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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 March 2011 (03.03.2011)

PCT

(10) International Publication Number
WO 2011/025424 A1

(51) International Patent Classification:
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/SE2009/050973

(22) International Filing Date:
28 August 2009 (28.08.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BERTZE, Åsa** [SE/SE]; Fridhemsgatan 31, S-112 40 Stockholm (SE). **VALKÓ, Andras Gergely** [HU/HU]; Virányos köz 3, HU-1125 Budapest (HU). **VERES, András** [HU/HU]; Bocskai u. 43-45 IX/203, HU-1113 Budapest (HU).

(74) Agent: **VALEA AB**; Box 7086, S-103 87 Stockholm (SE).

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

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

(54) Title: HANDLING ALARMS BASED ON USER SESSION RECORDS

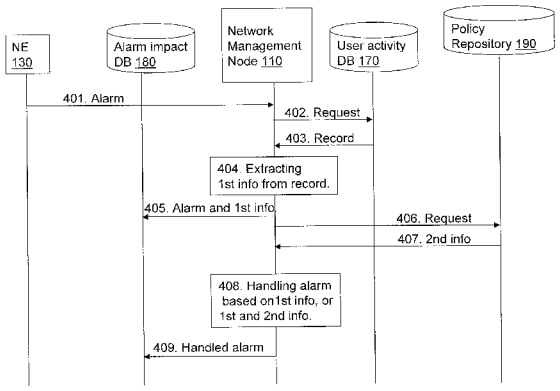

Fig. 4

(57) Abstract: A method is provided in a network management node (110) for handling an alarm caused by a fault in a communications system (100). An alarm caused by a fault in the communications system (100) is received (401) from a first network element (130) within the communications system (100). The alarm is associated with an identity of the first network element (130), and an alarm time associated with the time when the alarm was active. After receiving the alarm, the network management node sends (402) a request to a user activity database (170), requesting one or more matching records. Each of the matching records is requested to comprise an identity equal to the identity of the first network element (130) associated with the alarm, and a record time period that comprises the time when the alarm was active. The network management node receives (403) one or more matching records from the user activity database (170), which one or more matching user session records identify the user sessions being affected by the alarm, and then handles (408) the alarm based on the one or more matching user session records.

WO 2011/025424 A1

HANDLING ALARMS BASED ON USER SESSION RECORDS

TECHNICAL FIELD

The present invention relates to a method and an arrangement in a network management node. In particular, it relates to handling of an alarm caused by a fault in a communications system.

BACKGROUND

When a fault occurs somewhere in a communication network, a Network Element (NE) will send a notification, an alarm, to the network management system. The alarm usually contains certain information that the NE knows about the origin, probable cause and severity of the alarm, e.g.:

- Time - which gives the time the alarm was issued.
- Object ID - which identifies the Managed Object in the NE sending the alarm.
- Severity - which indicates the severity of the alarm, in a range lowest-highest.
- Event Type -which gives some indication of what happened.
- Probable Cause - which gives some indication of why it happened.
- Specific Problems - which clarifies what happened.
- Proposed Repair Actions - which gives some suggestion about what to do.

The task for the service provider (potentially aided by some automatic algorithms) is to analyze all the received alarms in terms of network and service impact, and trigger appropriate actions to mitigate the faults.

A non-trivial task in this process is to identify, based on a potentially very large number of alarms from different network elements, the actual faults (root causes) which are causing the alarms. This is generally referred to as alarm correlation, and there exists several methods, such as neural network assisted, rule, cognitive or flow-based methods, for performing alarm correlation.

Another important task in this process is to prioritize the received alarms, in order to judge which alarms are most important and need to be resolved first. The Severity fields of the individual alarms can serve as one input to this prioritization. There are methods

proposed that automatically assign alarm priority, based on neural networks that continuously learn from manually assigned priorities in trouble-tickets.

WO2005/032186 describes a method for Performance Management of Cellular Mobile Packet Data Networks which involves capturing raw traffic traces over standardized interfaces of an operational cellular mobile data network, and correlating the information to build a traffic and session database. This involves parsing through various signalling messages to construct the association between subscribers, sessions and transactions. As a result, a user session data base is created and maintained that contains traffic information for users and locating the session to certain cell locations and identities, among them IP addresses of certain nodes in the data path.

For a service provider it is important to be able to determine the severity of alarms in terms of user and service impact. Prioritization of alarms is today mostly performed manually by network administrators, based on their experience and support systems, which is a very time consuming task.

The alarm Severity field can help in a first rough prioritization of alarms, for example an alarm of Critical severity, indicating that a link between two NEs is broken is obviously more important to resolve than alarms of Minor severity. However, there is only a weak correlation between the alarm Severity field and the actual priority that is manually assigned to an alarm. Also when there are several NEs issuing alarms of the same severity at the same time the prioritization process becomes more complex, and the Severity field is of little help.

Two basic examples show the difficulty of user and service aware alarm prioritization:

- A High Priority alarm from an NE that is currently not serving any users should receive lower priority than a Medium Priority alarm from an NE that is serving 1000 Gold subscription users.
- An alarm from an NE that is currently delivering a high priority (e.g. high margin) end-user service should receive higher priority than an alarm from an NE that only delivers best effort traffic.

One main problem with existing methods is that they do not take into account the current user activity and traffic situation. Therefore it is not possible to prioritize the alarms in terms of how they affect users and services in the network.

SUMMARY

It is therefore an object of the invention to provide a mechanism that improves the handling of alarms in a communications network.

According to a first aspect of the invention, the object is achieved by a method in a network management node for handling an alarm caused by a fault in a communications system. The communications system comprises the network management node and network elements. The network elements are adapted to serve users. The network management node is accessible to a user activity database. The user activity database comprises user session records. Each user session record is associated with parameters relating to a user session, which parameters comprises a record time period during which period the user session took place, an identity of the user using the session, and an identity of each network element involved in the user session during the time period. An alarm caused by a fault in the communications system is received from a first network element within the communications system. The alarm is associated with an identity of the first network element, and an alarm time associated with the time when the alarm was active. After receiving the alarm, the network management node sends a request to the user activity database, requesting one or more matching records. Each of the matching records is requested to comprise an identity equal to the identity of the first network element associated with the alarm, and a record time period that comprises the time when the alarm was active. The network management node receives one or more matching records from the user activity database, which one or more matching user session records identify the user sessions being affected by the alarm. The network management node then handles the alarm based on the one or more matching user session records.

According to a second aspect of the invention, the object is achieved by a network management node within a communications system. The communications system comprises network elements. The network elements are adapted to serve users. The network management node is accessible to a user activity database, which user activity database comprises user session records. Each user session record is associated with parameters relating to a user session. The parameters comprises a record time period during which period the user session took place, an identity of the user using the session, and an identity of each network element involved in the user session during the time period. The network management node comprises a receiving unit configured to receive

from a first network element within the communications system, an alarm caused by a fault in the communications system. The alarm is associated with an identity of the first network element, and an alarm time associated with the time when the alarm was active. The network management node further comprises a requesting unit configured to send a request to the user activity database, requesting one or more matching records. Each of the matching records is requested to comprise an identity equal to the identity of the first network element associated with the alarm, and a record time period that comprises the time when the alarm was active. The receiving unit further is configured to receive one or more matching records from the user activity database. The one or more matching user session records identify the user sessions being affected by the alarm. The network management node further comprises a handling unit configured to handle the alarm based on the one or more matching user session records.

Thanks to the received user sessions records related to the alarm, the network management node can handle the alarm based on a more relevant foundation, which in turn means an improved handling of alarms in the communications network.

An advantage with the present solution is that it enables user and service aware handling of alarms, including better prioritization of alarms which takes into account how many and which users/services that are actually affected by an alarm.

A further advantage with the present solution is that it enables analysis of users and/or services that are often affected by alarms or parts of the network where many users are often affected by alarms. Such results may for example be used for network planning and optimization purposes.

A further advantage with the present solution is that it enables dynamic prioritization of alarms according to the service provider's user and service policies.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is described in more detail with reference to attached drawings illustrating exemplary embodiments of the invention and in which:

Figure 1 is a schematic block diagram illustrating embodiments of a communication network.

Figure 2 is a combined schematic block diagram and flowchart depicting embodiments of a method.

Figure 3 is a schematic diagram illustrating embodiments of a user activity database.

Figure 4 is a schematic diagram illustrating embodiments of a user activity database.

Figure 5 is a schematic block diagram illustrating embodiments of a communication network.

Figure 6 is a schematic block diagram illustrating embodiments of a network management node.

DETAILED DESCRIPTION

In brief the present solution and its embodiments are about the following:

For a received alarm a network management node accesses a user activity database to read the user activity in a network element or part of network element that generated the alarm. The network management node attaches such information to the basic network element alarm. The network management node then processes the alarm, and may further use also policy information about subscribers and services to prioritize between the enhanced alarms. The output may e.g. be a prioritization of alarms based on the service(s) they impact.

Figure 1 depicts a **communications system 100**. The communications system 100 uses technologies such as e.g. Long Term Evolution (LTE), Wideband Code Division Multiple Access (WCDMA), Global System for Mobile communications (GSM)/ Enhanced Data Rates for GSM Evolution (EDGE), Worldwide Interoperability for Microwave Access (WiMAX), System Architecture Evolution (SAE), Universal Mobile Telecommunications System (UMTS), IP technology, Ethernet technology.

The communications system 100 further comprises a **network management node 110** managing a **communications network 120** comprising **network elements 130, 140**. The network management node 110 may perform the activities, methods, procedures,

and tools that pertain to the operation, administration, maintenance, and provisioning of the communications system 100. This comprises e.g., configuration of the managed network elements 130, 140, analysis of the performance of the services and network elements 130, 140 in the communications system 100, and network planning and upgrade. The network management node 110 further handles alarms caused by faults in the communications system 110.

The network elements 130, 140 serves **user equipments 150, 160** used by end users from now on called users. The user equipments 150, 160 may be computers, mobile phones or any other user equipments capable of communicating with the communications network 120. The communication network may e.g. be a Wideband Code Division Multiple Access (WCDMA) network, an LTE/SAE network, a Wireless Local Area Network (WLAN), a Digital Subscriber Line (DSL) network, or an optical fibre network.

The network management node 110 may e.g. be an Operations Support Systems (OSS) node or any other node managing a communications network.

The network elements 130, 140 may e.g. be a NodeB (NB) base station, an Radio Network Controller (RNC), a Serving General packet radio service Support Node (SGSN), an Gateway General packet radio service Support Node (GGSN) or any other serving node within a WCDMA network, or an eNodeB (eNB) base station, a Mobility Management Entity (MME), a Service GateWay (SGW), a Packet data network GateWay (PGW), an Internet protocol Multimedia System (IMS) or any other network element in a LTE/SAE network, or an IP router in an IP-based network, or an Ethernet switch in an Ethernet network.

User activity database

Network-wide information about individual user activity and in some cases service usage is stored in a **user activity database 170**. The network management node 110 is accessible to this user activity database 170, which user activity database 170 stores the information in form of user session records.E ach user session record is associated with parameters relating to a user session, which parameters in its most general form comprises a record time period during which period the user session took place, and an identity of the user 150, 160 using the session. The user identity may be a global identifier of the user, such as e.g. the International Mobile Subscriber Identity IMSI of the user. The parameters further comprise an identity of each network element 130, 140 involved in the user session during its time period i.e. between the start time and end time of the session. These involved network elements may also be referred to as network resources. This may

be a list of the network elements 130, 140, and maybe also other network resources, that the user was active in during the time of this record. In some embodiments, the parameters associated with each user session record may further comprise object identities relating to identification of the parts of a network element 130, 140 being involved in the user session. The object identities may also be referred to as network resources. I.e. the network resources comprise, on the least detailed level, network elements. It may also comprise more detailed resources i.e. the object identities, within each network element, such as a logical function in a network element, or a specific board of a network element, or e.g. a specific cell in a network element 130, 140. Further, the user activity data base 170 may comprise service information, i.e. information about what type of services the user was using during the time of this record.

The network-wide information about individual user activity and service usage may be constructed by a user session analysis function e.g. within the network management node 110. This may be performed for example from interface probing at multiple measurement points, or from **reports sent 171** from the network elements 130, 140 if available. This information is stored in the user activity data base 170. Interface probing means capturing raw packet traces over standardized interfaces, and parsing through the traces in order to extract and correlate the information. E.g., interface probing of the S11 interface, between MME and SGW, and parsing the traces in order to reconstruct the session management procedures of each user.

The granularity of the network resources and service information data available in the user activity data base 170 may depend on the level of information that is reported by individual network elements 130, 140 to the network management node 110 and/or the information available from interface probes.

The Network resources can in the simple case be a list of network elements that the user is registered in. If more detailed information is available, then a more advanced user activity database 170 may include additional attributes, such as more detailed information about which parts of a network element that the user is "located" in, e.g. which cell, or which logical network element function.

The details of the service information field may also vary depending on the implementation of the user session analysis function. Examples of potential service information are:

• The bearers of a user and the Quality of Service (QoS) level of those. A bearer refers to a "virtual" connection between two endpoints (e.g. a UE and a PDN-GW) which is established in a LTE/SAE system before any traffic can be sent between the endpoints.

• Services used, e.g., Voice over IP (VoIP), Video Telephony, Mobile TV, web browsing, streaming, etc. e.g., obtained from service node reports.

• Traffic types used, e.g., web, Peer to Peer (P2P), e-mail, ftp download, video, streaming, e.g. obtained from deep packet inspection on traffic interface.

An example of a simple user activity database 170 is shown in **Figure 2**, which contains only information about user location in different network elements at different times, and no service usage information. Such information may be created by correlating just a few different network element reports.

A more advanced user activity database 170 example is shown in **Figure 3**, where a more detailed level of network resources as well as service information is comprised.

As mentioned above, the network management node 110 further handles alarms caused by faults in the communications system 110. It may be a variety of different faults such as a link failure, that a disk is full, that a board is faulty, that an interface card is dropping packets, etc. When a fault occurs somewhere in a communication network 120, a network element such as e.g. network element 130, will send a notification, an alarm, to the network management node 110, see arrow 175 in Figure 1.

The present solution method for handling an alarm caused by a fault in a communications system 100, according to some embodiments will no be described with reference to the combined signalling diagram and flowchart depicted in **Figure 4**. The method comprises the following steps, which steps may as well be carried out in another suitable order than described below:

Step 401

The network management node 110 receives an alarm caused by a fault in the communications system from one of the network elements, in this example the first network element 130. This may be performed by an alarm message being sent from the first network node 130 to the network management node 110 or to an alarm data base (not shown) being accessible by the management node 110. The network management node may read the alarm in the alarm data base after receiving a notification about a new alarm. The alarm is associated with an identity of the first network element 140 and an alarm time associated with the time when the alarm was active. The alarm may further be associated with an object identity. The object identity relates to an identification of a part of the network element 130, 140 that issued the alarm, and may be any managed object

in the network element 130, physical or logical. The object identity may for example by a specific piece of hardware, like a board, or a logical function in the network element. This may be referred to as Managed Object and is a well defined concept of how a network elements parts are modelled.

For example at time t an alarm from eNB x arrives to the network management node 110, which indicates that the connection to the antenna in cell 2 is broken. The following information may then be extracted from the alarm:

- NE identity = eNB x
- Object identity = cell 2
- Time = t

Step 402

To find out which users and sessions that are actually affected by the alarm, the network management node 110 sends a request to the user activity database 170, requesting one or more matching records, that matches the network element sending the alarm and any user session that were going on at the time the alarm was sent. I.e. where each of the matching records comprises an identity equal to the identity of the first network element 130 associated with the alarm, and a record time interval that comprises the time when the alarm was active.

In some embodiments, each of the matching records further is requested to comprise an object identity equal to the object identity comprised in the received alarm. For example, if the alarm identifies that that the connection to the antenna in cell 2 is broken in network element 1 that issued the alarm, then not all records from the user activity database that has network elements 1 as network element should be considered a match, but only the ones that have both network element 1 and cell 2 in the record. This makes the matching more precise if this information is available.

Step 403

If matching entries are found in the user activity database, the network management node 110 receives one or more matching records from the user activity database 170.

Step 404

This is an optional step. The network management node 110 extracts information from each matching record. The information extracted from the each match is in this document referred to as the first information. The first information comprises in its most

simple form, information about the user session associated with the matching record. The one or more user sessions extracted from the one or more matching records are the sessions being affected by the alarm. Further information may be extracted from the matching record, as mentioned above, such as a list of the network resources that the user was active in during the time of this record, service information, etc.

Step 405

This is an optional step. The network management node 110 may be accessible to an **alarm impact database 180**, see also Figure 1. In the most general embodiment, the alarm impact data base 180 stores the relationship between network element alarms and user sessions. I.e. as a result, each alarm is mapped to the set of user sessions that may have been impacted by the alarm in the alarm impact database 180.

Each data record in the alarm impact database 180 corresponds to one network element alarm. In addition, the alarm impact database may store, for each alarm data record, a list of user service information such as traffic information that is impacted by the alarm. In this optional step, the network management node 110 stores in the alarm impact database 180, the record for the received alarm being associated with the first information in the received one or more matching records from the user activity database 170, i.e. the first information associated with the set of user sessions impacted by the alarm. A copy of each alarm in the alarm database and copies of entries in the user activity database 170 may be stored in the alarm impact database, but as an alternative, pointers to the relevant entries in the alarm database and/or in the user activity database 170 may be stored.

If no match is found, information about this may be attached to the alarm and may be stored in the alarm impact database 180.

Step 406

This is also an optional step. The network management node 110 may be accessible to a **policy repository 190**, see also Figure 1. The policy repository 190 for subscriber and service policies may comprise information about priorities of different subscribers and services that are offered in the communication network 100. These policies are adjustable by the service provider, since they may depend for example on the service provider's business model. In this optional step the network management node 110 sends a request to the policy repository 190, requesting information. The information relating to the policy repository 190 is in this document is referred to as the second

information. The requested second information comprises information about user policies and/or service policies associated with each user and/or service affected by the alarm.

Step 407

This is also an optional step that will be taken if optional step 406 is taken. In this step the network management node 110 receives the requested second information from the policy repository.

Step 408

The network management node 110 then handles the alarm. In the most general embodiment the alarm is handled based on only the first information. In other embodiments, the alarm is handled based on both first information and the second information. In some embodiments this step of handling the alarm comprises establishing priority of the alarm, e.g. by computing the alarm priority. In other embodiments the handling may involve analysis of users and/or services that are often affected by alarms or parts of the network where many users are often affected by alarms. Such results may for example be used for network planning and optimization purposes. An advantage with the present solution is that the network management 110 may handle the alarm by using input from the alarm impact database 180 and the policy repository 190 in order to compute priorities for the different alarms. I.e., the user and service impact of each alarm may be used as basis for the prioritization. According to service provider policies the alarms are prioritized so that alarms affecting important users and services receive higher priority in the output alarm list.

Step 409

This step is optional. In this step the network management node 110 may store in the alarm impact database180, the established priority of the alarm associated with the record for the received alarm, i.e. in this way the priority information may be added to the alarm data record in the alarm impact database 180.

Figure 5 shows an example of the present solution in an LTE/SAE system. Only a few network elements are shown in the picture for simplicity, but there may be more network elements involved in the process. The network elements shown in the figure are:

- eNB – LTE Radio Base Station
- MME – Mobility Management Entity

- SGW – Serving Gateway
- PGW – Packet Data Network Gateway
- IMS – IP Multimedia Subsystem

Three user equipments UE1, UE2 and UE3 are shown in Figure 5. The different network elements may be configured to report when certain events happen, for example when a protocol message is sent or received, or when an internal procedure is completed or a decision is made. Each network element reports about information that is naturally available in the network element, e.g. with additional attributes such as timestamps and identities which enables correlation of events from different network elements across the system.

Reports from different network elements in the system are correlated, and the user activity database 170 is continuously updated with real-time information about user locations and service usage. In an LTE/SAE example the eNB may report about UE S1 contexts. S1 is the standardized interface between eNB and the Evolved Packet Core (EPC), and UE S1 context is a per UE logical connection between MME and eNB, and radio bearer handling (setups and releases). The MME may report about Packet Data Network (PDN) connection and Evolved Packet System (EPS) bearer handling, and the PGW may provide information about UE IP address allocation. The IMS system events may comprise information about user services, such as e.g. establishments of Voice over IP calls.

Figure 3 shows an example of a user activity database 170 after correlation of events from several network elements in an LTE/SAE system.

As an example, at time t an alarm from eNB 3 arrives to the Network Management node 110 e.g. to an Alarm Impact Analysis Function (AIAF) within the Network Management node 110, which indicates that the connection to the antenna in cell 2 is broken. As mentioned above, the following information is extracted from the alarm

- NE identity = eNB 3
- Time = t
- Object identity = cell 2

and the user activity database 170 is queried by the network management node 110 for matches with this information. The user activity database 170 may give a reply which means that there are currently 10 users which have a radio connection to cell 2 in eNB 3 and that 7 of these are using the VoIP service, and 3 are using web browsing.

The alarm impact database 180 is updated with information about the relation between this alarm and the 10 affected records in the user activity database 170.

The network management node 110, e.g. an Alarm Prioritizing Function (APF) within the network management node 110 then processes the enhanced alarms and combines it with information about user and subscriber policies for this service provider. The alarm is assigned a priority based on the 7 VoIP users and 3 web browsing users affected by the alarm.

The details of the network resources stored in the user activity database 170 may be low if the system does not support to locate a user in a more detailed manner. In the worst case only the network element is reported, which means that for high aggregation nodes (e.g., the MME an LTE/SAE system) there will be many users identified as potentially affected by an alarm.

To limit this effect an additional field may be included in the network element alarm. In addition to severity information in the alarms, the alarm impact database 180 may store a traffic impact factor. This factor may estimate the ratio of connections or sessions impacted by the alarm. One example is a core node, which has X internal boards to handle a traffic function. If one of them goes down, the ratio of impact may be estimated as 1/x. The traffic impact factor may then be taken into account by the network management node 110, in some embodiments by the APF when handling the alarm such as when estimating the priority of the alarm.

The traffic estimate may be provided by the network element generating the alarm, or be calculated by the network management node 110, in some embodiments by the AIAF.

Relating an alarm to the impact that it has on specific users and services, requires data to be collected from several sources in the network, and the processing and correlation of such data. A single network element can not determine the impact of an alarm on users and services for several reasons:

- The network element does not always have the necessary information about what services and users it is currently serving, e.g., in an LTE/SAE network the eNB does not know about the IMSIs of the users that it is serving.

- The network element does not have knowledge about user and service policies specified by the service provider, and therefore cannot prioritize alarms based on important users/services locally.

The advantage of handling the alarm on network management level such as in the present solution is that information from several different sources in the network can be

combined in order to provide a more relevant foundation for alarm handling. Connecting an alarm to affected user sessions on network management level enables detailed policy-based prioritization, as well as drill-downs to which users are affected by which alarms.

To perform the method steps above for handling an alarm caused by a fault in a communications system 100, the first network management node 110 comprises an arrangement depicted in **Figure 6**. As mentioned above, the network management node 110 is comprised within a communications system 100. The communications system 100 comprises the network elements 130, 140. The network elements 130, 140 are adapted to serve the users 150, 160.

The network management node 110 is accessible to the user activity database 170. The user activity database 170 comprises user session records. Each user session record is associated with parameters relating to a user session, which parameters comprises a record time period during which period the user session took place, an identity of the user 150, 160 using the session, and an identity of each network element 130, 140 involved in the user session during the time period.

The network management node 110 comprises a **receiving unit 600** configured to receive from the first network element 130 within the communications system 100, an alarm caused by a fault in the communications system 100. The alarm is associated with an identity of the first network element 130, and an alarm time associated with the time when the alarm was active.

The receiving unit 600 further is configured to receive one or more matching records from the user activity database 170. The one or more matching user session records identify the user sessions being affected by the alarm.

The network management node 110 further comprises a **requesting unit 610** configured to send a request to the user activity database 170, requesting one or more matching records. Each of the matching records is requested to comprise an identity equal to the identity of the first network element 130 associated with the alarm, and a record time period that comprises the time when the alarm was active.

In some embodiments each record of the user activity database further is associated with service information related to the user session in the user session record,

The network management node 110 further comprises a **handling unit 620** configured to handle the alarm based on the one or more matching user session records.

In some embodiments, the network management node 110 further comprises an **extracting unit 630** configured to extract a first information from each matching record, which first information comprises the user identity associated with the matching user session record.

The first information may further comprise all network elements 130, 140 being involved in the user session associated with the matching record, and/or information about one or more services related to the user session associated with the matching record.

In these embodiments, the handling unit 620 may further be configured to handle the alarm based on the one or more matching user session records and being based on the extracted first information.

In some embodiments the network management node 110 is accessible to the alarm impact database 180. In these embodiments the network management node 110 may further comprise **a storing unit 640** configured to store in the alarm impact database 180, a record for the received alarm being associated with the first information.

In some embodiments, the network management node 110 is accessible to the policy repository 190. In these embodiments, the requesting unit 610 may further be configured to send a request to a policy repository 190, requesting a second information. The second information comprises information about user policies and/or service policies associated with each user and/or service affected by the alarm. In these embodiments, the receiving unit 600 may further be configured to receive the requested second information from the policy repository 190, and the handling unit 620 may further be configured to handle the alarm based on the second information.

In some embodiments, the handling unit 620 further is configured to handle the alarm by establish a priority of the alarm, analyse users and/or services that are often affected by alarms, or parts of network where many users are often affected by alarms.

In some embodiments, the storing unit 640 is further configured to store the established priority of the alarm in the alarm impact database, associated with the record for the received alarm.

In some embodiments, the parameters associated with each user session record further comprises object identities relating to identification of the parts of a network element 130, 140 being involved in the user session. In these embodiments the received alarm may further be associated with an object identity, which object identity relates to an identification of a part of the network element 130, 140 that issued the alarm. Each of the matching records is further configured to be requested by the requesting unit 610 to comprise an object identity equal to the object identity comprised in the received alarm.

In some embodiments, the received alarm is further associated with a traffic impact factor. The traffic impact factor comprises an estimate of the ratio of connections or sessions impacted by the alarm. In this case the handling unit 620 further is configured to handle the alarm based on the extracted traffic impact factor.

The present mechanism for handling an alarm caused by a fault in a communications system 100 may be implemented through one or more processors, such as a processor 650 in the network management node 110 depicted in Figure 6, together with computer program code for performing the functions of the present solution. The program code mentioned above may also be provided as a computer program product, for instance in the form of a data carrier carrying computer program code for performing the present solution when being loaded into the network management node 110. One such carrier may be in the form of a CD ROM disc. It is however feasible with other data carriers such as a memory stick. The computer program code can furthermore be provided as pure program code on a server and downloaded to the network management node 110 remotely.

When using the word "comprise" or “comprising” it shall be interpreted as non-limiting, i.e. meaning "consist at least of".

The present invention is not limited to the above described preferred embodiments. Various alternatives, modifications and equivalents may be used. Therefore, the above embodiments should not be taken as limiting the scope of the invention, which is defined by the appending claims.

CLAIMS

1. A method in a network management node (110) for handling an alarm caused by a fault in a communications system (100),

the communications system (100) comprising the network management node (110) and network elements (130, 140),

which network elements (130, 140) are adapted to serve users (150, 160),

the network management node (110) is accessible to a user activity database (170), which user activity database (170) comprises user session records,

wherein each user session record is associated with parameters relating to a user session, which parameters comprises a record time period during which period the user session took place, an identity of the user (150, 160) using the session, and an identity of each network element (130, 140) involved in the user session during the time period,

the method comprising:

receiving (401) from a first network element (130) within the communications system (100), an alarm caused by a fault in the communications system (100), the alarm being associated with an identity of the first network element (130), and an alarm time associated with the time when the alarm was active,

sending (402) a request to the user activity database (170), requesting one or more matching records, where each of the matching records is requested to comprise an identity equal to the identity of the first network element (130) associated with the alarm, and a record time period that comprises the **time** when the alarm was active,

receiving (403) one or more matching records from the user activity database (170), which one or more matching user session records identify the user sessions being affected by the alarm,

handling (408) the alarm based on the one or more matching user session records.

2. Method according to claim 1, further comprising:

extracting (404) a first information from each matching record, which first information comprises the user identity associated with the matching user session record,

and wherein the step of *handling* (408) the alarm based on the one or more matching user session records, comprises being based on the extracted first information.

3. Method according to any of the claims 1-2, wherein the network management node (110) is accessible to a alarm impact database (180), the method further comprising:

storing (405) in the alarm impact database (180), a record for the received alarm being associated with the first information.

4. Method according to any of the claims 1-3, wherein the first information further comprises all network elements (130, 140) being involved in the user session associated with the matching record.

5. Method according to any of the claims 1-4, wherein each record of the user activity database further is associated with service information related to the user session in the user session record, and

wherein the extracted first information further comprises information about one or more services related to the user session associated with the matching record.

6. Method according to any of the claims 1-5, wherein the network management node (110) is accessible to a policy repository (190), the method further comprising:

sending (406) a request to a policy repository (190), requesting a second information, which second information comprises information about user policies and/or service policies associated with each user and/or service affected by the alarm,

receiving (407) the requested second information from the policy repository (190),

and wherein the step of handling (408) the alarm further is based on the second information.

7. Method according to any of the claims 1-6, wherein the step of handling (408) the alarm comprises establishing priority of the alarm, analysing of users and/or services that are often affected by alarms, or parts of the network where many users are often affected by alarms.

8. Method according to any of the claims 6-7, further comprising:

storing (409) the established priority of the alarm in the alarm impact database, associated with the record for the received alarm.

9. Method according to any of the claims 1-8, wherein the parameters associated with each user session record further comprises object identities relating to identification of the parts of a network element (130, 140) being involved in the user session, and wherein the received alarm further is associated with an object identity, which object identity relates to an identification of a part of the network element (130, 140) that issued the alarm, and wherein each of the matching records further is requested to comprise an object identity equal to the object identity comprised in the received alarm.

10. Method according to any of the claims 1-9, wherein the received alarm further is associated with a traffic impact factor, which traffic impact factor comprises an estimate of the ratio of connections or sessions impacted by the alarm, and wherein the step of handling (408) the alarm further is based on the extracted traffic impact factor.

11. A network management node (110) within a communications system (100), which communications system (100) comprises network elements (130, 140), the network elements (130, 140) being adapted to serve users (150, 160),

the network management node (110) being accessible to a user activity database (170), which user activity database (170) comprises user session records,

wherein each user session record is associated with parameters relating to a user session, which parameters comprises a record time period during which period the user session took place, an identity of the user (150, 160) using the session, and an identity of each network element (130, 140) involved in the user session during the time period,

the network management node (110) comprises a receiving unit (600) configured to receive from a first network element (130) within the communications system (100), an alarm caused by a fault in the communications system (100), the

alarm being associated with an identity of the first network element (130), and an alarm time associated with the time when the alarm was active,

characterized in that:

the network management node (110) comprises a requesting unit (610) configured to send a request to the user activity database (170), requesting one or more matching records, where each of the matching records is requested to comprise an identity equal to the identity of the first network element (130) associated with the alarm, and a record time period that comprises the time when the alarm was active,

the receiving unit (600) further is configured to receive one or more matching records from the user activity database (170), which one or more matching user session records identify the user sessions being affected by the alarm, and

the network management node (110) further comprises a handling unit (620) configured to handle the alarm based on the one or more matching user session records.

12. Network management node (110) according to claim 11, further comprising:

an extracting unit (630) configured to extract a first information from each matching record, which first information comprises the user identity associated with the matching user session record,

and wherein the handling unit (620) further is configured to handle the alarm based on the one or more matching user session records and being based on the extracted first information.

13. Network management node (110) according to any of the claims 11-12, wherein the network management node (110) is accessible to a alarm impact database (180), the network management node (110) further comprising a storing unit (640) configured to store in the alarm impact database (180), a record for the received alarm being associated with the first information.

14. Network management node (110) according to any of the claims 11-13, wherein the first information further comprises all network elements (130, 140) being involved in the user session associated with the matching record.

15. Network management node (110) according to any of the claims 11-14, wherein each record of the user activity database further is associated with service information related to the user session in the user session record, and wherein the extracted first information further comprises information about one or more services related to the user session associated with the matching record.

16. Network management node (110) according to any of the claims 11-15, wherein the network management node (110) is accessible to a policy repository (190),
and wherein the requesting unit (610) further is configured to send a request to a policy repository (190), requesting a second information, which second information comprises information about user policies and/or service policies associated with each user and/or service affected by the alarm,
and wherein the receiving unit (600) further is configured to receive the requested second information from the policy repository (190),
and wherein the handling unit (620) further is configured to handle the alarm based on the second information.

17. Network management node (110) according to any of the claims 11-16, and wherein the handling unit (620) further is configured to handle the alarm by establish a priority of the alarm, analyse users and/or services that are often affected by alarms, or parts of network where many users are often affected by alarms.

18. Network management node (110) according to any of the claims 16-17, wherein the storing unit (640) further is configured to store the established priority of the alarm in the alarm impact database, associated with the record for the received alarm.

19. Network management node (110) according to any of the claims 11-18, wherein the parameters associated with each user session record further comprises object identities relating to identification of the parts of a network element (130, 140) being involved in the user session, and wherein the received alarm further is associated with an object identity, which object identity relates to an identification of a part of the network element (130, 140) that issued the alarm, and wherein each of the matching records further is configured to be requested by the requesting unit (610)

to comprise an object identity equal to the object identity comprised in the received alarm.

20. Network management node (110) according to any of the claims 11-19, wherein the received alarm further is associated with a traffic impact factor, which traffic impact factor comprises an estimate of the ratio of connections or sessions impacted by the alarm, and wherein the handling unit (620) further is configured to handle the alarm based on the extracted traffic impact factor.

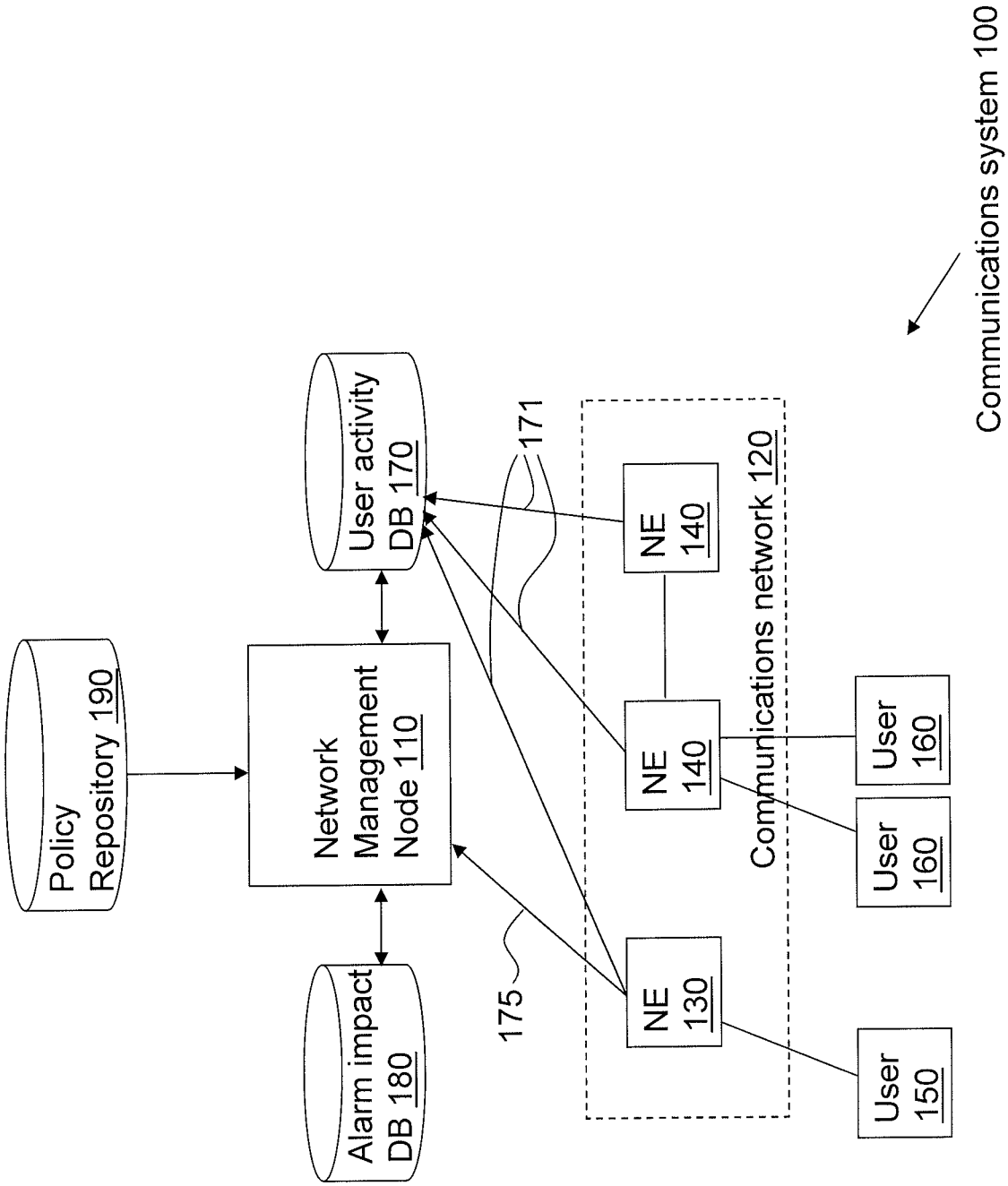
Communications system 100
Communications network 120
Policy Repository 190
Network Management Node 110
User activity DB 170
Alarm impact DB 180
171
175
NE 140
NE 140
NE 130
User 160
User 160
User 150

Fig. 1

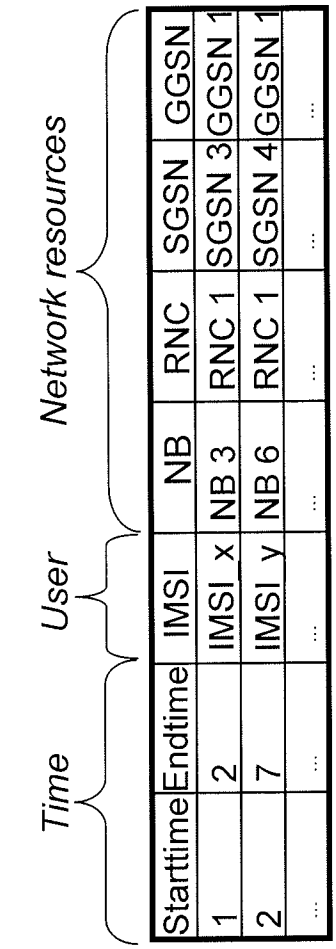
Time
User
Network resources
Starttime
Endtime
IMSI
NB
RNC
SGSN
GGSN
1
2
IMSI_x
NB 3
RNC 1
SGSN 3
GGSN 1
2
7
IMSI_y
NB 6
RNC 1
SGSN 4
GGSN 1

Fig. 2

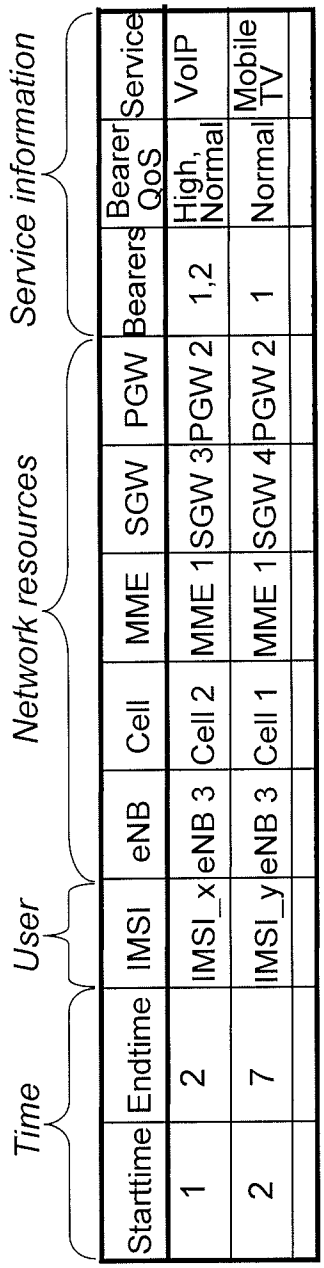
Time
User
Network resources
Service information
Starttime
Endtime
IMSI
eNB
Cell
MME
SGW
PGW
Bearers
Bearer QoS
Service
1
2
IMSI_x
eNB 3
Cell 2
MME 1
SGW 3
PGW 2
1,2
High, Normal
VoIP
2
7
IMSI_y
eNB 3
Cell 1
MME 1
SGW 4
PGW 2
1
Normal
Mobile TV

Fig. 3

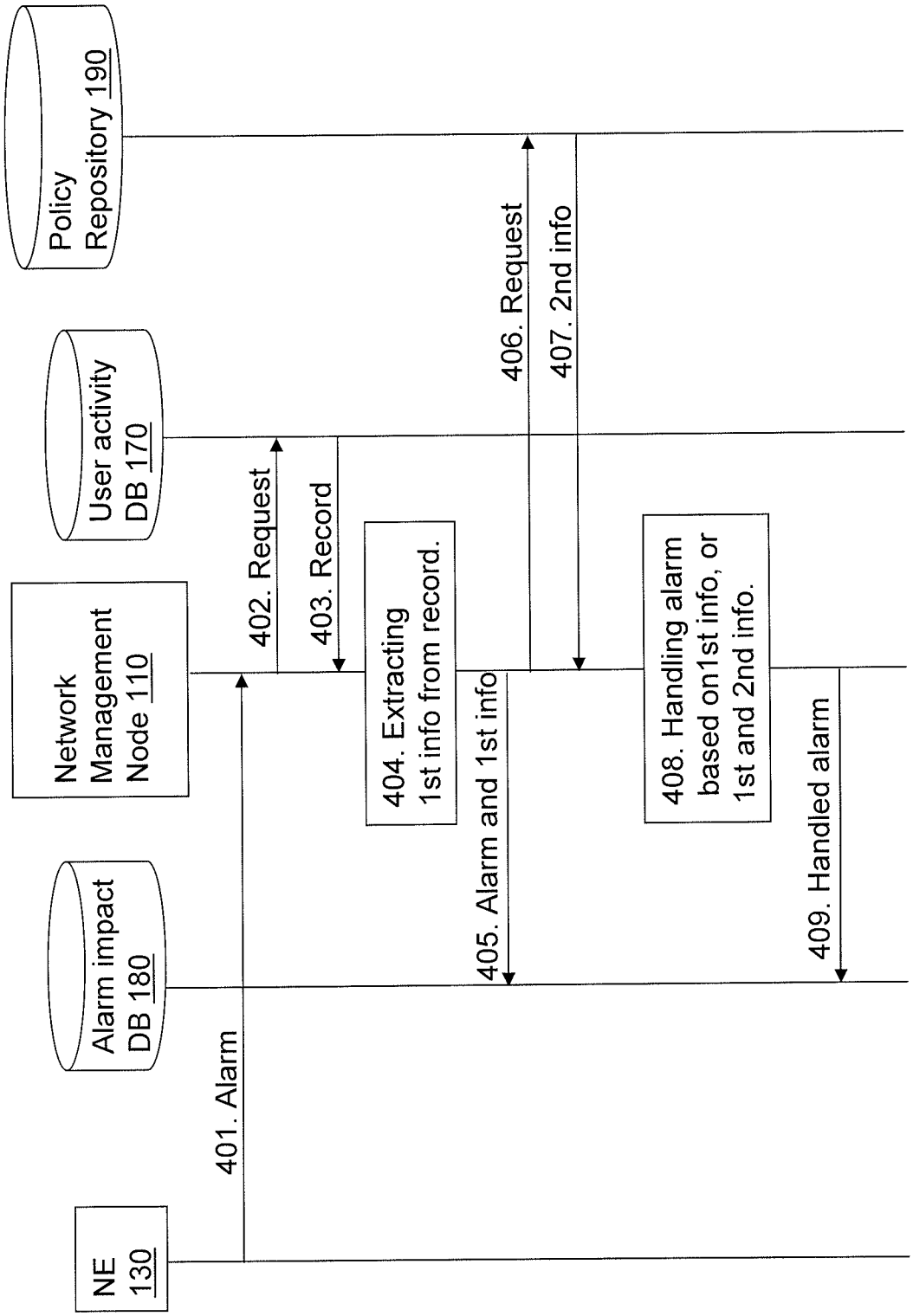
Policy Repository 190
User activity DB 170
Network Management Node 110
Alarm impact DB 180
NE 130
401. Alarm
402. Request
403. Record
404. Extracting 1st info from record.
405. Alarm and 1st info
406. Request
407. 2nd info
408. Handling alarm based on1st info, or 1st and 2nd info.
409. Handled alarm

Fig. 4

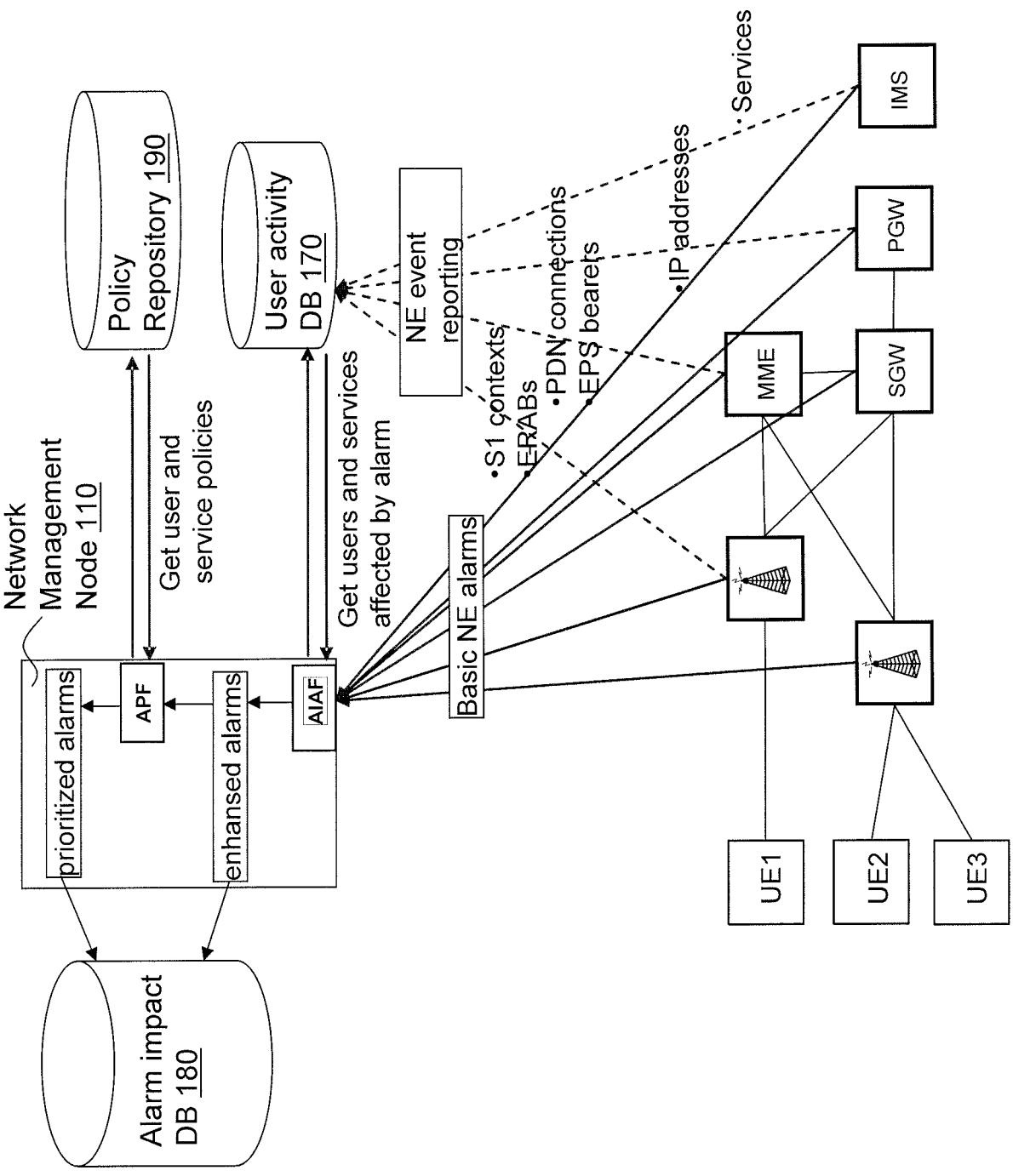
Network Management Node 110
Policy Repository 190
User activity DB 170
Alarm impact DB 180
Get user and service policies
Get users and services affected by alarm
APF
AIAF
prioritized alarms
enhansed alarms
Basic NE alarms
NE event reporting
•S1 contexts
•ERABs
•PDN connections
•EPS bearers
•IP addresses
•Services
IMS
PGW
SGW
MME
UE1
UE2
UE3

Fig. 5

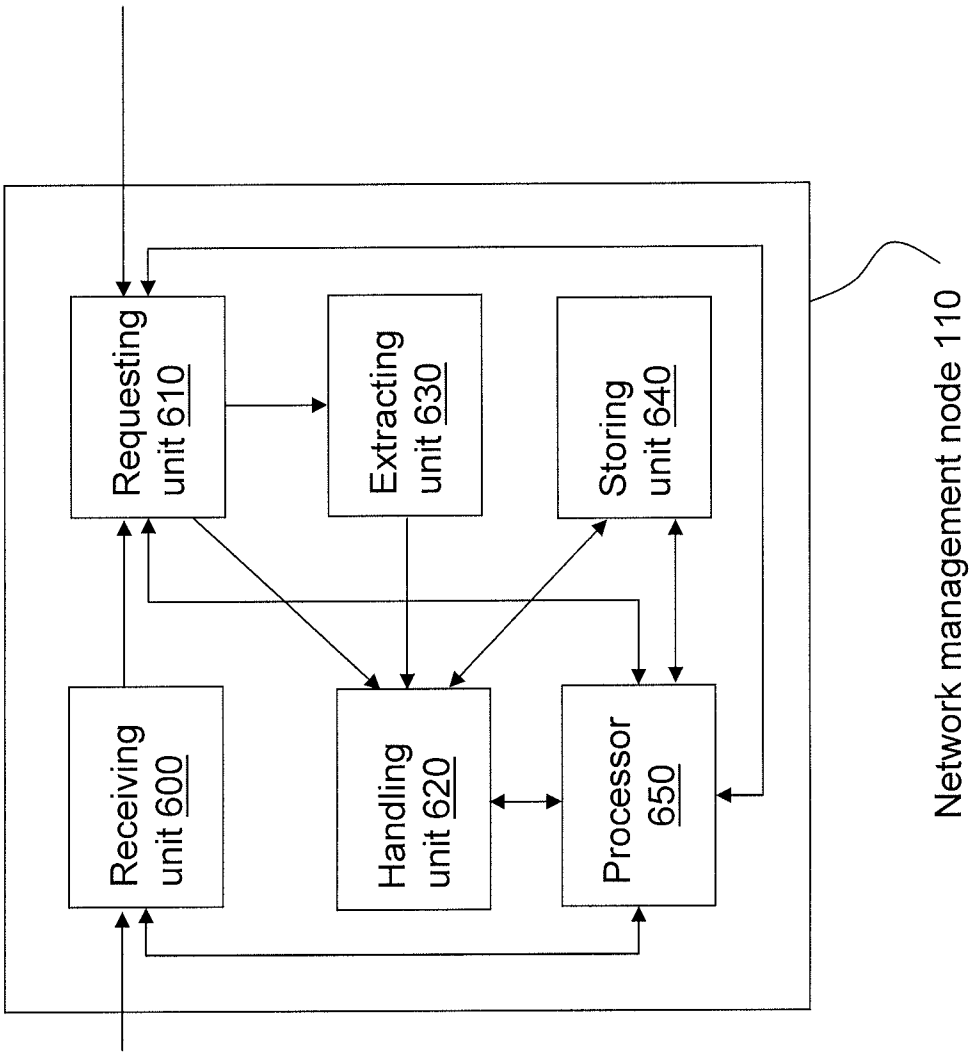
Requesting unit 610
Extracting unit 630
Storing unit 640
Receiving unit 600
Handling unit 620
Processor 650
Network management node 110

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050973

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04Q, H04W

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

SE,DK,FI,NO classes as above

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

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 20040024767 A1 (CHEN), 5 February 2004 (05.02.2004), figure 1, claims 1-2,5,9,12, abstract, paragraphs (0010),(0015)-(0016), (0019)-(0026),(0034)-(0037),(0041)	1-5,7-15, 17-20
	--	
Y	EP 1764981 A1 (TEKTRONIX INC.), 21 March 2007 (21.03.2007), abstract, paragraphs (0003)-(0007), (0017)-(0018),(0035)	1-5,7-15, 17-20
	--	
A	KR 100811847 B1, SAMSUNG ELECTRONICS CO LTD, 2008-03-10: (abstract) Retrieved from: WPI database	1-20
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
25 May 2010	26 -05- 2010
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Anders Ackeberg / JA A Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050973

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20060002409 A1 (MENON ET AL), 5 January 2006 (05.01.2006), abstract, paragraphs (0003), (0028)-(0030)	1-20
	--	
A	US 5761502 A (JACOBS), 2 June 1998 (02.06.1998), abstract	1-20
	--	
A	US 20090119545 A1 (PHAM ET AL), 7 May 2009 (07.05.2009), abstract, paragraphs (0004)-(0012), (0023),(0030)	1-20
	--	
A	WO 2006057588 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)), 1 June 2006 (01.06.2006), abstract	1-20
	--	
A	WO 2007059672 A1 (HUAWEI TECHNOLOGIES CO., LTD.), 31 May 2007 (31.05.2007), abstract	1-20
	--	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2009/050973

International patent classification (IPC)

H04L 12/24 (2006.01)

Download your patent documents at www.prv.se
The cited patent documents can be downloaded:

- From "Cited documents" found under our online services at www.prv.se (English version)
- From "Anförda dokument" found under "e-tjänster" at www.prv.se (Swedish version)

Use the application number as username. The password is **OJLLRPRRQI**.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.

US	20040024767	A1	05/02/2004	NONE			
EP	1764981	A1	21/03/2007	JP	2007089166	A	05/04/2007
				US	20070067264	A	22/03/2007
US	20060002409	A1	05/01/2006	NONE			
US	5761502	A	02/06/1998	CA	2241905	A	10/07/1997
				EP	0870383	A	14/10/1998
				JP	2000503183	T	14/03/2000
				WO	9724838	A	07/08/1997
US	20090119545	A1	07/05/2009	NONE			
WO	2006057588	A1	01/06/2006	CN	101069445	A	07/11/2007
				EP	1820359	A	22/08/2007
WO	2007059672	A1	31/05/2007	NONE			