



- (51) International Patent Classification:
H04L 41/0631 (2022.01) *H04L 41/0677* (2022.01)
- (21) International Application Number:
PCT/IN2024/051270
- (22) International Filing Date:
16 July 2024 (16.07.2024)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
202321047879 16 July 2023 (16.07.2023) 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). **MURARKA, Ankit**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **SAXENA, Gaurav**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **VERMA, Rahul**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN).

FICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **KOLARIYA, Jugal kishore**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **RANE, Manas**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **DE, Supriya**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **DEBASHISH, Kumar**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **MEHUL, Tilala**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **KUMAR, Kothagundla Vinay**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **GAYKI, Vinay**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **BHUSHAN, Shashank**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **LOBO, Ralph**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN).

(54) Title: SYSTEM AND METHOD FOR DETERMINING ROOT CAUSE OF ONE OR MORE ISSUES AT A PLURALITY OF NETWORK NODES

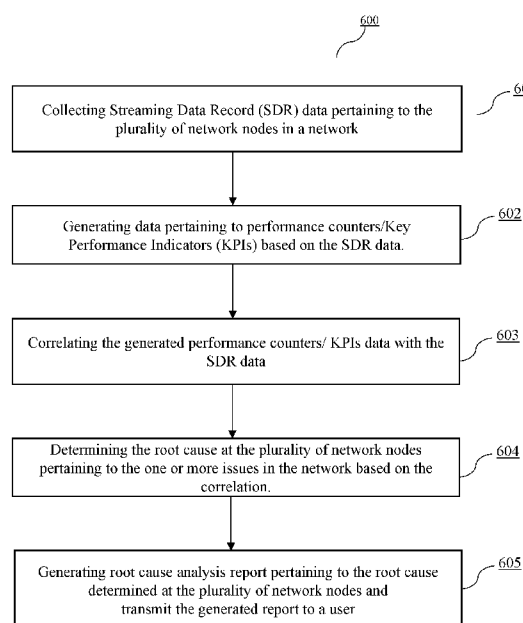


FIG. 6

(57) Abstract: The present disclosure relates to a system (104) and a method (600) for determining root cause of one or more issues at a plurality of network nodes (105). The system (104) includes a collection unit (212) to collect the Streaming Data Record (SDR) data pertaining to the plurality of network nodes (105) in the network (102). The system (104) includes a generation unit (214) to generate data pertaining to performance counters/Key Performance Indicators (KPIs). The system (104) includes a correlation unit (216) to correlate the generated performance counters/KPIs data with the SDR data. Further, the system (104) includes a determination unit (218) to determine the root cause based on the correlation. Furthermore, the system (104) includes a report generation unit (220) to generate a root cause analysis report pertaining to the root cause determined at the network nodes (105) and transmit the generated root cause analysis report to a user.

TRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **MEENA, Sunil**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **RAJANI, Manasvi**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **SAHU, Kishan**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **GANVEER, Chandra kumar**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **KUMAR, Yogesh**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **CHAUDHARY, Sanjana**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **KUSHWAHA, Avinash**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **VISHWAKARMA, Dharmendra kumar**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **SONI, Sajal**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN). **PODDAR, Harsh**; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD, 380006 (ID).

(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.

(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 DETERMINING ROOT CAUSE OF ONE OR MORE ISSUES AT A PLURALITY OF NETWORK NODES

FIELD OF THE INVENTION

[0001] The present invention generally relates to wireless communications, and more particularly relates to a system and method for determining root cause at a plurality of network nodes.

BACKGROUND OF THE INVENTION

[0002] Telecom service providers may face a variety of issues that impact their network and service reliability. It is important for the telecom service providers to identify potential issues and improve their network performance. The telecom service providers' identify potential issues by monitoring subscriber procedure level failure scenarios and performance counters/key performance indicators using different platforms, each ingesting different types of data. Typically, the telecom service providers process the data using independent platforms to identify subscriber procedure level failure scenarios and performance counters separately.

[0003] Processing the subscriber procedure level failure scenarios and the performance counters separately results in incomplete understanding of the network issues, prioritizing network optimization, inefficient resource allocation, inability to identify root cause, etc.

[0004] Therefore, there is a need in the art to provide a system and a method for correlating procedure level failure scenarios with network performance indicators to improve network service reliability, quality, and customer experience.

SUMMARY OF THE INVENTION

[0005] One or more embodiments of the present disclosure provide a system and method for determining root cause at a plurality of network nodes.

[0006] In one aspect of the present invention, a system for determining root cause of one or more issues at a plurality of network nodes is disclosed. The system includes a collection unit configured to collect Streaming Data Record (SDR) data pertaining to the plurality of network nodes in a network. The system includes a generation unit configured to generate data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data. The system includes a correlation unit configured to correlate the generated performance counters/KPIs data with the SDR data. Further, the system includes a determination unit configured to determine the root cause at the plurality of network nodes pertaining to the one or more issues in the network based on the correlation. In one embodiment, the system includes a report generation unit configured to generate a root cause analysis report pertaining to the root cause determined at the plurality of network nodes and the system further includes a transceiver configured to transmit the generated root cause analysis report to a user.

[0007] In one embodiment, the SDR data pertaining to the plurality of network nodes includes at least one of, a user defined policies provisioned with one or more clear codes, KPI thresholds and alerts.

[0008] In one embodiment, the generation unit generates data pertaining to performance counters/KPIs based on the SDR data by determining whether the user defined policies are breached, and in response to determining breach in the user defined policies, the generation unit generates data pertaining to the performance counters/KPIs.

[0009] In one embodiment, the data pertaining to the performance counters/KPIs are generated at periodic time intervals.

[0010] In one embodiment, the determination unit determines the root cause at the plurality of network nodes pertaining to the one or more issues in the network based on correlation by performing the root cause analysis to identify the root cause pertaining to the one or more issues at the plurality of network nodes in the network.

[0011] In another aspect of the present invention, a method for determining root cause of one or more issues at the plurality of network nodes is disclosed. The method includes the steps of collecting, by one or more processors, SDR data pertaining to the plurality of network nodes in the network. The method includes the steps of generating, by the one or more processors, data pertaining to performance counters/KPIs based on the SDR data. The method includes the steps of correlating, by the one or more processors, the generated performance counters/KPIs data with the SDR data. The method includes the steps of determining, by the one or more processors, the root cause at the plurality of network nodes pertaining to the one or more issues in the network based on the correlation.

[0012] In another aspect of the invention, a non-transitory computer-readable medium having stored thereon computer-readable instructions is disclosed. The computer-readable instructions are executed by a processor. The processor is configured to collect, SDR data pertaining to the plurality of network nodes in the network. The processor is further configured to generate, data pertaining to performance counters/KPIs based on the SDR data. The processor is further configured to correlate, the generated performance counters/KPIs data with the SDR data. The processor is further configured to determine, the root cause at the plurality of network nodes pertaining to the one or more issues in the network based on the correlation.

[0013] In another aspect of invention, User Equipment (UE) is disclosed. The UE includes one or more primary processors communicatively coupled to one or more processors, the one or more primary processors coupled with a memory. The processor

is configured to transmit the user defined policies provisioned with the one or more clear codes and KPI thresholds to the one or more processors via a user interface.

[0014] 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

[0015] 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.

[0016] **FIG. 1** is an exemplary block diagram of an environment for determining root cause at a plurality of network nodes in a network, according to various embodiments of the present invention;

[0017] **FIG. 2** is a block diagram of a system for determining root cause at the plurality of network nodes in the network, according to various embodiments of the present invention;

[0018] **FIG. 3** is schematic representation of a workflow of the system of **FIG. 2**, according to various embodiments of the present invention;

[0019] **FIG. 4** is an exemplary architecture of the system of **FIG. 3**, for determining root cause of one or more issues at the plurality of network nodes, according to various embodiments of the present invention;

[0020] **FIG. 5** is a signal flow diagram for determining root cause at the plurality of network nodes in the network, according to various embodiments of the present invention; and

[0021] **FIG. 6** shows a flow diagram of a method for determining root cause at the plurality of network nodes in the network, according to various embodiments of the present invention.

[0022] The foregoing shall be more apparent from the following detailed description of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0023] 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.

[0024] 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.

[0025] 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.

[0026] As per various embodiments depicted, the present invention discloses the system and method for determining root cause of one or more issues at a plurality of network nodes in the network. The present invention addresses the challenge of correlating procedure level failure scenarios with network performance indicators to improve network service reliability, quality, and customer experience. The present invention enables correlation of subscriber level and network level data to exactly find the root cause analysis of the issue.

[0027] Referring to **FIG. 1**, **FIG. 1** illustrates an exemplary block diagram of an environment **100** for determining root cause at a plurality of network nodes **105** in a network **102**, according to various embodiments of the present invention. In one embodiment, the plurality of network nodes **105** include by way of example but not limitation to one or more base stations **105a** and **105b** 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 environment **100** includes at least one User Equipment (UE) **101** configured to at least transmit the user defined policies from the at least first UE **101a** for determining root cause of one or more issues at the plurality of network nodes **105** in the network **102**. In one embodiment, the one or more issues at the plurality of network nodes **105** includes but are not limited to difficulties in verifying the UE **101** access rights or permissions to use specific network services or features, network congestion, network overload can sometimes lead to procedural failures due to timeouts or resource limitations, data breaches affecting multiple nodes, incorrect settings or misconfigurations that impact network operation.

[0028] In one embodiment, the at least one UE **101** is at least one of a first UE **101a**, a second UE **101b**, and a third UE **101c**. In one embodiment, each of the at least first UE **102a**, the second UE **102b**, and the third UE **102c** are configured to at least transmit the user defined policies to determine root cause of one or more issues at the plurality of network nodes **105** in the network **102**. At least the first UE **101a**, the second UE **101b** and the third UE **101c** are communicatively connected to a system **104** via the network **102**. In one embodiment, the at least the first UE **101a**, the second UE **101b** and the third UE **101c** are communicatively connected to the network **102** via the network nodes **105**. The first UE **101a**, the second UE **101b** and the third UE **101c** will henceforth collectively and individually be referred to as “the UE **101**” without limiting the scope and deviating from the scope of the present disclosure.

[0029] More information regarding the same will be provided with reference to the following figures.

[0030] In one embodiment, the UE **101** includes, but are not limited to, a handheld wireless communication device (e.g., a mobile phone, a smart phone, a tablet device, and so on), a wearable computer device (e.g., a head-mounted display computer device, a head-mounted camera device, a wristwatch computer device, and so on), a Global Positioning System (GPS) device, a laptop computer, a tablet computer, or another type of portable computer, a media playing device, a portable gaming system,

and/or any other type of computer device with wireless communication capabilities, and the like.

[0031] The environment **100** further includes the server **103** communicably coupled to the UE **101** via the network **102**. The server **103** includes 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, a defense facility, or any other facility that provides content.

[0032] The network **102** 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 **102** 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.

[0033] Further, the network **102** also includes, by the way of example but not limitation, one or more wireless interfaces/protocols such as, for example, 802.11 (Wi-Fi), 802.15 (including Bluetooth™), 802.16 (Wi-Max), 802.22, Cellular standards such as CDMA, CDMA2000, WCDMA, Radio Frequency (e.g., RFID), Infrared, laser, Near Field Magnetics, etc.

[0034] The environment **100** further includes the system **104** communicably coupled to the server **103** and the UE **101** via the network **102**. The system **104** is configured to determine root cause of one or more issues at the plurality of network nodes **105** in the network **102**. Further, the system **104** is adapted to be embedded within the server **103** or is embedded as the individual entity independent of the server **103**. However, for the purpose of description, the system **104** is described as an integral part of the server **103**, without deviating from the scope of the present disclosure.

[0035] Operational and construction features of the system **104** will be explained in detail with respect to the following figures.

[0036] Referring to **FIG. 2**, **FIG. 2** illustrates a block diagram of the system **104** for determining root cause of one or more issues at the plurality of network nodes **105** in the network **102**, according to various embodiments of the present invention. The system **104** includes the processor **202**, a memory **204**, a user interface **206**, a display unit **208**, an input device **210** and a database **222**. The one or more processors **202**, hereinafter referred to as the processor **202** 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 **104** includes one processor **202**. However, it is to be noted that the system **104** include multiple processors as per the requirement and without deviating from the scope of the present disclosure. Among other capabilities, the processor **202** is configured to fetch and execute computer-readable instructions stored in the memory **204**.

[0037] The memory **204** is 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 **204** may include any non-transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as EPROM,

flash memory, and the like. In an embodiment, the user interface **206** includes a variety of interfaces, for example, interfaces for data input and output devices, referred to as input/output devices, storage devices, and the like. The user interface **206** facilitates communication of the system **104**. In one embodiment, the user interface **206** provides a communication pathway for one or more components of the system **104**.

[0038] The user interface **206** may include functionality similar to at least a portion of functionality implemented by one or more computer system interfaces such as those described herein and/or generally known to one having ordinary skill in the art. The user interface **206** may be rendered on the display unit **208**, implemented using Liquid Crystal Display (LCD) display technology, Organic Light Emitting Diode (OLED) display technology, and/or other types of conventional display technology. The display unit **208** is integrated within the system **104** or connected externally. Further the request may be configured to receive requests, queries, or information from the user by using the input device **210**. The input device **210** may include, but not limited to, keyboard, buttons, scroll wheels, cursors, touchscreen sensors, audio command interfaces, magnetic strip reader, optical scanner, etc.

[0039] The system **104**, may further comprise the database **222**. The database **222** may be communicably connected to the processor **202**, and the memory **204**. The database **222** is configured to store and retrieve the data of the UE **101**.

[0040] Further, the processor **202**, 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 **202**. 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 **202** may be processor-executable instructions stored on a non-transitory machine-readable storage medium and the hardware for processor **202** may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the memory **204** may store instructions that,

when executed by the processing resource, implement the processor **202**. In such examples, the system **104** may comprise the memory **204** storing the instructions and the processing resource to execute the instructions, or the memory **204** may be separate but accessible to the system **104** and the processing resource. In other examples, the processor **202** may be implemented by electronic circuitry.

[0041] In order for the system **104** to determine root cause of one or more issues at the plurality of network nodes **105** in the network **102**. The processor **202** includes a collection unit **212**, a generation unit **214**, a correlation unit **216**, a determination unit **218** and a report generation unit **220** communicably coupled to each other. In an embodiment, the collection unit **212**, the generation unit **214**, the correlation unit **216**, the determination unit **218** and the report generation unit **220** are enabled by the processor **202** to determine root cause of one or more issues at the plurality of network nodes **105** in the network **102**.

[0042] The collection unit **212** of the processor **202** is communicably connected to the UE **101** via the network nodes **105** and the network **102**. Accordingly, the collection unit **212** is configured to collect a Streaming Data Record (SDR) data pertaining to the plurality of network nodes **105** in the network **102**. In one embodiment, the SDR data pertaining to the plurality of network nodes **105** includes at least one of, a user defined policies provisioned with one or more clear codes, KPI thresholds and alerts. In one embodiment, the user defined policies are provisioned in the collection unit **212**. The collection unit **212** runs one or more clear codes policy containing a list of clear codes. The list of clear codes defines as status codes that network nodes or software use to communicate specific conditions or events. These clear codes are designed to convey information quickly and efficiently about the state of the network node or the device. The list of clear codes includes, but not limited to, unassigned or unallocated number, no route to specific transit network, no route to destination, send special information, misdialed trunk prefix, channel unacceptable, operator determined barring, user busy, network out of order, no channel available, call rejected, etc.

[0043] In one embodiment, the KPI thresholds and alerts includes, but not limited to, call setup success rate, call drop rate, handover success rate, authentication success rate, Short Message Service (SMS) and/or Multimedia Messaging Service (MMS) delivery success rate, network availability, service activation time, latency, packet loss rate, etc.

[0044] In an embodiment, the collection unit **212** is configured to transmit the SDR data to the generation unit **214** for further processing. On receipt of the SDR data, the generation unit **214** is configured to determine the user defined policies are breached. In response to determining the user defined policies are breached, the generation unit **214** generates the data pertaining to the performance counters/KPIs based on the SDR data. In one embodiment, the data pertaining to the performance counters/KPIs are generated at periodic time intervals. For example, consider the network node **105a** was down from 2:45PM to 3:00PM, then the generation unit **214** generates the data that network node **105a** is down from 2:45PM to 3:00PM and transmit the network node **105a** data with the time period to the correlation unit **216**.

[0045] Furthermore, the generation unit **214** is configured to transmit the generated data pertaining to performance counters/KPIs to the correlation unit **216** for further processing. On receipt of the generated data pertaining to performance counters/KPIs from the generation unit **214**, the correlation unit **216** is configured to correlate the generated performance counters/KPIs data with the SDR data to generate the correlated data. The correlation unit **216** stores the correlation logic or correlation templates for clear codes and/or breached clear codes. The correlation of the generated performance counters/KPIs data with the SDR data is performed utilizing a correlation logic corresponding to breached user defined policies. Further the correlated data is transmitted to the determination unit **218**. In one embodiment, for example the correlation templates for clear codes are defined as rules or patterns that helps in correlating events, alarms, or logs across various network nodes to identify larger issues or patterns in the network node **105**.

[0046] On receipt of the correlated data, the determination unit **218** is configured to perform a root cause analysis to identify the one or more issues at the plurality of network nodes **105** in the network **102**. After performing the root cause analysis, the determination unit **218** determines the root cause at the plurality of network nodes **105** pertaining to the one or more issues in the network **102** based on the correlation. The determination unit **218** transmits the determined root cause at the plurality of network nodes **105** pertaining to the one or more issues in the network **102** to the report generation unit **220** for report generation. The report generation unit **220** is configured to generate the root cause analysis report pertaining to the root cause determined at the plurality of network nodes **105**. The root cause analysis report is transmitted to a transceiver **224**. The transceiver **224** is further configured to transmit the generated root cause analysis report to a user. Advantageously, the system **200** is capable of correlating procedure level failure scenarios with network performance indicators to improve network service reliability, quality, and customer experience.

[0047] In one embodiment, as explained above the correlation unit **216** stores the correlation logic or correlation templates for clear codes and/or breached clear codes. The correlation unit **216** is coupled to the database **222**. Storing the list of clear cause codes and/or breached clear codes in the database **222**, eliminates the usage of additional memory in the database **222**. Advantageously, by doing this, the system **104** achieves the data optimization and saves the memory space in the database **222** by storing only the correlated data and the correlation logic or correlation templates for clear codes and/or breached clear codes and the data optimization leads to improving the processing efficiency of the system **104**.

[0048] Referring to **FIG. 3**, **FIG. 3** illustrates an exemplary embodiment of determining root cause of one or more issues at the plurality of network nodes **105** in the network **102** of the system **104** of **FIG. 2**, according to various embodiments of the present invention. It is to be noted that the embodiment with respect to **FIG. 3** will be explained with respect to the first UE **101a** for the purpose of description and

illustration and should nowhere be construed as limited to the scope of the present disclosure.

[0049] As mentioned earlier in **FIG. 1**, each of the first UE **101a**, the second UE **101b**, and the third UE **101c** 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 **101a**. The first UE **101a** includes one or more primary processors **304** communicably coupled to the one or more processors **202** of the system **104**. The one or more primary processors **304** are coupled with a memory unit **306** storing instructions which are executed by the one or more primary processors **304**. Execution of the stored instructions by the one or more primary processors **304** enables the first UE **101a** to transmit the user defined policies provisioned with the one or more clear codes and the KPI thresholds to the processor **202** via a user interface **302** from the first UE **101a**. The execution of the stored instructions by the one or more primary processors **304** further enables the first UE **101a** to transmit the user defined policies provisioned with the one or more clear codes and the KPI thresholds to the one or more processors **202**.

[0050] As mentioned earlier, the one or more processors **202** is configured to transmit the request to the first UE **101a**. More specifically, the one or more processors **202** of the system **104** is configured to transmit the user defined policies provisioned with the one or more clear codes and KPI thresholds via the user interface **302** of the first UE **101a** to the one or more processors **202** of the system **104**.

[0051] The user interface **302** is configured to transmit the user defined policies provisioned with the one or more clear codes and the KPI thresholds to the collection unit **212** of the system **104** for determining root cause of one or more issues at the plurality of network nodes **105** in the network **102**.

[0052] In the preferred embodiment, the collection unit **212** of the processor **202** is communicably connected to the user interface **302** of the first UE **101a**. The collection unit **212** is configured to collect the Streaming Data Record (SDR) data pertaining to the plurality of network nodes **105** in the network **102**.

[0053] As per the illustrated embodiment, the system **104** includes the one or more processors **202**, the memory **204**, the user interface **206**, the display unit **208**, the input device **210** and the database **222**. The operations and functions of the one or more processors **202**, the memory **204**, the user interface **206**, the display unit **208**, the input device **210** and the database **222**, are already explained in **FIG. 2**. For the sake of brevity, a similar description related to the working and operation of the system **104** as illustrated in **FIG. 2** has been omitted to avoid repetition.

[0054] Further, the processor **202** includes the collection unit **212**, the generation unit **214**, the correlation unit **216**, the determination unit **218** and the report generation unit **220**. The operations and functions of the collection unit **212**, the generation unit **214**, the correlation unit **216**, the determination unit **218** and the report generation unit **220** are already explained in **FIG. 2**. Hence, for the sake of brevity, it is to be noted that a similar description related to the working and operation of the system **104** as illustrated in **FIG. 2** has been omitted to avoid repetition. The limited description provided for the system **104** in **FIG. 3**, should be read with the description as provided for the system **104** in the **FIG. 2** above, and should not be construed as limiting the scope of the present disclosure.

[0055] Referring to **FIG. 4**, **FIG. 4** is an exemplary architecture of the system **104** of **FIG. 3** for determining root cause of one or more issues at the plurality of network nodes **105**, according to various embodiments of the present invention. The architecture of the system **104** includes a probing agent **401**, an Integrated Performance Management (IPM) **402**, a correlation module **403**, a reporting module **404** and a user interface **302**. The probing agent **401** includes a sub-unit defined as the collection unit **212** to collect the SDR data of the UE **101** via the network nodes **105**.

In one embodiment, the SDR data is received via the user interface **302**. The SDR data includes the user defined policies provisioned with one or more clear codes, KPI thresholds and alerts. The policies are provisioned in the probing agent **401** via user interface **302**. The probing agent **401** runs the clear code policy containing the list of clear codes. The clear cause codes include, but not limited to, unassigned or unallocated number, no route to specific transit network, no route to destination, send special information, misdialed trunk prefix, channel unacceptable, operator determined barring, user busy, network out of order, no channel available, call rejected, etc. The probing agent **401** monitors for policy breaches and checks for the correlation logic for breached clear codes.

[0056] Further, the system **104** includes an Integrated Performance Management (IPM) module **402**. The IPM module **402** includes a sub-unit defined as the generation unit **212**. The IPM module **402** monitors the performance of the network nodes **105** in the network **102**. In one embodiment, the IPM module **204** monitors latency, availability, jitter, packet loss, and errors between two network end points. Further, the generation unit **214** generates performance counters/ KPIs based on the SDR data. The KPIs includes, but not limited to, call setup success rate, call drop rate, handover success rate, authentication success rate, SMS/MMS delivery success rate, network availability, service activation time, latency, packet loss rate, etc. The probing agent **401** transmit the generated performance counters/ KPIs based on the SDR data to the correlation module **403**.

[0057] Further, the system **104** includes the correlation module **403**. The correlation module **403** includes a sub-unit defined as the correlation unit **216**. The correlation unit **216** stores the correlation logic or correlation templates for clear codes and/or breached clear codes. The probing agent **401** transmit the generated performance counters/KPIs based on the SDR data to the correlation module **403** to correlate the logic corresponding to the breached clear code. Accordingly, the probing agent **401** perform the root cause analysis to identify the root cause pertaining to the one or more issues at the plurality of network nodes **105** in the network **102**. In one embodiment, the probing agent **401** includes a sub-unit defined as the determination unit **218** to

determine the root cause at the plurality of network nodes **105** pertaining to the one or more issues in the network **102** based on the correlation. The determined root cause at the plurality of network nodes **105** is transmitted to the reporting module **404**.

[0058] Further, the system **104** includes the reporting module **404**. The reporting module **404** includes a sub-unit defined as the report generation unit **218**. The report generation unit **218** generates the root cause analysis report pertaining to the root cause determined at the plurality of network nodes **105** and transmit the generated root cause analysis report to the user interface **302**.

[0059] Referring to **FIG. 5**, **FIG. 5** is an exemplary signal flow diagram for determining root cause of one or more issues at the plurality of network nodes **105**, according to various embodiments of the present invention. For the purpose of description, the signal flow diagram is described with the embodiments as illustrated in **FIG. 4** and should nowhere be construed as limiting the scope of the present disclosure.

[0060] At step **501**, the UE **101** transmit the user defined policies provisioned with the one or more clear codes and KPI thresholds to the one or more processor **202** of the system **104** via the user interface **302**.

[0061] At step **502**, the SDR data pertaining to the plurality of network nodes **105** in the network **102** is collected by the collection unit **212**. The SDR data includes the user defined policies provisioned with one or more clear codes, KPI thresholds and alerts.

[0062] At step **503**, upon collecting the SDR data pertaining to the plurality of network nodes **105** in the network **102**, the data pertaining to performance counters/KPIs based on the SDR data is generated by the generation unit **214**. The data pertaining to the performance counters/KPIs are generated at periodic time intervals. The generation unit **214** determine that the user defined policies are breached and in

response to determining, the generation unit **214** generates the data pertaining to the performance counters and/or KPIs.

[0063] At step **504**, upon generating the data pertaining to the performance counters/KPIs based on the SDR data by the generation unit **214**, the correlation unit **216** is configured to correlation of the generated performance counters/KPIs data with the SDR data. The correlation of the generated performance counters/KPIs data with the SDR data is performed utilizing a correlation logic corresponding to breached user defined policies.

[0064] At step **505**, upon correlation of the generated performance counters/KPIs data with the SDR data, the determination unit **218** is configured to perform a root cause analysis to identify the root cause pertaining to the one or more issues at the plurality of network nodes **105** in the network **102**. Further, the determination unit **218** determine the root cause at the plurality of network nodes **105** based on the correlation and transmit the determined root cause at the plurality of network nodes **105** to the report generation unit **220**.

[0065] At step **506**, upon determining the root cause at the plurality of network nodes **105**, the report generation unit **220** generates the root cause analysis report and transmit the generated root cause analysis report to the user.

[0066] Referring to **FIG. 6**, **FIG. 6** illustrates a flow diagram of the method **600** for determining root cause of one or more issues at the plurality of network nodes **105** in the network **102**, according to various embodiments of the present invention. The method **600** is adapted for determining root cause of one or more issues at the plurality of network nodes **105** in the network **102**. For the purpose of description, the method **600** is described with the embodiments as illustrated in **FIG. 2** and should nowhere be construed as limiting the scope of the present disclosure.

[0067] At step **601**, the method **600** includes the step of collecting the SDR data pertaining to the plurality of network nodes **105** in the network **102** by the collection

unit **212**. In one embodiment, the SDR data pertaining to the plurality of network nodes **105** includes at least one of, a user defined policies provisioned with one or more clear codes, KPI thresholds and alerts.

[0068] In one embodiment, the user defined policies are provisioned in the collection unit **212**. The collection unit **212** runs one or more clear codes policy containing the list of clear codes. The list of clear codes includes, but not limited to, unassigned (unallocated) number, no route to specific transit network, no route to destination, send special information, misdialed trunk prefix, channel unacceptable, operator determined barring, user busy, network out of order, no channel available, call rejected, etc.

[0069] In one embodiment, the KPI thresholds and alerts includes, but not limited to, call setup success rate, call drop rate, handover success rate, authentication success rate, SMS/MMS delivery success rate, network availability, service activation time, latency, packet loss rate, etc. Further, the collection unit **212** transmit the SDR data to the generation unit **214** for further processing.

[0070] At step **602**, the method **600** includes the step of generating the data pertaining to performance counters/KPIs based on the SDR data to determine the user defined policies are breached. In response to determining the user defined policies are breached, the generation unit **214** generates the data pertaining to the performance counters/KPIs based on the SDR data. In one embodiment, the data pertaining to the performance counters/KPIs are generated at periodic time intervals.

[0071] Furthermore, the generation unit **214** is configured to transmit the generated data pertaining to performance counters/KPIs to the correlation unit **216** for further processing.

[0072] At step **603**, the method **600** includes the step of correlating the generated performance counters/KPIs data with the SDR data by the correlation unit **216**. The correlation unit **216** is configured to correlate the generated performance

counters/KPIs data with the SDR data to generate the correlated data. The correlation unit **216** stores the correlation logic or correlation templates for clear codes and/or breached clear codes. The correlation of the generated performance counters/KPIs data with the SDR data is performed utilizing the correlation logic corresponding to breached user defined policies. Further, the correlated data is transmitted to the determination unit **218**.

[0073] At step **604**, the method **600** includes the step of determining the root cause at the plurality of network nodes **105** pertaining to the one or more issues in the network **102** based on correlation, by the determination unit **218**. The determination unit **218** perform the root cause analysis to identify the root cause pertaining to the one or more issues at the plurality of network nodes **105** in the network **102**. The determination unit **218** transmit the determined root cause at the plurality of network nodes **105** pertaining to the one or more issues in the network **102** to the report generation unit **220** for report generation.

[0074] At step **605**, the method **600** includes the step of generating the root cause analysis report pertaining to the root cause determined at the plurality of network nodes **105** and transmit the generated root cause analysis report to the user.

[0075] 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 **202**. The processor **202** is configured to collect the Streaming Data Record (SDR) data pertaining to the plurality of network nodes in a network. The processor **202** is further configured to generate data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data. The processor **202** is further configured to correlate the generated performance counters/KPIs data with the SDR data. The processor **202** is further configured to determine the root cause at the plurality of network nodes pertaining to the one or more issues in the network based on the correlation.

[0076] A person of ordinary skill in the art will readily ascertain that the illustrated embodiments and steps in description and drawings (FIG.1-6) 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.

[0077] The present disclosure incorporates technical advancement for determining root cause of one or more issues at plurality of network nodes. The invention takes advantage of enabling the correlation of the subscriber level and network level data to exactly find the root cause analysis of the issue in the network. Further, the system is capable of correlating procedure level failure scenarios with network performance indicators to improve the network and service reliability of the telecom service provider. The system is able to find out the exact root cause of the issue for a subscriber session. Furthermore, the system enables to differentiate and correlate the issue such as whether the issue is at global level due to a particular event/procedure degrading in the network or the issue was local i.e., only a particular subscriber was affected.

[0078] 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

- [0079] Environment - 100
- [0080] User Equipment - 101
- [0081] Network - 102
- [0082] Server - 103
- [0083] System - 104
- [0084] Network nodes - 105
- [0085] Processor - 202
- [0086] Memory - 204
- [0087] User interface - 206
- [0088] Display unit - 208
- [0089] Input device - 210
- [0090] Collection unit - 212
- [0091] Generation unit - 214
- [0092] Correlation unit - 216
- [0093] Determination unit - 218
- [0094] Report generation unit - 220
- [0095] Database - 222
- [0096] User interface - 302
- [0097] Primary processor - 304
- [0098] Memory unit - 306
- [0099] Probing agent - 401
- [00100] Integrated Performance Management (IPM) module - 402
- [00101] Correlation module - 403
- [00102] Reporting module - 404.

We Claim:

1. A method (600) for determining root cause of one or more issues at a plurality of network nodes (105), the method (600) comprising the steps of:
 - collecting, by one or more processors (202), Streaming Data Record (SDR) data pertaining to the plurality of network nodes (105) in a network (102);
 - generating, by the one or more processors (202), data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data;
 - correlating, by the one or more processors (202), the generated performance counters/ KPIs data with the SDR data; and
 - determining, by the one or more processors (202), the root cause at the plurality of network nodes (105) pertaining to the one or more issues in the network (102) based on the correlation.
2. The method (600) as claimed in claim 1, wherein the SDR data pertaining to the plurality of network nodes (105) includes at least one of, a user defined policies provisioned with one or more clear codes, KPI thresholds and alerts.
3. The method (600) as claimed in claim 1, wherein the step of generating, data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data, includes the steps of:
 - determining, by the one or more processors (202), whether the user defined policies are breached;
 - in response to determining, breach in the user defined policies, generating, by the one or more processors (202), data pertaining to the performance counters/Key Performance Indicators (KPIs).
4. The method (600) as claimed in claim 1, wherein the data pertaining to the performance counters/Key Performance Indicators (KPIs) are generated at periodic time intervals.

5. The method (600) as claimed in claim 1, wherein the correlation of the generated performance counters/ KPIs data with the SDR data is performed utilizing a correlation logic corresponding to breached user defined policies.
6. The method (600) as claimed in claim 1, wherein the step of determining, the root cause at the plurality of network nodes (105) pertaining to the one or more issues in the network (102) based on correlation, includes the step of:
 - performing, by the one or more processors (202), a root cause analysis to identify the root cause pertaining to the one or more issues at the plurality of network nodes (105) in the network (102).
7. The method (600) as claimed in claim 1, wherein the method (600) further comprising the steps of:
 - generating, by the one or more processors (202), a root cause analysis report pertaining to the root cause determined at the plurality of network nodes (105);
 - transmitting, by the one or more processors (202), the generated root cause analysis report to a user.
8. A system (104) for determining root cause of one or more issues at a plurality of network nodes (105), the system (104) comprises:
 - a collection unit (212), configured to, collect, Streaming Data Record (SDR) data pertaining to the plurality of network nodes (105) in a network (102);
 - a generation unit (214), configured to, generate, data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data;
 - a correlation unit (216), configured to, correlate, the generated performance counters/ KPIs data with the SDR data; and

- a determination unit (218), configured to, determine, the root cause at the plurality of network nodes (105) pertaining to the one or more issues in the network (102) based on the correlation.
9. The system (104) as claimed in claim 8, wherein the SDR data pertaining to the plurality of network nodes (105) includes at least one of, a user defined policies provisioned with one or more clear codes, KPI thresholds and alerts.
 10. The system (104) as claimed in claim 8, wherein the generation unit (214) generates, data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data, by:
 - determining, whether the user defined policies are breached;
 - in response to determining, breach in the user defined policies, generating, data pertaining to the performance counters/Key Performance Indicators (KPIs).
 11. The system (104) as claimed in claim 8, wherein the data pertaining to the performance counters/Key Performance Indicators (KPIs) are generated at periodic time intervals.
 12. The system (104) as claimed in claim 8, wherein the correlation of the generated performance counters/ KPIs data with the SDR data is performed utilizing a correlation logic corresponding to breached user defined policies.
 13. The system (104) as claimed in claim 8, wherein the determination unit (218) determines, the root cause at the plurality of network nodes (105) pertaining to the one or more issues in the network (102) based on correlation, by:
 - performing, a root cause analysis to identify the root cause pertaining to the one or more issues at the plurality of network nodes (105) in the network (102).

14. The system (104) as claimed in claim 8, wherein the system (104) further comprises:

a report generation unit (220), configured to, generate, a root cause analysis report pertaining to the root cause determined at the plurality of network nodes (105);

a transceiver, configured to, transmit, the generated root cause analysis report to a user.

15. A User Equipment (UE) (101), comprising:

one or more primary processors (304) communicatively coupled to one or more processors (202), the one or more primary processors (304) coupled with a memory (306), wherein said memory (306) stores instructions which when executed by the one or more primary processors (304) causes the UE (101) to:

transmit, the user defined policies provisioned with the one or more clear codes and KPI thresholds to the one or more processors (202) via a user interface (302);

wherein the one or more processors (202) is configured to perform the steps as claimed in claim 1.

16. A non-transitory computer-readable medium having stored thereon computer-readable instructions that, when executed by a processor (202), causes the processor (202) to:

collect, Streaming Data Record (SDR) data pertaining to the plurality of network nodes (105) in a network (102);

generate, data pertaining to performance counters/Key Performance Indicators (KPIs) based on the SDR data;

correlate, the generated performance counters/ KPIs data with the SDR data; and

determine, the root cause at the plurality of network nodes (105) pertaining to the one or more issues in the network (102) based on the correlation.

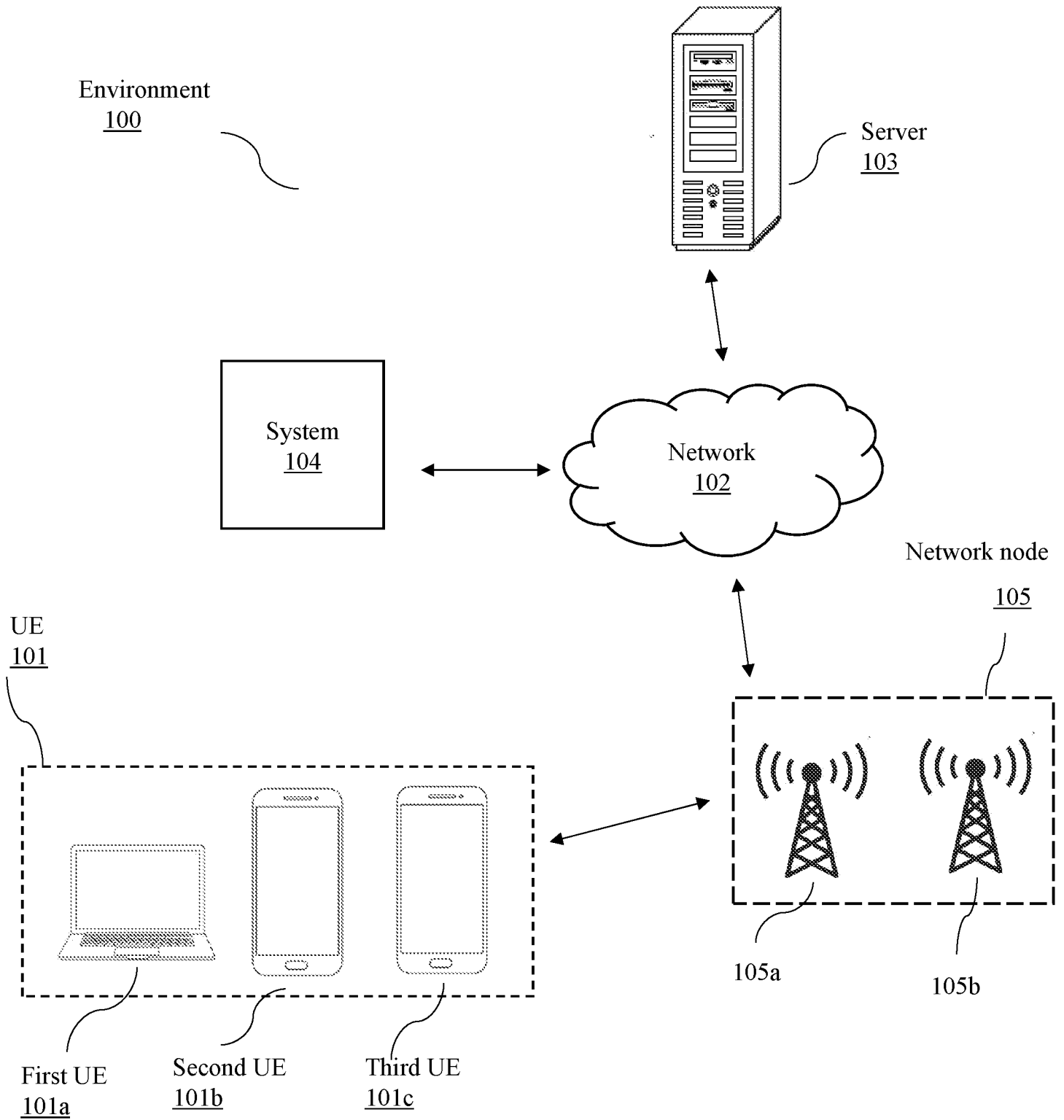


FIG. 1

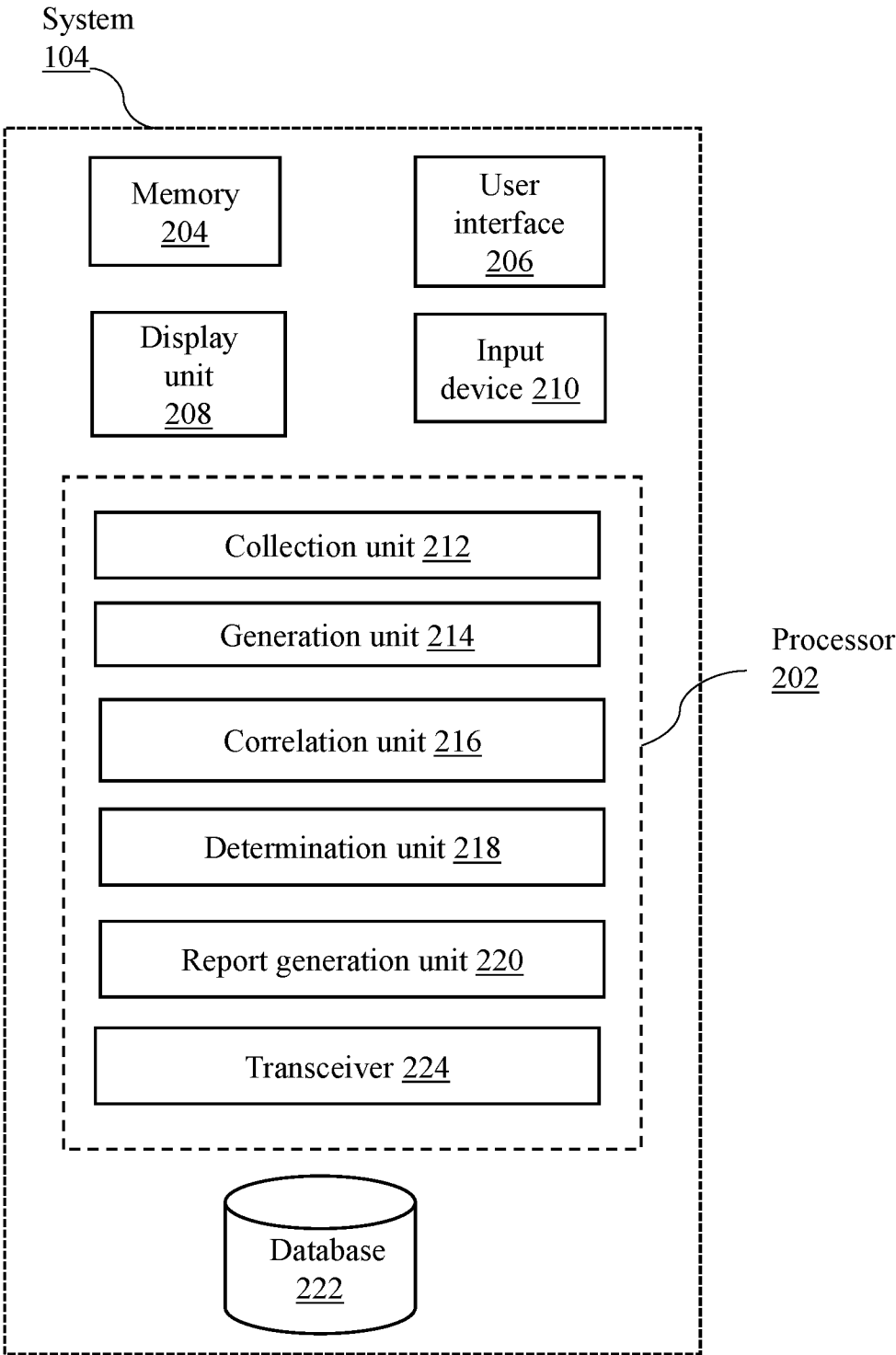


FIG. 2

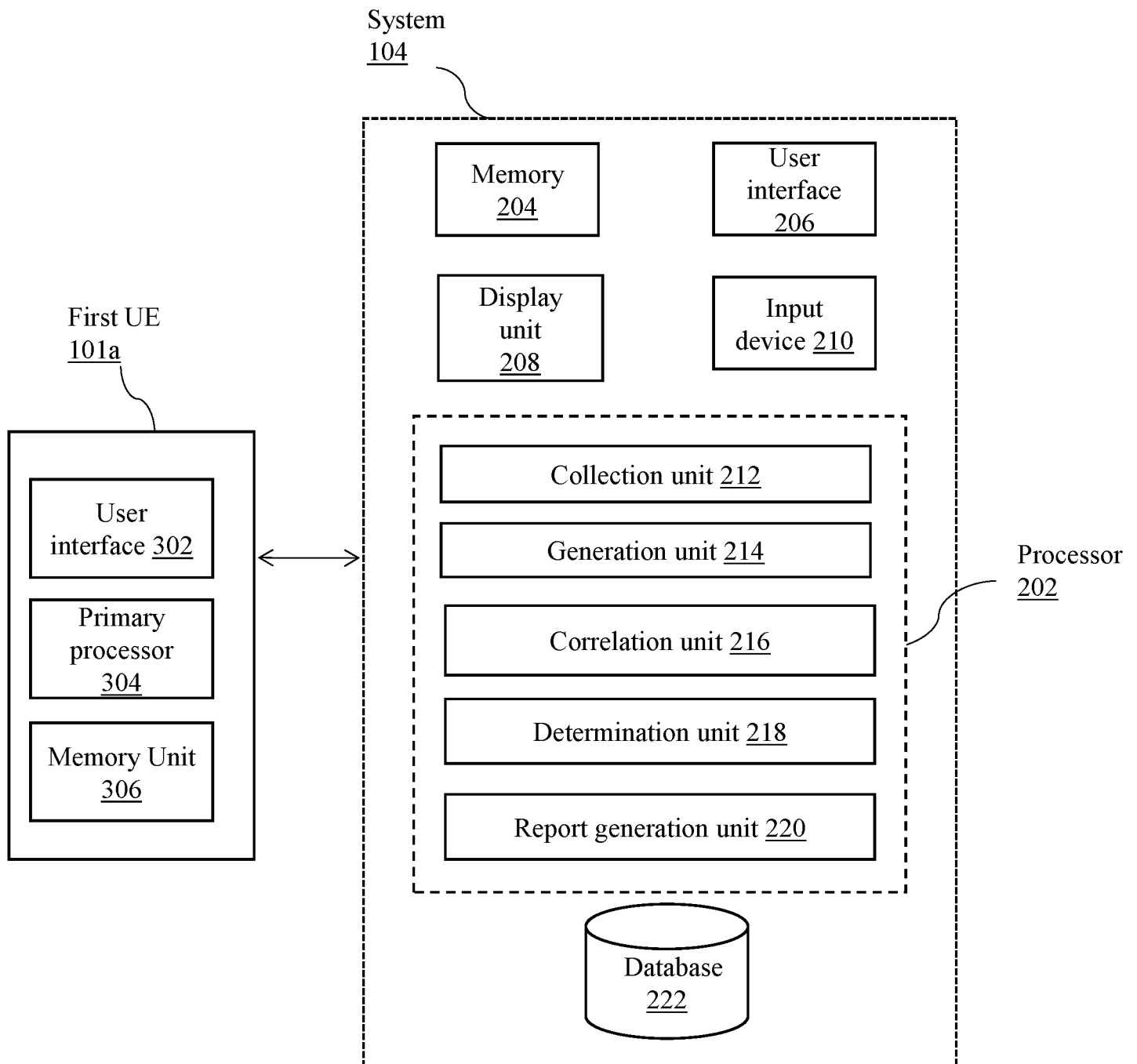


FIG. 3

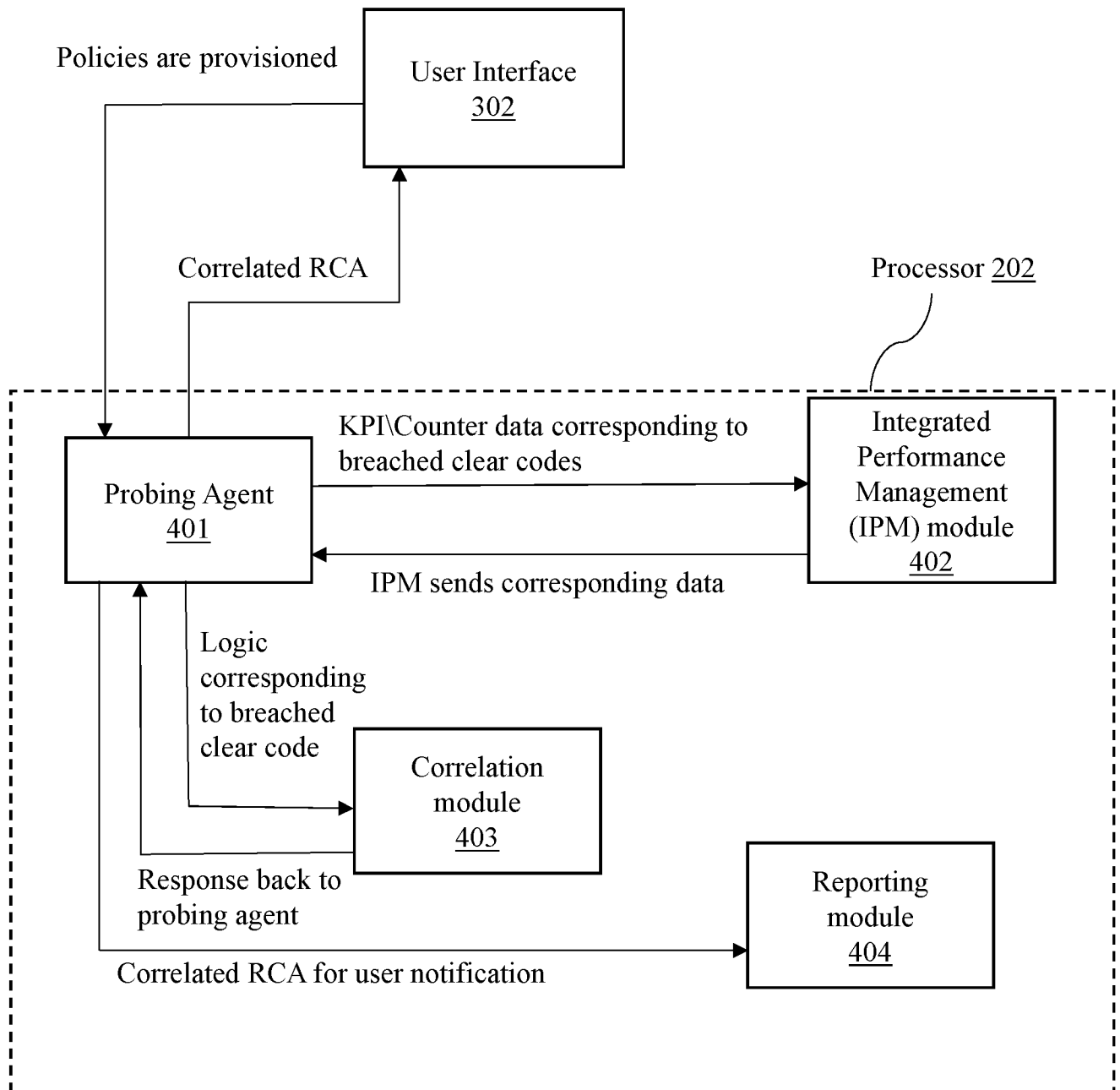


FIG. 4

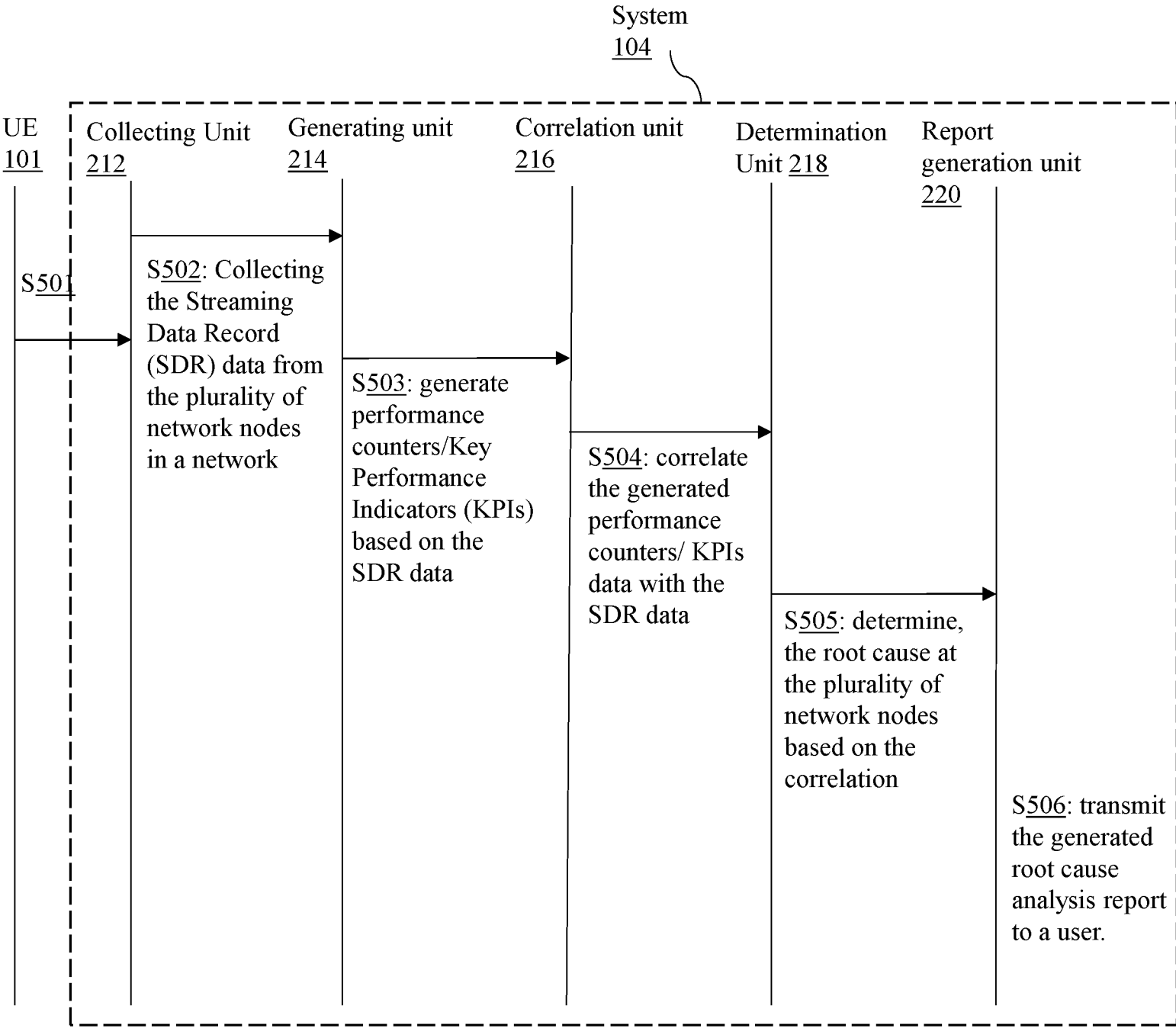


FIG. 5

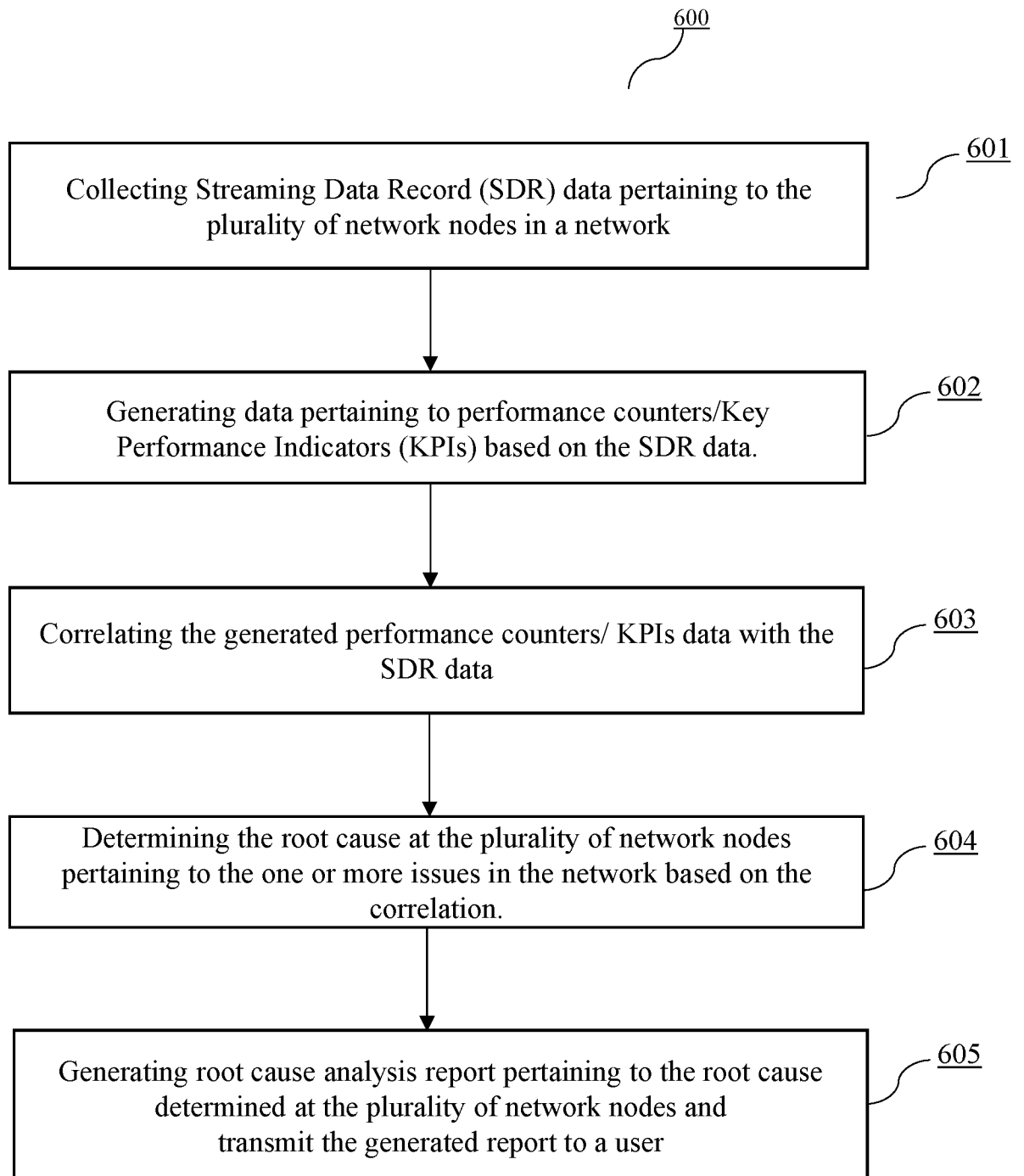


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/051270

A. CLASSIFICATION OF SUBJECT MATTER
H04L41/0631, H04L41/0677 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)

PatSeer, IPO Internal Database

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP2019511787A (ANRITSU CORP.) 25 April, 2019 (25-04-2019) (English translation copy from Google patents) Whole document specifically abstract and description	1-16
Y	WO2022073591A1 (HUAWEI TECHNOLOGY CO LTD.) 14 April, 2022 (14-04-2022) Whole document specifically abstract and description	1-16

☐ 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

"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

"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

26-11-2024

Date of mailing of the international search report

26-11-2024

Name and mailing address of the ISA/

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

Authorized officer

Mohammad Shoaib

Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IN2024/051270

Citation	Pub.Date	Family	Pub.Date
JP 2019511787 A	25-04-2019	EP 3436951 B1	20-03-2024
		CN 108780418 A	09-11-2018
		WO 2017172541 A1	05-10-2017
		US 10686681 B2	16-06-2020
WO 2022073591 A1	14-04-2022	EP 4214909 A1	26-07-2023