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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
09 January 2025 (09.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/008968 A1

(51) International Patent Classification:
H04L 65/1016 (2022.01) *H04L 65/1069* (2022.01)
H04L 65/1104 (2022.01)

(21) International Application Number:
PCT/IN2024/050955

(22) International Filing Date:
27 June 2024 (27.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202321044343 03 July 2023 (03.07.2023) 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**; Tower-7, 15B, Beverly Park, Sector-14 Koper Khairane, Maharashtra, Navi Mumbai 400701 (IN). **BISHT, Birendra**; B-2101, Yashaskaram CHS, Plot -39, Sector -27, Kharghar, Maharashtra, Navi Mumbai 410210 (IN). **SINGH, Harbinder Pal**; Wing B1, Flat No 402, Lakhani Suncoast, Sector 15, CBD Belapur, Maharashtra, Navi Mumbai 400614 (IN). **KUMAR, Abhay**; River Dale C-105, Casa Rio, Palava City, Dombivli East, Maharashtra, Dombivli East 4212204 (IN). **KELKAR, Priti**; A-205, The NEST CHSL, Near Nandanvan Industrial Estate, Off telephone exchange Road, Behind Parmeshwari Center, Mulund (West), Mumbai 400080 (IN). **ESLAVATH, Mahendra**; 14-2-322/1/a, Behind SFS school, Maruthi nagar, Ballepalli, Telanagana, Khammam 507002 (IN). **VERMA, Himanshu**; C-14, Guru Nanak Pura, Modi Nagar, Uttar Pradesh, Ghaziabad 201204 (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: METHOD AND SYSTEM OF HANDLING SESSION INITIATION PROTOCOL PACKETS DISTRIBUTION IN A NETWORK

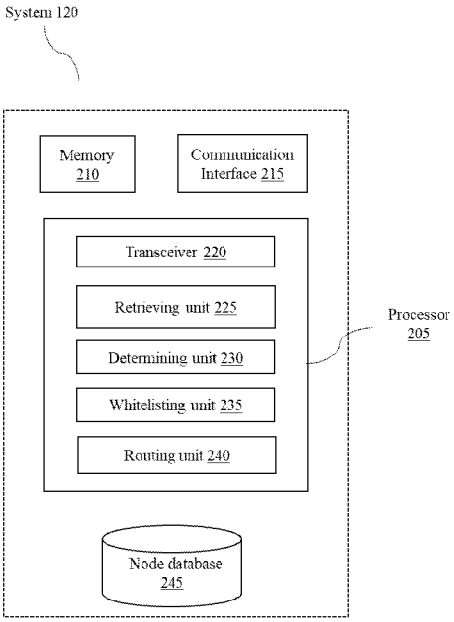

FIG. 2

(57) Abstract: The present disclosure relates to a system (120) and a method (500) of handling Session Initiation Protocol (SIP) packets distribution in a network. The method includes the step of receiving one or more SIP packets addressed to at least one IP Multimedia Subsystem (IMS) node from a User Equipment (UE) (110). The method includes the step of retrieving a relevant fully qualified domain name (FQDN) associated with the at least one IMS node and one or more IP addresses. The method includes the step of determining a status of the at least one IMS node as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses. The method includes the step of routing the received SIP packet to the at least one IMS node when the status of the at least one IMS node is determined as available or blacklisted.

WO 2025/008968 A1

[Continued on next page]

(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))*

METHOD AND SYSTEM OF HANDLING SESSION INITIATION PROTOCOL PACKETS DISTRIBUTION IN A NETWORK

FIELD OF THE INVENTION

[0001] The present invention generally relates to wireless communication networks, and more particularly relates to a method and system for handling Session Initiation Protocol (SIP) packets distribution in the networks.

BACKGROUND OF THE INVENTION

[0002] The IP Multimedia Subsystem (IMS) network is a framework for delivering multimedia services over IP networks. It provides a standardized architecture for integrating various communication services, such as voice, video, and messaging, into a single network. The IMS network consists of several nodes, including Application Server (AS) nodes and Media Gateway Control Function (MGCF) nodes, which play crucial roles in the system.

[0003] When a node in the IMS system goes down, such as the AS node or the MGCF node, it can lead to several problems. One of the main issues is service disruption. The affected node may be responsible for handling specific services or functionalities, and its failure can result in the loss of those services. For example, if an AS node responsible for handling voice calls goes down, users may experience call failures or an inability to initiate new calls.

[0004] Another problem that can occur is a loss of network redundancy. In an IMS network, redundancy is often built into the system to ensure high availability and fault tolerance. When a node fails, it can disrupt the redundancy mechanisms, potentially leading to a single point of failure. This can make the network more vulnerable to further failures and increase the risk of service outages.

[0005] 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 session initiation protocol packets distribution in the network.

BRIEF SUMMARY OF THE INVENTION

[0006] One or more embodiments of the present disclosure provide a method and system of handling Session Initiation Protocol (SIP) packets distribution in a network.

[0007] In one aspect of the present invention, the method of handling Session Initiation Protocol (SIP) packets distribution in the network is disclosed. The method includes the step of receiving, by one or more processors, one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node from a User Equipment (UE). The method includes the step of retrieving, by the one or more processors, from a node database, a relevant fully qualified domain name (FQDN) associated with the at least one IMS node. The method further includes the step of retrieving, by the one or more processors, one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node from a Domain Name System (DNS) unit. The method includes the step of determining, by the one or more processors, a status of the at least one IMS node as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node with a pre-defined threshold. The method includes the step of routing, by the one or more processors, the received SIP packet to the at least one IMS node when the status of the at least one IMS node is determined as available. The method further includes the step of routing, by the one or more processors, the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node is determined as blacklisted.

[0008] In one embodiment, the node database includes a list of FQDNs corresponding to a plurality of IMS nodes.

[0009] In another embodiment, the status of the at least one IMS node is determined as blacklisted, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node is equal to or above the pre-defined threshold within a pre-defined time interval.

[0010] In yet another embodiment, the status of the at least one IMS node is determined as available, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node is below the pre-defined threshold within a pre-defined time interval.

[0011] In yet another embodiment, the one or more processors, determines a failure of the one or more IP addresses associated with the at least one IMS node when a response is not received from the at least one IMS node within a pre-defined time interval.

[0012] In yet another embodiment, the pre-defined threshold corresponds to non-allowable number of failures for the one or more IP addresses associated with the at least one IMS node.

[0013] In yet another embodiment, the at least one blacklisted IMS node is whitelisted subsequent to a pre-determined time period based on a type of the at least one IMS node.

[0014] In yet another embodiment, the type of the at least one IMS node includes at least one of, an Application Server (AS) node or a Media Gateway Control Function (MGCF) node.

[0015] In yet another embodiment, the one or more processors determines the subsequent available IMS node by checking, at a pool including the at least one blacklisted IMS node and a plurality of IMS nodes that share similar characteristics and/or functionalities related to the at least one blacklisted IMS node. The one or more processors determines the subsequent available IMS node by identifying, the subsequent available IMS node present in the pool in response to determining that the number of failures of the one or more IP addresses associated with the said IMS node is below the pre-defined threshold within the pre-defined time interval.

[0016] In another aspect of the present invention, a system for handling Session Initiation Protocol (SIP) packets distribution in a network is disclosed. The system includes a transceiver, configured to receive, one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node from a User Equipment (UE). The system includes a retrieving unit configured to retrieve, from a node database, a relevant fully qualified domain name (FQDN) associated with the at least one IMS node. The system further includes the retrieving unit configured to retrieve, one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node from a Domain Name System (DNS) unit. The system includes a determining unit, configured to, determine, a status of the at least one IMS node as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node with a pre-defined threshold. The system includes a routing unit, configured to route the received SIP packet to the at least one IMS node when the status of the at least one IMS node is determined as available. The system further includes a routing unit, configured to route the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node is determined as blacklisted.

[0017] In another aspect of the present invention, a User Equipment (UE) is disclosed. The UE includes one or more primary processors and a memory. The one or more primary processors are coupled with one or more processors. The memory stores instructions which when executed by the one or more primary processors causes the UE to transmit Session Initiation Protocol (SIP) packets to a network in order to avail one or more services.

[0018] 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

[0019] 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.

[0020] **FIG. 1** is an exemplary block diagram of an environment of handling Session Initiation Protocol (SIP) packets distribution in a network, according to one or more embodiments of the present disclosure;

[0021] **FIG. 2** is an exemplary block diagram of a system of handling the SIP packets distribution in the network, according to one or more embodiments of the present disclosure;

[0022] **FIG. 3** is a schematic representation of the present system of **FIG. 1** workflow, according to one or more embodiments of the present disclosure;

[0023] **FIG. 4** illustrates an exemplary block diagram of workflow between one or more processors, and a first pool, according to one or more embodiments of the present disclosure; and

[0024] **FIG. 5** is a flow diagram illustrating a method of handling SIP packets distribution in the network, according to one or more embodiments of the present disclosure.

[0025] The foregoing shall be more apparent from the following detailed description of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0026] 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.

[0027] 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.

[0028] 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.

[0029] In a preferred embodiment, the system and method are configured to obtain FQDN (Fully Qualified Domain Name) corresponding to the IP Multimedia Subsystem (IMS) nodes of the IP network. Based on the obtained FQDNs, the system determines IP addresses corresponding to the IMS nodes and subsequently, based on the IP addresses, determines the health of the IMS nodes as either available or blacklisted. Accordingly, when the system has to send one or more Session Initiation Protocol (SIP) packets to the IMS node in an IMS network, the system is able to efficiently handle the SIP packet as per the health of the destination IMS node.

[0030] **FIG. 1** illustrates an exemplary block diagram of an environment **100** of handling Session Initiation Protocol (SIP) packets distribution in a network **105,** according to one or more embodiments of the present disclosure. The environment **100** includes the network **105**, a User Equipment (UE) **110**, a server **115**, a system **120,** and at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node **125**. The UE **110** aids a user to interact with the system **120** for transmitting Session Initiation Protocol (SIP) packets to the network **105** in order to avail one or more services.

[0031] The term "at least one IMS node" and "plurality of IMS nodes" are used interchangeably hereinafter, without limiting the scope of the invention.

[0032] The term "SIP packet" could be referred to as "one or more SIP packets", hereinafter, without limiting the scope of the invention.

[0033] For the purpose of description and explanation, the description will be explained with respect to one or more UEs **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 **110** is configured to connect to the server **115** via the network **105**.

[0034] 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.

[0035] In accordance with one aspect of the present invention, each of the first UE **110a**, the second UE **110b**, and the third UE **110c** is configured to facilitate the transmission of a request via the network **105** for the purpose of availing a variety of services. The scope of said services is inclusive of, but not limited to, engaging with the server **115** for the purpose of submitting a request thereto and transmitting SIP packets to the network **105**, all aforementioned activities being conducted over the network **105**. This configuration enables a streamlined and efficient interaction between the UE **110** and the network resources, thereby enhancing the utility and performance of the network **105** in providing said services.

[0036] 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.

[0037] 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.

[0038] 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.

[0039] The environment **100** further includes the at least one IMS node **125** 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 at least one IMS node **125**, in the context of telecommunications and networking, refers to an element within an IP Multimedia Subsystem (IMS) architecture. The at least one IMS node **125** is a framework for delivering multimedia and communication services over IP networks, including voice, video, messaging, and data services. The at least one IMS node **125** works together to provide these services in a standardized and interoperable manner.

[0040] The at least one IMS node **125** includes an Application Server (AS) node **130**, and a Media Gateway Control Function (MGCF) node **135.** The AS node **130** refers to a component in a network architecture that is responsible for running and managing applications, services, and processes. The AS node **130** typically provides a platform where applications can be deployed, executed, and accessed by clients or users over the network **105**. The MGCF node **135** is a key component in

telecommunications networks, specifically in the context of Voice over Internet Protocol (VoIP) and the IMS architectures. The MGCF node **135** is responsible for controlling the flow of media (voice, video, data) between circuit-switched networks (such as traditional telephone networks) and packet-switched networks (such as IP networks).

[0041] 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.

[0042] Operational and construction features of the system **120** will be explained in detail with respect to the following figures.

[0043] Referring to **FIG. 2**, **FIG. 2** illustrates an exemplary block diagram of the system **120** of handling SIP packets distribution 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**, a communication interface **215,** and a node database **245**. 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.

[0044] The information related to the request pertaining to handling SIP packets distribution is 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.

[0045] The information related to the request pertaining to handling the SIP packets distribution is 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 **120**. In one embodiment, the communication interface **215** provides a communication pathway for one or more components of the system **120**. Examples of the one or more components include, but are not limited to, the UE **110** and the node database **245**.

[0046] The node database **245** is configured to store the request pertaining to handling the SIP packets distribution which is transmitted by the UE **110**. Further, the node database **245** provides structured storage, support for complex queries, and enables efficient data retrieval and analysis. The node database **245** 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.

[0047] 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.

[0048] In order for the system **120** to handle the SIP packets distribution in the network **105**, the processor **205** includes a transceiver **220**, a retrieving unit **225**, a determining unit **230**, a whitelisting unit **235** and a routing unit **240** communicably coupled to each other for handling the SIP packets distribution in the network **105.**

[0049] The transceiver **220**, the retrieving unit **225**, the determining unit **230**, the whitelisting unit **235**, and the routing unit **240,** 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.

[0050] The transceiver **220** is configured to receive the one or more SIP packets addressed to the at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node **125** from the UE **110.** The one or more Session Initiation Protocol (SIP) is a signaling protocol that enables a Voice Over Internet Protocol (VoIP) by defining the messages sent between endpoints and managing the actual elements of a call. The SIP supports voice calls, video conferencing, instant messaging, and media distribution. The SIP packets refer to the messages exchanged between the UE **110** or applications in a SIP-based communication system. The one or more SIP packets are used to initiate, modify, and terminate communication sessions between users. The at least one IMS node **125** is a network element that implements the IP Multimedia Subsystem architecture, which is a standardized framework for delivering multimedia services over IP networks. The at least one IMS node **125** facilitates the integration of various communication services, including voice, video, messaging, and presence, over IP-based networks.

[0051] On receiving the one or more SIP packets addressed to the at least one IMS node **125** from the UE **110,** the retrieving unit **225** is configured to retrieve from the node database **245**, a relevant Fully Qualified Domain Name (FQDN) associated with the at least one IMS node **125**. The relevant FQDN is referred to as a complete and unique address that specifies the exact location of a specific node within an IMS network. In an embodiment, the node database **245** includes a list of FQDNs corresponding to the at least one IMS node **125**. In an embodiment, the at least one IMS node **125** includes, but not limited to, a first IMS node, and a second IMS node. In an embodiment, each FQDN corresponds to the at least one IMS node **125**, which is the Application Server (AS) node **130**, the Media Gateway Control Function (MGCF) node **135**, or any other node within the IMS system. The FQDNs serve as

identifiers for the nodes and are used for various purposes, such as routing, addressing, and establishing connections within the IMS network.

[0052] The retrieving unit **225** is configured to retrieve one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node **125** from a Domain Name System (DNS) unit. The DNS unit refers to a specific configuration related to DNS servers or services. The DNS unit is a distributed system used to translate domain names into IP addresses to communicate over the network **105**. The DNS unit might indicate a certain capacity, performance level, or configuration aspect of the server **115** or the system **120**.

[0053] In an example, when the retrieving unit **225** initiates the resolution process, it sends DNS queries to the server **115**, providing the FQDNs of the at least one IMS node **125**. The server **115** then looks up the IP addresses associated with each FQDN and returns them to the system **120**. By obtaining the IP addresses through DNS resolution, the retrieving unit **225** establishes connections with the at least one IMS node **125** using the appropriate IP addresses. The retrieving unit **225** allows for communication and interaction between the system **120** and the at least one IMS node **125** within the system **120**.

[0054] Upon retrieving the one or more IP addresses pertaining to the retrieved FQDN corresponding to each of the plurality of IMS nodes, the retrieved one or more IP addresses are stored in the node database **245**. When the retrieving unit **225** resolves the FQDNs of the IMS nodes, it obtains the one or more IP addresses for each node. The one or more IP addresses are stored in the node database **245**. The retrieving unit **225** establishes connections with the IMS nodes using the stored IP addresses, enabling efficient communication and interaction within the system **120.**

[0055] Upon storing the retrieved one or more IP addresses in the node database **245**, the determining unit **230** is configured to determine a status of the at least one IMS node **125** as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node **125** with a pre-defined threshold.

[0056] Accordingly, in one embodiment, the status of the at least one IMS node **125** is determined as blacklisted, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node **125** is equal to or above the pre-defined threshold within a pre-defined time interval. The predefined threshold refers to a specific value or criterion set in advance that serves as a boundary or limit for making decisions or taking actions. In one embodiment, for example, the pre-defined threshold includes 100 SIP packets on the at least one IMS node **125**. The at least one IMS node **125** receives 101 SIP packets. The system **120** is configured to blacklist the AS node **130** for the predetermined time interval.

[0057] In another embodiment, the status of the at least one IMS node **125** is determined as available, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node **125** is below the pre-defined threshold within the pre-defined time interval. In an exemplary embodiment, the predetermined time interval may range from seconds to hours. On completion of the predetermined time interval, the system **120** categorizes the AS node **130** as available, without performing any status check.

[0058] In an example, if the at least one IMS node **125** has more than one corresponding IP addresses and a first IP address is blacklisted, then all the remaining IP addresses for the at least one IMS node **125** are checked. Accordingly, the status of the at least one IMS node **125** is determined based on the availability of the corresponding IP addresses. In an example, if even one corresponding IP address is available, the status of the at least one IMS node **125** is stored as available. In case none of the IP addresses of the at least one IMS node **125** is available, the status of the at least one IMS node **125** is categorized as blacklisted.

[0059] Further, the determining unit **230** is configured to determine a failure of the one or more IP addresses associated with the at least one IMS node **125** when a response is not received from the at least one IMS node **125** within the pre-defined time interval. For instance, in case the at least one IMS node **125** is the AS node **130** the system **120** blacklists the AS node **130** for the predetermined time interval. In an

exemplary embodiment, the predetermined time interval may range from seconds to hours. On completion of the predetermined time interval, the system **120** categorizes the AS node **130** as available, without performing any status check.

[0060] As per the illustrated embodiment, the pre-defined threshold corresponds to non-allowable number of failures for the one or more IP addresses associated with the at least one IMS node **125**. For instance, in case the at least one IMS node **125** is an AS node **130**. The pre-defined threshold includes 500 SIP packets on the AS node **130**. In case the AS node **130** receives 501 SIP packets**,** the system **120** is configured to blacklist the AS node **130** for the predetermined time interval. On completion of the predetermined time interval, the system **120** categorizes the AS node **130** as available, without performing any status check.

[0061] The determining unit **230** is configured to determine the subsequent available IMS node by checking at a pool including the at least one blacklisted IMS node. In an embodiment, the pool includes, but not limited to, a first pool, a second pool, and the like. The pool refers to the plurality of IMS nodes that share similar characteristics or functionalities. The determining unit **230** is configured to determine the subsequent available IMS node by identifying the subsequent available IMS node present in the pool in response to determining that the number of failures of the one or more IP addresses associated with the at least one IMS node **125** is below the pre-defined threshold within the pre-defined time interval.

[0062] The whitelisting unit **235** of the system **120** is configured to whitelist the at least one blacklisted IMS node subsequent to the predefined time interval based on the type of the at least one IMS node **125**. In an embodiment, the type of the at least one IMS node **125** includes at least one of, a plurality of Application Server (AS) nodes **130** or a plurality of Media Gateway Control Function (MGCF) node **135**. In an embodiment, the plurality of AS nodes **130** includes, but not limited to an AS node **130-1**, and an AS node **130-2**.

[0063] When the blacklisted node starts responding to the at least one IMS node **125**, it will be whitelisted again. Thus, whitelisting unit **235** of the at least one IMS

node **125** is done only after ensuring it is in an operational state. In this whitelisting of non-operational nodes is averted and accordingly related failures are avoided, resulting in network resource optimization and reduced overheads.

[0064] On determining the subsequent available IMS node, the routing unit **240** is configured to route the received SIP packets to the at least one IMS node **125** when the status of at least one IMS node **125** is determined as available. If the predefined threshold is not reached, the status of the at least one IMS node **125** is categorized as available.

[0065] Further, the routing unit **240** is configured to route the received SIP packets to the subsequent available IMS node, when the status of the at least one IMS node **125** is determined as blacklisted. If the predefined threshold is reached, the status of the at least one IMS node **125** is categorized as blacklisted. In an example, the routing unit **240** is configured to route the received SIP packets to the second IMS node from the same pool as the first IMS node, when the first IMS node is determined to be not available. The system **120** selects the second IMS node from the same pool as the first IMS node and routes the SIP packets to the second IMS node for ensuring continuity of communication and exchange information to the UE **110**.

[0066] A routing mechanism helps maintain the flow of communication and prevents disruptions caused by the unavailability of the first IMS node. It allows for efficient utilization of resources within the at least one IMS node **125** and ensures that the intended actions or requests are carried out by the alternative node from the same pool. By doing so, the system **120** receives any request sent to unreachable or error-responding node, which can be easily routed to another node, which saves response time. When a failure response is received for a particular node, the particular node can retry the request with a different node under the same pool based on failure response and maintains flexibility in managing access control.

[0067] **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 SIP packets distribution 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.

[0068] As mentioned earlier in **FIG.1**, In an embodiment, the first UE **110a** may encompass electronic apparatuses. These devices are illustrative of, but not restricted to, personal computers, laptops, tablets, smartphones (including phones), or other devices enabled for web connectivity. The scope of the first UE **110a** explicitly extends to a broad spectrum of electronic devices capable of executing computing operations and accessing networked resources, thereby providing users with a versatile range of functionalities for both personal and professional applications. This embodiment acknowledges the evolving nature of electronic devices and their integral role in facilitating access to digital services and platforms. In an embodiment, the first UE **110a** can be associated with multiple users. Each UE **110** is communicatively coupled with the processor **205** via the network **105**.

[0069] The first UE **110a** includes one or more primary processors **305** communicably coupled to the one or more processors **205** of the system **120**. The one or more primary processors **305** are coupled with a memory unit **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 transmit the SIP packets to the network **105** in order to avail one or more services.

[0070] Furthermore, the one or more primary processors **305** within the UE **110** are uniquely configured to execute a series of steps as described herein. This configuration underscores the processor's capability to handle the SIP packets distribution. The operational synergy between the primary processors and the additional processors,

guided by the executable instructions stored in the memory unit **310**, facilitates a seamless handling of the SIP packets distribution.

[0071] As mentioned earlier in **FIG.2**, the one or more processors **205** of the system **120** is configured to receive the one or more SIP packets addressed to at least one IMS node **125** from the UE **110,** retrieve from the node database **245**, the relevant FQDN associated with the at least one IMS node **125**, retrieve one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node **125** from the DNS unit, determine the status of the at least one IMS node **125** as one of, blacklisted and available, and route the received SIP packet to the at least one IMS node **125** when the status of the at least one IMS node **125** is determined as available, and further route the received SIP packet to the subsequent available IMS node, when the status of the at least one IMS node **125** is determined as blacklisted.

[0072] 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.

[0073] Further, the processor **205** includes the transceiver **220**, the retrieving unit **225**, the determining unit **230**, and the routing unit **240**. The operations and functions of the transceiver **220**, the retrieving unit **225**, the determining unit **230**, and the routing unit **240** 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.

[0074] **FIG. 4** illustrates an exemplary block diagram of workflow between the one or more processors **205** of the system **120**, and the first pool, according to one or more embodiments of the present disclosure. It is to be noted that the embodiment with respect to **FIG. 4** will be explained with respect to the first pool for the purpose of description and illustration and should nowhere be construed as limited to the scope of the present disclosure.

[0075] The system **120** includes the UE **110**. The system **120** can monitor traffic and operations related to the first pool of at least one IMS node, for example, Application Server (AS) nodes **130**. Further, the system **120** is connected to the node database **245**. The IP addresses for all the AS nodes **130** are stored. Further, the node database **245** also includes the status of each of the AS node **130**. The status may be either "available" if the AS node **130** is available or "blacklisted" in case the AS node **130** is not available.

[0076] In an exemplary embodiment, the system **120** receives the one or more SIP packets from the UE **110** which is directed towards the AS node **130-1**. On receiving the one or more SIP packets, the system **120** determines the availability of the AS node **130-1** based on the status of the AS node **130** as stored in the node database **245**. In the event that the AS nodes **130-1** is blacklisted, the system **120** is configured to route the SIP packets to another AS node, for example, the AS node **130-2**, from the same pool, i.e., Pool 1. Thus, efficient handling of the SIP packet is ensured. In an example, the other AS or IMS node, is selected from the same pool based on predefined process, such as weightage or priority-based process. In another embodiment, the selection of the other IMS nodes is based on logic or selection defined by an admin.

[0077] Furthermore, in an embodiment, the system **120** is provisioned to allow the admin to selectively operate the IP addresses of the at least one IMS node **125**. For instance, let's consider that the AS nodes **130-1** of pool 1 have at least four ('4') IP addresses. According to the invention, the system **120** provides the admin with an option of making one or more IP addresses act as non-functional. Thus, the network traffic is directed to specific IP addresses, as desired by the admin.

[0078] **FIG. 5** is a flow diagram illustrating a method **500** of handling SIP packets distribution in the network **105**, 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.

[0079] At step **505,** the method **500** includes the step of receiving the one or more SIP packets addressed to the at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node **125** from the UE **110** by the transceiver **220.**

[0080] At step **510,** the method **500** includes the step of retrieving from the node database **245**, the relevant Fully Qualified Domain Name (FQDN) associated with the at least one IMS node **125** by the retrieving unit **225** based on receiving the one or more SIP packets addressed to the at least one IMS node **125** from the UE **110**. The FQDNs serve as identifiers for the nodes and are used for various purposes, such as routing, addressing, and establishing connections within the IMS network.

[0081] At step **515,** the method **500** includes the step of retrieving the one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node **125** from the DNS unit by the retrieving unit **225**.

[0082] At step **520,** the method **500** includes the step of determining the status of the at least one IMS node **125** as one of, blacklisted and available, based on comparing the determined number of failures of the one or more IP addresses associated with the at least one IMS node **125** with the pre-defined threshold by the determining unit **230**.

[0083] At step **525,** the method **500** includes the step of routing the received SIP packets to the at least one IMS node **125** when the status of at least one IMS node **125** is determined as available by the routing unit **240**. If the threshold is not reached, the status of the at least one IMS node **125** is categorized as available.

[0084] At step **530,** the method **500** includes the step of routing the received SIP packet to the subsequent available IMS node by the routing unit **240**, when the status of at least one IMS node **125** is determined as blacklisted. If the threshold is reached,

the status of the at least one IMS node **125** is categorized as blacklisted. In an example, the routing unit **240** is configured to route the received SIP packet to the second IMS node from the same pool as the first IMS node, when the first IMS node is determined to be not available.

[0085] The routing mechanism helps maintain the flow of communication and prevents disruptions caused by the unavailability of the first IMS node. It allows for efficient utilization of resources within the at least one IMS node **125** and ensures that the intended actions or requests are carried out by the alternative node from the same pool. By doing so, the method **500** receives any request sent to unreachable or error-responding node can be easily routed to another node, which saves response time. When a failure response is received for a particular node, the particular node can retry the request with a different node under the same pool based on failure response and maintains flexibility in managing access control.

[0086] The present invention 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 the one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node **125** from a User Equipment (UE) **110**. The processor **205** is configured to retrieve from a node database **245**, a relevant fully qualified domain name (FQDN) associated with the at least one IMS node **125**. The processor **205** is further configured to retrieve one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node **125** from a Domain Name System (DNS) unit. The processor **205** is further configured to determine, a status of the at least one IMS node **125** as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node **125** with a pre-defined threshold. The processor **205** is configured to route the received SIP packet to the at least one IMS node **125** when the status of at least one IMS node **125** is determined as available. The processor **205** is

further configured to route the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node **125** is determined as blacklisted.

[0087] 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.

[0088] The present disclosure incorporates technical advancement of handling Session Initiation Protocol (SIP) packets distribution in the network for retrieving all IP addresses corresponding to the IMS node. This ensures that the system has a comprehensive understanding of the available IP addresses associated with each IMS node. By considering all IP addresses, the accuracy of status determination increases. This allows for more precise assessment of the availability of IMS nodes, enabling packets to be handled more appropriately based on their accurate health status.

[0089] The present invention offers significant advantages by retrieving all IP addresses corresponding to the IMS node. This approach enhances the accuracy of health determination as the system considers the health status of all the IP addresses associated with the node, rather than relying on just one IP address. By considering multiple IP addresses, the system gains a more comprehensive understanding of the node's availability and makes more informed decisions regarding packet handling. This increased accuracy in health determination ensures that packets are handled

appropriately based on the precise status of the IMS node. Consequently, the system can optimize resource allocation, improve network efficiency, and enhance overall performance.

[0090] Another advantage of the invention is the categorization of IMS node health as either "available" or "blacklisted". The status of the at least one node is determined based on predefined conditions, such as the number of failures within a given time interval. This proactive monitoring and categorization of health status allows for efficient management of IMS nodes. It enables the system to make informed decisions regarding routing, load balancing, and resource allocation within the network.

[0091] 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

[0092] Environment - 100;

[0093] Network - 105;

[0094] User Equipment - 110;

[0095] Server - 115;

[0096] System - 120;

[0097] At least one IMS node- 125;

[0098] Application Server node- 130;

[0099] AS node- 130-1;

[00100] AS node- 130-2;

[00101] Media Gateway Control Function node – 135;

[00102] Processor -205;

[00103] Memory – 210;

[00104] Communication interface– 215;

[00105] Transceiver- 220;

[00106] Retrieving unit - 225;

[00107] Determining unit - 230;

[00108] Whitelisting unit- 235;

[00109] Routing unit- 240;

[00110] Node database - 245;

[00111] One or more primary processors – 305;

[00112] Memory of user equipment – 310.

We Claim:

1. A method (500) of handling Session Initiation Protocol (SIP) packets distribution in a network (105), the method (500) comprises the steps of:

receiving (505), by one or more processors (205), one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node (125) from a User Equipment (UE) (110);

retrieving (510), by the one or more processors (205), from a node database (245), a relevant fully qualified domain name (FQDN) associated with the at least one IMS node (125);

retrieving (515), by the one or more processors (205), one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node (125) from a Domain Name System (DNS) unit;

determining (520), by the one or more processors (205), a status of the at least one IMS node (125) as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node (125) with a pre-defined threshold;

routing (525), by the one or more processors (205), the received SIP packet to the at least one IMS node (125) when the status of the at least one IMS node (125) is determined as available; and

routing (530), by the one or more processors (205), the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node (125) is determined as blacklisted.

2. The method (500) as claimed in claim 1, wherein the node database (245) includes a list of FQDNs corresponding to a plurality of IMS nodes.

3. The method (500) as claimed in claim 1, wherein the status of the at least one IMS node (125) is determined as blacklisted, when the determined number of failures of the one or more IP addresses associated with the at least one IMS

node (125) is equal to or above the pre-defined threshold within a pre-defined time interval.

4. The method (500) as claimed in claim 1, wherein the status of the at least one IMS node (125) is determined as available, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node (125) is below the pre-defined threshold within a pre-defined time interval.

5. The method (500) as claimed in claim 1, wherein the one or more processors (205), determines a failure of the one or more IP addresses associated with the at least one IMS node (125) when a response is not received from the at least one IMS node (125) within a pre-defined time interval.

6. The method (500) as claimed in claim 1, wherein the pre-defined threshold corresponds to non-allowable number of failures for the one or more IP addresses associated with the at least one IMS node.

7. The method (500) as claimed in claim 1, wherein the at least one blacklisted IMS node is whitelisted subsequent to a pre-determined time period based on a type of the at least one IMS node (125).

8. The method (500) as claimed in claim 7, wherein the type of the at least one IMS node (125) includes at least one of, an Application Server (AS) node (130) or a Media Gateway Control Function (MGCF) node (135).

9. The method (500) as claimed in claim 1, wherein the one or more processors (205) determines the subsequent available IMS node by:

checking, at a pool including the at least one blacklisted IMS node and the plurality of IMS nodes that share similar characteristics and/or functionalities related to the at least one blacklisted IMS node; and

identifying, the subsequent available IMS node present in the pool in response to determining that the number of failures of the one or more IP addresses associated with the said IMS node is below the pre-defined threshold within the pre-defined time interval.

10. A User Equipment (UE) (110), comprising:

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

transmit, Session Initiation Protocol (SIP) packets to a network (105) in order to avail one or more services; and

wherein the one or more processors (205) is further configured to perform the method as claimed in claim 1.

11. A system (120) of handling Session Initiation Protocol (SIP) packets distribution in a network (105), the system (120) comprising:

a transceiver (220), configured to, receive, one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node (125) from a User Equipment (UE) (110);

a retrieving unit (225), configured to:

retrieve, from a node database (245), a relevant fully qualified domain name (FQDN) associated with the at least one IMS node (125);

retrieve, one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node (125) from a Domain Name System (DNS) unit;

a determining unit (230), configured to, determine, a status of the at least one IMS node (125) as one of, blacklisted and available, based on comparing a

determined number of failures of the one or more IP addresses associated with the at least one IMS node (125) with a pre-defined threshold; and

a routing unit (240), configured to:

route, the received SIP packet to the at least one IMS node (125) when the status of the at least one IMS node (125) is determined as available; and

route, the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node (125) is determined as blacklisted.

12. The system (120) as claimed in claim 11, wherein the node database (245) includes a list of FQDNs corresponding to a plurality of IMS nodes.

13. The system (120) as claimed in claim 11, wherein the status of the at least one IMS node (125) is determined as blacklisted, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node (125) is equal to or above the pre-defined threshold within a pre-defined time interval.

14. The system (120) as claimed in claim 11, wherein the status of the at least one IMS node (125) is determined as available, when the determined number of failures of the one or more IP addresses associated with the at least one IMS node (125) is below the pre-defined threshold within a pre-defined time interval.

15. The system (120) as claimed in claim 11, wherein the determining unit (230), determines a failure of the one or more IP addresses associated with the at least one IMS node (125) when a response is not received from the at least one IMS node (125) within a pre-defined time interval.

16. The system (120) as claimed in claim 11, wherein the pre-defined threshold corresponds to non-allowable number of failures for the one or more IP addresses associated with the at least one IMS node (125).

17. The system (120) as claimed in claim 11, wherein a whitelisting unit (235) of the system, whitelists the at least one blacklisted IMS node subsequent to a pre-determined time period based on a type of the at least one IMS node (125).

18. The system (120) as claimed in claim 11, wherein the type of the at least one IMS node (125) includes at least one of, an Application Server (AS) node (130) or a Media Gateway Control Function (MGCF) node (135).

19. The system (120) as claimed in claim 11, wherein the determining unit (230), determines the subsequent available IMS node by:

checking, at a pool including the at least one blacklisted IMS node and the plurality of IMS nodes that share similar characteristics and/or functionalities related to the at least one blacklisted IMS node; and

identifying, the subsequent available IMS node present in the pool in response to determining that the number of failures of the one or more IP addresses associated with the said IMS node is below the pre-defined threshold within the pre-defined time interval.

20. A non-transitory computer-readable medium having stored thereon computer-readable instructions that, when executed by a processor (205), causes the processor (205) to:

receive, one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node (125) from a User Equipment (UE) (110);

retrieve, from a node database (245), a relevant fully qualified domain name (FQDN) associated with the at least one IMS node (125);

retrieve, one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node (125) from a Domain Name System (DNS) unit;

determine, a status of the at least one IMS node (125) as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node (125) with a pre-defined threshold; and

route, the received SIP packet to the at least one IMS node (125) when the status of the at least one IMS node (125) is determined as available; and

route, the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node (125) is determined as blacklisted.

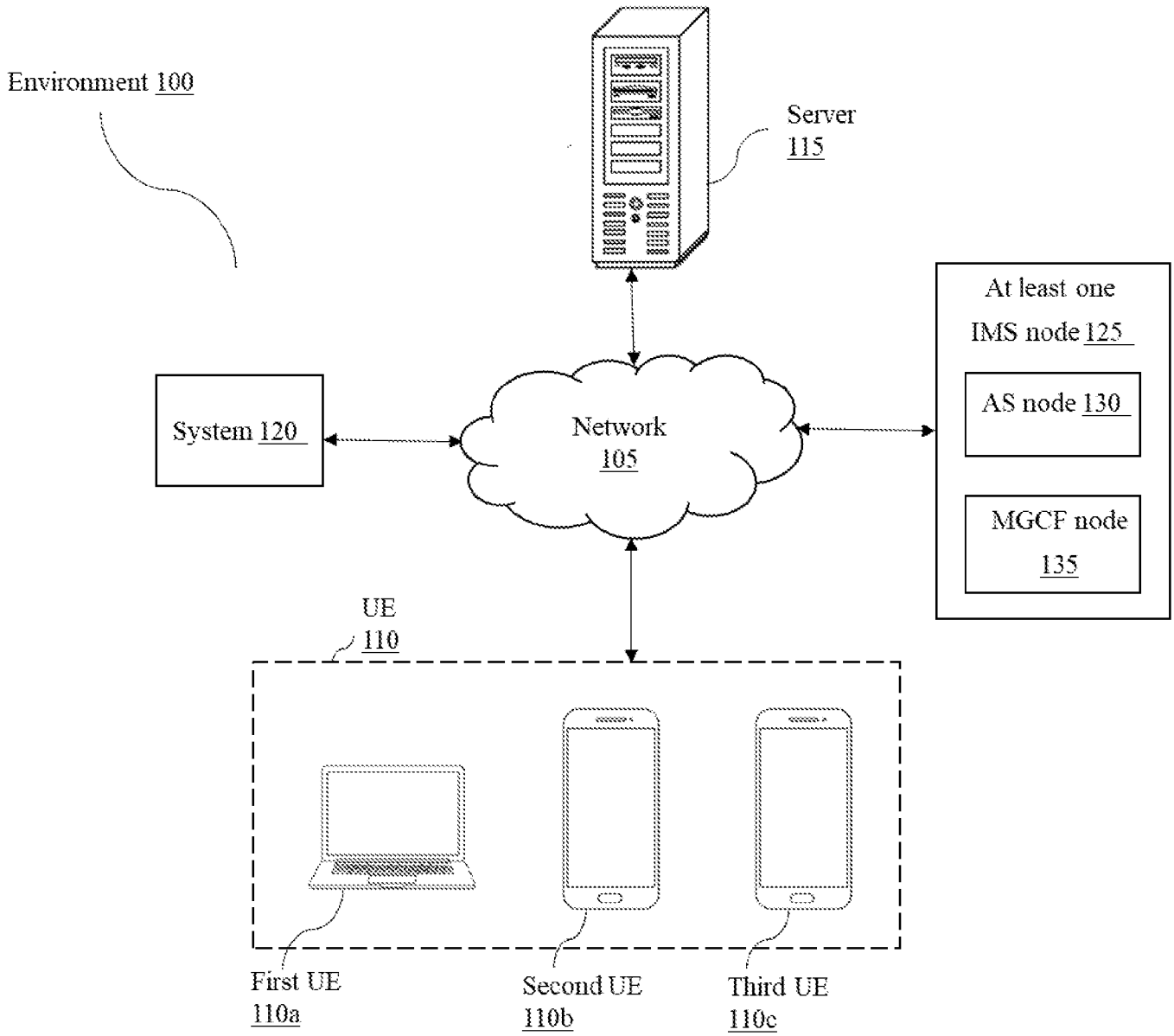
Environment 100
Server 115
At least one IMS node 125
AS node 130
MGCF node 135
System 120
Network 105
UE 110
First UE 110a
Second UE 110b
Third UE 110c

FIG. 1

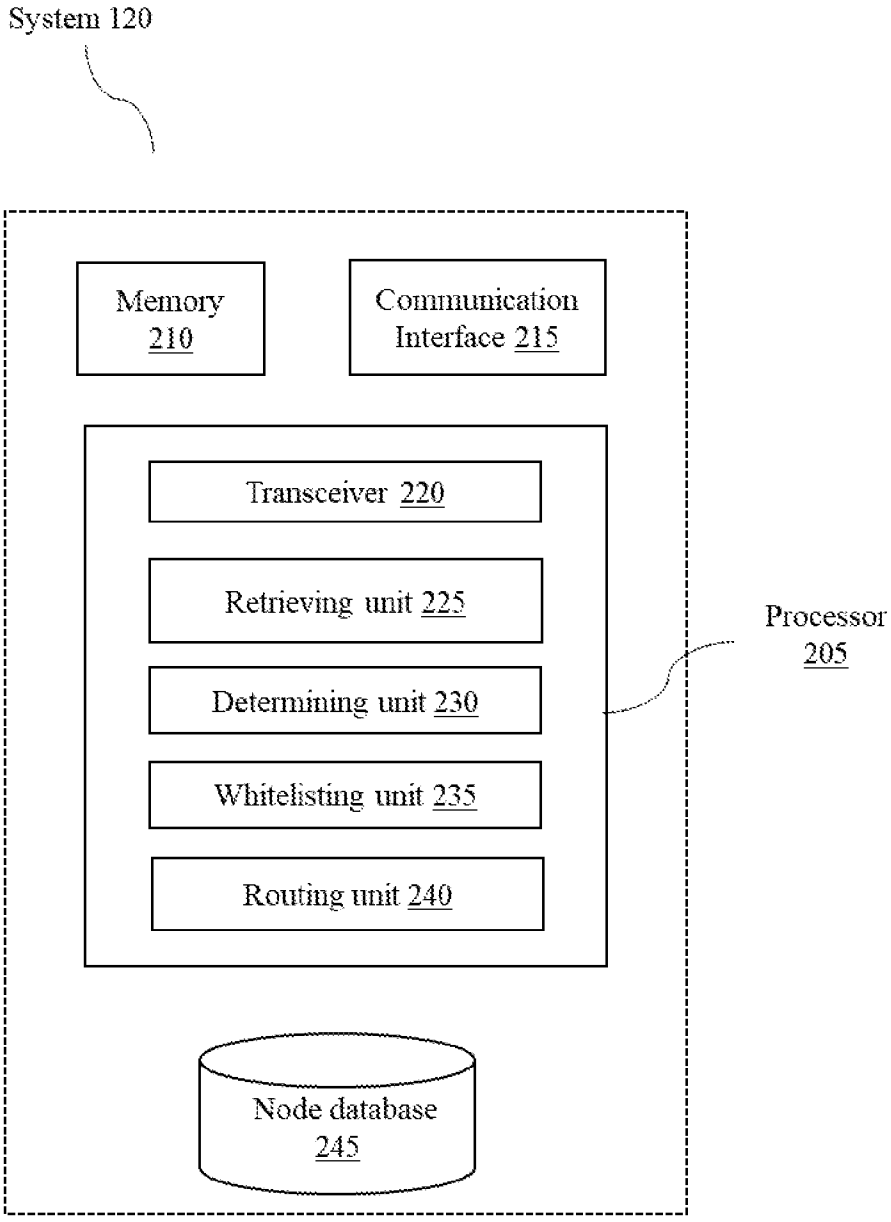
System 120
Memory 210
Communication Interface 215
Transceiver 220
Retrieving unit 225
Determining unit 230
Whitelisting unit 235
Routing unit 240
Processor 205
Node database 245

FIG. 2

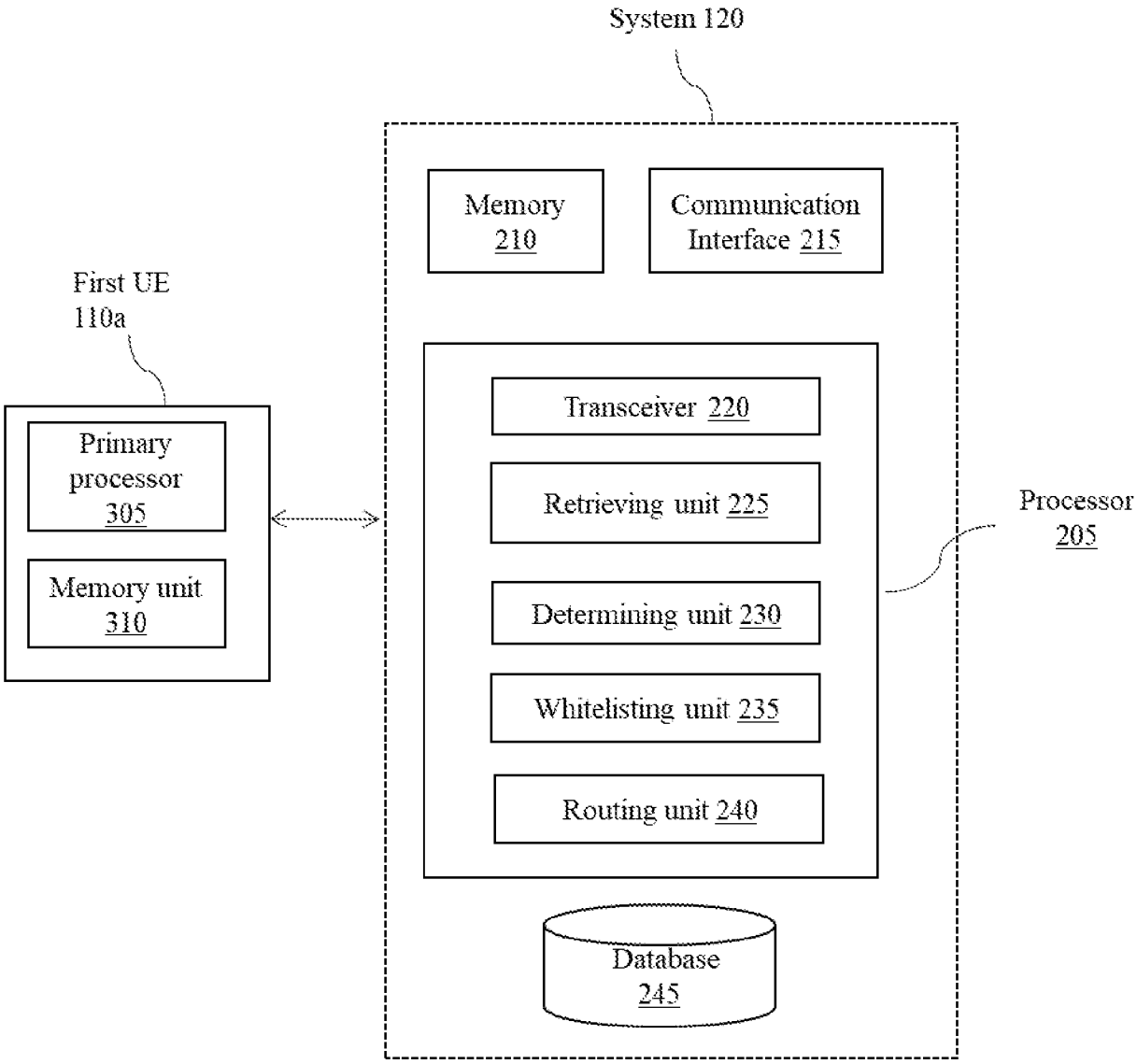
System 120
Memory 210
Communication Interface 215
First UE 110a
Primary processor 305
Memory unit 310
Transceiver 220
Retrieving unit 225
Determining unit 230
Whitelisting unit 235
Routing unit 240
Processor 205
Database 245

FIG. 3

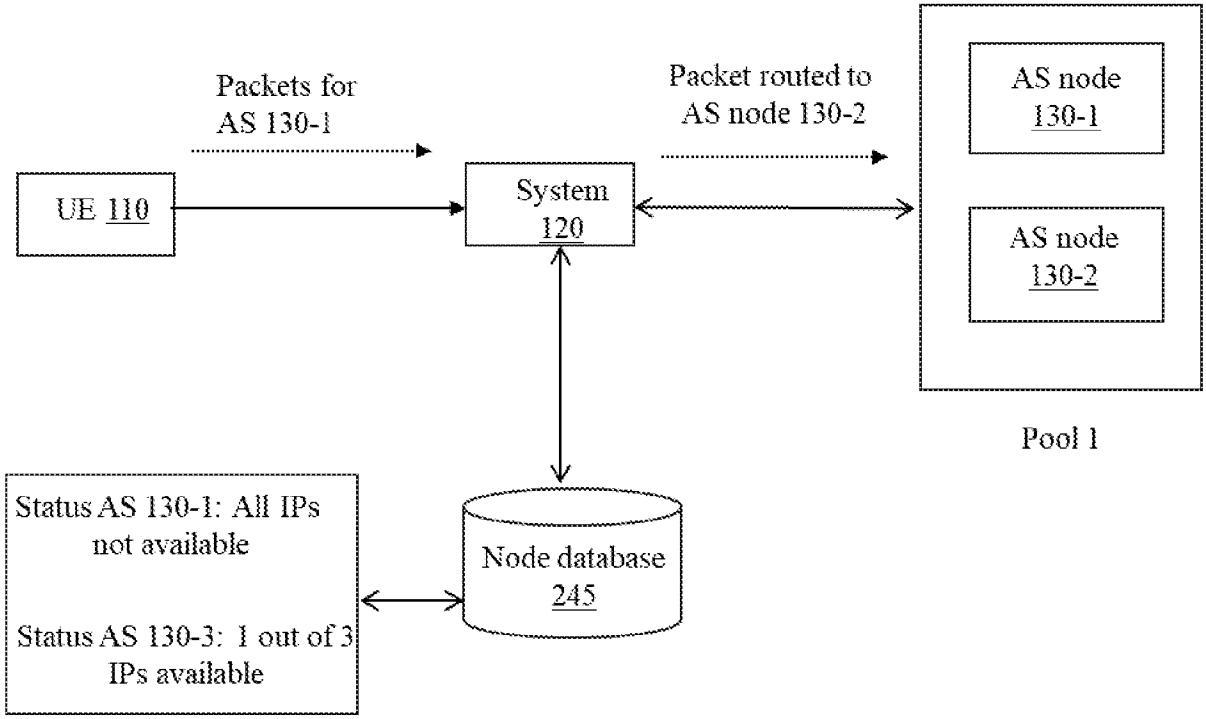
Packets for
AS 130-1
Packet routed to
AS node 130-2
AS node
130-1
AS node
130-2
UE 110
System
120
Pool 1
Status AS 130-1: All IPs
not available
Status AS 130-3: 1 out of 3
IPs available
Node database
245

FIG. 4

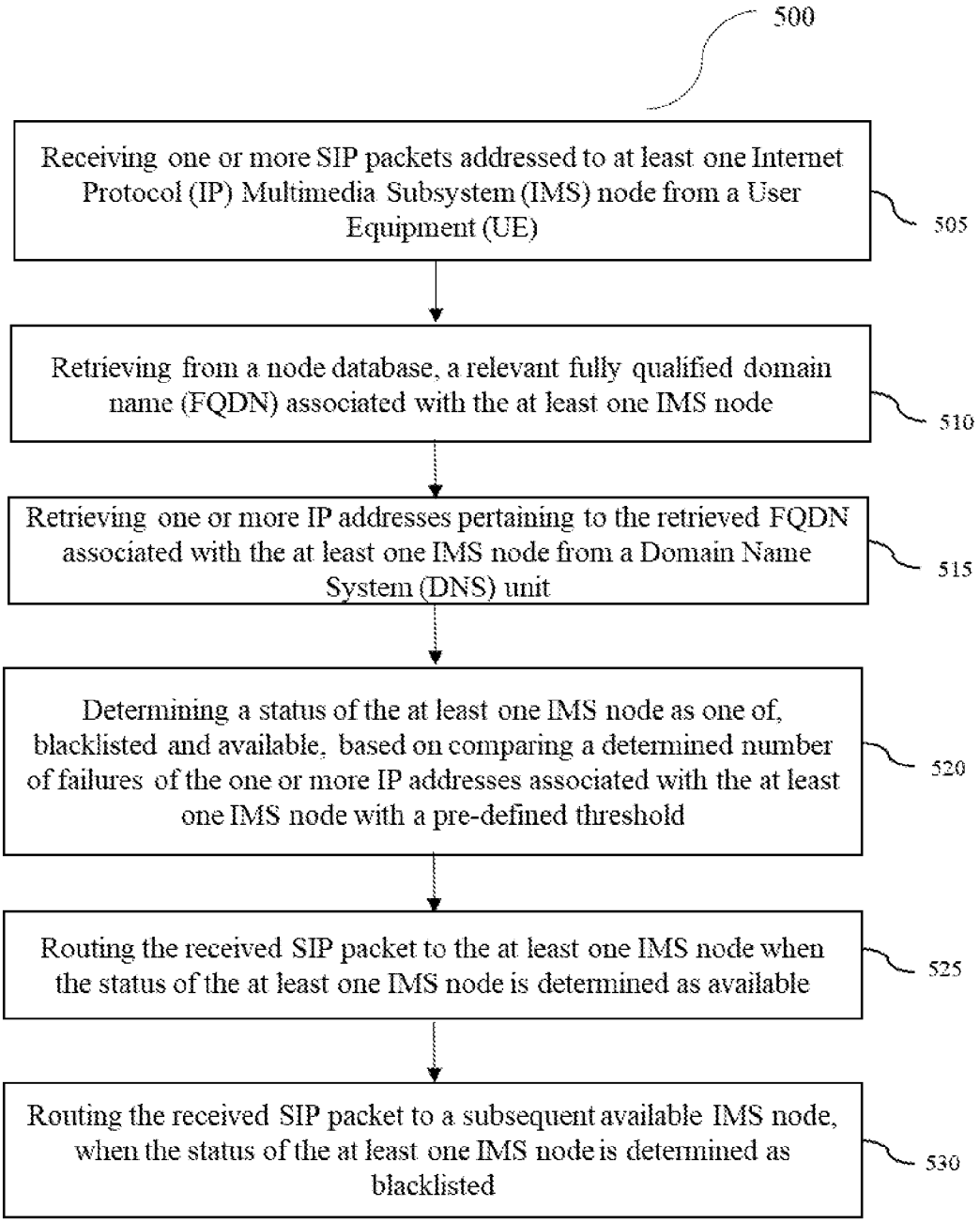
500
Receiving one or more SIP packets addressed to at least one Internet Protocol (IP) Multimedia Subsystem (IMS) node from a User Equipment (UE)
505
Retrieving from a node database, a relevant fully qualified domain name (FQDN) associated with the at least one IMS node
510
Retrieving one or more IP addresses pertaining to the retrieved FQDN associated with the at least one IMS node from a Domain Name System (DNS) unit
515
Determining a status of the at least one IMS node as one of, blacklisted and available, based on comparing a determined number of failures of the one or more IP addresses associated with the at least one IMS node with a pre-defined threshold
520
Routing the received SIP packet to the at least one IMS node when the status of the at least one IMS node is determined as available
525
Routing the received SIP packet to a subsequent available IMS node, when the status of the at least one IMS node is determined as blacklisted
530

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/050955

A. CLASSIFICATION OF SUBJECT MATTER
H04L65/1016,H04L65/1104,H04L65/1069 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: SIP, IMS, threshold, timer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US20210044629A1 (TELEFONAKTIEBOLAGET LM ERICSSON AB) 11 February 2021 (11/02/2021) Whole document	1-20
Y	WO2014134220A1 (T-MOBILE USA, INC.) 04 September 2014 (04/09/2014) Whole document	1-20

☐ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29-10-2024	29-10-2024
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/IN2024/050955

Citation	Pub.Date	Family	Pub.Date
US 20210044629 A1	11-02-2021	WO 2019177501 A1	19-09-2019
WO 2014134220 A1	04-09-2014	US 20140248848 A1	04-09-2014