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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
26 January 2017 (26.01.2017)

WIPO | PCT

(10) **International Publication Number**
WO 2017/012654 A1

(51) **International Patent Classification**: ***H04W 24/00*** (2009.01)

(21) **International Application Number**: PCT/EP2015/066669

(22) **International Filing Date**: 21 July 2015 (21.07.2015)

(25) **Filing Language**: English

(26) **Publication Language**: English

(71) **Applicant**: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-164 83 Stockholm (SE).

(72) **Inventors**: **HÓCZA, András**; Molnair u. 13/B, H-2626 Nagymaros (HU). **KOVÁCS, Benedek**; Vas utca 18, H-1088 Budapest (HU).

(74) **Agent**: **LIND, Robert**; Marks & Clerk LLP, Fletcher House (2nd Floor), Heatley Road, The Oxford Science Park, Oxford Oxfordshire OX4 4GE (GB).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: PREDICTIVE PROCEDURE HANDLING

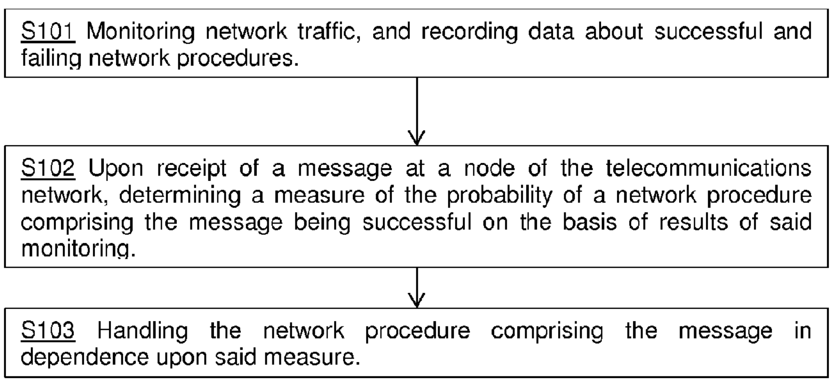

Figure 6

(57) **Abstract**: A method in a telecommunications network. Network traffic is monitored, and data about successful and failing network procedures is recorded. Upon receipt of a message at a node of the telecommunications network, a measure of the probability of a network procedure comprising the message being successful on the basis of results of said monitoring is determined; and the network procedure comprising the message is handled in dependence upon said measure of the probability.

WO 2017/012654 A1

Predictive Procedure Handling

Technical Field

The invention relates to the handling of network procedures in a telecommunications network. In particular, the invention relates to the handling of network procedures using probabilistic techniques.

Background

As new telecommunications standards with more features are brought out, the network procedures involved become more complex. For example, attaching to a 2G or 3G network typically requires three Home Location Register (HLR) or Home Subscriber Service (HSS) queries, whereas attachment and registration to an IP Multimedia Subsystem (IMS) enabled Long Term Evolution (LTE) network typically requires eleven or more queries to the HSS. Each particular network procedure (e.g. registration, session initiation, etc.) consists of a particular set of messages (which may vary slightly depending on network configuration, user settings, or current network status).

As an example, Figure 1 shows the layout of a typical mobile telecommunications network, and Figures 2 and 3 show the signalling involved for a User Equipment (UE) to register with an IMS network (the boxes labelled “initial EPC attach to default APN” (Access Point Name) and “Connect to IMS APN” in Figure 3 each comprise the messages shown in Figure 2).

While the nodes themselves have been similarly upgraded to cope with the increased demand, the higher signalling requirements for each procedure in new standards can result in greater sensitivity in the network to “blind load phenomena”. Blind loads are system loads resulting from procedures which will eventually be rejected.

There are two circumstances in which blind loads can occur:

a) In a partial network failure, e.g. when a certain node fails, or an interface of a node fails, requests to be served by this node will timeout, and the procedure which the requests relate to may be dropped.

b) In mass registration events, where the network is facing a large number of a specific procedure (for example registration). Such behaviour may be triggered when a node restarts, and therefore all users who would normally be assigned to that node attempt to reattach immediately, or when an unexpected event occurs and many users wish to initiate the same procedure (e.g. in the event of a large emergency, where many users attempt to contact others or phone for help).

Taking registrations as an example, the registration procedure is shown in Figures 2 and 3. If a failure occurs at a late stage of registration, e.g. if the MMTel AS has failed, and this causes the registration to be dropped, then all of the messages which are part of the procedure are effectively useless, and would be considered blind load. In a mass registration event, if the sheer number of requests causes a node to fail, then the problem is exacerbated, especially as nodes may not have the capacity to re-attempt failing requests as well as handling incoming requests, which could potentially cause nodes earlier in the chain to fail as well.

Current solutions for addressing the node failure include timeout mechanisms, resending the failed message(s), and/or reselecting the destination node. An example is described in IETF RFC 2543.

Another countermeasure which may be used to reduce blind load is “blacklisting” nodes for which messages have failed – e.g. if sending messages to a node fails a certain number of times within a certain time period, then no further messages are sent to that node until the time expires. This can cause further issues, as when a node is taken off the blacklist, the sudden rush or requests can cause it to fail again – resulting in oscillatory behaviour where the node repeatedly fails, is blacklisted, is restored, and then fails again.

A further countermeasure is throttling traffic on the network – i.e. not allowing more than a certain number of requests per unit time over an interface, either by rejecting new requests after a certain limit, or by a priority based throttling approach where procedures at a later stage are allowed through, and procedures at earlier stages are dropped. However, such throttling will often drop sequences which would have been successful if left to run their course. If no throttling is used, then it is very likely that many requests will get rejected and retried until the network is overwhelmed – and then when the network eventually fails and is restored, the UEs all attempt to register again, and it fails again.

Static throttling does not consider the procedure in progress – this can often result in procedures being rejected at a late stage, which causes a high level of blind load.

Priority based throttling is extremely complex and hard to design for a network using equipment from multiple vendors. Partial implementation is possible, but rarely results in enough of a gain in stability to offset the cost or the extra dropped procedures.

Summary

In order to reduce blind load in the network more effectively, an approach is proposed in which traffic through the network is monitored, results of this monitoring are used to build up a model, and that model is used to compute a measure of the probability that a message will result in a successful procedure. That measure can then be used to predictively apply throttling to the network where necessary, for example by preferring to terminate network procedures which have a low probability of being successful, or by modifying the procedure onto a more probable path.

According to an aspect of the present invention, there is provided a method in a telecommunications network. Network traffic is monitored, and information about successful and failing network procedures is recorded. Upon receipt of a message at a node of the telecommunications network, a measure of the probability of a network procedure comprising the message being successful on the basis of results of said monitoring is determined; and the network procedure comprising the message is handled in dependence upon said measure of the probability.

Each step may be performed at said node of the telecommunications network, or some steps may be performed at different nodes.

According to a further aspect, there is provided apparatus configured to operate in a telecommunications network. The apparatus comprises a model builder and a model applicator. The model builder is configured to monitor network traffic through the node, and record successful and failing network procedures. The model applicator is configured to determine, for a message received at the apparatus or another node of the network, a measure of the probability of a network procedure comprising the message being a successful network procedure on the basis of results of said monitoring, and to cause the apparatus or the other node to handle the network procedure comprising the message in dependence upon said measure of the probability.

According to a further aspect, there is provided a computer program comprising computer readable code which, when run on an apparatus, causes the apparatus to perform a method according to the first aspect.

According to a further aspect, there is provided a system in a telecommunications network comprising an apparatus mentioned above.

Further embodiments of the invention are described in the appended claims.

Brief Description of the Drawings

Figure 1 is a network diagram of a typical telecommunications network;
Figures 2 and 3 are signalling diagrams showing an exemplary network procedure;
Figure 4 is a schematic diagram of an apparatus according to an embodiment;
Figure 5 is an exemplary output of an N-gram model; and
Figure 6 is a flowchart of a method according to an embodiment.

Detailed Description

In order to reduce the blind load, an approach is proposed below to model the likelihood of success of network procedures, and to apply the model in order to improve network congestion. The modelling and application of the model can be implemented in a variety of ways.

In the simplest embodiment, nodes of the network record the messages which pass through them, and note which ones result in successful interactions. This would clearly result in a very large dataset very quickly, and so only certain properties of the messages may be noted, e.g. the type of message (INVITE, REGISTER, 200OK, etc), the destination, and the next hop node. This allows the data to be consolidated by keeping a count of how many messages with matching properties result in successful or failing network procedures.

For example, it might be determined that 99% of REGISTER requests which are directed to a specific S-CSCF are successful, and that only 10% of INVITE requests directed to a certain external network are successful. When throttling is required, the node handling the messages may drop the INVITE requests directed to the external network as they have a low probability of success, and are unlikely to result in actual session establishment.

As a further example, it may be determined that 99% of requests with a first next hop node are successful, but only 80% of otherwise equivalent requests with a second next hop node. The node handling the requests may route some traffic which is intended to go via the second next hop node instead via the first next hop node in order to improve network reliability.

Other techniques may be used to improve the accuracy of the modelling – for example, techniques from the field of natural language modelling may be used, such as N-grams. Such techniques may be used as a procedure in a telecoms system such as VoLTE is composed of individual messages which may be arranged and executed in various different ways – analogously to words in a sentence. A procedure consists of messages, and machine learning natural language techniques can be adapted to determine the likelihood that a particular sequence of messages results in a successful procedure – i.e. whether the sequence results in an error response or a response indicating success.

There are, broadly speaking, three stages to such modelling: feature selection, model building, and model application.

The feature selection stage involves choosing the parameters on which the model will be based. Selecting irrelevant features will tend to reduce the accuracy of the model, and selecting redundant features will tend to slow down the operation of the model.

For modelling of messages in a telecommunications network, there are two classes of features:

Message features are those which are intrinsic to the messages, for example:

- message type (e.g. REGISTER, INVITE, 200 OK, etc.)
- Sender
- Receiver
- Direction (incoming or outgoing)
- State changes caused or requested by the message
- Request and response codes
- User ID
- Message routing (e.g. the next hop and previous hop nodes in the route the message is taking)

Network features are those which are related to the network as a whole, rather than to an individual message, for example:

- network topology
- network load (either overall load, or load on each link)
- scheduled maintenance
- known failures or other issues

The initial feature space will generally be user defined – e.g. by specifying which features are input into the model. The lists above show only a small proportion of an initial feature space – the feature space may contain all possible information which could be useful in the creation of a model. This feature set may be further refined by machine learning algorithms by analysing which features have the best correlation with success or failure of a procedure, for example by Principal Component Analysis. Reducing the feature set in this way will speed up both the training process for the model, and the application of the model, as the complexity of each operation increases rapidly with increased numbers of features.

The model building step involves “training” the machine learning software on a corpus of training data which contains all of the features of the initial feature space for a large number of procedures. The corpus may be obtained by monitoring traffic in the network. Each message of the corpus may be represented by a combination of the features identified in the feature selection step. This allows the size of the corpus to be reduced, as information such as timestamps which is not relevant to the selected features can be disregarded. The procedures in the corpus are then used to build up a data set which can be used to compute the probability of newly seen procedures, according to the model used.

One model which may be applied is an “N-gram” model. In N-gram models, sequences of N messages are considered, and the probability of success or failure is computed for that sequence based on appearances of that sequence within the corpus. The probability of unknown sequences may be derived from that of known sequences. N-gram models can handle unknown messages (i.e. messages not included in the corpus), but they will generally be assigned a very low probability.

In one embodiment of using the N-gram model, a predetermined number (N-1) of previous messages in the same network procedure as the message is identified. Determining a measure of the probability comprises comparing the message and the previous messages to a list of received message sequences from results of monitoring, each consisting of N messages.

In another embodiment of using the N-gram model, wherein step of monitoring network traffic through the node, and recording successful and failing network procedures comprises, for each sequence of messages of a specified sequence length (N) received as part of a network procedure, the probability is determined that said sequence results in a successful network procedure. The step of determining a measure of the probability comprises matching the message and the previous messages to one of said sequences, and retrieving the probability that said sequence results in a successful network procedure.

An exemplary output of the N-gram model is shown in Figure 5. The first column shows the identifiers for the messages, which encode various features of the messages. The second column shows the assigned probability for the messages, as well as the number of messages in the sequence on which that probability is based (i.e. the entry [3gram] 0.46786 denotes that the probability of 0.46786 has been assigned based on a 3 message sequence (a 3-gram)).

A further set of training may be performed on a second corpus of procedures, to ensure that the probabilities predicted by the model are correct. The model is applied to messages in the second corpus, and the number of errors (i.e. when the model predicts a successful procedure as failing, or a failing procedure as succeeding) is determined. Provided the number of errors is acceptably low, the model may be used.

In order to apply the model, responses based on the computed probabilities must be defined. For example, the system may choose to drop a procedure if the probability of success is below a threshold, in order to reduce blind load in other nodes. The system may modify a message if the probability of success is below a second threshold, but there is an alternate route with a higher probability (e.g. the message is directed to a failing node, but the procedure can be completed using an alternative, more reliable node). The system may raise an alert if the probability is below a third threshold – this alert may be to the network operator, indicating a likely problem, or to the sender of the message, and may indicate a preferred route for the message or a preferred alternative to the procedure.

Figure 4 shows a schematic of an apparatus 101 for building and applying the model mentioned above. The model builder 102 performs the model building steps, and the model applicator 103 performs the model application steps. The model builder 102 and model applicator 103 may be implemented as software modules, as processors within a node, as separate nodes, or together in the same node, or as processes in a distributed computing solution.

The model builder 102 is configured to monitor network traffic through the node, and record successful and failing network procedures. The model applicator 103 is configured to determine, for a message received at the apparatus 101 or another node of the network, a measure of the probability of a network procedure comprising the message being a successful network procedure on the basis of results of said monitoring, and to cause the apparatus 101 or the other node to handle the network procedure comprising the message in dependence upon said measure of the probability.

The model builder and model applicator may be implemented as software modules, as processors within a node, as separate nodes, or together in the same node, or as processes in a distributed computing solution.

As a first example, a particular Wi-Fi network may have a low quality which causes voice and video calls over that network to be frequently dropped. Training the model on training data including such voice and video calls will result in sequences used to establish such voice or video calls being given a low probability (due to the large number of failures). When a session establishment for a voice or video call originating or terminating within the Wi-Fi network is received, the model will predict a low possibility of success. The model applicator can then cause the session establishment to be dropped, for example in a way which would cause it to be reattempted using LTE (or other non-WiFi connectivity).

As a second example, the model applicator may be configured to recognise low probability messages, and to drop any messages which have a probability below a certain threshold in order to reduce blind load.

The model applications may be determined by a further machine learning process. Using the training corpus of network procedures, a “correct” decision can be computed for each procedure, and this data can be used to adjust the response thresholds or response types used by the model applicator. For example, if a procedure was allowed to continue at an early stage, but failed at a later stage, this may indicate that the threshold for dropping or modifying that procedure at an early stage should be raised. Similarly, if the model applicator proposed dropping a large number of procedures which are eventually successful, then this may indicate that the threshold probabilities should be lowered.

The model may be constantly updated by incorporating live network traffic into the model building.

Figure 6 is a flowchart of a method according to an embodiment. Network traffic in the telecommunications network is monitored, and data about successful and failing network procedures is recorded (S101). Upon receipt of a message at a node of the telecommunications network, a measure is determined on the basis of results of the monitoring (S102). The measure is a measure of the probability of a network procedure, comprising the message, being successful. The network procedure comprising the message is then handled in dependence upon the measure.

Monitoring network traffic may comprise monitoring a network load level and/or network error states.

Determining the measure of the probability may comprise the following steps. a) determining a context of the message and comparing the context of the message to recorded network procedures; b) identifying previous network procedures which match the context of the message, and c) determining a proportion of the previous network procedures which were successful.

Although the invention has been described in terms of preferred embodiments as set forth above, it should be understood that these embodiments are illustrative only and that the claims are not limited to those embodiments. Those skilled in the art will be able to make modifications and alternatives in view of the disclosure which are contemplated as falling within the scope of the appended claims. Each feature disclosed or illustrated in the present specification may be incorporated in the invention, whether alone or in any appropriate combination with any other feature disclosed or illustrated herein.

CLAIMS:

1. A method in a telecommunications network, the method comprising:

monitoring network traffic, and recording information about successful and failing network procedures;

upon receipt of a message at a node of the telecommunications network, determining a measure of the probability of a network procedure comprising the message being successful on the basis of results of said monitoring; and

handling the network procedure comprising the message in dependence upon said measure of the probability.

2. A method according to claim 1, wherein each step is performed at said node of the telecommunications network.

3. A method according to claim 1 or 2, wherein handling the network procedure in dependence upon said measure comprises one or more of:

rejecting the network procedure if the measure is below a first threshold;

modifying the message in order to re-route the message or other messages of the network procedure to an alternative path if the measure is below a second threshold; and

alerting a sender of the message and/or a network operator if the measure is below a third threshold.

4. A method according to claim 3, wherein one or more of said thresholds is determined based on a machine learning algorithm applied to a corpus of training data, the corpus of training data comprising a plurality of recorded network procedures.

5. A method according to any one of the preceding claims, wherein determining the measure of the probability comprises:

determining a context of the message and comparing the context of the message to recorded network procedures;

identifying previous network procedures which match the context of the message; and

determining a proportion of the previous network procedures which were successful.

6. A method according to any one of the preceding claims, and comprising identifying a predetermined number (N-1) of previous messages in the same network procedure as the message, wherein determining a measure of the probability comprises comparing the message and the previous messages to a list of received message sequences from results of said monitoring, each consisting of N messages.

7. A method according to claim 5, wherein said step of monitoring network traffic through the node, and recording successful and failing network procedures comprises, for each sequence of messages of a specified sequence length (N) received as part of a network procedure, determining the probability that said sequence results in a successful network procedure, and wherein the step of determining a measure of the probability comprises matching the message and the previous messages to one of said sequences, and retrieving the probability that said sequence results in a successful network procedure.

8. A method according to any preceding claim, wherein monitoring network traffic comprises monitoring properties of each message sent and/or received by the node, the properties comprising any one or more of:

message type;
direction of the message;
sender;
receiver;
state changes caused or requested by the message;
request and/or response codes in the message; and
user IDs associated with the message.

9. A method according to any preceding claim, wherein monitoring network traffic comprises monitoring a network load level and/or network error states.

10. Apparatus (101) configured to operate in a telecommunications network, the apparatus comprising:

a model builder (102) configured to monitor network traffic through the node, and record successful and failing network procedures;

a model applicator (103) configured to determine, for a message received at the apparatus or another node of the network, a measure of the probability of a network procedure comprising the message being a successful network procedure on the basis of results of said monitoring, and to cause the apparatus or the other node to handle the network procedure comprising the message in dependence upon said measure of the probability.

11. Apparatus according to claim 10, wherein the apparatus is configured to handle the network procedure in dependence upon said measure by performing one or more of:

rejecting the network procedure if the measure is below a first threshold;

modifying the message in order to re-route the network procedure to an alternative path if the measure is below a second threshold;

alerting a sender of the message and/or a network operator if the measure is below a third threshold.

12. Apparatus according to claim 10 or 11, wherein the model applicator is configured to determine the measure of the probability by:

determining a context of the message and comparing the context of the message to recorded network procedures;

identifying previous network procedures which match the context of the message; and

determining a proportion of the previous network procedures which were successful.

13. Apparatus according to any of claims 10 to 12, wherein the model applicator is configured to identify a predetermined number (N-1) of previous messages in the same network procedure as the message, wherein determining a measure of the probability comprises comparing the message and the previous messages to a list of received message sequences from results of said monitoring, each consisting of N messages.

14. Apparatus according to claim 13, wherein of the model builder is configured to, for each sequence of messages of a specified sequence length (N) received as part of a network procedure, determine the probability that said sequence results in a successful network procedure, and wherein the model applicator is configured to

determine the measure of the probability by matching the message and the previous messages to one of said sequences, and retrieving the probability that said sequence results in a successful network procedure.

15. Apparatus according to any of claims 10 to 14, wherein the model builder is configured to monitor properties of each message sent and/or received by the node, the properties comprising any one or more of:

message type;
direction of the message;
sender;
receiver;
state changes caused or requested by the message;
request and/or response codes in the message;
user IDs associated with the message.

16. Apparatus according to any of claims 10 to 15, wherein the model builder is configured to monitor a network load level and/or network error states.

17. A computer program comprising computer readable code which, when run on an apparatus, causes the apparatus to perform a method according to any of claims 1 to 9.

18. A system in a telecommunications network comprising an apparatus according to any of claims 10 to 16.

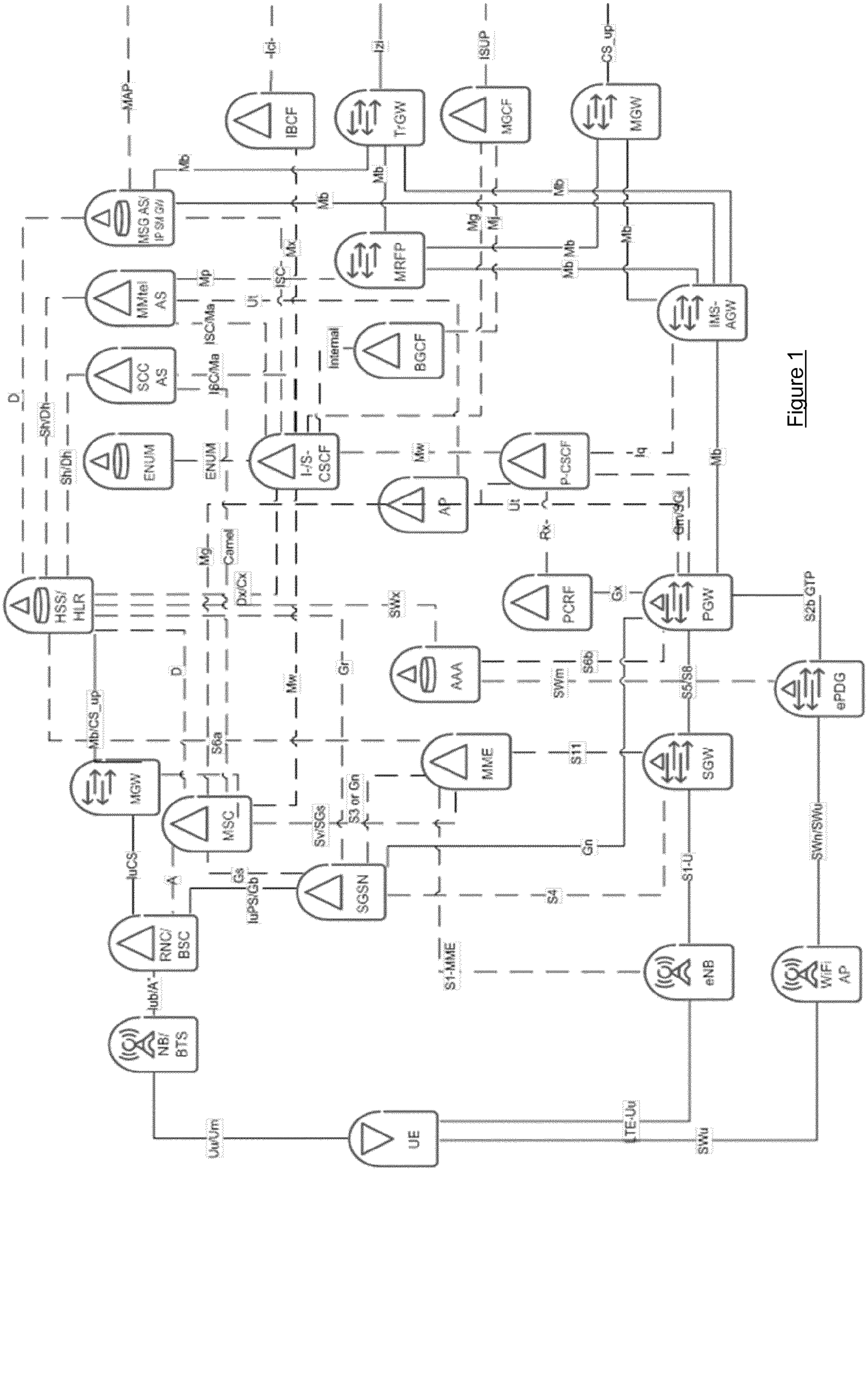
UE
NB/ BTS
RNC/ BSC
SGSN
MSC
MGW
MME
SGW
eNB
WiFi AP
ePDG
AAA
PGW
PCRF
HSS/ HLR
ENUM
I-/S-CSCF
AP
P-CSCF
SCC AS
MMtel AS
BGCF
MSG AS/ IP SM GW
MRFP
IMS-AGW
IBCF
TrGW
MGCF
MGW
Uu/Um
Iub/A*
IuCS
A
Gs
IuPS/Gb
LTE-Uu
SWu
S1-MME
S1-U
S4
Gn
Sv/SGs
S3 or Gn
S6a
S11
SWn/SWu
S5/S8
SWm
S6b
S2b GTP
Gx
Rx
Gm/SGi
Ut
Iq
Mb
Mb/CS_up
D
Mw
Gr
SWx
Dx/Cx
Camel
Mg
Sh/Dh
ENUM
ISC/Ma
Internal
Mp
Mx
Mi
MAP
Ici
Izi
ISUP
CS_up

Figure 1

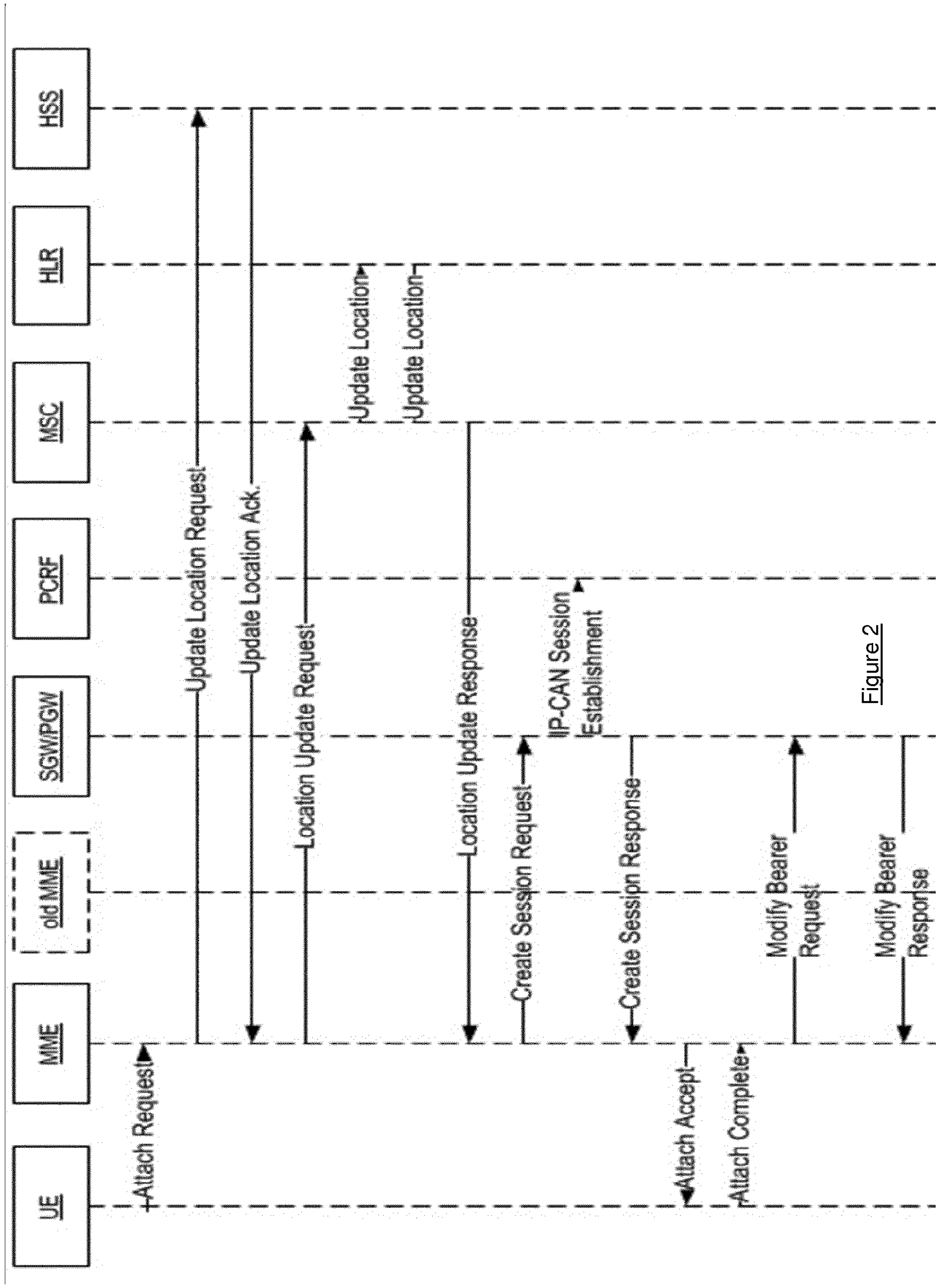
UE
MME
old MME
SGW/PGW
PCRF
MSC
HLR
HSS
Attach Request
Update Location Request
Update Location Ack.
Location Update Request
Update Location
Update Location
Location Update Response
Create Session Request
IP-CAN Session Establishment
Create Session Response
Attach Accept
Attach Complete
Modify Bearer Request
Modify Bearer Response

Figure 2

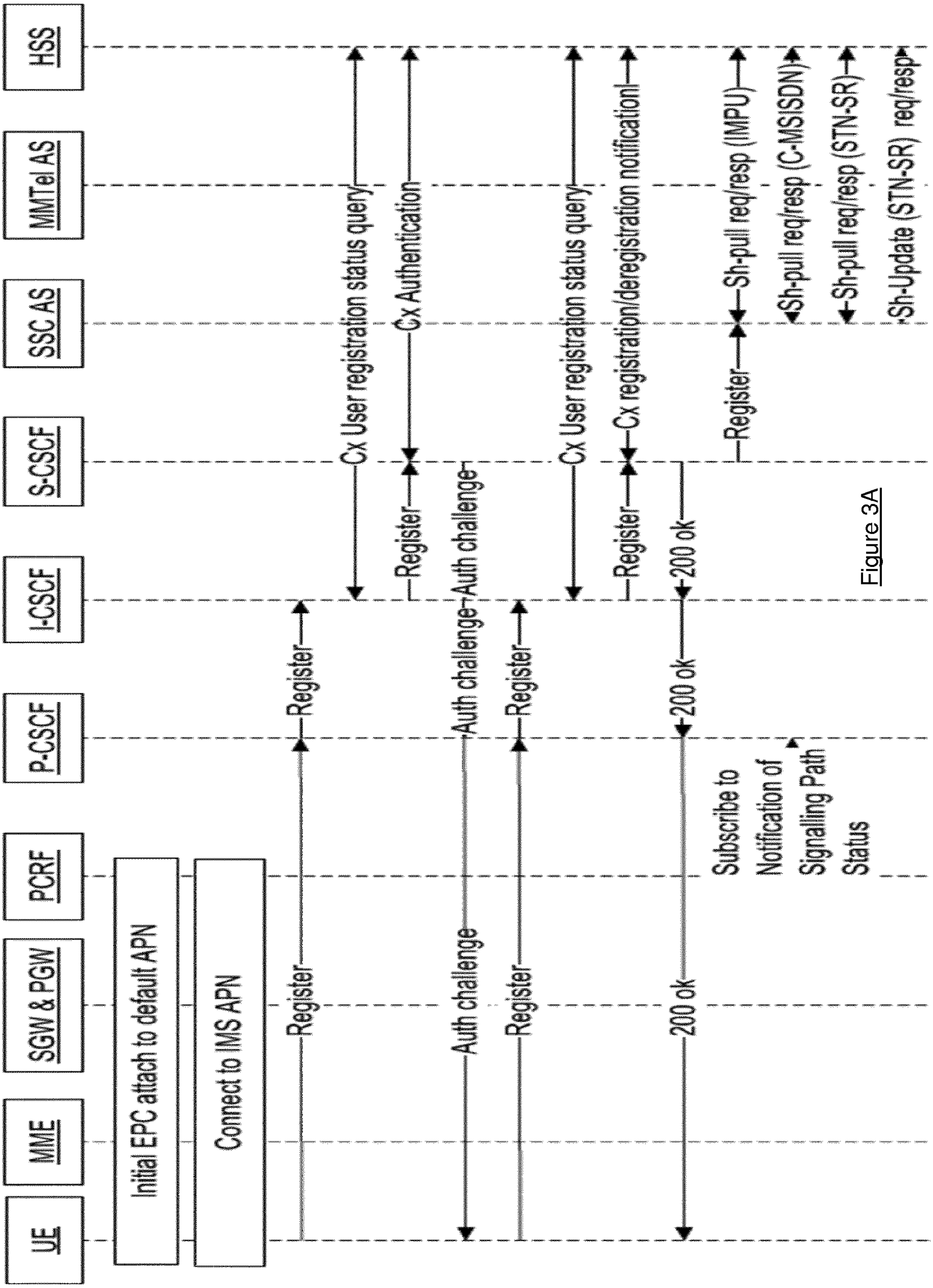
UE
MME
SGW & PGW
PCRF
P-CSCF
I-CSCF
S-CSCF
SSC AS
MMTel AS
HSS
Initial EPC attach to default APN
Connect to IMS APN
Register
Cx User registration status query
Cx Authentication
Auth challenge
Cx registration/deregistration notification
200 ok
Sh-pull req/resp (IMPU)
Sh-pull req/resp (C-MSISDN)
Sh-pull req/resp (STN-SR)
Sh-Update (STN-SR) req/resp
Subscribe to Notification of Signaling Path Status

Figure 3A

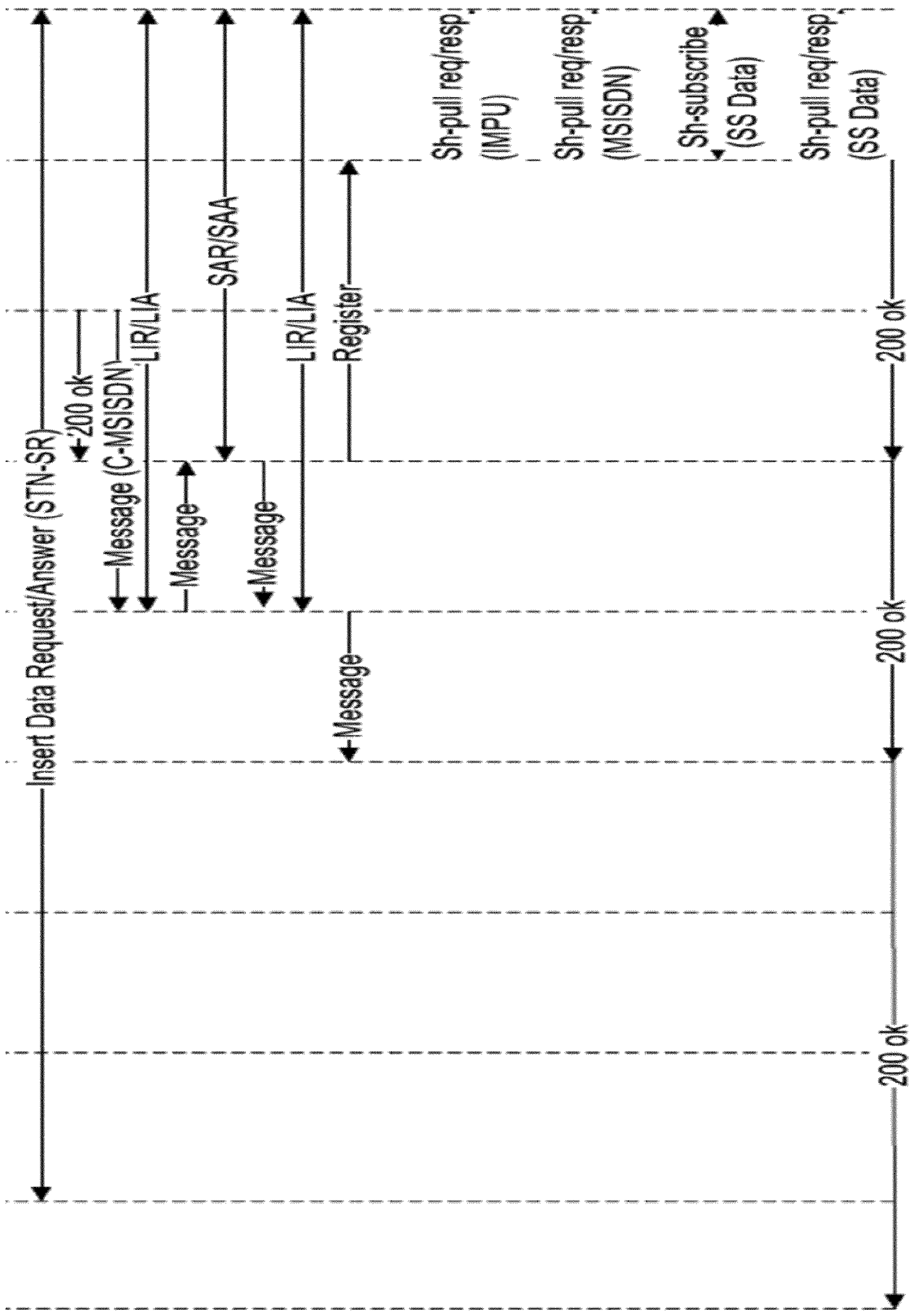
Insert Data Request/Answer (STN-SR)
200 ok
Message (C-MSISDN)
LIR/LIA
Message
Message
SAR/SAA
LIR/LIA
Register
Message
Sh-pull req/resp (IMPU)
Sh-pull req/resp (MSISDN)
Sh-subscribe (SS Data)
Sh-pull req/resp (SS Data)
200 ok
200 ok
200 ok

Figure 3B

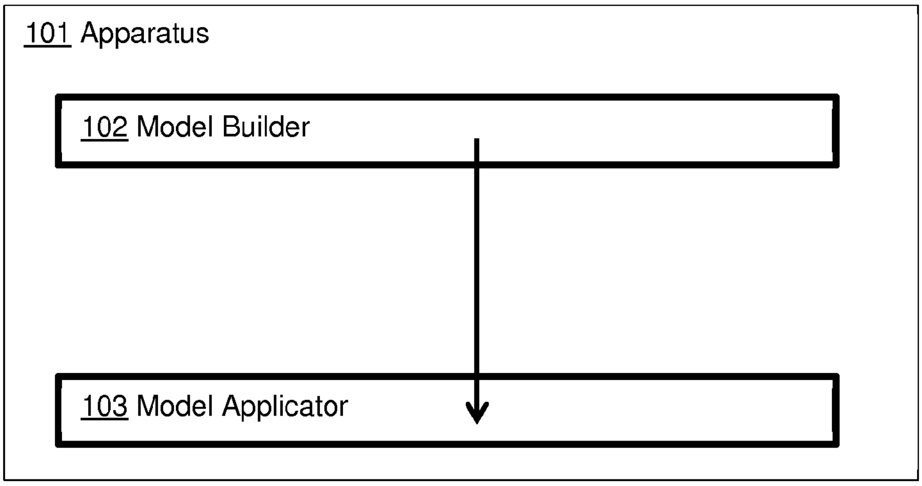

Figure 4

	REGISTER_FR_SIPNUM_TO_UsA_UA_MTAS	[2gram] 0.000584824
	DIAMETER_296_MTAS_283_HSS	[3gram] 0.46786
	DIAMETER_296_HSS_268_2001	[3gram] 0.995349
	DIAMETER_296_MTAS_283_HSS	[3gram] 0.614911
	DIAMETER_296_HSS_268_2001	[3gram] 0.992359
	DIAMETER_296_MTAS_283_HSS	[3gram] 0.614911
	DIAMETER_296_HSS_268_2001	[3gram] 0.992359
	200_FR_SIPNUM_TO_UsA_SR_MTAS	[3gram] 0.0104326
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	[3gram] 0.0243902
	100_FR_UsA_TO_SNUM_SR_MTAS	[3gram] 0.833333
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	[3gram] 0.0806451
Unlikely message →	**INVITE_FR_UsA_TO_SNUM_UA_MTAS**	**[1gram] 5.06249e-007**
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	**[1gram] 6.64977e-006**
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	**[1gram] 6.64977e-006**
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	**[1gram] 6.64977e-006**
	BYE_FR_UsA_TO_SNUM_UA_MTAS	**[1gram] 6.03729e-006**
	200_FR_UsA_TO_SNUM_SR_MTAS	[2gram] 0.304348
	REGISTER_FR_SIPNUM_TO_UsA_UA_MTAS	[2gram] 0.000215221
	200_FR_SIPNUM_TO_UsA_SR_MTAS	[3gram] 0.833333
	DIAMETER_296_MTAS_283_HSS	[3gram] 0.981395
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	**[1gram] 1.46987e-007**
	DIAMETER_296_MTAS_283_HSS	**[1gram] 0.000581213**
	INVITE_FR_UsA_TO_SNUM_UA_MTAS	**[1gram] 4.34705e-007**
Error message →	**408_FR_UsA_TO_SNUM_SR_MTAS**	**[OOV] #INF**

1 sentences, 24 words, 1 OOVs
logprob= -59.8246 ppl= 199.961 ppl1= 247.163

Figure 5

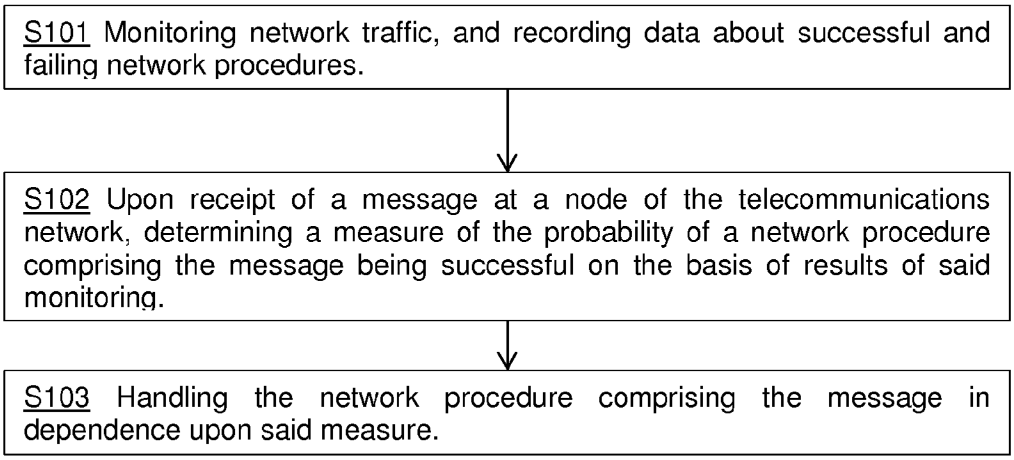
S101 Monitoring network traffic, and recording data about successful and failing network procedures.
S102 Upon receipt of a message at a node of the telecommunications network, determining a measure of the probability of a network procedure comprising the message being successful on the basis of results of said monitoring.
S103 Handling the network procedure comprising the message in dependence upon said measure.

Figure 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/066669

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W24/00
ADD.

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)
H04W

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 1 489 876 A1 (LUCENT TECHNOLOGIES INC [US]) 22 December 2004 (2004-12-22) paragraph [0005] paragraph [0016] - paragraph [0020] figures 1,4 -----	1,10,17,18 2-9,11-16
Y	US 2007/153789 A1 (BARKER CHARLES R JR [US] ET AL) 5 July 2007 (2007-07-05) paragraph [0060] - paragraph [0063] -----	2-9,11-16
X	CN 101 005 688 A (HUAWEI TECH CO LTD [CN]) 25 July 2007 (2007-07-25) the whole document -----	1,10,17,18
A	WO 2008/008412 A2 (LUCENT TECHNOLOGIES INC [US]; YE SIGEN [US]; ZHANG QINQING [US]) 17 January 2008 (2008-01-17) page 7, line 27 - page 9, line 2 figure 2 -----	1-18

☐ 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

"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
7 March 2016	11/03/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Rabe, Marcus

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/066669

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1489876 A1	22-12-2004	DE 602004001811 T2	04-01-2007
		EP 1489876 A1	22-12-2004
		JP 2005012806 A	13-01-2005
		KR 20040111069 A	31-12-2004
		US 2004259528 A1	23-12-2004
US 2007153789 A1	05-07-2007	DE 112006003603 T5	13-11-2008
		KR 20080091195 A	09-10-2008
		US 2007153789 A1	05-07-2007
		WO 2007081649 A2	19-07-2007
CN 101005688 A	25-07-2007	NONE	
WO 2008008412 A2	17-01-2008	CN 101491017 A	22-07-2009
		CN 103179011 A	26-06-2013
		EP 2044737 A2	08-04-2009
		JP 5612307 B2	22-10-2014
		JP 2009543523 A	03-12-2009
		JP 2014212569 A	13-11-2014
		KR 20090030302 A	24-03-2009
		US 2008013462 A1	17-01-2008
		WO 2008008412 A2	17-01-2008