining the partial policy decision and the first subset prior to receiving
the information enabling the partial policy decision, and

30 wherein receiving the information enabling the partial policy decision comprises receiving a
token that enables evaluation of the partial policy decision.

15. The method of claim 11, further comprising:

receiving, at the first network function, information to disable evaluation of the partial policy
decision at the second network function, wherein the information is received from the

second network function in response to the second subset of the set of conditions not being satisfied.

16. The method of claim 11, wherein evaluating the first subset comprises evaluating the first subset in response to receiving the first event trigger at the first network function.

5 17. The method of claim 16, wherein receiving the information enabling evaluation of the partial policy decision comprises receiving the information enabling evaluation of the partial policy decision in response to the second network function receiving a second event trigger and determining that the second subset of the set of conditions is satisfied.

18. The method of claim 17, further comprising:

10 receiving information disabling evaluation of the partial policy decision in response to the second network function receiving a third event trigger and determining that second subset of the set of conditions is not satisfied.

19. The method of claim 11, further comprising:

15 subscribing, at the first network function, to receive event triggers from at least one of the second network function or a third network function.

20. The method of claim 11, wherein the second subset is an empty set.

21. A method, comprising:

20 selectively configuring a first network function to evaluate a first subset of a set of conditions defined by a policy provisioned to a second network function dependent upon a second subset of the set of conditions being satisfied; and
selectively enforcing a rule defined by the policy dependent on the first subset of the set of conditions being satisfied.

22. The method of claim 21, wherein selectively configuring the first network function to evaluate the first subset comprises configuring the first network function to evaluate the first subset in response to
25 the second network function determining that the second subset is satisfied.

23. The method of claim 22, wherein selectively enforcing the rule comprises enforcing the rule in response to the first network function determining that the first subset is satisfied.

24. The method of claim 23, wherein the first network function is configured to evaluate the first subset in response to receiving a first event trigger, and wherein the second network function is
30 configured to evaluate the second subset in response to receiving a second event trigger.

25. An apparatus comprising:

network hardware configured to receive a policy that defines a rule to be enforced for users of the communication system in response to a set of conditions being satisfied; and

computing hardware configured to implement a first network function for evaluating a first subset of the set of conditions, wherein the network hardware is configured to provide, in response to the first subset of the set of conditions being satisfied, information to configure a second network function to evaluate a partial policy decision that indicates that the rule is to be enforced in response to a second subset of the set of conditions being satisfied.

26. The apparatus of claim 25, further comprising:

storage hardware, wherein the network hardware, computing hardware, and storage hardware are configured to implement a network slice including virtual network resources configured to receive the policy and provide the information to configure the second network function, and virtual computing resources configured to evaluate the first subset of the set of conditions.

27. An apparatus comprising:

network resources configured to receive information enabling a partial policy decision that defines a rule to be enforced for users of the communication system in response to a first subset of a set of conditions being satisfied, wherein the information is received from a second network function in response to a second subset of the set of conditions being satisfied; and

computing resources configured to implement a first network function for evaluating the first subset of the set of conditions, wherein the network resources are configured to provide information to configure an enforcement point to enforce the rule in response to the first subset of the set of conditions being satisfied.

28. The apparatus of claim 27, further comprising:

storage hardware, wherein the network hardware, computing hardware, and storage hardware are configured to implement a network slice including virtual network resources configured to receive the information enabling the partial policy decision and provide the information to configure the enforcement point to enforce the rule, and virtual computing resources configured to evaluate the first subset of the set of conditions.

1/5

100

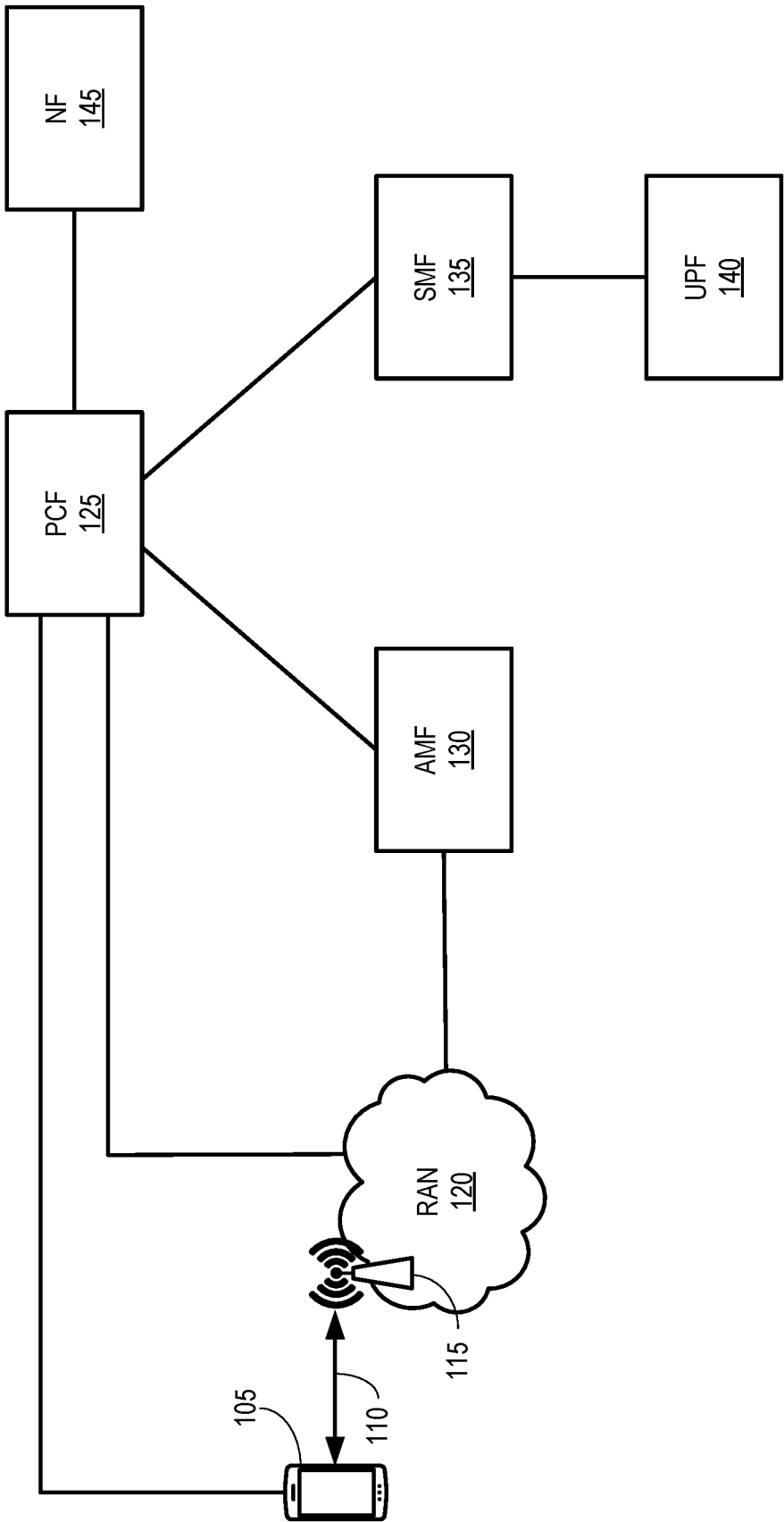
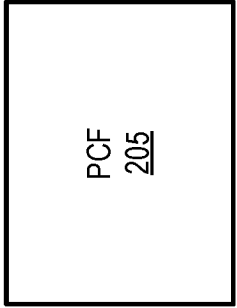
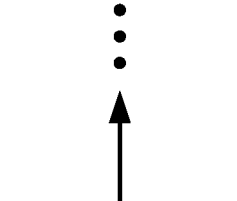
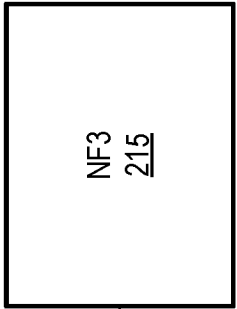


FIG. 1

200

2/5



...

FIG. 2

300

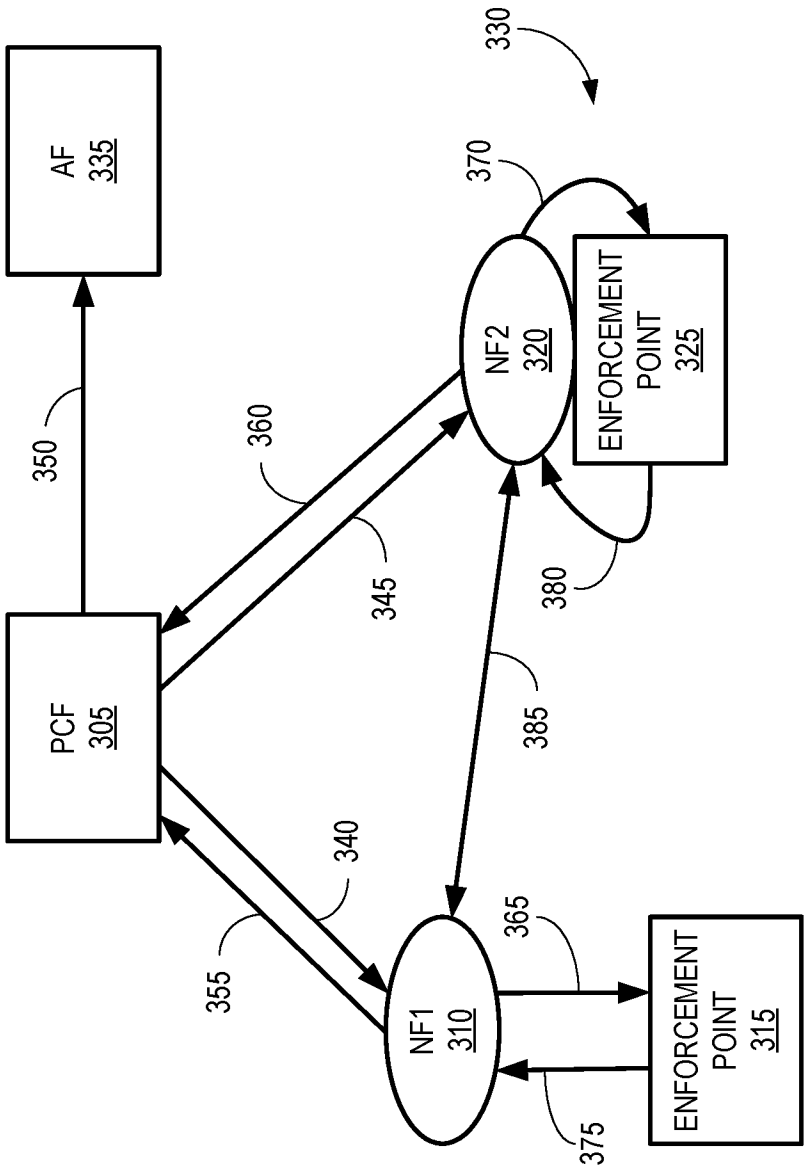
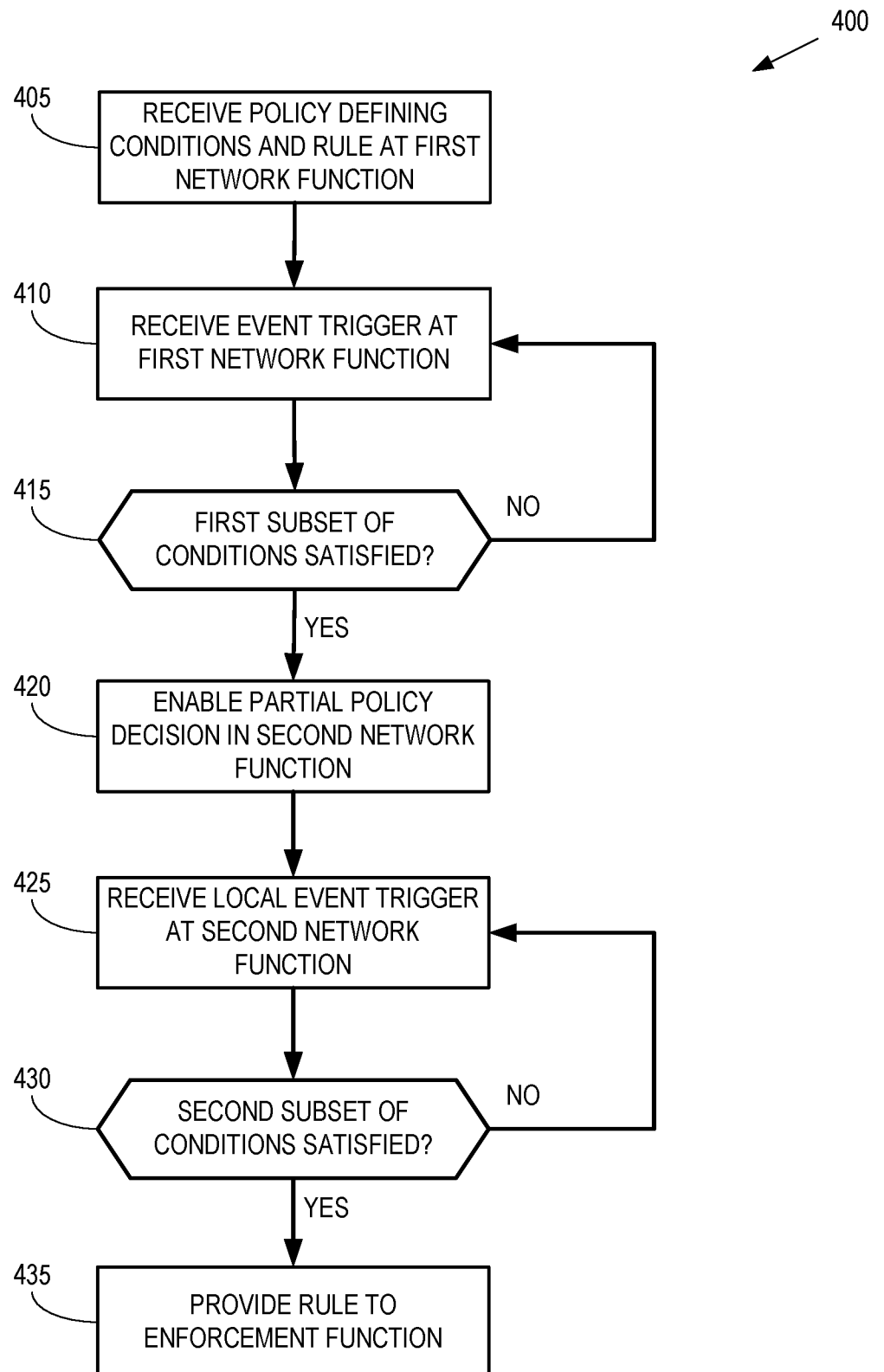


FIG. 3

4/5

**FIG. 4**

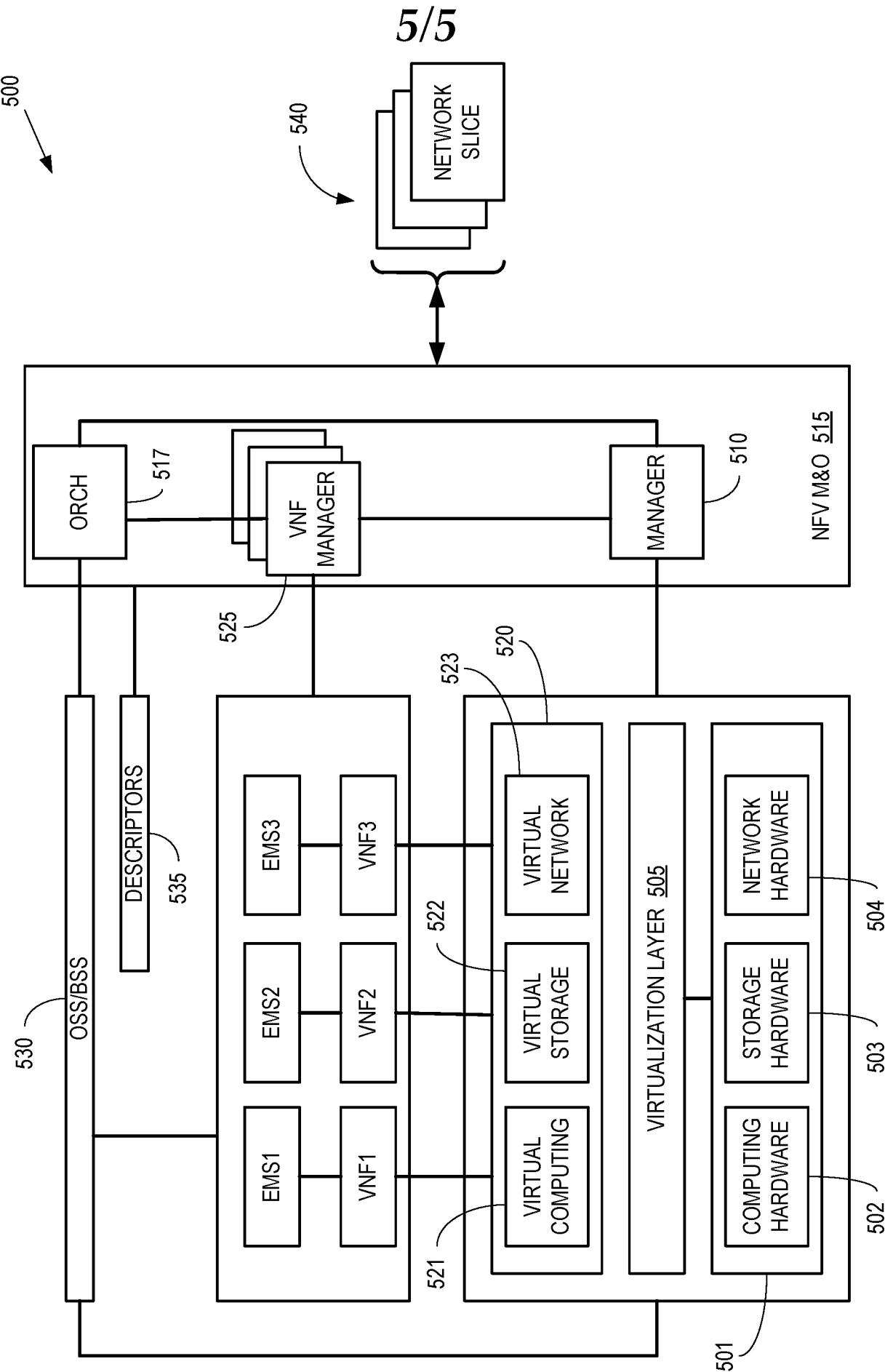


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/023199

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/24 G06F9/50 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

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 9 237 155 B1 (CAVAGE MARK [US] ET AL) 12 January 2016 (2016-01-12) column 1 - column 15 column 17 - column 20; claims 1-17; figures 1-9	1-28
X	US 2014/130119 A1 (GOLDSCHLAG DAVID [US] ET AL) 8 May 2014 (2014-05-08) paragraph [0013] - paragraph [0020] paragraph [0040] - paragraph [0063] paragraph [0067] - paragraph [0115] paragraph [0125] - paragraph [0156] paragraph [0185] paragraph [0203] - paragraph [0257]; claims 1-17; figures 1-13	1-3,5-9, 11-13, 15-19, 21-25,27



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

18 September 2017

Date of mailing of the international search report

25/09/2017

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Camba, Sonia

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2017/023199

Patent document cited in search report	Publication date	Patent family member(s)	Publication date	
US 9237155	B1	12-01-2016	US 9237155 B1	12-01-2016
			US 2016127265 A1	05-05-2016

US 2014130119	A1	08-05-2014	US 2014130119 A1	08-05-2014
			US 2017026413 A1	26-01-2017
