



(51) International Patent Classification:

H04L 69/22 (2022.01) H04L 45/00 (2022.01)

H04L 47/2441 (2022.01)

(21) International Application Number:

PCT/IN2024/050959

(22) International Filing Date:

27 June 2024 (27.06.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

202321045253 05 July 2023 (05.07.2023) IN

(71) Applicant: **JIO PLATFORMS LIMITED** [IN/IN]; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN).

(72) Inventors: **BHATNAGAR, Aayush**; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN). **JHA, Adityakar**; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN). **RANJAN, Anu**; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN). **MALHOTRA,**

Pankaj; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN). **SENGUPTA, Swarup**; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN). **MAMGAIN, Ranjan**; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN). **VASHISHTH, Yog**; Office-101, Saffron, Nr. Centre Point, Panchwati 5 Rasta, Ambawadi, Gujarat, Ahmedabad 380006 (IN).

(74) Agent: **JAPHET, Chinthan**; K Law (Krishnamurthy and Co.), 4th Floor, Prestige Takt, No 23, Kasturba Road Cross, Bangalore, Bangalore 560 001 (IN).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: SYSTEM AND METHOD FOR HANDLING PACKET PROCESSING RULES IN A NETWORK

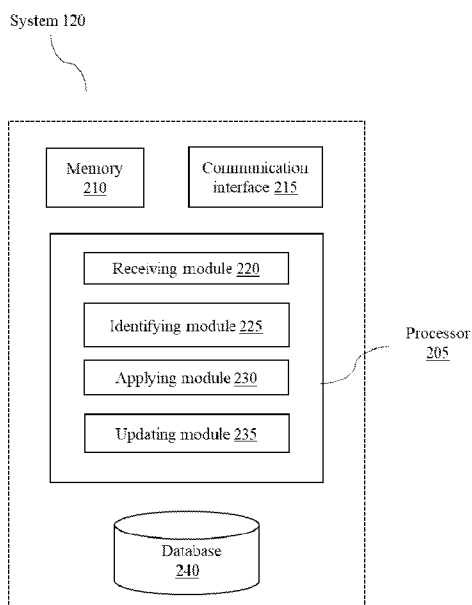


FIG. 2

(57) Abstract: The present disclosure relates to a system (120) and a method (500) for handling packet processing rules in a network (105). The system (120) includes a receiving module (220) to receive a request pertaining to at least one packet processing rule change. The system (120) further includes an identifying module (225) to identify a Data Plane (DP) core from a plurality of DP cores (408) based on a session ID included in the received request. The system (120) further includes an applying module (230) configured to apply a lock to the identified DP core. The system (120) further includes an updating module (235) configured to update the at least one packet processing rule change utilizing the locked DP core.

(84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEM AND METHOD FOR HANDLING PACKET PROCESSING RULES IN A NETWORK

FIELD OF THE INVENTION

[0001] The present invention generally relates to wireless communication systems, and more particularly relates to a system and a method for handling packet processing rules in a network.

BACKGROUND OF THE INVENTION

[0002] In a typical network architecture, a CP (Control Plane) and a DP (Data Plane) are separate entities responsible for different functions. The CP is responsible for making high-level decisions and managing the overall network. It handles tasks such as routing protocols, network topology discovery, and configuring network devices. On the other hand, the DP is responsible for the actual forwarding and processing of network packets. It handles tasks such as packet classification, traffic shaping, and forwarding decisions based on the established rules.

[0003] In mobile networks, certain events, such as frequent handovers, idle/active events, barring, quota consumptions/reporting may trigger a rule change with regard to how the packets from a User Equipment (UE) may need to be processed in relation to the occurred event. When a rule change request is made in the CP, such as modifying a packet processing rule or adding a new rule, the CP communicates this request to the DP. The DP then applies the requested changes to its packet processing pipeline or forwarding tables. The CP-DP interaction ensures that the control plane makes the necessary changes to the packet processing rules, and those changes are propagated to the DP cores running in the data plane for actual packet forwarding and processing.

[0004] In a conventional technique, for applying a rule change for packet handling of the UE, the CP halts or locks the operation of all the DP cores as the UE traffic may land on any DP core. Applying the rule changes in a network by halting or locking the operation of all DP cores may carry significant drawbacks that result in the wastage of network resources. For instance, one notable drawback is the service disruption caused

by halting the DP cores. This disruption leads to packet loss, increased latency, and potential unavailability for the affected UE. Consequently, user experience suffers, particularly for time-sensitive applications.

[0005] Another drawback owing to halting of all the cores during the rule change may be wastage of system hardware resources. When the DP cores are halted, their computational power and memory resources remain idle. This underutilization negatively impacts network efficiency, especially in high-throughput environments where rapid packet processing is critical. Thus, in such cases, the network fails to make the most of its hardware resources, leading to inefficiencies and decreased overall performance.

[0006] Therefore, there is a need for an advancement of a system and method that can overcome at least one of the above shortcomings, particularly for handling packet processing rules in the network.

BRIEF SUMMARY OF THE INVENTION

[0007] One or more embodiments of the present disclosure provide a system and method of handling packet processing rules in a network.

[0008] In one aspect of the present invention, a method of handling packet processing rules in a network is provided. The method includes the step of receiving, by one or more processors, a request pertaining to at least one packet processing rule change. The method includes the step of identifying, by the one or more processors, a Data Plane (DP) core from a plurality of DP cores. The DP core is identified based on a session ID included in the request. The method includes the step of applying, by the one or more processors, a lock to the identified DP core. The remaining DP cores of the plurality of DP cores remain in an unlocked state. The method further includes the step of updating, by the one or more processors, the at least one packet processing rule change utilizing the locked DP core.

[0009] In one embodiment, the locked DP core is unlocked post updating the at least one packet processing rule change, thereby the DP core is adapted to process packets for an at least one User Equipment (UE).

[0010] In another embodiment, the at least one packet processing rule is associated with the at least one UE.

[0011] In yet another embodiment, the request is triggered due to occurrence of network related events. The network related events are one of, handover, idle event, active event, barring, and quota consumption.

[0012] In yet another embodiment, the session ID serves as an identifier assigned to one of, a session and a connection, established between the network and the at least one UE.

[0013] In yet another embodiment, the method further includes the step of retrieving the session ID of the at least one UE from the request. The method further includes determining an Internet Protocol (IP) address of the at least one UE based on the session ID and a UE IP table. The UE IP table corresponds to a mapping database that associates the session IDs with the respective IP address of the UEs. The method further includes applying, a hash function to the determined IP address in order to map the determined IP address to a specific DP core. The method further includes receiving, details pertaining to the specific DP core based on applying the hash function to the determined IP address, the details include one of an identity of the specific DP core, location of the specific DP core within the network, thereby identifying the DP core from the plurality of DP cores.

[0014] In yet another embodiment, the method further includes the step of transmitting, by the one or more processors, a lock command to the identified DP core to halt one or more operations pertaining to the identified DP core based upon applying the lock to the identified DP core.

[0015] In another aspect of the present invention, a system for handling packet processing rules in a network is disclosed. The system includes a receiving module configured to receive a request pertaining to at least one packet processing rule change. The system further includes an identifying module configured to identify a Data Plane (DP) core from a plurality of DP cores based on a session ID included in the received request. The system further includes an applying module configured to apply a lock to the identified DP core. The remaining DP cores of the plurality of DP cores remain in an unlocked state. The system further includes an updating module configured to update the at least one packet processing rule change utilizing the locked DP core.

[0016] In another aspect of the present invention, a User Equipment (UE) is disclosed. The UE includes one or more primary processors communicatively coupled to one or more processors in a system. The one or more primary processors coupled with a memory. The memory stores instructions which when executed by the one or more primary processors cause the UE to generate and transmit a request pertaining to at least one packet processing rule change to the one or more processors.

[0017] Other features and aspects of this invention will be apparent from the following description and the accompanying drawings. The features and advantages described in this summary and in the following detailed description are not all-inclusive, and particularly, many additional features and advantages will be apparent to one of ordinary skill in the relevant art, in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] The accompanying drawings, which are incorporated herein, and constitute a part of this disclosure, illustrate exemplary embodiments of the disclosed methods and systems in which like reference numerals refer to the same parts throughout the

different drawings. Components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Some drawings may indicate the components using block diagrams and may not represent the internal circuitry of each component. It will be appreciated by those skilled in the art that disclosure of such drawings includes disclosure of electrical components, electronic components or circuitry commonly used to implement such components.

[0019] **FIG. 1** is an exemplary block diagram of an environment of handling packet processing rules in a network, according to one or more embodiments of the present disclosure;

[0020] **FIG. 2** is an exemplary block diagram of a system of handling packet processing rules in the network, according to one or more embodiments of the present disclosure;

[0021] **FIG. 3** is a schematic representation of the present system of **FIG. 1** workflow, according to one or more embodiments of the present disclosure;

[0022] **FIG. 4** illustrates an exemplary block diagram of workflow between one or more processors, and a plurality of Data Plane (DP) cores, according to one or more embodiments of the present disclosure; and

[0023] **FIG. 5** is a flow diagram illustrating a method of handling packet processing rules in a network, according to one or more embodiments of the present disclosure.

[0024] The foregoing shall be more apparent from the following detailed description of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0025] Some embodiments of the present disclosure, illustrating all its features, will now be discussed in detail. It must also be noted that as used herein and in the

appended claims, the singular forms "a", "an" and "the" include plural references unless the context clearly dictates otherwise.

[0026] Various modifications to the embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. However, one of ordinary skill in the art will readily recognize that the present disclosure including the definitions listed here below are not intended to be limited to the embodiments illustrated but is to be accorded the widest scope consistent with the principles and features described herein.

[0027] A person of ordinary skill in the art will readily ascertain that the illustrated steps detailed in the figures and here below are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0028] As per various embodiments depicted, the present invention discloses the system and method of handling packet processing rules in a network. The present invention provides a method for applying rule changes in a network's packet processing system. The method involves receiving the rule change request for modifying a packet processing rule associated with a User Equipment (UE) in the network. The method further identifying a Data Plane (DP) core responsible for handling the packets from the UE using the session ID included in the request. Upon identifying the DP core, the method further applying a lock exclusively to that core

while leaving other cores unaffected. This ensures that the operations of other cores are not stalled, optimizing network resource utilization. Subsequently, the method includes updating the rule within the locked DP core to reflect the desired changes in packet processing rule. Once the packet processing rule is updated, the lock on the DP core is released, allowing it to resume normal operations.

[0029] Referring to **FIG. 1**, **FIG. 1** illustrates an exemplary block diagram of an environment **100** of handling packet processing rules in a network **105**, according to one or more embodiments of the present disclosure. The environment **100** includes a network **105**, a User Equipment (UE) **110**, a server **115**, and a system **120**. The UE **110** aids a user to interact with the system **120** for generating and transmitting a request pertaining to at least one packet processing rule change to one or more processors **205** (as shown in **FIG. 2**).

[0030] The terms “user equipment,” and “at least one UE,” and variations thereof, as used herein, are used interchangeably, without limiting the scope of the present disclosure.

[0031] For the purpose of description and explanation, the description will be explained with respect to the UE **110**, or to be more specific will be explained with respect to a first UE **110a**, a second UE **110b**, and a third UE **110c**, and should nowhere be construed as limiting the scope of the present disclosure. Each of the UE **110** from the one or more UEs **110a, 110b,110n** is configured to connect to the server **115** via the network **105**.

[0032] In an embodiment, each of the first UE **110a**, the second UE **110b**, and the third UE **110c** is one of, but not limited to, any electrical, electronic, electro-mechanical or an equipment and a combination of one or more of the above devices such as virtual reality (VR) devices, augmented reality (AR) devices, laptop, a general-purpose computer, desktop, personal digital assistant, tablet computer, mainframe computer, or any other computing device.

[0033] The network **105** includes, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof. The network **105** may include, but is not limited to, a Third Generation (3G), a Fourth Generation (4G), a Fifth Generation (5G), a Sixth Generation (6G), a New Radio (NR), a Narrow Band Internet of Things (NB-IoT), an Open Radio Access Network (O-RAN), and the like.

[0034] The network **105** may also include, by way of example but not limitation, at least a portion of one or more networks having one or more nodes that transmit, receive, forward, generate, buffer, store, route, switch, process, or a combination thereof, etc. one or more messages, packets, signals, waves, voltage or current levels, some combination thereof, or so forth. The network **105** may also include, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, a VOIP or some combination thereof.

[0035] The environment **100** includes the server **115** accessible via the network **105**. The server **115** may include by way of example but not limitation, one or more of a standalone server, a server blade, a server rack, a bank of servers, a server farm, hardware supporting a part of a cloud service or system, a home server, hardware running a virtualized server, one or more processors executing code to function as a server, one or more machines performing server-side functionality as described herein, at least a portion of any of the above, some combination thereof. In an embodiment, the entity may include, but is not limited to, a vendor, a network operator, a company, an organization, a university, a lab facility, a business enterprise side, a defence facility side, or any other facility that provides service.

[0036] The environment **100** further includes the system **120** communicably coupled to the server **115** and each of the first UE **110a**, the second UE **110b**, and the third UE **110c** via the network **105**. The system **120** is adapted to be embedded within the server **115** or is embedded as the individual entity. However, for the purpose of description, the system **120** is described as an integral part of the server **115**, without deviating from the scope of the present disclosure.

[0037] Operational and construction features of the system **120** will be explained in detail with respect to the following figures.

[0038] Referring to **FIG. 2**, **FIG. 2** illustrates an exemplary block diagram of the system **120** of handling packet processing rules in the network **105**, according to one or more embodiments of the present disclosure. The system **120** includes one or more processors **205**, a memory **210**, and a communication interface **215**. The one or more processors **205**, hereinafter referred to as the processor **205** may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, single board computers, and/or any devices that manipulate signals based on operational instructions. As per the illustrated embodiment, the system **120** includes one processor **205**. However, it is to be noted that the system **120** may include multiple processors as per the requirement and without deviating from the scope of the present disclosure.

[0039] The information related to the request pertaining to the at least one packet processing rule change may be provided or stored in the memory **210**. Among other capabilities, the processor **205** is configured to fetch and execute computer-readable instructions stored in the memory **210**. The memory **210** may be configured to store one or more computer-readable instructions or routines in a non-transitory computer-readable storage medium, which may be fetched and executed to create or share data packets over a network service. The memory **210** may include any non-transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as EPROMs, FLASH memory, unalterable memory, and the like.

[0040] The information related to the request pertaining to the at least one packet processing rule change may be rendered on the communication interface **215**. The communication interface **215** includes a variety of interfaces, for example, interfaces for a Graphical User Interface (GUI), a web user interface, a Command Line Interface (CLI), and the like. The communication interface **215** facilitates communication of the system **125**. In one embodiment, the communication interface **215** provides a communication pathway for one or more components of the system **125**. Examples of such components include, but are not limited to, the UE **110** and a database **240**.

[0041] The database **240** is configured to store the request pertaining to the at least one packet processing rule change which is generated and transmitted by the UE **110**. Further, the database **240** provides structured storage, support for complex queries, and enables efficient data retrieval and analysis. The database **240** is one of, but is not limited to, one of a centralized database, a cloud-based database, a commercial database, an open-source database, a distributed database, an end-user database, a graphical database, a No-Structured Query Language (NoSQL) database, an object-oriented database, a personal database, an in-memory database, a document-based database, a time series database, a wide column database, a key value database, a search database, a cache databases, and so forth. The foregoing examples of database types are non-limiting and may not be mutually exclusive e.g., a database can be both commercial and cloud-based, or both relational and open-source, etc.

[0042] Further, the processor **205**, in an embodiment, may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processor **205**. In the examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processor **205** may be processor-executable instructions stored on a non-transitory machine-readable storage medium and the hardware for processor **205** may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the memory **210** may store instructions that,

when executed by the processing resource, implement the processor **205**. In such examples, the system **120** may comprise the memory **210** storing the instructions and the processing resource to execute the instructions, or the memory **210** may be separate but accessible to the system **120** and the processing resource. In other examples, the processor **205** may be implemented by electronic circuitry.

[0043] In order for the system **120** to handle packet processing rules in the network **105**, the processor **205** includes a receiving module **220**, an identifying module **225**, an applying module **230**, and an updating module **235** communicably coupled to each other for handling packet processing rules in the network **105**.

[0044] The receiving module **220**, the identifying module **225**, the applying module **230**, and the updating module **235** in an embodiment, may be implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processor **205**. In the examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processor **205** may be processor-executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the processor may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the memory **210** may store instructions that, when executed by the processing resource, implement the processor. In such examples, the system **120** may comprise the memory **210** storing the instructions and the processing resource to execute the instructions, or the memory **210** may be separate but accessible to the system **120** and the processing resource. In other examples, the processor **205** may be implemented by electronic circuitry.

[0045] In order for the system **120** to handle packet processing rules in the network **105**, the receiving module **220**, the identifying module **225**, the applying module **230**, and the updating module **235** are communicably coupled to each other. In this regard, the receiving module **220** is configured to receive a request pertaining to at least one

packet processing rule change. In an embodiment, the request is triggered due to occurrence of network related events. The network related events include, but are not limited to, handover, idle event, active event, barring, and quota consumption. In an embodiment, the at least one packet processing rule is associated with the at least one UE 110.

[0046] Accordingly, as per one embodiment, the processor 205 receives the request from a network entity, such as a Session Management Function (SMF) 402 (shown in FIG.4) via N4 interface. The SMF 402 is responsible for initiating and releasing communication sessions between the UE 110 and the network 105. The SMF 402 is configured to determine a user plane path for data transmission between the UE 110 and a User Plane Function (UPF). The SMF 402 communicates the packet processing rule change request from the at least one UE 110 to the processor 205 over N4 interface. Further, the processor 205 is configured to obtain a session Identifier (ID) from the request and subsequently query a UE Internet Protocol (IP) table based on receiving the request.

[0047] On receipt of the request by the receiving module 220, the identifying module 225 is configured to identify a Data Plane (DP) core from a plurality of DP cores 408 (shown in FIG. 4) based on the session ID included in the received request. The DP core is responsible for handling the actual forwarding of user data. The data plane is the part of a network architecture that deals with transmission and reception of user traffic, as opposed to a control plane, which manages the signaling and control functions. In a 5G network architecture, for example, the DP core includes elements like the User Plane Function (UPF). The UPF is responsible for routing and forwarding user data packets, enforcing Quality of Service (QoS) policies, and ensuring the efficient and reliable transport of user data between the UE 110 and the network 105.

[0048] The plurality of DP cores 408 include, but not limited to a first DP core 408a, a second DP core 408b, and a third DP core 408c. For the purpose of description and explanation, the description will be explained with respect to the plurality of DP cores 408, or to be more specific will be explained with respect to the first DP core 408a,

the second DP core **408b**, and the third DP core **408c**, and should nowhere be construed as limiting the scope of the present disclosure.

[0049] Accordingly, as per one embodiment, the session ID serves as an identifier assigned to one of, a session and a connection, established between the network **105** and the at least one UE **110**. The session ID of the at least one UE **110** is retrieved from the packet processing rule change request. The session ID helps to track and differentiate the packets belonging to different sessions. An IP address of the at least one UE **110** is determined based on the session ID and the UE IP table **404**. The UE IP table **404** corresponds to a mapping database that associates the session IDs with the respective IP address of the UEs **110**.

[0050] Accordingly, as per one or more embodiments, the UE IP table **404** contains information about the various sessions of the at least one UE **110** within the network and their respective IP addresses. Using the session ID as a reference, the processor **205** looks up the UE IP table **404** to find the entry that corresponds to the session ID. By doing so, the processor **205** can retrieve the specific IP address associated with the identified session. After retrieving the specific IP address, the processor **205** provides the IP address as an input to a hash operator **406**.

[0051] Accordingly, as per one or more embodiments, the hash operator **406** applies a hash function to the determined IP address in order to map the determined IP address to a specific DP core. Details pertaining to the specific DP core is received based on applying the hash function to the determined IP address. The hash function is a function that takes a set of inputs such as messages of any arbitrary size and returns a fixed-size string of bytes. The output of the hash function, once applied to the input, is the fixed-size string of characters or numbers, which is known as a hash value or a hash code. The exact form of the output depends on the specific hash function used. In one embodiment, the details include one of an identity of the specific DP core, location of the specific DP core within the network, thereby identifying the DP core from the plurality of DP cores **408**. The details of the specific DP core obtained through the hash function, are provided back to the processor **205**. This information

allows the processor **205** to be aware of the specific DP core that is responsible for processing the packets associated with the at least one UE **110**.

[0052] The processor **205** accurately determines the DP core that is currently processing the packets for the at least one UE **110** session and enables targeted application of the packet processing rule changes to the specific DP core only, ensuring that the modifications are applied only to the DP core handling the UE's packet traffic. In all uplink traffic, the UE IP is available in a source address of inner Packet Data Unit (PDU) IP header and in downlink traffic, UE IP is available in a destination address of the IP header. Based on the UE IP address, the received uplink/downlink packets are pushed to the identified DP core where the packet processing is intended.

[0053] On identification of the specific DP core by the identifying module **225**, the applying module **230** is configured to apply a lock to the identified DP core which is handling the packets from the at least one UE **110**. The remaining DP cores of the plurality of DP cores **408** remain in an unlocked state. In an example, the lock is only placed on the identified DP core, while leaving all the other DP cores unaffected and free to operate and ensures that the packet processing operations for other UEs or network traffic flows can proceed without being impacted by the packet processing rule change process for the at least one UE **110**. Further, a lock command is transmitted to the identified DP core to halt one or more operations pertaining to the identified DP core. By applying the lock selectively, the processor **205** optimizes resource utilization, minimizes disruptions, improves processing speed, reduces memory space requirement, and thereby enabling efficient and continuous packet forwarding across the network.

[0054] On locking of the identified DP core by the applying module **230**, the updating module **235** is configured to update the at least one packet processing rule change utilizing the locked DP core. The locked DP core is utilized for updating the at least one packet processing rule pertaining to the at least one UE **110** which is handled by the identified DP core. By updating the packet processing rule, the

processor **205** introduces modifications or adjustments to the packet processing rule within the identified DP core. Further, the processor **205** is configured to unlock the locked DP core post updating the at least one packet processing rule change, thereby the DP core is adapted to process the packets for the at least one UE **110**.

[0055] Accordingly, as per one embodiment, the processor **205** releases the lock on the identified DP core after the packet processing rule is updated. In this step, the lock is lifted to allow the DP core to resume its regular packet processing activities, including handling packets from the UE **110** that were subject to the rule update. By doing so, the system **120** applies the lock exclusively to the identified Data Plane (DP) core handling packets from the UE **110**, which prevents unnecessary halting or disruption of operations on other DP cores. The system **120** optimizes resource utilization to ensure that the network's resources are not wasted, and that packet processing continues smoothly across all other cores, thereby improving processing speed and reducing memory space requirement.

[0056] **FIG. 3** is a schematic representation of the system **120** in which various entities operations are explained, according to one or more embodiments of the present disclosure. Referring to **FIG. 3**, describes the system **120** for handling packet processing rules in the network **105**. It is to be noted that the embodiment with respect to **FIG. 3** will be explained with respect to the first UE **110a** for the purpose of description and illustration and should nowhere be construed as limited to the scope of the present disclosure.

[0057] As mentioned earlier in **FIG.1**, each of the first UE **110a**, the second UE **110b**, and the third UE **110c** may include an external storage device, a bus, a main memory, a read-only memory, a mass storage device, communication port(s), and a processor. The exemplary embodiment as illustrated in the **FIG. 3** will be explained with respect to the first UE **110a**. The first UE **110a** includes one or more primary processors **305** communicably coupled to the one or more processors **205** of the system **125**.

[0058] The one or more primary processors **305** are coupled with a memory **310** storing instructions which are executed by the one or more primary processors **305**. Execution of the stored instructions by the one or more primary processors **305** enables the first UE **110a** to generate and transmit the request pertaining to the at least one packet processing rule change to the one or more processors **205**.

[0059] As mentioned earlier in **FIG. 2**, the one or more processors **205** of the system **120** is configured to receive the request pertaining to the at least one packet processing rule change, identify the DP core from the plurality of DP cores based on the session ID included in the received request, apply the lock to the identified DP core, and update the at least one packet processing rule change utilizing the locked DP core.

[0060] As per the illustrated embodiment, the system **120** includes the one or more processors **205**, the memory **210**, and the communication interface **215**. The operations and functions of the one or more processors **205**, the memory **210**, and the communication interface **215** are already explained in **FIG. 2**. For the sake of brevity, a similar description related to the working and operation of the system **120** as illustrated in **FIG. 2** has been omitted to avoid repetition.

[0061] Further, the processor **205** includes the receiving module **220**, the identifying module **225**, the applying module **230**, and the updating module **235**. The operations and functions of the receiving module **220**, the identifying module **225**, the applying module **230**, and the updating module **235** are already explained in **FIG. 2**. Hence, for the sake of brevity, a similar description related to the working and operation of the system **120** as illustrated in **FIG. 2** has been omitted to avoid repetition. The limited description provided for the system **120** in **FIG. 3**, should be read with the description provided for the system **120** in the **FIG. 2** above, and should not be construed as limiting the scope of the present disclosure.

[0062] **FIG. 4** illustrates an exemplary block diagram of workflow of the processor **205**, and the plurality of DP cores **408**, according to one or more embodiments of the present disclosure. The plurality of DP cores **408** include, but not limited to the first

DP core **408a**, the second DP core **408b**, and the third DP core **408c**. For the purpose of description and explanation, the description will be explained with respect to the plurality of DP cores **408**, or to be more specific will be explained with respect to the first DP core **408a**, the second DP core **408b**, and the third DP core **408c**, and should nowhere be construed as limiting the scope of the present disclosure.

[0063] The processor **205** is configured to receive the request from the network entity, such as the Session Management Function (SMF) **402** via the N4 interface. The SMF **402** is responsible for initiating and releasing communication sessions between the UE **110** and the network **105**. The SMF **402** is configured to determine the user plane path for data transmission between the UE **110** and the UPF. The SMF **402** communicates the packet processing rule change request from the at least one UE **110** to the processor **205** over the N4 interface. Further, the processor **205** is configured to obtain the session ID from the request and subsequently query the UE IP table based on receiving the request.

[0064] Accordingly, as per one embodiment, the UE IP table **404** contains information about the various sessions of the first UE **110** within the network **105** and their respective IP addresses. Using the session ID as the reference, the processor **205** looks up the UE IP table **404** to find the entry that corresponds to the session ID. By doing so, the processor **205** can retrieve the specific IP address associated with the identified session. After retrieving the specific IP address, the processor **205** provides the IP address as an input to the hash operator **406**.

[0065] Accordingly, as per one or more embodiments, the hash operator **406** applies the hash function to the determined IP address in order to map the determined IP address to the specific DP core. Details pertaining to the specific DP core is received based on applying the hash function to the determined IP address. In one embodiment, the details include one of an identity of the specific DP core, location of the specific DP core within the network, thereby identifying the DP core from the plurality of DP cores. The details of the DP core are returned to the processor **205**. In one embodiment, the details include one of an identity of the specific DP core, location of the specific

DP core within the network, thereby identifying the DP core from the plurality of DP cores. This information allows the processor **205** to be aware of the specific DP core that is responsible for processing the packets associated with the at least one UE **110**.

[0066] Accordingly, as per one or more embodiments, let us consider for example, the third DP core **408c** is identified to be the specific DP core that is handling the traffic from the at least one UE **110**. The processor **205** is configured to transmit the lock command to the third DP core **408c** to halt one or more operations pertaining to the identified DP core. By applying the lock selectively, the processor **205** optimizes resource utilization and minimizes disruptions, improves processing speed, reduces memory space requirement, and thereby enabling efficient and continuous packet forwarding across the network.

[0067] Accordingly, as per one or more embodiments, the third DP core **408c** finishes any queued processing and subsequently enters a lock state. In this step, the lock is lifted to allow the third DP core **408c** to resume its regular packet processing activities, including handling packets from the at least one UE **110** that were subject to the rule update. The processor **205** is further configured to unlock the locked third DP core **408c** post updating the at least one packet processing rule change, thereby the third DP core **408c** is adapted to process packets for the at least one UE **110**. The processor **205** releases the lock on the third DP core **408c** after the packet processing rule is updated. Thereafter, the packet processing rule is updated and post rule update, the lock is released to process the packets for the at least one UE **110**.

[0068] **FIG. 5** is a flow diagram illustrating a method **500** for network planning, according to one or more embodiments of the present invention. For the purpose of description, the method **500** is described with the embodiments as illustrated in **FIG. 2** and should nowhere be construed as limiting the scope of the present disclosure.

[0069] At step **505**, the method **500** includes the step of receiving a request pertaining to at least one packet processing rule change by the receiving module **220**. In an embodiment, the request is triggered due to occurrence of network related events.

The network related events include, but are not limited to, handover, idle event, active event, barring, and quota consumption. In an embodiment, the at least one packet processing rule is associated with the at least one UE **110**. The processor **205** receives the request from a network entity, such as a Session Management Function (SMF) via N4 interface. The SMF **402** is responsible for initiating and releasing communication sessions between the UE **110** and the network **105**. The SMF **402** is configured to determine a user plane path for data transmission between the UE **110** and a User Plane Function (UPF). The SMF **402** communicates the packet processing rule change request from the at least one UE **110** to the processor **205** over N4 interface. Further, the processor **205** is configured to obtain a session Identifier (ID) from the request and subsequently query a UE Internet Protocol (IP) table based on receiving the request.

[0070] At step **510**, the method **500** includes identifying a DP core from a plurality of DP cores based on the session ID included in the received request by the identifying module **225** based on receipt of the request by the receiving module **220**. The DP core is responsible for handling the actual forwarding of user data. The data plane is the part of a network architecture that deals with transmission and reception of user traffic, as opposed to a control plane, which manages the signaling and control functions. In a 5G network architecture, for example, the DP core includes elements like the User Plane Function (UPF). The UPF is responsible for routing and forwarding user data packets, enforcing Quality of Service (QoS) policies, and ensuring the efficient and reliable transport of user data between the UE **110** and the network **105**.

[0071] Accordingly, as per one embodiment, the session ID serves as an identifier assigned to one of, a session and a connection, established between the network and the at least one UE **110**. The session ID of the at least one UE **110** is retrieved from the packet processing rule change request. The session ID helps to track and differentiate the packets belonging to different sessions. The IP address of the at least one UE **110** is determined based on the session ID and the UE IP table **404**. The UE IP table **404** corresponds to a mapping database that associates the session IDs with the respective IP address of the UEs.

[0072] Accordingly, as per one embodiment, the UE IP table **404** contains information about the various sessions of UEs **110** within the network and their respective IP addresses. Using the session ID as a reference, the one or more processors **205** looks up the UE IP table **404** to find the entry that corresponds to the session ID. By doing so, the one or more processors **205** can retrieve the specific IP address associated with the identified session. After retrieving the specific IP address, the one or more processors **205** provides the IP address as an input to a hash operator **406** (shown in FIG. 4).

[0073] Accordingly, as per one or more embodiments, the hash operator **406** applies a hash function to the determined IP address in order to map the determined IP address to a specific DP core. Details pertaining to the specific DP core is received based on applying the hash function to the determined IP address. In one embodiment, the details include one of an identity of the specific DP core, location of the specific DP core within the network, thereby identifying the DP core from the plurality of DP cores. The details of the specific DP core obtained through the hash function, are provided back to the one or more processors **205**. This information allows the one or more processors **205** to be aware of the specific DP core that is responsible for processing the packets associated with the at least one UE **110**.

[0074] The processor **205** accurately determines the DP core that is currently processing the packets for the at least one UE **110** session and enables targeted application of the packet processing rule changes to the specific DP core only, ensuring that the modifications are applied only to the DP core handling the UE's packet traffic. In all uplink traffic, the UE IP is available in a source address of inner Packet Data Unit (PDU) IP header and in downlink traffic, UE IP is available in a destination address of the IP header. Based on the UE IP address, the received uplink/downlink packets are pushed to the identified DP core where the packet processing is intended.

[0075] The processor **205** accurately determines the DP core that is currently processing the packets for the at least one UE **110** session and enables targeted application of the packet processing rule changes to the specific DP core only, ensuring

that the modifications are applied only to the DP core handling the UE's packet traffic. In all uplink traffic, the UE IP is available in a source address of inner Packet Data Unit (PDU) IP header and in downlink traffic, UE IP is available in a destination address of the IP header. Based on the UE IP address, the received uplink/downlink packets are pushed to the identified DP core where the packet processing is intended.

[0076] At step **515**, the method **500** includes applying a lock to the identified DP core which is handling the packets from the at least one UE **110** by the applying module **230**. The remaining DP cores of the plurality of DP cores remain in an unlocked state. In an example, the lock is only placed on the identified DP core, while leaving all the other DP cores unaffected and free to operate. This approach ensures that the packet processing operations for other UEs or network traffic flows can proceed without being impacted by the ongoing rule change process for the specific UE. Further, a lock command is transmitted to the identified DP core to halt one or more operations pertaining to the identified DP core. By applying the lock selectively, the processor **205** optimizes resource utilization and minimizes disruptions, improves processing speed, reduces memory space requirement, and thereby enabling efficient and continuous packet forwarding across the network.

[0077] At step **520**, the method **500** includes the step of updating the at least one packet processing rule change utilizing the locked DP core for processing of packets pertaining to the UE which are handled by the identified DP core by the updating module **235**. By updating the rule, the processor **205** introduces modifications or adjustments to the packet processing rule within the identified DP core. Further, the processor **205** is configured to unlock the locked DP core post updating the at least one packet processing rule change, thereby the DP core is adapted to process packets for the at least one UE **110**.

[0078] Accordingly, as per one embodiment, the processor **205** releases the lock on the identified DP core after the packet processing rule is updated. In this step, the lock is lifted to allow the DP core to resume its regular packet processing activities,

including handling packets from the UE **110** that were subject to the rule update. By doing so, the system applies the lock exclusively to the identified Data Plane (DP) core handling packets from the UE **110**, which prevents unnecessary halting or disruption of operations on other DP cores. The method **500** optimizes resource utilization to ensure that the network's resources are not wasted, and that packet processing continues smoothly across all other cores, thereby improving processing speed and reducing memory space requirement.

[0079] The present invention further discloses a non-transitory computer-readable medium having stored thereon computer-readable instructions. The computer-readable instructions are executed by a processor **205**. The processor **205** is configured to receive a request pertaining to at least one packet processing rule change. The processor **205** is further configured to identify a Data Plane (DP) core from a plurality of DP cores **408**. The DP core is identified based on a session ID included in the request. The processor **205** is further configured to apply a lock to the identified DP core. The remaining DP cores of the plurality of DP cores **408** remain in an unlocked state. The processor **205** is further configured to update the at least one packet processing rule change utilizing the locked DP core.

[0080] The present invention further discloses a non-transitory computer-readable medium having stored thereon computer-readable instructions. The computer-readable instructions are executed by a processor **205** upon identifying the DP core from the plurality of DP cores **408**. The processor **205** is configured to retrieve the session ID of at least one User Equipment (UE) **110** from the request. The processor **205** is further configured to determine an Internet Protocol (IP) address of the at least UE based on the session ID and a UE IP table **404**. The UE IP table **404** corresponds to a mapping database that associates session IDs with the respective IP addresses of the UEs **110**. The processor **205** is further configured to apply a hash function to the determined IP address in order to map the determined IP address to a specific DP core. The processor **205** is further configured to receive, details pertaining to the specific DP core based on applying the hash function to the determined IP address, the details

include one of an identity of the specific DP core, location of the specific DP core within the network, thereby identifying the DP core from the plurality of DP cores 408.

[0081] A person of ordinary skill in the art will readily ascertain that the illustrated embodiments and steps in description and drawings (FIG.1-5) are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0082] The present disclosure incorporates technical advancement of applying rule changes in a network's packet processing system. For instance, by applying the lock exclusively to the identified Data Plane (DP) core handling packets from the User Equipment (UE), which prevents unnecessary halting or disruption of operations on other DP cores. The optimized resource utilization ensures that the network's resources are not wasted, and that packet processing continues smoothly across all other cores.

[0083] The present disclosure offers several advantages by locking the specific DP core to independently utilize plurality of CPUs with higher throughput, increase scale performance and reduce latency with increasing the number of DP cores which function independently, as that helps in spreading a load between the DP cores thus reducing the average reception queue length per core. The uplink/downlink traffic of the UE is pinned to the specific DP core, which reduces synchronization overheads and global cache invalidations and increases cache effectiveness by localizing the session specific structures per core.

[0084] The present invention offers multiple advantages over the prior art and the above listed are a few examples to emphasize on some of the advantageous features. The listed advantages are to be read in a non-limiting manner.

REFERENCE NUMERALS

- [0085] Environment - 100;
- [0086] Network - 105;
- [0087] User Equipment - 110;
- [0088] Server - 115;
- [0089] System - 120;
- [0090] Processor -205;
- [0091] Memory – 210;
- [0092] Communication interface– 215;
- [0093] Receiving Module- 220;
- [0094] Identifying Module - 225;
- [0095] Applying Module - 230;
- [0096] Updating Module - 235;
- [0097] Database - 240;
- [0098] One or more primary processors – 305;
- [0099] Memory unit– 310;
- [00100] SMF- 402;
- [00101] UE IP Table- 404;
- [00102] Hash operator – 406;
- [00103] Plurality of Data Plane cores- 408.

We Claim:

1. A method (500) of handling packet processing rules in a network (105), the method (500) comprising the steps of:
 - receiving (505), by one or more processors (205), a request pertaining to at least one packet processing rule change;
 - identifying (510), by the one or more processors (205), a Data Plane (DP) core from a plurality of DP cores (408), wherein the DP core is identified based on a session ID included in the request;
 - applying (515), by the one or more processors (205), a lock to the identified DP core, wherein the remaining DP cores of the plurality of DP cores (408) remain in an unlocked state; and
 - updating (520), by the one or more processors (205), the at least one packet processing rule change utilizing the locked DP core.
2. The method (500) as claimed in claim 1, wherein the locked DP core is unlocked post updating the at least one packet processing rule change, thereby the DP core is adapted to process packets for an at least one User Equipment (UE) (110).
3. The method (500) as claimed in claim 1, wherein the at least one packet processing rule is associated with the at least one user equipment (110).
4. The method (500) as claimed in claim 1, wherein the request is triggered due to occurrence of network related events, wherein the network related events is one of, handover, idle event, active event, barring, and quota consumption.
5. The method (500) as claimed in claim 1, wherein the session ID serves as an identifier assigned to one of, a session and a connection, established between the network (105) and at least one user equipment (110).

6. The method (500) as claimed in claim 1, wherein identifying, by the one or more processors (205), the DP core from the plurality of DP cores comprises the steps of:
 - retrieving, the session ID of at least one UE (110) from the request;
 - determining, an Internet Protocol (IP) address of the at least one UE (110) based on the session ID and a UE IP table (404), the UE IP table (404) corresponds to a mapping database that associates session IDs with the respective IP address of the UEs (110);
 - applying, a hash function to the determined IP address in order to map the determined IP address to a specific DP core; and
 - receiving, details pertaining to the specific DP core based on applying the hash function to the determined IP address, the details include one of an identity of the specific DP core, location of the specific DP core within the network (105), thereby identifying the DP core from the plurality of DP cores (408).
7. The method (500) as claimed in claim 1, wherein the step of, applying, a lock to the identified DP core, includes the step of:
 - transmitting, by the one or more processors (205), a lock command to the identified DP core to halt one or more operations pertaining to the identified DP core.
8. A non-transitory computer-readable medium having stored thereon computer-readable instructions that, when executed by a processor (205), cause the processor (205) to:
 - receive a request pertaining to at least one packet processing rule change;
 - identify a Data Plane (DP) core from a plurality of DP cores (408), wherein the DP core is identified based on a session ID included in the request;
 - apply a lock to the identified DP core, wherein the remaining DP cores of the plurality of DP cores remain in an unlocked state; and

update the at least one packet processing rule change utilizing the locked DP core.

9. The non transitory computer-readable medium as claimed in claim 8, wherein to identify the DP core from a plurality of DP cores (408), cause the processor (205) to:

retrieve, the session ID of the at least one UE (110) from the request;

determine, an Internet Protocol (IP) address of the at least UE (110) based on the session ID and a UE IP table (404), the UE IP table (404) corresponds to a mapping database that associates session IDs with the respective IP address of the UEs (110);

apply, a hash function to the determined IP address in order to map the determined IP address to a specific DP core; and

receive, details pertaining to the specific DP core based on applying the hash function to the determined IP address, the details include one of an identity of the specific DP core, location of the specific DP core within the network, thereby identifying the DP core from the plurality of DP cores (408).

10. A system (120) of handling packet processing rules in a network, the system (120) comprising:

receiving module (220) configured to receive a request pertaining to at least one packet processing rule change;

identifying module (225) configured to identify a Data Plane (DP) core from a plurality of DP cores (408) based on a session ID included in the received request;

applying module (230) configured to apply a lock to the identified DP core, wherein the remaining DP cores of the plurality of DP cores (408) remain in an unlocked state; and

updating module (235) configured to update the at least one packet processing rule change utilizing the locked DP core.

11. The system (120) as claimed in claim 10, wherein the one or more processors (205) is further configured to unlock the locked DP core post updating the at least one packet processing rule change, thereby the DP core is adapted to process packets for a User Equipment (110).
12. The system (120) as claimed in claim 10, wherein the at least one packet processing rule is associated with the at least one User Equipment (110).
13. The system (120) as claimed in claim 10, wherein the request is triggered due to occurrence of network related events, wherein the network related events is one of, handover, idle event, active event, barring, and quota consumption.
14. The system (120) as claimed in claim 10, wherein the session ID serves as an identifier assigned to one of, a session and a connection, established between the network (105) and the at least one UE (110).
15. The system (120) as claimed in claim 10, wherein to identify the DP core from a plurality of DP cores (408), the one or more processors (205) is configured to:
 - retrieve, the session ID of at least one User Equipment (UE) (110) from the request;
 - determine, an Internet Protocol (IP) address of the at least UE (110) based on the session ID and a UE IP table (404), the UE IP table (404) corresponds to a mapping database that associates session IDs with the respective IP address of the UEs (110);
 - apply, a hash function to the determined IP address in order to map the determined IP address to a specific DP core; and
 - receive, details pertaining to the specific DP core based on applying the hash function to the determined IP address, the details include one of an identity of

the specific DP core, location of the specific DP core within the network (105), thereby identifying the DP core from the plurality of DP cores (408).

16. The system (120) as claimed in claim 10, wherein the applying module (230) is further configured to:

transmit, a lock command to the identified DP core to halt one or more operations pertaining to the identified DP core.

17. A User Equipment (UE) (110) comprising:

one or more primary processors (305) communicatively coupled to one or more processors (205) in a system, the one or more primary processors (305) coupled with a memory (310), wherein said memory (310) stores instructions which when executed by the one or more primary processors (305) causes the UE (110) to:

generate and transmit a request pertaining to at least one packet processing rule change to the one or more processors (205);

wherein the one or more processors (205) are configured to perform the steps as claimed in claim 1.

1/5

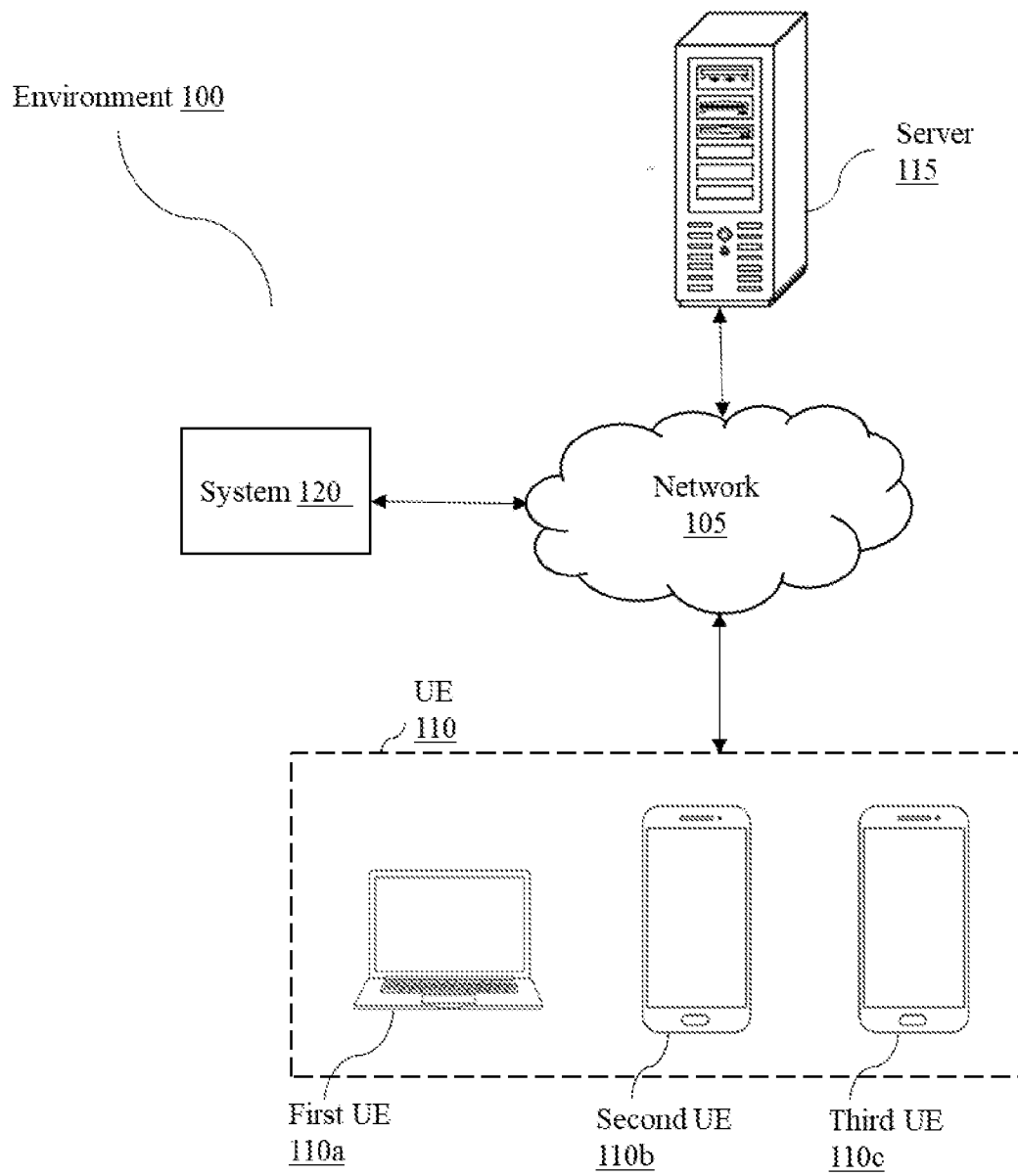


FIG. 1

2/5

System 120

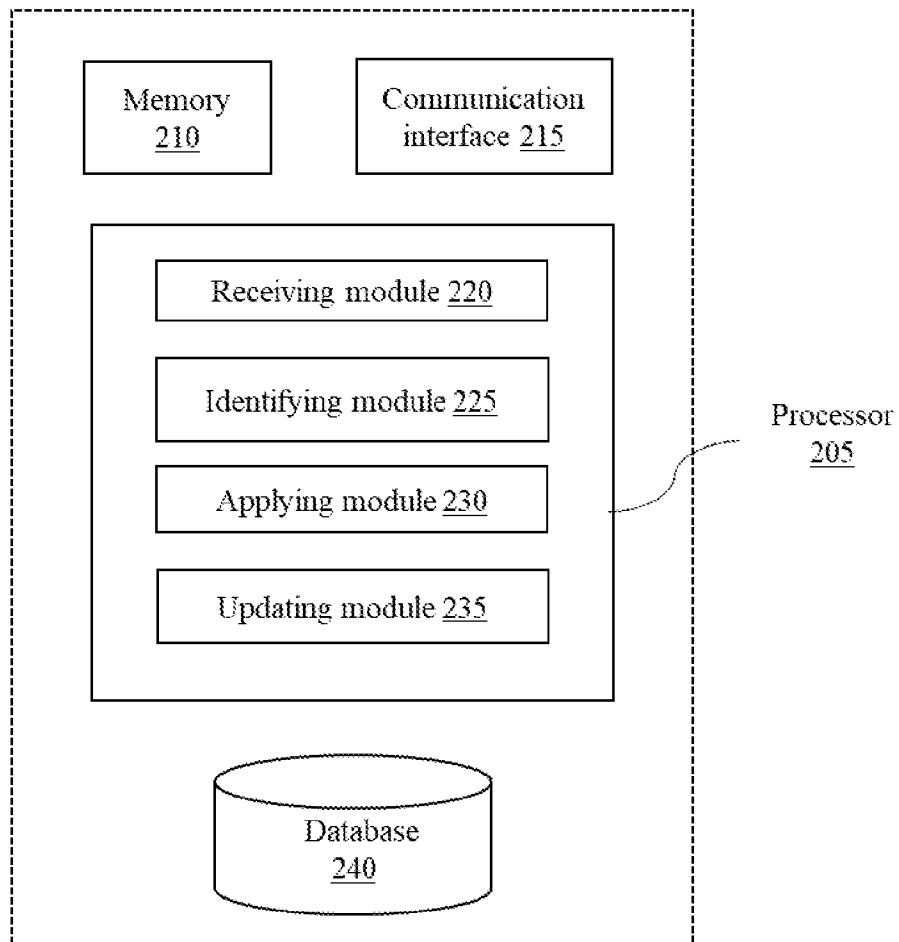


FIG. 2

3/5

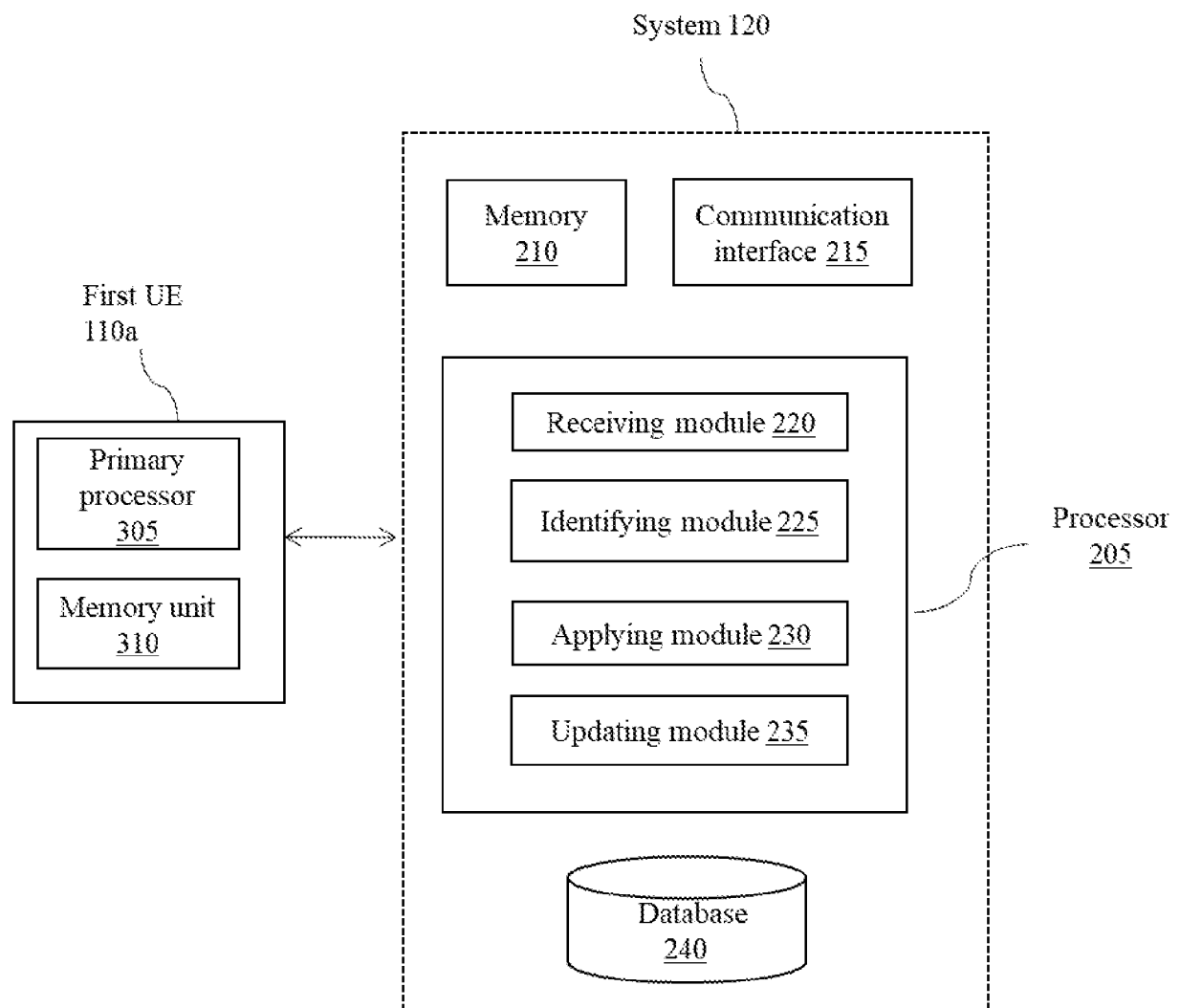


FIG. 3

4/5

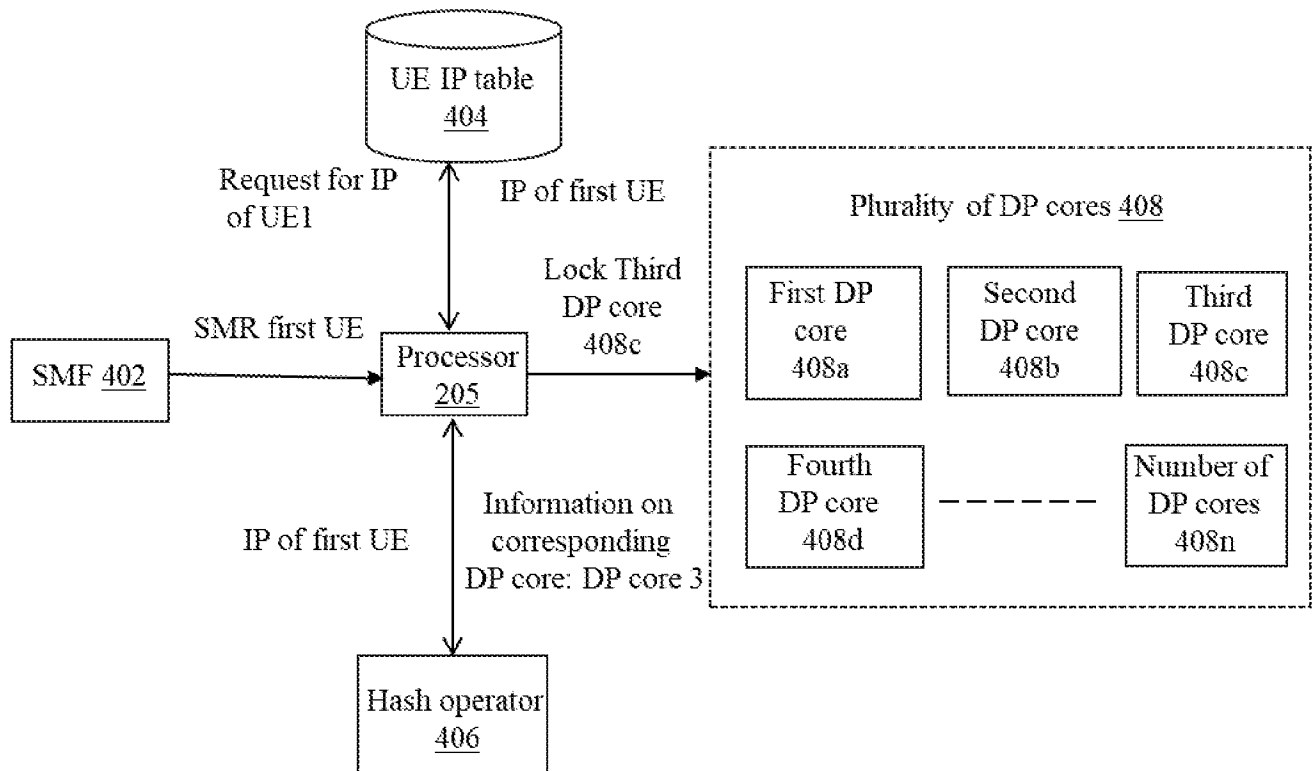


FIG. 4

5/5

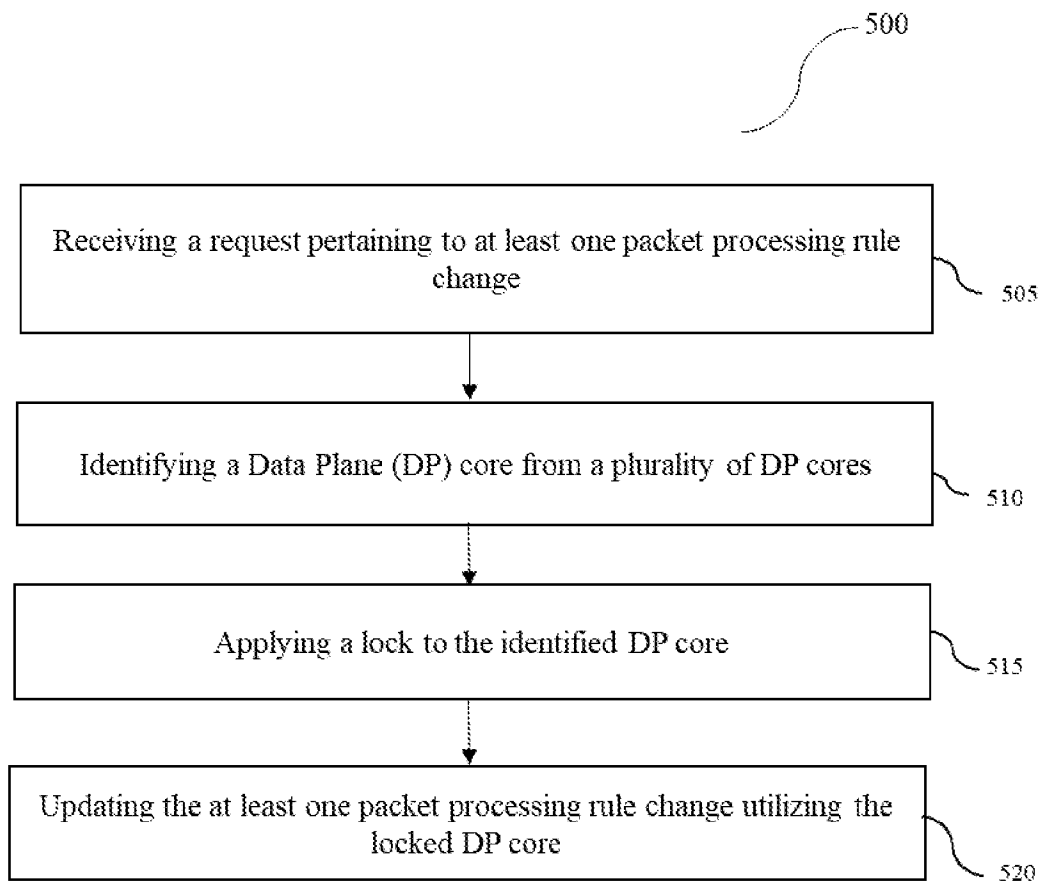


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/050959

A. CLASSIFICATION OF SUBJECT MATTER
H04L69/22, H04L47/2441, H04L45/00 Version=2024.01

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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

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

Databases: PatSeer, IPO Internal Database
Keywords: Rule, policies, packet, data plane

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US10511669B2 (VERIZON PATENT AND LICENSING INC) 17 December 2019 (17/12/2019) Whole document	1-17
Y	US10122735B1 (MARVELL ISRAEL MISL LTD) 06 November 2018 (06/11/2018) Whole document	1-17

☐ 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	"I" 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
"D" document cited by the applicant in the international application	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search

30-10-2024

Date of mailing of the international search report

30-10-2024

Name and mailing address of the ISA/

Indian Patent Office
Plot No.32, Sector 14, Dwarka, New Delhi-110075
Facsimile No.

Authorized officer

Shagun Garg

Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/IN2024/050959

Citation	Pub.Date	Family	Pub.Date
US 10511669 B2	17-12-2019	US 20190335002 A1	31-10-2019