



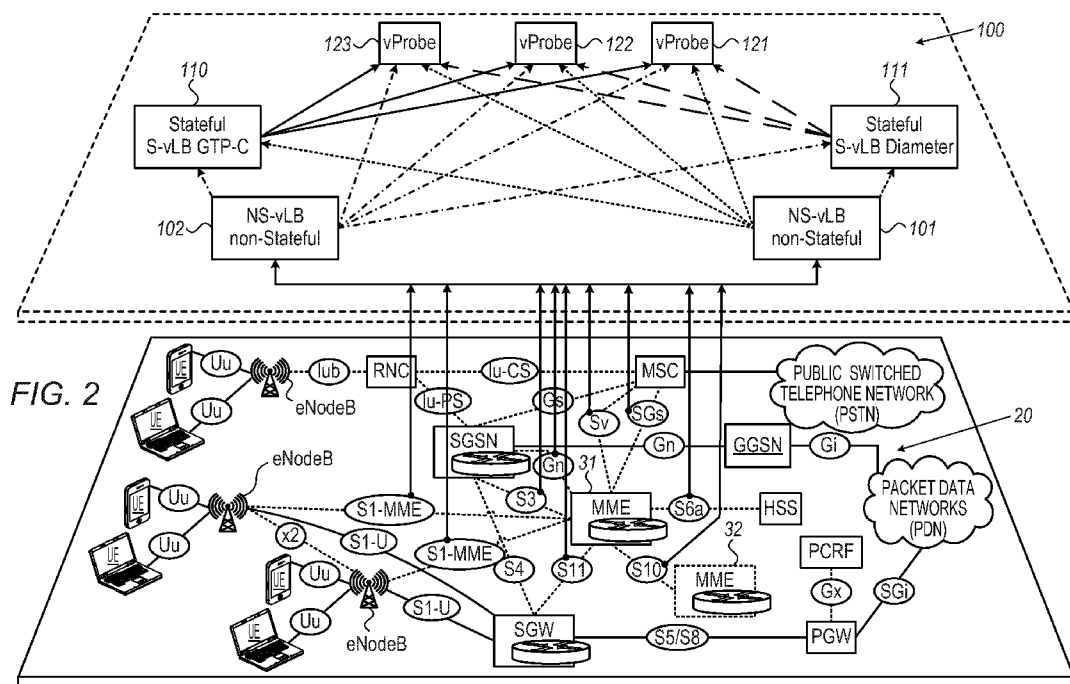
- (51) International Patent Classification:
H04L 12/70 (2013.01)
- (21) International Application Number:
PCT/IB2016/054332
- (22) International Filing Date:
21 July 2016 (21.07.2016)
- (25) Filing Language:
English
- (26) Publication Language:
English
- (30) Priority Data:
62/334,170 10 May 2016 (10.05.2016) US
- (71) Applicant: **RADCOM LTD.** [IL/IL]; Raoul Wallenberg
24, 6971920 Tel Aviv (IL).
- (72) Inventors: **HARARI, Eyal David**; Hapardes Street 35,
5552584 Kiryat Ono (IL). **ILAN, Tomer Tuvia**; He Beiyar
Street 56, 4805656 Rosh Haayin (IL).
- (74) Agent: **A.C. ENTIS-IP-LTD.** et al.; 6 Raoul Wallenberg
Street, 69719 Tel Aviv (IL).
- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,
HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA,
LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN,
MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE,
PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE,
SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:
— with international search report (Art. 21(3))

(54) Title: LOAD BALANCING SYSTEM



(57) Abstract: A load balancing system that operates to categorize communication packets as to whether they are contextual or not and determines a decision relevant to data in a first contextual packet with respect to a predetermined task based on data comprised in a second contextual packet.

WO 2017/195005 A1

LOAD BALANCING SYSTEM

FIELD

[0001] Embodiments of the invention relate to load balancing tasks comprised in monitoring a communication network.

BACKGROUND

[0002] Modern communication networks support large, varied, and growing populations of users and an ever increasing gamut of user services and user applications for users who access the networks using any of various stationary and/or mobile user equipment (UE). The networks span not only global populations and geography, but a plethora of methods, devices, infrastructures, and protocols for propagating data, voice, and video content provided by a host of different large and small service providers.

[0003] As the various software and hardware resources that support the networks, configure paths along which network packets propagate in the networks, and provide services mediated by the networks have become more sophisticated, the resources have become fungible and logically abstracted away from their particular physical structures. The physical devices and apparatus underlying modern communication networks have become commodity resources that are configurable by software to provide virtualizations of network functions, referred to as “Network Functions Virtualization” (NFV), and “Software Defined Networks” (SDNs). And dedicated physical devices that provide particular network functionalities have been or are being replaced by software entities that access the physical commodities of a network, and/or other software entities of the network, on an “as need” basis to communicate with each other and provide functionalities required by the networks. The zoology of software entities are conventionally referred to as virtual entities, with a particular virtual entity typically distinguished by a name of a functionality it provides.

[0004] The extensive, complex infrastructure of many modern communication networks typically comprise a mix of dedicated physical devices and an ever increasing, if not dominant number, of virtual network entities engaged in an incessant packet exchange chatter approaching hundreds of gigabits per second (Gbps). Monitoring and troubleshooting the networks as much as possible in real time to maintain performance that provides acceptable quality of service

(QoS) and user quality of experience (QoE) for the multitude of services that the networks provide has become a demanding challenge.

SUMMARY

[0005] An aspect of an embodiment of the disclosure relates to providing an optionally virtualized load balancing system that is relatively easily scalable and configured to efficiently distribute data propagating in a packet switched communication network to probes that operate to process the data and provide the network with information relevant to understanding, monetizing, and/or controlling, optionally, network performance. In an embodiment, the virtualized load balancing system, which may be referred to as a “Smart-vLB system” or simply a “Smart-vLB”, comprises a hierarchical architecture comprising at least one “non-stateful” virtual load balancer (NS-vLB) and at least one stateful virtual load balancer (S-vLB). The at least one NS-vLB and at least one S-vLB cooperate to distribute data in packets that the Smart-vLB receives from the network for processing, to a plurality of probes, optionally comprising virtual probes (vProbes). In an embodiment, the communication network comprises an evolved packet system (EPS) network, which as discussed below may also be referred to as an LTE (long term evolution) network.

[0006] The at least one NS-vLB in the Smart-vLB receives packets that may be mirrored from at least one port in the network and distinguishes between packets, optionally referred to as “contextual packets”, that it receives, and packets, optionally referred to as “non-contextual packets”, which it receives. A contextual packet is a packet comprising data that may not be processed for a given desired purpose without reference to data from another, associated contextual packet and may advantageously be processed by a same virtual probe that processes data from the associated contextual packet. For example, a contextual packet may comprise data that may not be directly associated with a session or transaction to which it belongs but may be associated with another, associated, packet to determine a session or transaction to which the contextual packet belongs. Packets may be deemed associated by sharing a common attribute, such as by way of example, sharing a same network protocol or application, and/or belonging to a same network session or transaction. A non-contextual packet, is a packet comprising data that may be processed for a given desired purpose without reference to data from another packet and may for the given desired purpose be processed by a probe that is different from a probe that

processes other packets for the same desired purpose. A non-contextual packet may by way of example be a packet that may be directly associated with a session or transaction to which it belongs without reference to data in another packet.

[0007] In an embodiment, each of the at least one NS-vLB is configured to transmit non-contextual packets that it receives for processing to a given physical or virtual probe of optionally a plurality of physical or virtual probes without reference to information in another packet. The NS-vLB is configured to transmit associated contextual packets characterized by a same shared attribute to a same S-vLB. The S-vLB transmits contextual packets for processing to a vProbe having an identity which the S-vLB determines based on information from at least one of a plurality of other packets that it receives. The S-vLB transmits a contextual packet that it receives for processing to a vProbe having an identity which the S-vLB determines based on information from at least one other packet that the S-v-LB receives.

[0008] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter

BRIEF DESCRIPTION OF FIGURES

[0010] Non-limiting examples of embodiments of the invention are described below with reference to figures attached hereto that are listed following this paragraph. Identical features that appear in more than one figure are generally labeled with a same label in all the figures in which they appear. A label labeling an icon representing a given feature of an embodiment of the invention in a figure may be used to reference the given feature. Dimensions of features shown in the figures are chosen for convenience and clarity of presentation and are not necessarily shown to scale.

[0011] Fig. 1 schematically shows a long term evolution, LTE, communications network;

[0012] Fig. 2 schematically shows a Smart-vLB comprising NS-vLBs and S-vLBs operating to load balance processing of data comprised in control packets transmitted by network entities of the LTE shown in Fig. 1, in accordance with an embodiment of the disclosure;

[0013] Fig. 3 shows a flow diagram of a procedure by which the NS-vLBs comprised in the Smart-vLB shown in Fig. 2 distribute packets that the Smart-vLB receives from the LTE network, in accordance with an embodiment of the invention;

- [0014] Figs. 4A and 4B show a flow diagram of a procedure by which one of the S-vLBs comprised in the Smart-vLB shown in Fig. 2 distribute packets that it receives from a NS-vLB in the Smart-vLB, in accordance with an embodiment of the invention; and
- [0015] Figs. 5A-5C show a flow diagram of a procedure by which another of the S-vLBs comprised in the Smart-vLB shown in Fig. 2 distribute packets that it receives from a NS-vLB in the Smart-vLB, in accordance with an embodiment of the invention;
- [0016] Fig. 6 schematically shows a Smart-vLB comprising NS-vLBs and S-vLBs operating to load balance processing of data comprised in control packets propagated to and from a Serving Gateway (SGW), and/or a Packet Data Network Gateway (PGW) of the LTE shown in Fig. 1, in accordance with an embodiment of the disclosure; and
- [0017] Figs. 7A and 7B show flow diagrams of procedures by which and NS-vLB and an S-vLB comprised in the Smart-vLB shown in Fig. 6 operate to distribute packets, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION

- [0018] In the following detailed description, a Smart-vLB that is configured in accordance with an embodiment of the disclosure to load balance processing of control data transmitted in packets by entities comprised in an LTE communications network is described with reference to Figs. 1-7B. Features and functioning of the LTE network are discussed with reference to Fig. 1. Fig. 2 schematically shows the Smart-vLB operating to load balance processing of data in control packets transmitted to and/or from an MME comprised in the LTE network shown in Fig. 1. Whereas the Smart-vLB in Fig. 2 is shown by way of example comprising two NS-vLBs and two S-vLBs, practice of an embodiment of the disclosure is not limited to Smart-vLBs comprising two each of NS-vLBs and S-vLBs. A Smart-vLB in accordance with an embodiment of the disclosure may comprise more or less than two NS-vLBs and more or less than two S-vLBs. Procedures by which component NS-vLBs and S-vLBs in the Smart-vLB process packets that the Smart-vLB receives from the LTE network are discussed with reference to the flow diagrams shown in Figs. 3A-5C and 7A-7B.
- [0019] In the discussion, unless otherwise stated, adjectives such as “substantially” and “about” modifying a condition or relationship characteristic of a feature or features of an embodiment of the disclosure, are understood to mean that the condition or characteristic is defined to within

tolerances that are acceptable for operation of the embodiment for an application for which the embodiment is intended. Wherever a general term in the disclosure is illustrated by reference to an example instance or a list of example instances, the instance or instances referred to, are by way of non-limiting example instances of the general term, and the general term is not intended to be limited to the specific example instance or instances referred to. Unless otherwise indicated, the word “or” in the description and claims is considered to be the inclusive “or” rather than the exclusive or, and indicates at least one of, or any combination of more than one of items it conjoins.

[0020] Fig. 1 schematically shows network elements comprised in a mobile communication network 18 comprising a 3rd Generation Wireless Mobile Communication (3G) network 19 and an evolved packet system (EPS) communications network 20 that operates to connect a user’s mobile communication equipment, (UE) to one or more Packet Data Networks (PDNs), and/or, as a circuit switch fallback option, to the Public Switched Telephone Network (PSTN). Network 20 may operate to provide a user’s UE with communications to the Internet and/or to stationary and/or mobile communication equipment of other users (not shown). In Fig. 1 mobile user equipment, UE, is schematically represented by smartphone and laptop icons 22.

[0021] EPS network 20 comprises a packet switched core network referred to as an Evolved Packet Core (EPC) core network indicated by a dashed boundary labeled EPC and a Long Term Evolution (LTE) radio access network referred to as an Evolved Universal Terrestrial Radio Access Network E-UTRAN indicated by a dashed boundary labeled E-UTRAN. E-UTRAN provides user equipment with wireless radio frequency (RF) channel connectivity to the core network EPC. The core network EPC provides a UE connected to the core network via an E-UTRAN radio channel with a communications connection to a PDN via an internet protocol (IP) packet flow “pipeline”, conventionally referred to as a “bearer”. The acronym LTE is conventionally used when referring to an evolved packet system (EPS) network comprising both the LTE E-UTRAN and the evolved packet core EPC, and network 20 shown in Fig. 1 may be referred to as LTE network 20, or simply LTE.

[0022] E-UTRAN comprises a network of RF communication base stations referred to as evolved NodeB (eNodeB) base stations. Each eNodeB comprises an RF transceiver and integral controller that controls the RF transceiver to establish radio communication channels between UEs in a limited geographic region referred to as a cell, and the core network EPC. Legacy base

stations, referred to as NodeB base stations used in 3G networks, do not comprise integral controllers but are connected to radio network controllers (RNCs), operate using RF transmission technologies different from those used by eNodeBs and have limited functionalities in comparison to eNodeB base stations. Core network EPC is capable of communicating with and connecting a UE connected to a NodeB with a PDN network, and LTE network 20 is schematically shown connected to a NodeB base station of 3G network 19 via an RNC and a Serving GPRS (General Packet Radio Service) Support Node, (SGSN) of the 3G network. The SGSN node is responsible for delivery of packets from and to UEs that are connected to a NodeB base station rather than an eNodeB base station. The SGSN is connected to the Internet via a GGSN (GPRS Gateway Support Node). Whereas in Fig. 1 mobile network 18 is shown comprising a E-UTRAN having two eNodeBs and a 3G network having one NodeB, an LTE may and typically does comprise more than two eNodeBs and a 3G network comprising more than one NodeB.

[0023] Core network EPC of LTE 20 comprises a plurality of logical nodes, which are supported by virtual and/or physical network entities. The network nodes include, a Serving Gateway (SGW), a PDN gateway (PGW), a Home Subscriber Server (HSS), a Mobile Switching Center (MSC) server, and a Mobile Management Entity (MME). The SGW is a node of the LTE network through which data packets from a UE connected to an eNodeB enter the EPC to be propagated from the UE through the EPC to their destinations, or exit the EPC to propagate to the eNodeB and the UE after propagating through the EPC from their sources. The SGW serves as a local mobility anchor for data bearers when the UE moves between cells of different eNodeBs. The PGW is a node through which UE data packets from a UE connected to the EPC exit the EPC to propagate to a PDN or enter the EPC from a PDN to propagate to the UE. The PGW is responsible for allocating an IP address to the UE and handling various administrative and charging tasks in accordance with information received by the PGW from a node referred to as a Policy and Charging Rules Function (PCRF) node. The HSS node contains user subscription data, such as a QoS profile and any restriction that might limit user roaming. The HSS also contains dynamic information such as an identity of an MME to which the user UE may currently be connected. The MSC node supports signaling between an MME and a UE Subscriber Identity Module (SIM) and Short Message Services (SMS) for a UE connected to the EPC via a NodeB.

[0024] The MME is a central control and signaling node that communicates with and orchestrates the activities of the other nodes and the UE in managing the resources of the LTE to establish, route, and maintain IP packet flow between a UE and a PDN. An EPC generally comprises more than one MME and may hand over connection to a UE from one to another of the MMEs as the UE moves between cells of different eNodeBs. In Fig. 1 LTE 20 is shown comprising two MMEs, a first MME 31 represented by a solid line rectangle and indicated by dotted lines as communicating with UEs shown in the figures, and a second MME 32, shown in dashed lines, to which first MME 31 may hand over UEs as the UEs move between cells.

[0025] Communication between two nodes in an LTE network is governed by an interface that configures what data the nodes exchange, how packets that contain the data are formatted, and how the packets are transmitted between the nodes. Communication between different node pairs is typically governed by different interfaces. An interface that configures communications between two nodes is indicated in Fig. 1 by an alphanumeric identifying the interface shown in an ellipse overlying a dashed or solid line that extends between the two nodes. For example, eNodeBs in an LTE network exchange control signaling with via an X2 interface, and an X2 is shown in an ellipse overlying a dashed line shown connecting the two eNodeBs in LTE network 20, and a UE communicates with an eNodeBs via a Uu interface shown in an ellipse overlying a solid line between the UE and the eNode B. Similarly as indicated in Fig. 1, the MME node communicates control data with an eNodeB via an S1-MME interface. The S1-MME interface defines data to be exchanged and packet formatting in accordance with an S1-AP protocol and configures transmission of the data between the MME and the eNodeB using the SCTP (Stream Control Transmission Protocol) transport protocol. The MME node communicates with the SGW node via an S11 interface, which tunnels UDP packets between the nodes using a General Packet Radio Service Tunneling Protocol (GTP) referred to as GTP-C. And, the HSS communicates with the MME via an S6a interface that configures data in accordance with a Diameter protocol and transmits Diameter messages using SCTP.

[0026] Fig. 2 schematically shows a Smart-vLB 100 coupled to LTE network 20 operating to load balance processing of data comprised in control packets transmitted between MME node 31 and other nodes in the LTE network, in accordance with an embodiment of the disclosure. By way of example, Smart-vLB 100 is assumed to comprise two, optionally virtual, non-Stateful load balancers, NS-vLBs, 101 and 102, and two, optionally virtual, Stateful load balancers, S-

vLB 110 and S-vLB 111, and is shown load balancing packets it receives from LTE network 20 between, optionally three, vProbes 121, 122, and 123.

[0027] It is noted that whereas Smart-vLB 100 is schematically shown in Fig. 2 and assumed to comprise virtual component entities, any or any combination of component entities of a Smart-vLB in accordance with an embodiment, such a non-Stateful load balancer and/or a Stateful load balancer may comprise and/or have access to any of various physical and/or virtual processors and memories that may be required to support functionalities for which the component entities are responsible. A component entity may be a physical or virtual entity or a combination of physical and virtual entities and may comprise or have access to a memory having any electronic and/or optical circuitry suitable for storing data and/or computer executable instructions. The memory may, by way of example, comprise or have access to any one, or any combination of more than one of a flash memory, random access memory (RAM), read only memory (ROM), and/or erasable programmable read-only memory (EPROM). Similarly, a component entity may comprise and/or have access to a processor having any electronic and/or optical processing circuitry configured to operate and provide functionalities that the component entity may require. The processor may by way of example comprise any one, or any combination of more than one of, a standard x86 processor, microprocessor, an application specific circuit (ASIC), field programmable array (FPGA) and/or system on a chip (SOC).

[0028] Smart-vLB 100 is shown in Fig. 2 by way of example coupled to LTE 20 to receive control packets mirrored from interfaces S1-MME, S3 and Gn., S11, Sv and SGs, S6a and S10 between MME 31, and eNodeBs, SGSN, SGW, MSC, HSS, and MME32, respectively. Link controllers (not shown) in MME 31 are configured to distribute substantially equal numbers of mirrored packets from LTE network 20 to each non-Stateful vLB, NS-vLB 101 and 102. Diameter packets mirrored to Smart-vLB 100 from interface S6a and GTP-C tunneled packets mirrored from interfaces, Sv, S3, S11 and S10 are selected as contextual packets. Packets mirrored to Smart-vLB 100 from interfaces S1-MME and SGs are considered non-contextual packets. Each NS-vLB 101 and 102 forwards non-contextual packets that it receives in substantially equal numbers to a given vProbe 121, 122, and 123 without reference to data in another packet. On the other hand, both NS-vLB 101 and 102 forward Diameter packets that they receive to S-vLB 111, and GTP-C packets they receive to S-vLB 110. Each S-vLB load balancer forwards a packet it receives to a vProbe 121,

122, or 123 having an identity which the S-vLB determines based on information from a at least one of a plurality of other packets that it receives.

[0029] For convenience of reference, S-vLBs 110 and 111 are labeled by the types of packets they respectively receive. S-vLB 110 is labeled “GTP-C” and S-vLB 111 is labeled “Diameter”.

[0030] Fig. 3 shows a flow diagram of an algorithm 200 by which NS-vLB 101 or NS-vLB 102, generically referred to as an NS-vLB, may determine where to forward packets they receive, in accordance with an embodiment of the disclosure.

[0031] In a block 202 the NS-vLB receives and optionally time stamps a packet from the selected MME interfaces shown in Fig. 2, and in a decision block 204 determines if the packet contains Application, Layer 7 of the Open System Interconnection (OSI) model, data. If the packet does not contain L7 data, in a block 205 the NS-vLB discards the packet and returns to block 202. If on the other hand it is an L7 packet, NS-vLB may proceed to a block 206 to determine if the packet is an S1AP protocol packet. If it is, NS-vLB optionally proceeds to a block 207 and extracts an eNode-B IP address of an eNodeB from which or to which the packet was sent. Based on the extracted eNodeB IP address, NS-vLB computes, optionally in a block 208, an address of a destination vProbe, to which to forward the packet. By way of example, to compute a vProbe destination address, in block 208 NS-vLB may hash the extracted IP address, and use a look-up table (LUT) that maps hashes of IP addresses of eNodeBs from which MME 31 may receive a packet to determine to which vProbe, 121, 122, or 123 to forward the packet. In a block 209 NS-vLB may encapsulate the packet for tunneling to the determined destination vProbe address, and in a block 210 may transmit the packet to the destination vProbe. Any suitable tunneling protocol such as the GRE (General Routing Encapsulation) tunneling protocol may be used in block 210 to tunnel the packet to the destination vProbe. After transmitting the S1AP packet to its destination vProbe, NS-vLB returns to block 202 to receive another packet from the selected MME interfaces.

[0032] If a packet received by NS-vLB is found to be an L7 packet in decision block 204, but not an S1AP packet in decision block 206, NS-vLB may proceed to determine in a decision block 212 if the received packet is an SGs protocol packet. If the packet is an SGs packet, optionally in a block 213, NS-vLB extracts an MSC IP address from the packet. Optionally, in blocks 208, 209, 210, NS-vLB proceeds to determine an IP address of a destination vProbe 121, 122, or 123, to which to forward the packet based on the extracted MSC IP address, and tunnel

the packet to the destination vProbe. Thereafter, NS-vLB may return to block 202 to receive another packet.

[0033] If a received packet is determined to be an L7 packet but not an S1AP or SGs packet, NS-vLB may proceed from decision block 212 to a decision block 214 to determine if the packet is a GTP-C packet. If it is a GTP-C packet, NS-vLB may proceed to blocks 215 and 216 to tunnel the packet to GTP-C stateful load balancer S-vLB 110 (Fig. 2). Following transmission of the packet to GTP-C S-vLB 110, NS-vLB may return to block 202 to receive another packet. If on the other hand in decision block 214 NS-vLB finds that the packet is not a GTP-C packet, NS-vLB may proceed to a block 217 to determine if the packet is a Diameter packet. If it is a Diameter packet, NS-vLB may proceed to blocks 218 and 219 to tunnel the packet to Diameter stateful load balancer S-vLB 111 (Fig. 2), and thereafter return to block 202.

[0034] If on the other hand, in decision block 217 NS-vLB finds that the packet is not a Diameter packet, NS-vLB may proceed to blocks 220 and 221 to tunnel the packet to a default vProbe or vProbe group, which may be any one of vProbes 121, 122, or 123 and thereafter return to block 202.

[0035] Figs. 4A-4B show a flow diagram of an algorithm 300 by which, optionally, Diameter stateful virtual load balancer S-vLB 111 (Fig. 2) processes Diameter packets it receives from non-stateful NS-vLB load balancers 101 and 102.

[0036] In a block 302 Diameter stateful load balancer S-vLB 111 receives an SCTP (Stream Control Message Protocol) packet comprising one or more complete and/or fragmented Diameter messages. In a decision block 304 load balancer S-vLB 111 determines if the SCTP packet comprises fragmented Diameter messages or a single, complete, non-fragmented, Diameter message. If the packet is a “fragmented packet”, comprising fragmented Diameter messages, load balancer S-vLB 111 proceeds to a block 306 and reassembles a Diameter message, a fragment of which is comprised in the SCTP packet. Reassembly comprises aggregating a sufficient number of SCTP packets to provide load balancer S-vLB 111 with a sufficient number of fragments to enable reassembly of a complete Diameter message. Following reassembly, load balancer 111 may proceed to a decision block 308. If in decision block 304, load balancer S-vLB 111 determines that the SCTP packet received in block 302 is not fragmented, load balancer S-vLB 111 may proceed directly to decision block 308.

[0037] In decision block 308 load balancer S-vLB 111 optionally determines if the Diameter message is an Authentication Information Request message, and if it is, may proceed to a block 310 in which the load balancer extracts an IMSI (International Mobile Subscriber Identity) and a hop-to-hop identifier (H2H ID), source and destination IP addresses that respectively identify a UE associated with the Diameter message and a session in which the UE is engaged. In a block 312 load balancer 111 stores the IMSI, H2H ID, and source and destination addresses in a transaction table that the load balancer maintains in a memory. Thereafter the load balancer may proceed to a block 328 in which, based on the extracted H2H ID it determines an IP address of a vProbe 121, 122, or 123, to which the load balancer will forward the packet or packets containing the Diameter message for processing. In a block 330 load balancer S-vLB 111 encapsulates the Diameter message packet or packets for tunneling to the determined IP address, and in a block 332 transmits the Diameter message to the vProbe IP address.

[0038] In a block 334, load balancer S-vLB 111 determines if the transmitted Diameter message is a last Diameter message in the SCTP packet. If it is, load balancer S-vLB 111 proceeds to a junction “X” and returns to block 302 to receive and process another SCTP packet. On the other hand, if it is not a last Diameter message, load balancer S-vLB 111 may proceed to a junction “Y” and returns to block 304 to determine if there is another Diameter message in the packet for processing and if it is fragmented.

[0039] In processing a Diameter message, if in decision block 308 load balancer S-vLB 111 determines that the Diameter message is not an Authentication Information Request message, the load balancer may proceed to a decision block 314 to determine if the Diameter message is a response to an Authentication Information Request message. If the message is not a response to an Authentication Information Request message load balancer S-vLB 111 may proceed from decision block 314 to a block 326 to extract a H2H ID from the message and in blocks 328-332 to transmit the message to a vProbe having an IP address determined from the H2H ID. In block 334 the load balancer determines whether to return to block 302 and receive another SCTP packet or to block 304 to process another Diameter message comprised in the current SCTP packet.

[0040] If in block 314 load balancer S-vLB 111 determines that the Diameter message is an Authentication Information Answer message the load balancer may proceed to a block 316 and extract an H2H ID from the message. In a block 318 the load balancer may attempt to match the

extracted H2H ID, source and destination IP addresses with an H2H ID, source and destination IP addresses message previously logged into the transaction table to identify a Diameter Authentication Information Request message with which the Authentication Information Answer message is associated. In a decision block 320, if the matching attempt is successful, Diameter load balancer S-vLB 111 proceeds to a block 323 and generates a data record comprising the authentication vector extracted in block 316 from the Diameter Authentication Information Answer message and the IMSI extracted from the associated Diameter Authentication Information Request message. The combination of an encryption key comprised in the authentication vector and the IMSI enable a vProbe 121, 122, or 123 to decipher a packet that it receives which is associated with the session associated with the IMSI. In a block 324 load balancer S-vLB 111 may transmit the data record to each of vProbes 121, 122, and 123.

[0041] Optionally, following transmission of the data record, load balancer S-vLB 111 may proceed to blocks 328 - 332 to determine a destination IP address of a vProbe 121, 122, or 123 to which the Diameter Authentication Information Answer message should be sent. The destination IP address determined for the Authentication Information Answer message is based on the H2H ID associated with the Authentication Information Answer message, which H2H ID is shared with the Authentication Information Request message matched to the Authentication Information Answer message in block 318. As a result, the vProbe IP address determined for the Diameter Authentication Information Answer message is the same as the vProbe IP address determined for the associated Diameter Authentication Information Request message. And in block 332, after encapsulation in block 330, the Diameter Authentication Information Answer message is transmitted to the same vProbe for analysis to which the associated Diameter Authentication Information Request message was sent. After transmission of the Diameter Authentication Information Answer, message load balancer 111 may proceed to block 334 to determine whether to return to block 302 and receive another SCTP packet or to block 304 to process the next Diameter message in the current SCTP packet. It is noted that whereas in the above description load balancer S-vLB 111 proceeds to blocks 328-332 after having generated and transmitted an associated data record, in an embodiment load balancer S-vLB 111 may generate and transmit the data record after having proceeded to execute, or during execution of, blocks 328-332.

[0042] In a case for which in decision block 320 load balancer S-vLB 111 determines that matching in block 318 has failed, the load balancer may proceed to perform a “Wait and See”

procedure. In the Wait and See procedure load balancer S-vLB 111 stores the Diameter Authentication Information Answer message in a holding memory, optionally a RAM (random access memory). In the holding memory the Diameter message may be stored with other messages in order of their respective time stamps provided by the non-Stateful load balancer NS-vLB 101 or NS-vLB 102 from which the message was forwarded to load balancer S-vLB 111. In an embodiment, the load balancer S-vLB 111 processes the message in order of its time stamp following a predetermined from a time at which the message was stored in the holding memory to make at least one additional attempt at matching the Authentication Information Answer message with an Authentication Information Request message. If in a decision block 322 the at least one additional attempt is successful, load balancer S-vLB 111 may proceed to blocks 323 and 324 to generate and transmit an IMSI plus authentication vector data record to all vProbes 121, 122, and 123. If however, in decision block 322 load balancer 111 determines that the at least one additional attempt has failed, the load balancer may proceed to execute blocks 328-334.

[0043] In an embodiment, to reduce a probability that an Authentication Information Answer message reaches GTP-C load balancer S-vLB 111 before the associated Authentication Information Request message reaches the load balancer, the load balancer may store all Diameter messages that it receives in a holding memory prior to attempting to match messages. The load balancer holds the messages in the holding memory for a given delay time before processing to reduce the probability that the load balancer will not find a match for an Authentication Information Answer

[0044] Figs. 5A-5C show a flow diagram of an algorithm 400 by which, optionally, GTP-C, stateful virtual load balancer S-vLB 110 (Fig. 2) processes GTP-C packets it receives from non-stateful NS-vLB load balancers 101 and 102.

[0045] In a block 402 load balancer S-vLB 110 receives a GTP-C message packet, and optionally in a block 410 determines if the message is a create session request. If it is, in a block 411 the load balancer extracts a sequence number, an IMSI, and a GTP-C MME F-TEID (Fully Qualified Tunnel Endpoint Identifier) located in the packet payload. In a block 412 load balancer S-vLB 110 may store the MME F-TEID and IMSI in a session table that the load balancer maintains, and in a block 413 stores the packet in a holding memory, optionally a RAM. From block 413 the load balancer may return to block 402 to receive another packet.

[0046] If in decision block 410 load balancer S-vLB 110 determines that the message is not a create session message, the load balancer may proceed to a decision block 420 to determine if the message is a create session response message. If it is, load balancer S-vLB 110, optionally in a block 421, extracts a sequence number and a GTP-C SGW F-TEID and optionally proceeds to find a match for the extracted sequence number with a previously extracted create session request sequence number stored in the session table. Load balancer S-vLB 110 may store the GTP-C SGW F-TEID in the session table and optionally proceed to a block 471. In block 471 based on the GTP-C MME F-TEID extracted from the associated create session request and stored in the session table in block 412, load balancer 110 determines an IP address for a vProbe 121, 122, or 123 to which to send for processing the session response packet and its associated session request packet stored in block 413 in RAM. In a block 472, the load balancer encapsulates the packets for tunneling, and in a block 473 transmits the encapsulated packets to the determined IP-address of the destination vProbe. Load balancer S-vLB 110 may then return to block 402 to receive another GTP-C packet.

[0047] If in decision block 420 load balancer S-vLB 110 determines that the GTP-C message is not a create session response, the load balancer may proceed to a decision block 430 to determine if the message is a modify bearer request message. If it is, load balancer S-vLB 110 may proceed to a block 431 in which the load balancer extracts a GTP-C F-TEID an S1-U eNodeB F-TEID, and an eNodeB S1-U IP address *[is this correct?]* from the packet. In a block 432 load balancer 110 matches the extracted GTP-C TEID with a GTP-C SGW F-TEID previously stored in the load balancer session table for a create session response and stores the S1-U eNodeB F-TEID and eNodeB S1-U IP address in the session table so that it may be associated with the create session response of the same GTP-C SGW F-TEID. In a block 434 the load balancer stores the packet in the holding memory RAM and may return to block 402 to receive another packet.

[0048] If in decision block 430 load balancer S-vLB 110 determines that the packet is not a modify bearer request, the load balancer may continue to a decision block 440 to determine if the message is a modify bearer response message. If it is a modify bearer response message, the load balancer may proceed to a block 441 to extract a GTP-C F-TEID from the packet as well as an S1-U SGW F-TEID, and in a block 442 match the extracted GTP-C F-TEID with a GTP-C MME F-TEID previously stored in the session table. In a block 443 load balancer S-vLB 110

stores the extracted S1-U SGW F-TEID in the session table so that it may be associated with the other data in the session table having the same GTP-C MME-TEID. In a block 444 load balancer S-vLB 110 generates a data record comprising the IMSI, S1-U eNodeB F-TEID, and the S1-U SGW F-TEID that are stored in the session table and associated with the same GTP-C MME F-TEID. In a block 445 the load balancer may determine a vProbe IP address based on the eNodeB S1-U IP address extracted in block 431 for the modify bearer request associated with the modify bearer response. And in a block 446 the load balancer may transmit the data record to the vProbe 121, 122, or 123 having the determined vProbe IP address. Load balancer S-vLB 110 may then proceed to blocks 471-473 to transmit the associated modify bearer request and modify bearer response packets for processing to a vProbe having an IP address determined from the GTP-C MME F-TEID that is associated with the modify session request and response packets. The vProbe to which the associated modify bearer request and modify bearer response packets are sent is also the same vProbe to which the create session request and response packets associated with the same GTP-C MME F-TEID were transmitted. From block 473 the load balancer may return to block 402 to receive another packet.

[0049] In decision block 440 if load balancer S-vLB 110 determines that the packet is not a modify bearer response, the load balancer may proceed to a block 450 to determine if the packet is another type of message packet different from a create session or modify bearer request. If it is, in a block 451 the load balancer extracts a GTP-C TEID from the packet and in a block 452 matches the extracted GTP-C TEID with a GTP-C MME TEID or a GTP-C SGW F-TEID previously stored in the session table. Load balancer S-vLB 110 may then proceed to blocks 471-473 to transmit the packet to a vProbe having an IP address determined from the GTP-C MME F-TEID associated with the session to which the create session request and response packets associated with the same GTP-C MME F-TEID belong. The load balancer may then proceed to block 402 to receive another packet.

[0050] It is noted that whereas a Wait and See procedure is described with respect to load balancer S-vLB 111 it may also be used where necessary by load balancer S-vLB 110.

[0051] The above discussion describes a Smart-vLB system balancing data processing for packets transmitted via MME interfaces in accordance with an embodiment of the disclosure. However, a Smart-vLB in accordance with an embodiment is not limited to load balancing for packets transmitted via MME interfaces, and may be configured to load balance for

communication interfaces via which entities of a network other than an MME communicate. By way of example, Fig. 6 schematically shows a Smart-vLB 100 coupled to LTE network 20 operating to load balance processing of data comprised in control plane and user plane packets transmitted between the SGW node, the PGW node, and other nodes in the LTE network, in accordance with an embodiment of the disclosure. In the figure Smart-vLB 100 is shown by way of example coupled to LTE 20 to receive control packets mirrored from interfaces S1-U, S4, S11, S5, S8, SGi, Gn, Gi, Gx. It is noted that whereas Fig. 2 shows Smart-vLB coupled only to MME interfaces, and Fig. 6 shows the Smart-vLB coupled only to SGW and PGW interfaces, a Smart-vLB may simultaneously be coupled to interfaces of more than one network entity and be configured to substantially simultaneously be responsible for load balancing communications for all the more than one network entity.

[0052] Fig. 7A shows a flow diagram of an algorithm 500 by which NS-vLB 101 or NS-vLB 102, may determine where to forward packets they receive from an SGW interface to which Smart-vLB 100 is coupled, in accordance with an embodiment of the disclosure.

[0053] In a block 502 the NS-vLB (NS-vLB 101 or NS-vLB 102) receives and optionally time stamps a packet from the selected SGW interfaces shown in Fig. 6, and in a decision block 504 determines if the packet contains a GTP-C protocol; packet. If it is a GTP-C packet, NS-vLB may proceed to blocks 506 and 508 to tunnel the packet to GTP-C stateful load balancer S-vLB 110 (Fig. 6). Following transmission of the packet to S-vLB 110, NS-vLB may return to block 502 to receive another packet. If on the other hand in decision block 504 NS-vLB finds that the packet is not a GTP-C packet, NS-vLB may proceed to a block 510 to determine if the packet is a Diameter packet. If it is a Diameter packet, NS-vLB may proceed to blocks 512 and 514 to tunnel the packet to Diameter stateful load balancer S-vLB 111 (Fig. 6), and thereafter return to block 502.

[0054] If on the other hand, in decision block 510 NS-vLB finds that the packet is not a Diameter packet, NS-vLB may proceed to decision block 516 to determine if the packet is a GTP-U, Gi, or SGi packet and if not, discards the packet or transmits the packet to a default vProbe, and returns to block 502 to receive another packet. On the other hand, if in decision block 510, NS-vLB determines that it is a GTP-U, Gu, or SGi packet, NS-vLB may proceed to a block 518. In block 518 NS-vLB may extract an MS IP address from the packet and in a block 520 the NS-vLB may determine an address for a destination vProbe, vProbe 121, 122, or 123, to

which to transmit the packet for processing. In a block 522 NS-vLB encapsulates the packet for tunneling and transmits the encapsulated packet to the determined address of the destination vProbe. Following transmission NS-vLB may return to block 502 to receive another packet.

[0055] Fig. 7B shows a flow diagram of an algorithm 600 by which, optionally, GTP-C, stateful virtual load balancer S-vLB 110 (Fig. 6) processes a GTP-C packet mirrored from a SGW interface to which Smart-vLB 100 is coupled that S-vLB 110 receives from non-stateful NS-vLB load balancer 101 or 102.

[0056] In a block 602 load balancer S-vLB 110 receives a GTP-C message packet, and optionally in a block 610 determines if the message is a create session request. If it is, in a block 611 the load balancer extracts a sequence number, an IMSI, and a GTP-C MME F-TEID (Fully Qualified Tunnel Endpoint Identifier) located in the packet. In a block 612 load balancer S-vLB 110 may store the sequence number, MME F-TEID, and IMSI in a session table that the load balancer maintains, and in a block 613 stores the packet in a holding memory, optionally a RAM. From block 613 the load balancer may return to block 602 to receive another packet.

[0057] If in decision block 610 load balancer S-vLB 110 determines that the message is not a create session message, the load balancer may proceed to a decision block 620 to determine if the message is a create session response message. If it is, GTP-C virtual load balancer S-vLB 110, optionally in a block 621, extracts a sequence number, a GTP-C SGW F-TEID and a MS IP (Mobile Station IP Address). Thereafter in a block 622, S-vLB 110 optionally proceeds to find a match for the extracted sequence number with a previously extracted create session request sequence number stored in the session table. In a block 623 load balancer S-vLB 110 may store the GTP-C SGW F-TEID in the session table and, optionally, proceed to a block 650. In block 650 based on the MS IP address extracted from the associated create session request and stored in the session table in block 623, load balancer S-vLB 110 determines an IP address for a destination vProbe 121, 122, or 123 to which to send for processing, the session response packet and its associated session request packet stored in RAM in block 613. In a block 652, the load balancer may encapsulate the packets for tunneling and transmit the encapsulated packets to the determined IP-address of the destination vProbe. Load balancer S-vLB 110 may then return to block 602 to receive another GTP-C packet.

[0058] If in decision block 420 load balancer S-vLB 110 determines that the GTP-C message is not a create session response, the load balancer may proceed to a decision block 630 to extract a

GTP-C F-TEID from the packet. In a block 632 load balancer S-vLB 110 matches the extracted GTP-C TEID with a GTP-C MME F-TEID or GTP-C SGW F-TEID previously stored in the load balancer session table and may proceed to block 650. In block 650 S-vLB 110 calculates an IP address for a destination vProbe 121, 122, or 123 to which to send the packet for processing based on the MS IP address stored in the session table for the GTP-C MME F-TEID or GTP-C SGW

F-TEID matched with the GTP- TEID in block 632. In a block 652, S-vLB 110 encapsulates the packet and transmits the packet to the determined IP address of the destination vProbe and may return to block 602 to receive another packet.

[0059] There is therefore provided in accordance with an embodiment of the disclosure, a load balancing system for a packet switched communication network, the load balancing system comprising: at least one first load balancer configured to receive packets propagated in the network and characterize a received packet as non-contextual if the packet does not comprise data that requires, or is required by, data in another packet to make a determination relevant to data in the packet or the other packet with respect to a predetermined task, and characterize the received packet as contextual if the packet comprises data that requires, or is required by, data in another packet to make a determination relevant to data in the packet or the other packet with respect to a predetermined task; and at least one second load balancer configured to receive contextual packets from the at least one first load balancer and determine a decision relevant to data in a first contextual packet that it receives with respect to a predetermined task based on data comprised in a second contextual packet that it receives from the at least one first load balancer.

[0060] Optionally, the at least one second load balancer is configured to select the second contextual packet by determining which of the contextual packets received by the at least one second load balancer comprises data that matches data in the first contextual packet other than the data on which to base the decision. Additionally or alternatively, the predetermined task comprises determining a network address of a vProbe to which to transmit both the first and second contextual packets. In an embodiment, the predetermined task comprises generating a data record comprising data extracted from both the first and second contextual packets.

[0061] In the description and claims of the present application, each of the verbs, “comprise” “include” and “have”, and conjugates thereof, are used to indicate that the object or objects of the verb are not necessarily a complete listing of components, elements or parts of the subject or subjects of the verb.

[0062] Descriptions of embodiments of the invention in the present application are provided by way of example and are not intended to limit the scope of the invention. The described embodiments comprise different features, not all of which are required in all embodiments of the invention. Some embodiments utilize only some of the features or possible combinations of the features. Variations of embodiments of the invention that are described, and embodiments of the invention comprising different combinations of features noted in the described embodiments, will occur to persons of the art. The scope of the invention is limited only by the claims.

CLAIMS

1. A load balancing system for a packet switched communication network, the load balancing system comprising:

at least one first load balancer configured to receive packets propagated in the network and characterize a received packet as non-contextual if the packet does not comprise data that requires, or is required by, data in another packet to make a determination relevant to data in the packet or the other packet with respect to a predetermined task, and characterize the received packet as contextual if the packet comprises data that requires, or is required by, data in another packet to make a determination relevant to data in the packet or the other packet with respect to a predetermined task; and

at least one second load balancer configured to receive contextual packets from the at least one first load balancer and determine a decision relevant to data in a first contextual packet that it receives with respect to a predetermined task based on data comprised in a second contextual packet that it receives from the at least one first load balancer.

2. The load balancing system according to claim 1 wherein the at least one second load balancer is configured to select the second contextual packet by determining which of the contextual packets received by the at least one second load balancer comprises data that matches data in the first contextual packet other than the data on which to base the decision.

3. The load balancing system according to claim 1 or claim 2 wherein the predetermined task comprises determining a network address of a vProbe to which to transmit both the first and second contextual packets.

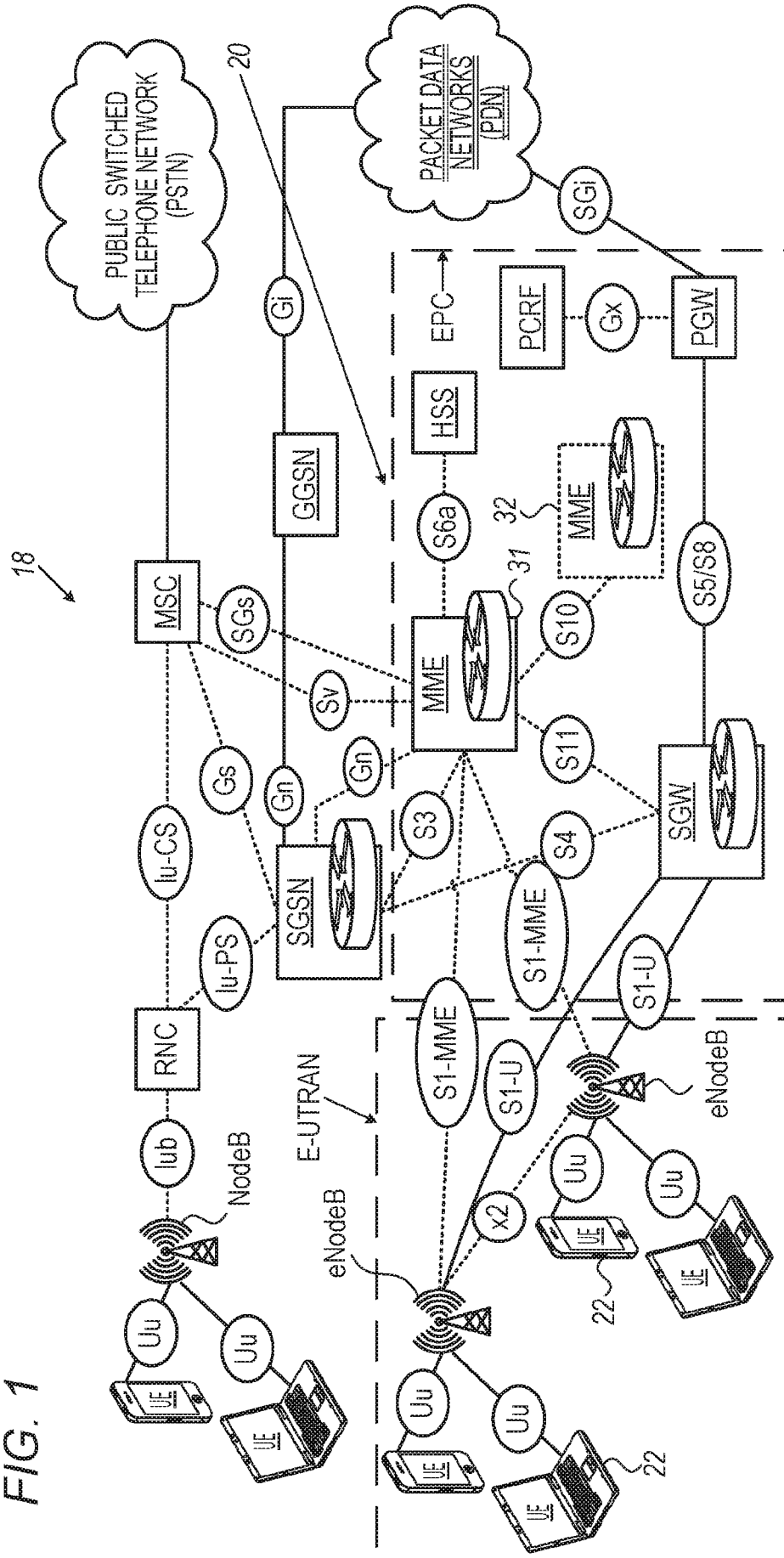
4. The load balancing system according to any of claims 1-3 wherein the predetermined task comprises generating a data record comprising data extracted from both the first and second contextual packets.

5. The load balancing system according to claim 2 wherein the first and second contextual packets are GTP-C (General Packet Radio Service Tunneling Protocol) packets.

6. The load balancing system according to claim 5 wherein the matching data comprises a sequence number of a create session shared by the first and second contextual packets
7. The load balancing system according to claim 5 or claim 6 wherein the data on which to base the decision comprises a GTP-C MME (Mobile Management Entity) F-TEID (Fully Qualified Tunnel Endpoint Identifier), or an MS IP (Mobile Station Internet Protocol) address.
8. The load balancing system according to claim 7 wherein the predetermined task comprises determining of an IP address of a vProbe to which to send the first and second contextual packets.
9. The load balancing system according to claim 2 wherein the matching data comprises a GTP-C TEID in the first contextual packet and a GTP-C SGW (Serving Gateway) F-TEID or a GTP-C MME F-TEID in the second contextual packet.
10. The load balancing system according to claim 9 wherein the data on which to base the decision comprises the GTP-C MME F-TEID.
11. The load balancing system according to claim 10 wherein the predetermined task comprises determining of an IP address of a vProbe to which to send the first and second contextual packets.
12. The load balancing system according to claim 10 or claim 11 wherein the first and second packets are modify bearer packets and the predetermined task comprises generating a data record comprising an IMSI (International Mobile Subscriber Identity), an S1-U eNodeB F-TEID, and S1-U SGW F-TEID.
13. The load balancing system according to claim 2 wherein the matching data comprises a H2H ID (Hop-to-Hop Identifier), a source IP address and a destination IP address in both the first and second contextual packets.

14. The load balancing system according to claim 13 wherein the data on which to base the decision comprises the H2H ID.
15. The load balancing system according to claim 14 wherein the predetermined task comprises determining of an IP address of a vProbe to which to send the first and second contextual packets.
16. The load balancing system according to claim 15 wherein the packets are authentication packets and the predetermined task comprises generating a data record comprising an IMSI, and authentication vector from data comprised in the first and second contextual packets.
17. The load balancing system according to any of the preceding claims wherein the at least one and/or the at least one second load balancer is a virtual load balancer.
18. The load balancing system according to any of the preceding claims wherein the network comprises an LTE network.

FIG. 1



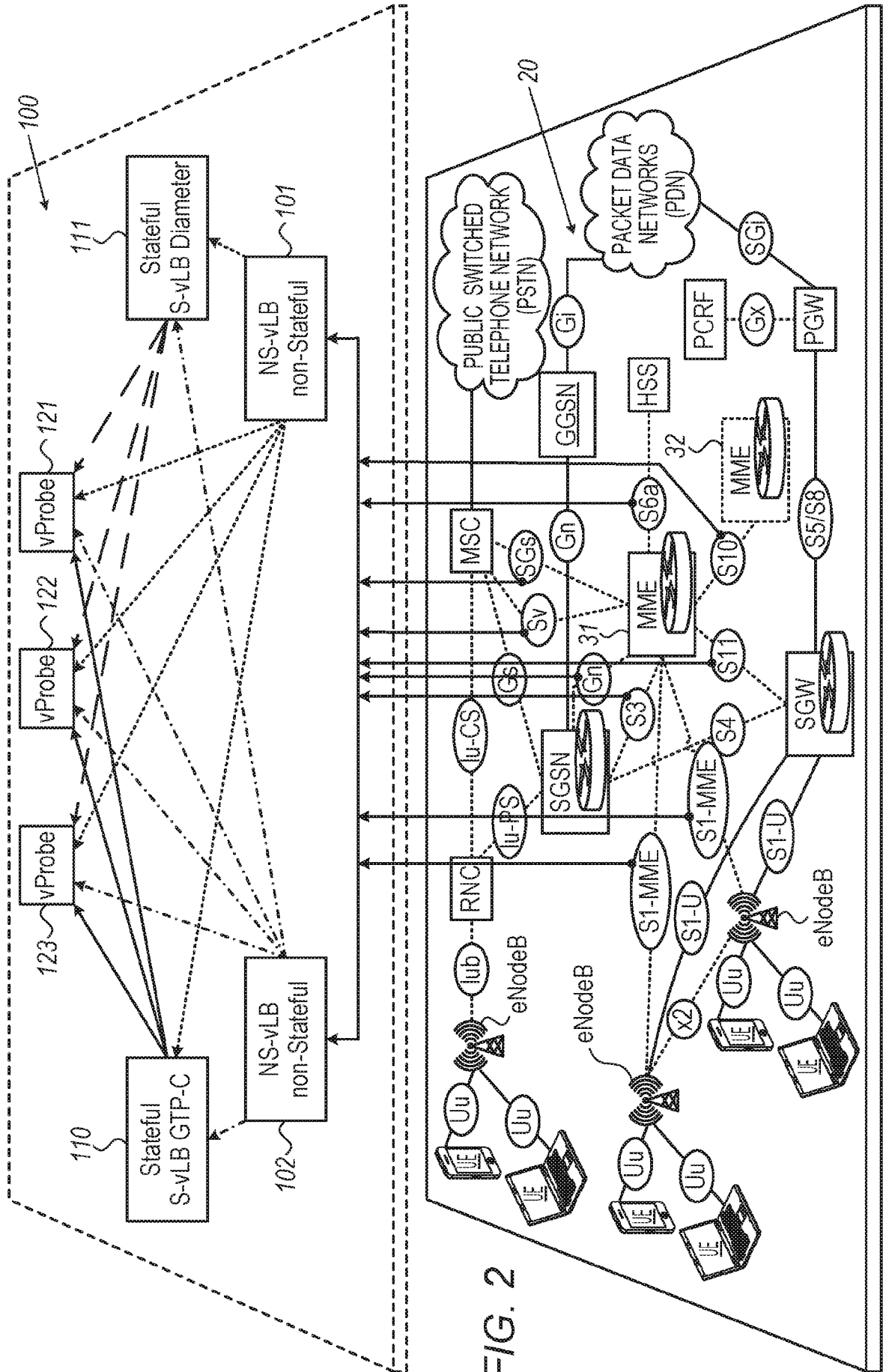
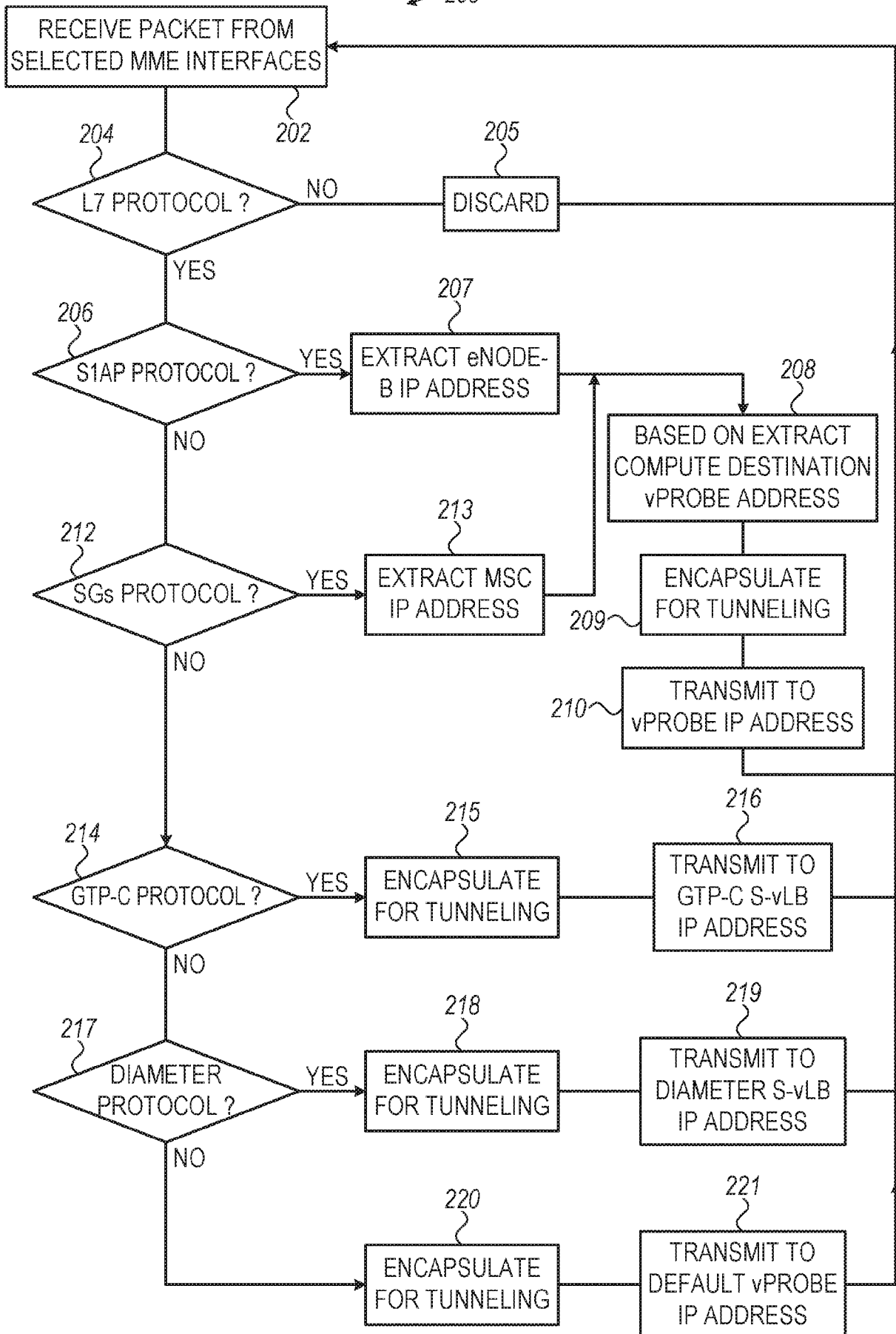


FIG. 2

FIG. 3



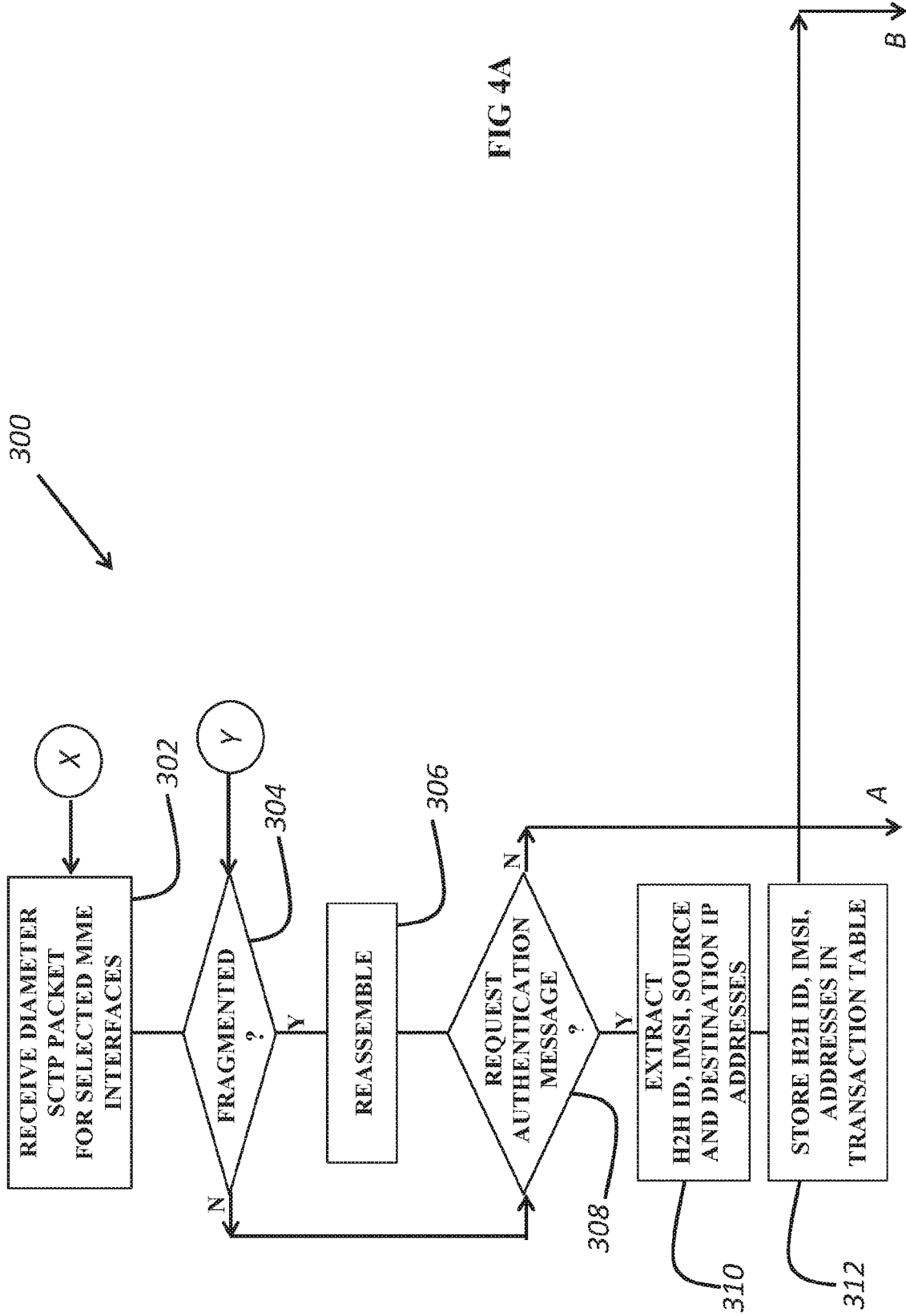


FIG 4A

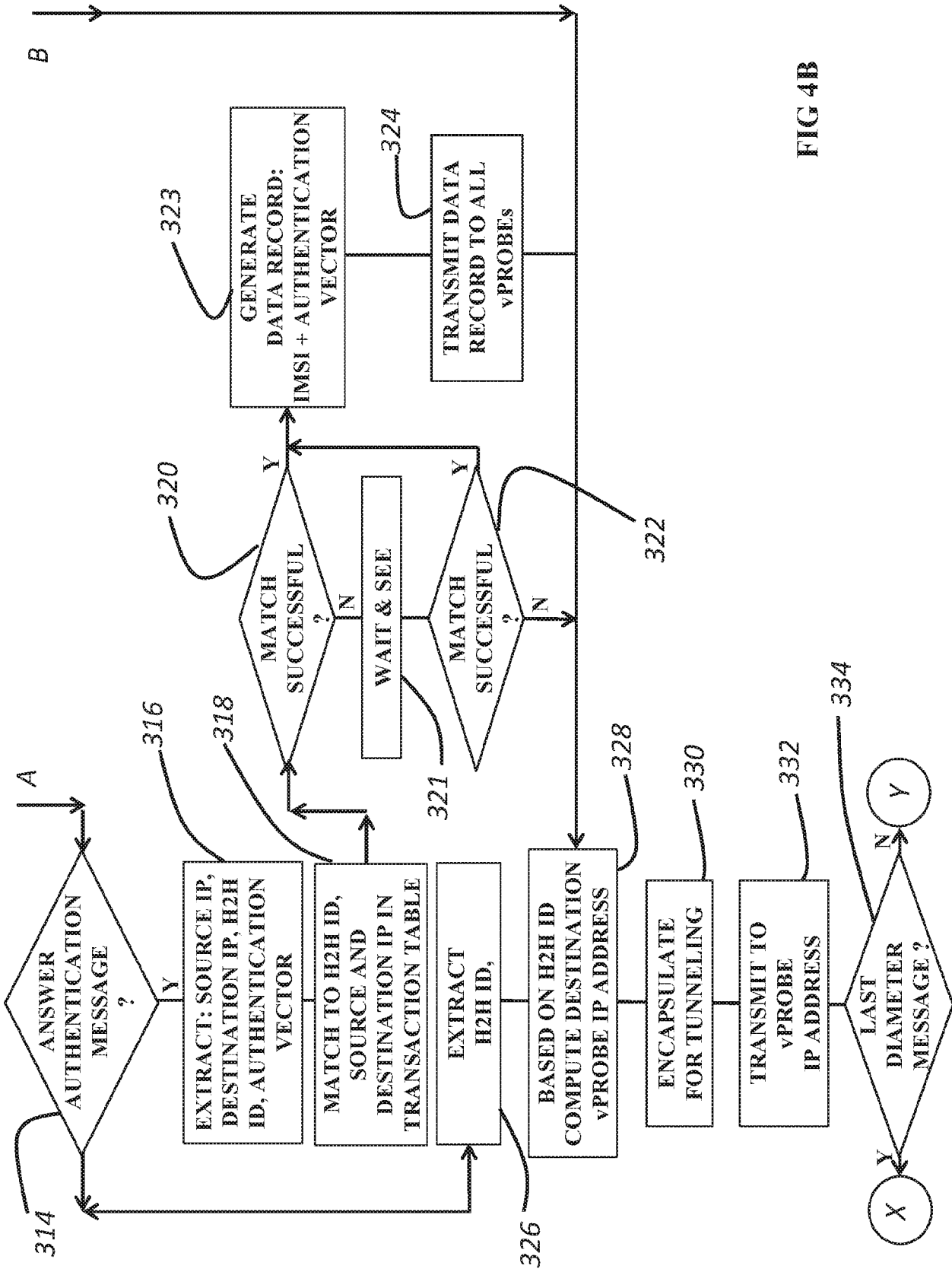


FIG 4B

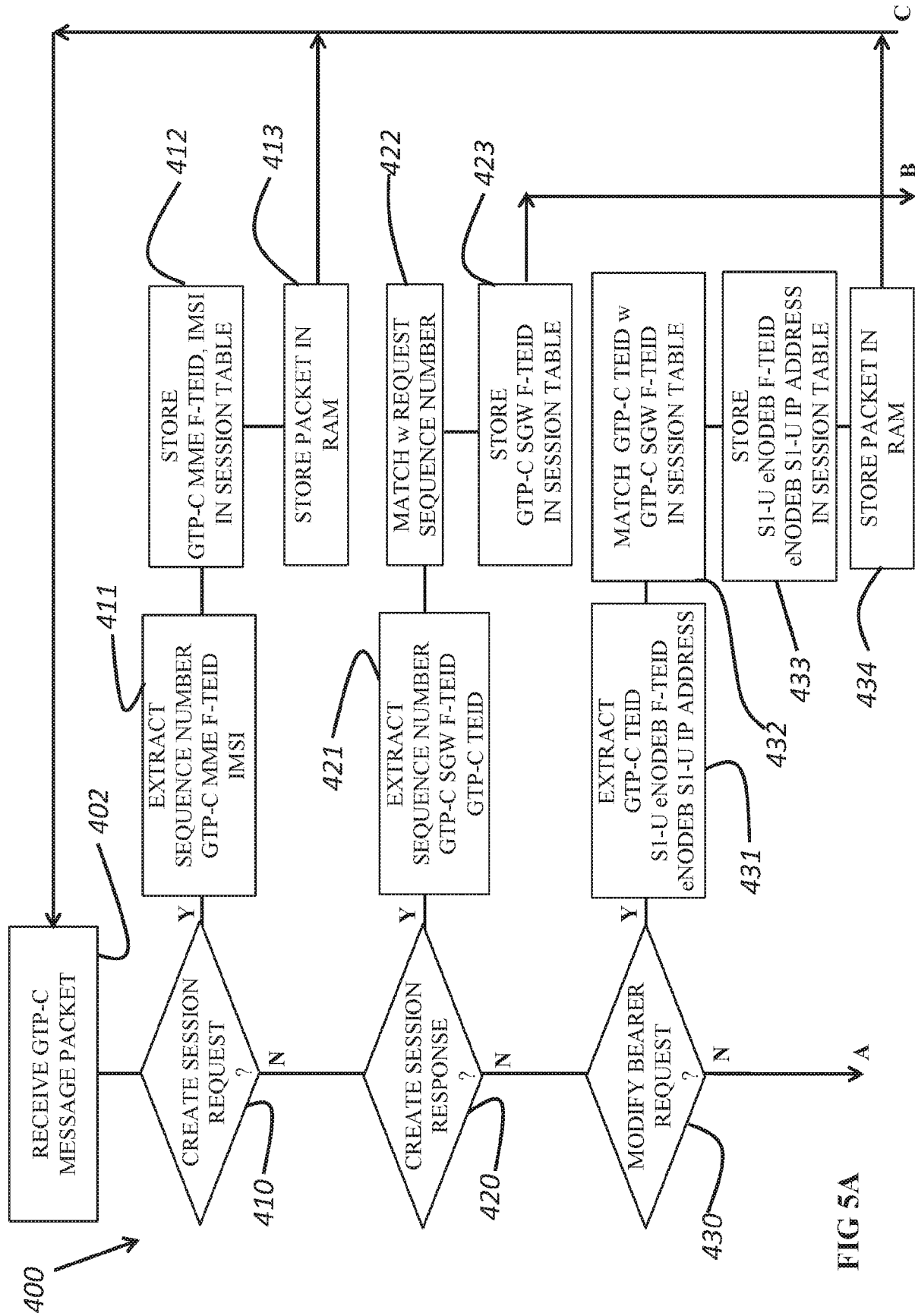


FIG 5A

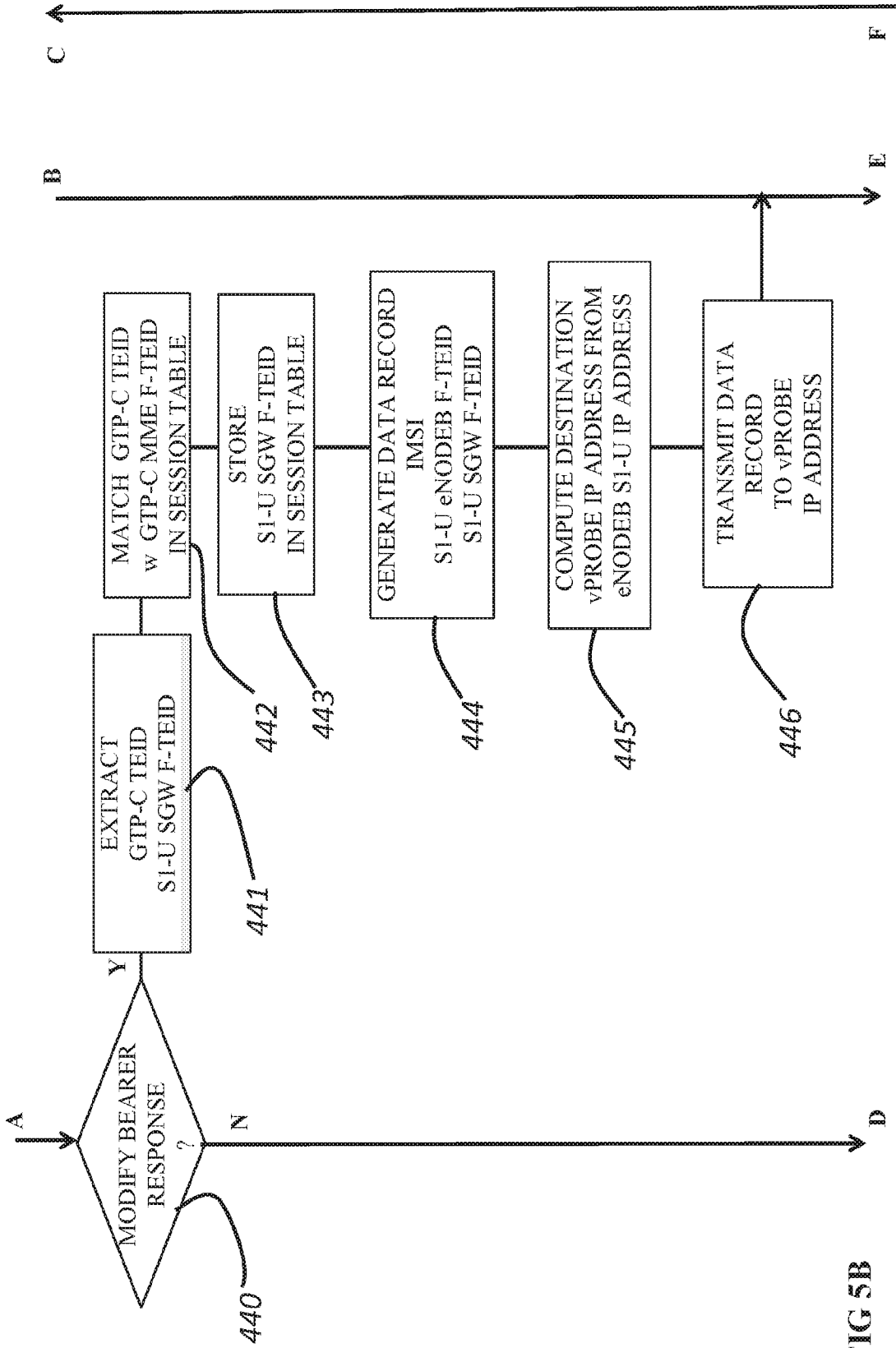


FIG 5B

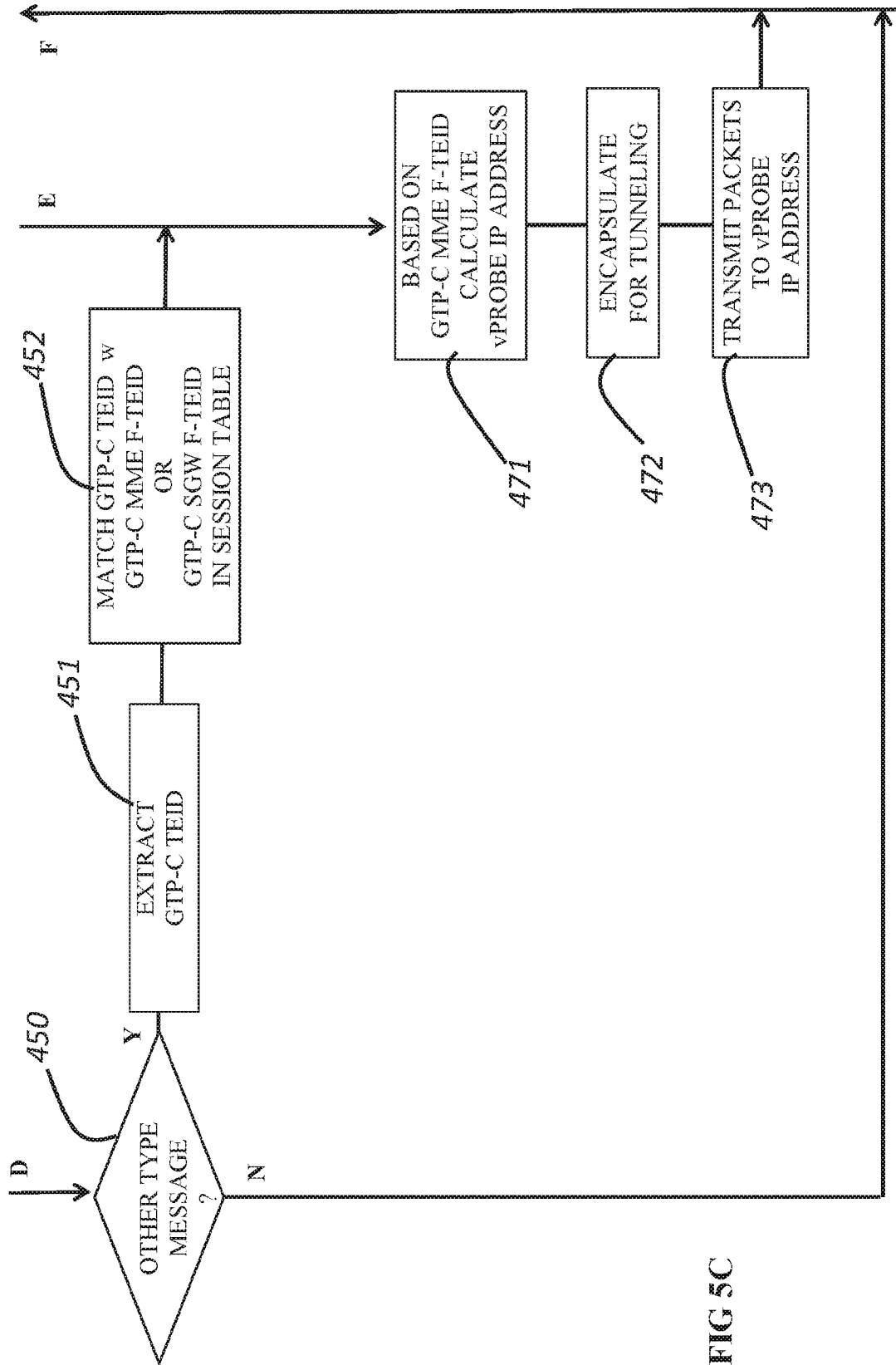


FIG 5C

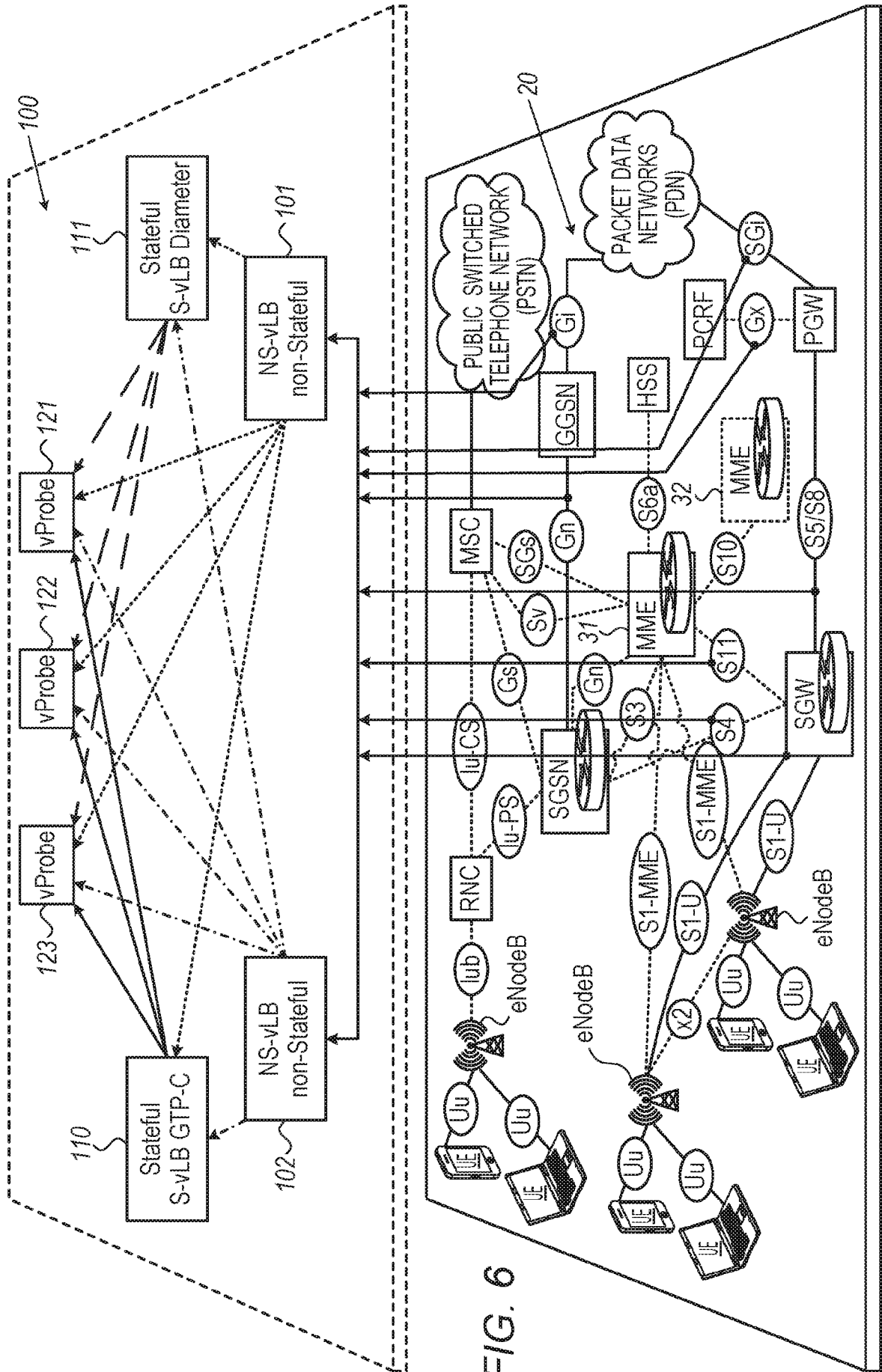


FIG. 6

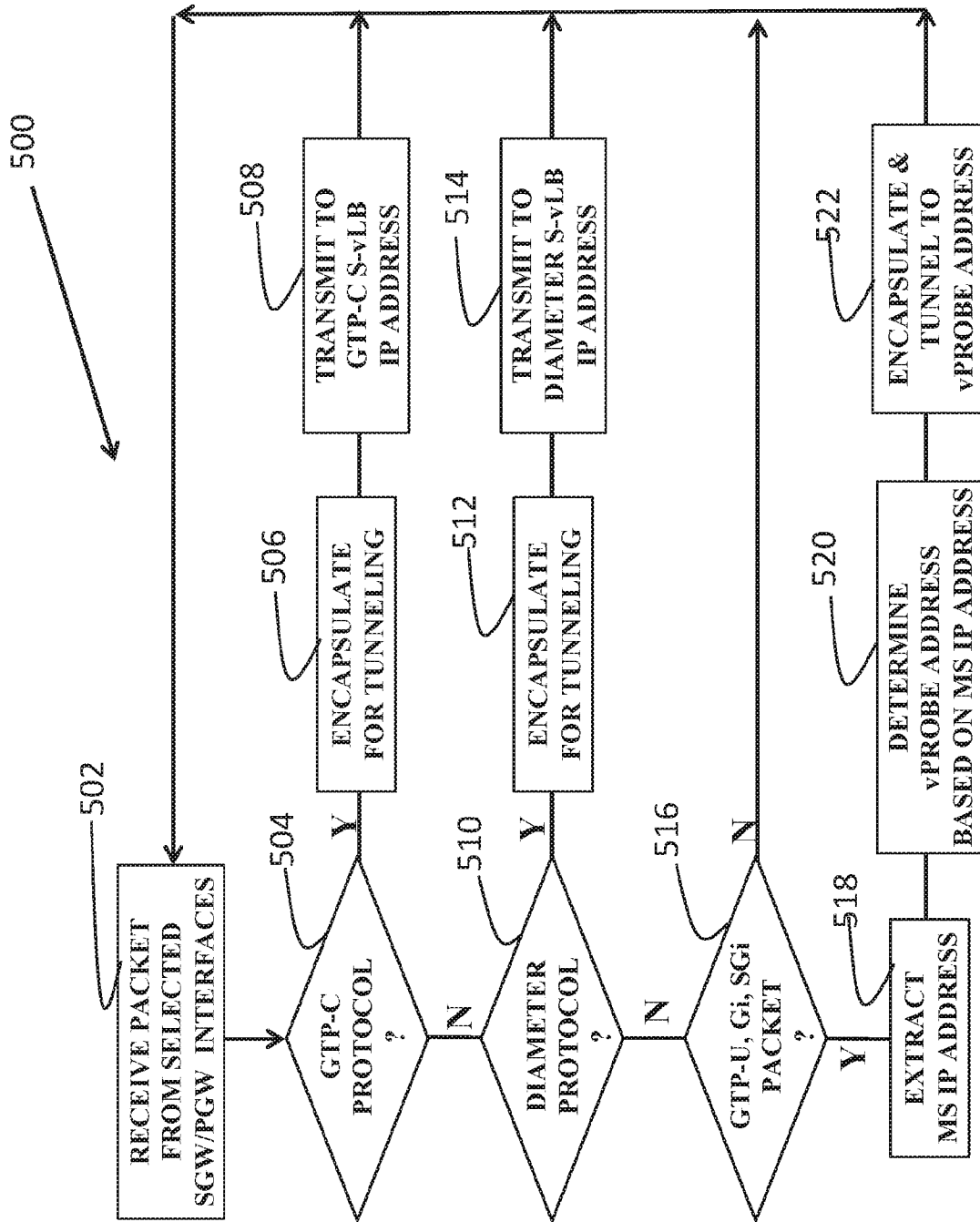


FIG 7A

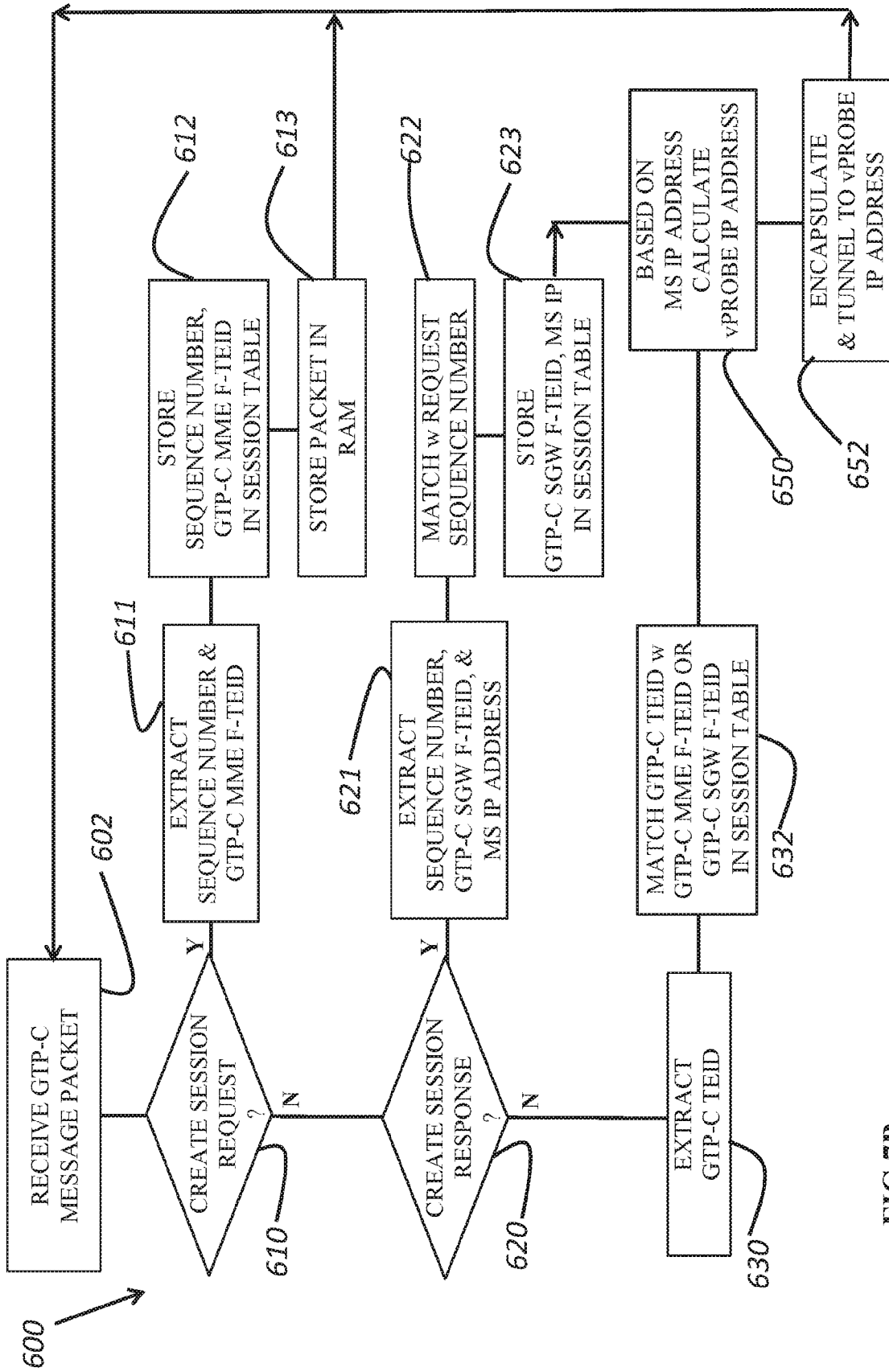


FIG 7B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2016/054332

A. CLASSIFICATION OF SUBJECT MATTER IPC (2016.01) H04L 12/70		
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) IPC (2016.01) H04L 12/70		
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) Databases consulted: USPTO, THOMSON INNOVATION		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2003198189 A1 ROBERTS DAVE 23 Oct 2003 (2003/10/23) paragraphs [0004], [0055]	1-18
A	US 5598535 A IBM [US] 28 Jan 1997 (1997/01/28) the whole document	1-18
A	US 2011225372 A1 PIROG JERRY [US] 15 Sep 2011 (2011/09/15) the whole document	1-18
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> 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 24 Nov 2016		Date of mailing of the international search report 27 Nov 2016
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616		Authorized officer MOSKOVICH Elad Telephone No. 972-2-5651607

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No. PCT/IB2016/054332
--

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 2003198189 A1	23 Oct 2003	US 2003198189 A1	23 Oct 2003
		US 7804785 B2	28 Sep 2010
		AU 2003218160 A1	03 Nov 2003
		WO 03090413 A1	30 Oct 2003
US 5598535 A	28 Jan 1997	US 5598535 A	28 Jan 1997
		US 5754768 A	19 May 1998
US 2011225372 A1	15 Sep 2011	US 2011225372 A1	15 Sep 2011
		US 8935483 B2	13 Jan 2015
		CN 101873253 A	27 Oct 2010
		CN 101873253 B	04 Jun 2014
		EP 2247040 A2	03 Nov 2010
		EP 2247040 A3	07 Dec 2011
		JP 2010259045 A	11 Nov 2010
		JP 5537956 B2	02 Jul 2014
		KR 20100118054 A	04 Nov 2010
		KR 101639438 B1	13 Jul 2016
		TW 201108668 A	01 Mar 2011
		TW 1390913 B	21 Mar 2013
		US 2010238937 A1	23 Sep 2010
		US 8243737 B2	14 Aug 2012
		US 2010293345 A1	18 Nov 2010
		US 8255644 B2	28 Aug 2012
		US 2011225168 A1	15 Sep 2011
		US 8321385 B2	27 Nov 2012
		US 2010272117 A1	28 Oct 2010
		US 8352669 B2	08 Jan 2013
US 2010293353 A1	18 Nov 2010		
US 8407707 B2	26 Mar 2013		
US 2010238938 A1	23 Sep 2010		

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2016/054332

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 8473657 B2	25 Jun 2013
		US 2012005391 A1	05 Jan 2012
		US 8489791 B2	16 Jul 2013
		US 2011225337 A1	15 Sep 2011
		US 8489792 B2	16 Jul 2013
		US 2011225334 A1	15 Sep 2011
		US 8489794 B2	16 Jul 2013
		US 2011225376 A1	15 Sep 2011
		US 8499137 B2	30 Jul 2013
		US 2011225588 A1	15 Sep 2011
		US 8505013 B2	06 Aug 2013
		US 2011222553 A1	15 Sep 2011
		US 8514874 B2	20 Aug 2013
		US 2012158729 A1	21 Jun 2012
		US 8515965 B2	20 Aug 2013
		US 2011225589 A1	15 Sep 2011
		US 8537832 B2	17 Sep 2013
		US 2011225391 A1	15 Sep 2011
		US 8539199 B2	17 Sep 2013
		US 2012020251 A1	26 Jan 2012
		US 8547878 B2	01 Oct 2013
		US 2012020371 A1	26 Jan 2012
		US 8565250 B2	22 Oct 2013
		US 2012020370 A1	26 Jan 2012
		US 8576862 B2	05 Nov 2013
		US 2012020223 A1	26 Jan 2012
		US 8615013 B2	24 Dec 2013
		US 2012020210 A1	26 Jan 2012
		US 8619787 B2	31 Dec 2013
		US 2012020366 A1	26 Jan 2012
		US 8638805 B2	28 Jan 2014

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2016/054332

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 2012131283 A1	24 May 2012
		US 8677075 B2	18 Mar 2014
		US 2012036351 A1	09 Feb 2012
		US 8683221 B2	25 Mar 2014
		US 2012236857 A1	20 Sep 2012
		US 8705531 B2	22 Apr 2014
		US 2012155495 A1	21 Jun 2012
		US 8761204 B2	24 Jun 2014
		US 2012020250 A1	26 Jan 2012
		US 8837501 B2	16 Sep 2014
		US 2012023295 A1	26 Jan 2012
		US 8843682 B2	23 Sep 2014
		US 2012020369 A1	26 Jan 2012
		US 8848723 B2	30 Sep 2014
		US 2011225394 A1	15 Sep 2011
		US 8868889 B2	21 Oct 2014
		US 2012023498 A1	26 Jan 2012
		US 8869150 B2	21 Oct 2014
		US 2012020249 A1	26 Jan 2012
		US 8869151 B2	21 Oct 2014
		US 2012020367 A1	26 Jan 2012
		US 8869156 B2	21 Oct 2014
		US 2013086332 A1	04 Apr 2013
		US 8873550 B2	28 Oct 2014
		US 2013089109 A1	11 Apr 2013
		US 8874878 B2	28 Oct 2014
		US 2013125127 A1	16 May 2013
		US 8910168 B2	09 Dec 2014
		US 2011222552 A1	15 Sep 2011
		US 8910171 B2	09 Dec 2014
		US 2012002546 A1	05 Jan 2012

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2016/054332

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 8917738 B2	23 Dec 2014
		US 2011222540 A1	15 Sep 2011
		US 8943507 B2	27 Jan 2015
		US 2013042038 A1	14 Feb 2013
		US 8949500 B2	03 Feb 2015
		US 2012300772 A1	29 Nov 2012
		US 8949578 B2	03 Feb 2015
		US 2013089098 A1	11 Apr 2013
		US 8949582 B2	03 Feb 2015
		US 2012230341 A1	13 Sep 2012
		US 8949838 B2	03 Feb 2015
		US 2010293312 A1	18 Nov 2010
		US 9081742 B2	14 Jul 2015
		US 2013091330 A1	11 Apr 2013
		US 9152564 B2	06 Oct 2015
		US 2013304926 A1	14 Nov 2013
		US 9154442 B2	06 Oct 2015
		US 2012020368 A1	26 Jan 2012
		US 9160684 B2	13 Oct 2015
		US 2011289279 A1	24 Nov 2011
		US 9183145 B2	10 Nov 2015
		US 2012084498 A1	05 Apr 2012
		US 9195464 B2	24 Nov 2015
		US 2011289180 A1	24 Nov 2011
		US 9218290 B2	22 Dec 2015
		US 2012076153 A1	29 Mar 2012
		US 9300597 B2	29 Mar 2016
		US 9444737 B2	13 Sep 2016
		US 2011289179 A1	24 Nov 2011
		US 9444757 B2	13 Sep 2016
		US 2013089099 A1	11 Apr 2013

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2016/054332

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		US 9461930 B2	04 Oct 2016
		US 2013128896 A1	23 May 2013
		US 9485200 B2	01 Nov 2016
		US 2013097345 A1	18 Apr 2013
		US 2013142205 A1	06 Jun 2013
		US 2014153575 A1	05 Jun 2014