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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2010 (23.09.2010)

PCT

(10) International Publication Number
WO 2010/105808 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04M 3/436* (2006.01)

(21) International Application Number:
PCT/EP2010/001667

(22) International Filing Date:
17 March 2010 (17.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09003822.5 17 March 2009 (17.03.2009) EP

(71) Applicants *(for all designated States except US)*: **NEC EUROPE LTD.** [DE/DE]; Kurfuersten-Anlage 36, 69115 Heidelberg (DE). **NEC CORPORATION** [JP/JP]; 7-1, Shiba 5-chome, Minato-ku, Tokyo, 108-8001 (JP).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KUNZ, Andreas** [DE/DE]; Schlatterstrasse 5, 68542 Heddesheim (DE). **SCHMID, Stefan** [DE/DE]; In der Neckarhelle 30, 69118 Heidelberg (DE). **TAMURA, Toshiyuki** [NL/JP]; New Well Terrace, Miyamaedaira 1-9-27, Kawasaki (JP). **PRASAD, Anand** [JP/JP]; 3-12-12 Kinunodai, Tsukubamirai, Ibaraki 300-2436 (JP).

(74) Agent: **MAISCH, Thomas**; Ullrich & Naumann, Luisenstrasse 14, 69115 Heidelberg (DE).

(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, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

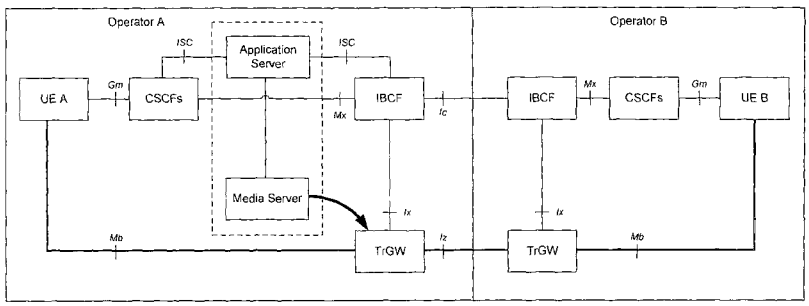
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, 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).

Published:

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

(54) **Title**: A METHOD FOR ROUTING AN IMS COMMUNICATION AND A NETWORK

Fig. 3



(57) **Abstract**: For allowing an improvement of performance of a network while retaining a reliable detection of unsolicited communications a method for routing an IMS (IP Multimedia Subsystem) communication from a network element of an originating network to a network element of the same network or of a terminating network is claimed, wherein a process for detecting unsolicited communications is performed by a detection application within the originating network and/or within the terminating network for evaluating communications as being unsolicited or permitted. The method is characterized in that a permitted communication will be routed from the network element of the originating network to the network element of the same network or of the terminating network without being routed through the detection application. Further, an according network is claimed, preferably for carrying out the above mentioned method.

WO 2010/105808 A1

A METHOD FOR ROUTING AN IMS COMMUNICATION AND A NETWORK

The present invention relates to a method for routing an IMS (IP Multimedia Subsystem) communication from a network element of an originating network to a network element of the same network or of a terminating network, wherein a process for detecting unsolicited communications is performed by a detection application within the originating network and/or within the terminating network for evaluating communications as being unsolicited or permitted. Further, the present invention relates to a network, comprising an originating network, wherein an IMS (IP Multimedia Subsystem) communication is routed from a network element of the originating network to a network element of the same network or of a terminating network and wherein a process for detecting unsolicited communications is performed by a detection application within the originating network and/or within the terminating network for evaluating communications as being unsolicited or permitted.

Within the IP Multimedia Subsystem (IMS) the occurrence of unsolicited communication could increase due to the expected low prices or even flatrate service for voice calls. Also other multimedia communications could be subject to this issue. The work on Prevention of Unsolicited Communication in IMS (PUCI) enables the IMS to detect these unsolicited communications like SPAM calls, for example. PUCI can do the so called Turing tests where the suspicious communication is rerouted to a special Application Server (AS) and a Media Gateway (MGW) for the user plane accordingly. Such a Turing test, for example, requires an end user action, e.g. dialing of a dynamically announced number. When the communication is identified as an unsolicited communication, it is forwarded to the mailbox or just rejected, but when the communication is identified as a normal communication, it is forwarded to the terminating party. Thus, the communication can be routed from a network element of an originating network to a network element of the same network or of a terminating network, wherein the communication is evaluated as being permitted by a detection application like PUCI.

The problem now results in the fact that the whole communication would be anchored in the MGW of the detection application even if it is not an unsolicited

communication. This could result in serious scalability issues for the MGW. The MGW used for PUCI checking is also referred to as (PUCI) Media Server in this document.

Further information about IMS technology is obtainable from IMS specification TS 23.228, http://www.3gpp.org/ftp/Specs/archive/23_series/23.228/23228-920.zip.

Further information with regard to PUCI is obtainable from PUCI Technical Report TR 33.937, http://www.3gpp.org/ftp/Specs/archive/33_series/33.937/33937-900.zip.

The PUCI testing could be done either in the originating network or in the terminating network or in both networks. Figs. 1 and 2 show the problem in case of either originating or terminating networks as in the combinational case the two scenarios simply could be merged, because the testing in each network is executed independently.

Scenario 1: PUCI testing in the originating network

In the scenario 1 illustrated in Fig. 1, the network element of the originating network is designated as UE A (User Equipment A). UE A originates a communication in the operator A network – the originating network – towards a network element of a terminating network – the UE B (User Equipment B) in the terminating network – which is designated as operator B network. Operator A will take care about the PUCI testing before the communication gets routed to the terminating network. For this case, a S-CSCF (Serving-Call Session Control Function) needs to invoke the PUCI AS to execute the Turing test, therefore it is further required to route the user plane to the Media Server to play the appropriate announcements and check the answer/UE A interactions. When the communication is identified as a permitted communication, the S-CSCF will forward the communication to a IBCF (Interconnection Border Control Function) as exit point for the signaling of the operator A network. The user plane traffic will be forwarded to a TrGW (Transition Gateway) as exit point for the user plane traffic of the operator A network. This means that all communications will go through the Media Server and could cause a high load there, as it would apply to

every originated communication in this network that involves PUCI testing during communication establishment.

Scenario 2: PUCI testing in the terminating network

In the scenario 2 depicted in Fig. 2, the UE A originates a communication in the operator A network towards the UE B in the operator B network. The operator B does PUCI testing for all incoming communications in his network, independently whether the previous operator's network performed PUCI testing or not. For this case, the IBCF invokes the PUCI application server and takes care that the communication gets routed towards the Media Server for detailed Turing testing. If the communication gets identified as a permitted communication, then it gets forwarded towards the terminating UE B. This means that all communications will go through the Media Server and could cause a high load there, as it would apply to every terminating communication in this network that involves PUCI testing during communication establishment.

Both known scenarios result in a high load at the detection application resulting in a reduced performance of the overall network.

It is an object of the present invention to improve and further develop a method for routing an IMS communication and an according network for allowing an improvement of performance of the overall network while retaining a reliable detection of unsolicited communications.

In accordance with the invention, the aforementioned object is accomplished by a method comprising the features of claim 1 and a network comprising the features of claim 20.

According to claim 1 the method is characterized in that a permitted communication will be routed from the network element of the originating network to the network element of the same network or of the terminating network without being routed through the detection application.

According to claim 20 the network is characterized by means for routing a permitted communication from the network element of the originating network to the network element of the same network or of the terminating network without being routed through the detection application.

According to the invention it has been recognized that it is possible to enhance the overall performance of the network by simply optimizing the routing of a permitted communication. In concrete terms a permitted communication will be routed from the network element of the originating network to the network element of the same network or of the terminating network without being routed through the detection application. After the evaluation of a communication as being permitted the routing of the permitted communication could be updated and directed to the destination network element along a suitable communication path. By avoiding of routing of the communication through the detection application the load at the detection application can be significantly reduced. Thus, an improvement of performance of the overall network can be provided while retaining a reliable detection of unsolicited communications, as the process for detecting unsolicited communications will not be affected by an updated routing of the communication after the evaluation of the communication as being permitted.

Preferably, the detection application or a network element hosting the detection application could be removed, preferably from a user plane, after a communication has been evaluated as being permitted. Thus, a permitted communication can be routed to the destination network element without being routed through the detection application.

Within a preferred embodiment the communication or a user plane could be directly routed from the network element of the originating network to a TrGW (Transition Gateway). During such a routing the detection application is no longer on the routing path.

For providing a reliable detection of unsolicited communications the detection application could be a PUCI application. However, other types of processes for

detecting unsolicited communications could be used within the inventive method and network.

Within a concrete embodiment the detection application could comprise an AS (Application Server) and an MS (Media Server). However, the use of further or other components is possible within the detection application.

For realizing a very effective routing of the communication a direct interface between an IBCF (Interconnection Border Control Function) and the AS could be realized. Preferably by such an interface an information exchange could be enabled between the IBCF and the AS. All detection application related information could be exchanged, e.g. test parameters, test results, PUCI scoring etc. Further, information with regard to a rerouting of the communication could be provided.

With regard to a very effective method for routing the communication the IBCF could be enabled to forward an incoming communication directly to the AS.

With regard to a very fast process for detecting unsolicited communications the detection application could be implemented at a border node/gateway of the originating network and/or of the terminating network. In such cases wide areas of the originating and/or terminating networks have not to be involved within the detection process. This will further improve performance of the network.

As it is desired to detect unsolicited communication as fast as possible at the border of the network the detection application could be implemented within an IBCF and/or a TrGW.

For routing the permitted communication preferably directly to the network element of the same network or of the terminating network a user plane could be updated in a suitable manner. By such an updating process the permitted communication could be reliably routed without being routed through the detection application.

Preferably, SIP (Session Initiation Protocol) signalling could be used to update the user plane or to indicate to the network element of the originating network or to a

B2BUA (Back-to-Back User Agent) in the path that the permitted communication shall not be routed through the detection application. However, other methods could be used for this updating and/or indication process.

The SIP signalling which could be used within the claimed method could comprise a SIP UPDATE, NOTIFY or SIP REFER mechanism. The concrete design of the updating process can be adapted to the respective and individual application case or situation.

Within a preferred realization of the inventive method the detection application, preferably an application server AS, could send a REFER message to the network element of the originating network or to a B2BUA with a refer to the network element of the same network or of the terminating network. As a reaction of such an REFER message the network element of the originating network could initiate an INVITE or re-INVITE to the network element of the same network or of the terminating network – the destination network element.

The INVITE or re-INVITE could be sent from a P-CSCF (Proxy-Call Session Control Function) to a S-CSCF (Serving-Call Session Control Function) and could there be detected to be the re-INVITE of the previous REFER.

The S-CSCF could send the INVITE or re-INVITE directly to the IBCF of the originating network.

Preferably in cases, in which the detection application is provided within the terminating network, the B2BUA could reside in an IBCF and/or a TrGW. In such cases a permitted communication could be rerouted without involving the originating network element. Thus, a very fast routing of the permitted communication could be realized.

Within a concrete embodiment the network element of the originating network – the originating network element – could be a User Equipment or a previously passed network node or an IBCF. Further, the network element of the same network or of the terminating network – the destination network element – could be a User Equipment.

The present invention describes a method how to reroute an IMS communication between the source entity, e.g. UE of caller, or a previously passed network node – the network element of an originating network – and the destination entity, e.g. UE of callee – network element of the same network or of a terminating network. It is possible to use SIP signaling, e.g. the REFER message, to indicate to the source or a B2BUA in the path (e.g. the Interconnection Border Control Function (IBCF) and Transition Gateway (TrGW)) that the communication – after it has passed the process for detecting unsolicited communications, e.g. the PUCI test – should no longer be routed through the detection application, e.g. Media Gateway (MGW), anymore.

According to a further aspect of the present invention, it is proposed to provide a detection application, e.g. PUCI functionality, in the IBCF and TrGW, as it is desired to detect unsolicited communication as fast as possible at the border of the network. The invention describes within preferred embodiments the additional signaling steps and how the relevant nodes need to be enhanced to enable this optimization, and also what extensions are needed to provide detection application functionality, e.g. PUCI functionality, at the border entity.

Within preferred embodiments of the invention a route optimization is enabled by allowing IMS to remove network nodes that have been included into the user plane path for PUCI testing, after a communication has been indentified legitimate. This reduces load within the detection application, e.g. on the MGW, which is used for PUCI testing. It is enabled to provide a detection application, e.g. PUCI, within the edge node of an operator network. Further, direct detection application testing is provided at the IBCF without involving the S-CSCF.

Further, an enhancement of the IBCF/TrGW is possible to act as a B2BUA to hide the rerouting towards the originating network element or party.

Within the present invention the detection application, e.g. a media server, can be removed out of the user plane path, after a communication has been identified as legitimate or permitted. This improves the overall performance of the network, as

communications do not remain anchored in a detection application node after the detection process, e.g. in a PUCI node after the PUCI checking.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end, it is to be referred to the patent claims subordinate to patent claim 1 on the one hand, and to the following explanation of preferred examples of embodiments of the invention, illustrated by the drawing on the other hand. In connection with the explanation of preferred embodiments of the invention by the aid of the drawing, generally preferred embodiments and further developments of the teaching will be explained. In the drawings

Fig. 1 is illustrating a PUCI testing in the originating network,

Fig. 2 is illustrating a PUCI testing in the terminating network,

Fig. 3 is illustrating a first embodiment of a method for routing an IMS communication according to the invention,

Fig. 4 is illustrating within a diagram a preferred realization of a rerouting of a permitted communication according to the first embodiment,

Fig. 5 is illustrating a second embodiment of a method for routing an IMS communication according to the invention and

Fig. 6 is illustrating within a diagram the realization of the rerouting of a permitted communication according to the second embodiment.

Within the following description two scenarios for performing the rerouting of a permitted communication are explained on the basis of a PUCI testing procedure.

Within all Fig. 1 to 6 the term "CSCFs" means all components of a CSCF, e.g. P-CSCF, S-CSCF etc.

Scenario 1: PUCI testing in the originating network

In this preferred scenario, the PUCI testing is done in the originating network, so the communication did not reach the IBCF for the breakout into the terminating network. This chapter describes how the Media Server reroutes the user plane so that the user plane is directly sent to the TrGW and not through the Media Server for the remaining communication.

Step 1: the media is routed to the media server so that the PUCI application server can play announcements and can evaluate the user interaction whether the communication might be unsolicited or not. This is already shown in Fig. 1.

Step 2: now after successful PUCI testing, i.e. the PUCI test is passed and the communication is identified as a normal or permitted communication and not as unsolicited, it is beneficial that the Media Server is out of the path. The user plane needs to be updated and rerouted to the TrGW so that the communication can breakout into the terminating network. This is shown in Fig. 3.

There are several possibilities to do the routing update, e.g. using SIP UPDATE, NOTIFY or, as described in the following example, using SIP REFER mechanism where the PUCI AS sends a REFER to UE B back to UE A.

The principle also applies in case the terminating party (UE B) belongs to the originating operator network. In this case, no IBCF/TrGW are involved, yet the Media Server will be removed from the user plane path between the UE A and UA B.

Fig. 4 shows a diagram depicting how the rerouting is realized with the example of using SIP REFER for updating the media path:

Description step by step

1. UE A sends an INVITE to UE B.
2. P-CSCF forwards to the S-CSCF and S-CSCF invokes iFC (initial Filter Criteria) to do PUCI testing.

3. S-CSCF sends INVITE to the PUCI AS.
4. PUCI AS executes the PUCI testing, i.e. answer the call.
5. PUCI AS sends 200 OK back to UE A.
6. S-CSCF sends the 200 OK to the P-CSCF and then to the UE A.
7. UE A establishes media path to the media server, as it has received the 200 OK.
8. PUCI AS plays announcement and monitors the user interaction.
9. PUCI AS evaluates the user interaction, e.g. whether the user pressed the right keys on the UE how he was asked in the announcement. Here the communication was identified as not an unsolicited communication, i.e. a normal communication.
10. PUCI AS decides to reroute the communication to the final destination including updating of the media path. The PUCI AS sends a REFER message towards the UE A with a refer to UE B.
11. The S-CSCF forwards the REFER to the P-CSCF and then its send to the UE A.
12. The UE A initiates a re-INTIVE to the UE B.
13. The INTIVE is send from the P-CSCF to the S-CSCF and there detected to be the re-INVITE of the previous REFER.
14. The S-CSCF sends INVITE directly to the IBCF of operator A.
15. The IBCF forwards the INVITE to the operator B IBCF where the communication is delivered to the terminating UE B.
16. The UE B acknowledges the INVITE with a 200 OK, and sends through the operator B network to the IBCF of the operator A.
17. The IBCF forwards the 200 OK to the S-CSCF.
18. The S-CSCF forwards the 200 OK to the P-CSCF and further to the UE A.
19. The UE A now detects the acknowledgement of the UE B and therefore acknowledges the REFER from the PUCI AS. The UE A sends a 200 OK towards the PUCI AS.
20. Now the P-CSCF forwards the 200 OK to the S-CSCF and then forward it to the PUCI AS.
21. The PUCI AS then hang up the communication.
22. The hangup is send through the CSCFs towards the UE A.
23. UE A acknowledges the hangup with a 200 OK towards the PUCI AS.

24. The CSCFs forwards the 200 OK to the PUCI AS.
25. Now the media – user plane – to the media server is terminated and the media path to the UE A is established.

Scenario 2: PUCI testing in the terminating network

In this second preferred scenario, the PUCI testing is done in the terminating network, so the communication already went through the IBCF of the network of operator B. This chapter describes how the Media Server reroutes the user plane so that the user plane is directly sent from the TrGW and not through the Media Server for the remaining communication.

Step 1: the media is routed from the TrGW to the media server so that the PUCI application server can play announcements and can evaluate the user interaction whether the communication might be unsolicited or not. This is already shown in Fig. 2.

Step 2: now after successful PUCI testing, i.e. the PUCI test is passed and the communication is identified as a normal or permitted communication and not as unsolicited, it is beneficial that the Media Server is out of the path. The user plane needs to be updated and rerouted to the TrGW so that the communication can breakout into the terminating network. This is shown in Fig. 5.

There are several possibilities to do the routing update, e.g. using SIP UPDATE, NOTIFY or the in the following example described SIP REFER mechanism where the PUCI AS sends a REFER to UE B back to UE A.

Fig. 6 shows a diagram depicting how the rerouting is realized with the example of using SIP REFER for updating the media path.

Description step by step:

1. UE A sends an INVITE towards UE B, here the elements of operator network A are not shown

2. The IBCF B receives the INVITE as the first contact point of the operator B's network. The IBCF acts like a B2BUA in this case. It detects the INVITE and routes the communication request to the PUCI AS for further testing
3. IBCF forwards the INVITE to the PUCI AS
4. PUCI AS executes the PUCI testing, i.e. answers the call
5. PUCI AS sends 200 OK back to the IBCF
6. IBCF sends 200 OK back to UE A
7. UE A establishes media path to the media server in the operator B network
8. PUCI AS plays announcement and monitors the user interaction
9. PUCI AS evaluates the user interaction, e.g. whether the user pressed the right keys on the UE how he was asked in the announcement. Here the communication was identified as not an unsolicited communication, i.e. a normal communication.
10. PUCI AS decides to reroute the communication to the final destination including updating of the media path. The PUCI AS sends a REFER message towards the UE A with a refer to UE B
11. The IBCF detects the REFER and acts like a B2BUA to send the INVITE
12. The IBCF initiates a INTIVE towards the UE B to the S-CSCF, the S-CSCF forwards the INVITE to the P-CSCF
13. The P-CSCF forwards the INVITE to the UE B
14. UE B answers with sending a 200 OK as acknowledgement to the P-CSCF
15. The P-CSCF forwards the 200 OK to the S-CSCF and further forwards the 200 OK to the IBCF
16. The IBCF detects the acknowledgement and acknowledges the REFER with a 200 OK to the PUCI AS
17. The PUCI AS sends a hangup message back to the IBCF
18. The IBCF acknowledges the hangup with a 200 OK
19. Now the media to the media server is terminated and the media path to the UE B is established

Within Fig. 1, 2, 3 and 5 are shown different designations of interfaces between different components of the operator A and operator B networks. Such designations can be Gm, ISC, Mx, Ic, Ix, Iz and Mb.

Both above embodiments provide a reduction of load on the Media Server by removing it from the end-to-end user plane path for every permitted communication. The originating or source UE and/or IBCF/TrGW are allowed to reroute a communication that has been evaluated as being permitted in order to bypass the Media Server or detection application, to avoid unnecessary entities in the user plane path.

A permitted IMS communication can be rerouted between the source network element or entity (e.g. UE of caller) or a previously passed network node and the destination network element or entity (e.g. UE of callee) or another node at the network border.

PUCI or detection application functionality can be supported in the IBCF and TrGW, as it is desired to detect unsolicited communication as fast as possible at the border of a network.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. A method for routing an IMS (IP Multimedia Subsystem) communication from a network element of an originating network to a network element of the same network or of a terminating network, wherein a process for detecting unsolicited communications is performed by a detection application within the originating network and/or within the terminating network for evaluating communications as being unsolicited or permitted,
characterized in that a permitted communication will be routed from the network element of the originating network to the network element of the same network or of the terminating network without being routed through the detection application.

2. A method according to claim 1, wherein the detection application or a network element hosting the detection application will be removed after a communication has been evaluated as being permitted.

3. A method according to claim 1 or 2, wherein the detection application is a PUCI (Prevention of Unsolicited Communication in IMS) application.

4. A method according to one of claims 1 to 3, wherein the detection application is comprising an AS (Application Server) and an MS (Media Server).

5. A method according to claim 4, wherein a direct interface is realized between an IBCF (Interconnection Border Control Function) and the AS.

6. A method according to claim 4 or 5, wherein an information exchange is enabled between the IBCF and the AS.

7. A method according to claim 5 or 6, wherein the IBCF will be enabled to forward an incoming communication directly to the AS.

8. A method according to one of claims 1 to 7, wherein the detection application is implemented at a border node/gateway of the originating network and/or of the terminating network.

9. A method according to one of claims 1 to 8, wherein the detection application is implemented within an IBCF (Interconnection Border Control Function) and/or a TrGW (Transition Gateway).

10. A method according to one of claims 1 to 9, wherein a user plane will be updated for routing the permitted communication preferably directly to the network element of the same network or of the terminating network.

11. A method according to one of claims 1 to 10, wherein SIP (Session Initiation Protocol) signalling is used to update the user plane or to indicate to the network element of the originating network or to a B2BUA (Back-to-Back User Agent) in the path that the permitted communication shall not be routed through the detection application.

12. A method according to claim 11, wherein the SIP signalling is comprising a SIP UPDATE, NOTIFY or SIP REFER mechanism.

13. A method according to claim 12, wherein the detection application, preferably an Application Server AS, is sending a REFER message to the network element of the originating network or to a B2BUA with a refer to the network element of the same network or of the terminating network.

14. A method according to claim 13, wherein the network element of the originating network is initiating an INVITE or re-INVITE to the network element of the same network or of the terminating network.

15. A method according to claim 14, wherein the INVITE or re-INVITE will be sent from a P-CSCF (Proxy-Call Session Control Function) to a S-CSCF (Serving-Call Session Control Function) and there will be detected to be the re-INVITE of the previous REFER.

16. A method according to claim 15, wherein the S-CSCF is sending the INVITE or re-INVITE directly to the IBCF of the originating network.

17. A method according to one of claims 11 to 16, wherein the B2BUA resides in an IBCF (Interconnection Border Control Function) and/or a TrGW (Transition Gateway).

18. A method according to one of claims 1 to 17, wherein the network element of the originating network is a User Equipment (UE A) or a previously passed network node or an IBCF.

19. A method according to one of claims 1 to 18, wherein the network element of the same network or of the terminating network is a User Equipment (UE B).

20. A network, preferably for carrying out the method according to any one of claims 1 to 19, comprising an originating network, wherein an IMS (IP Multimedia Subsystem) communication is routed from a network element of the originating network to a network element of the same network or of a terminating network and wherein a process for detecting unsolicited communications is performed by a detection application within the originating network and/or within the terminating network for evaluating communications as being unsolicited or permitted,
c h a r a c t e r i z e d by means for routing a permitted communication from the network element of the originating network to the network element of the same network or of the terminating network without being routed through the detection application.

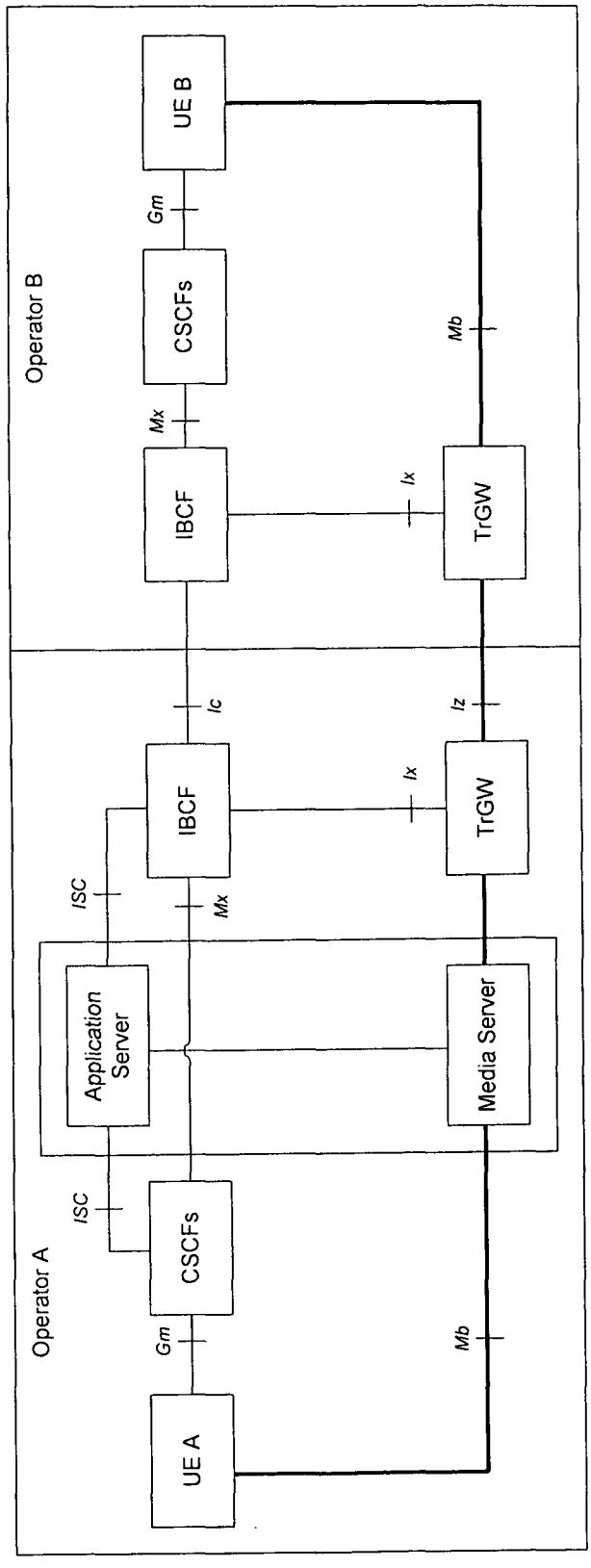

Operator B
UE B
Gm
CSCFs
Mx
IBCF
Ix
TrGW
Mb
Ic
Iz
Ix
IBCF
TrGW
ISC
Mx
Application Server
Media Server
ISC
CSCFs
Operator A
Gm
Mb
UE A

Fig. 1

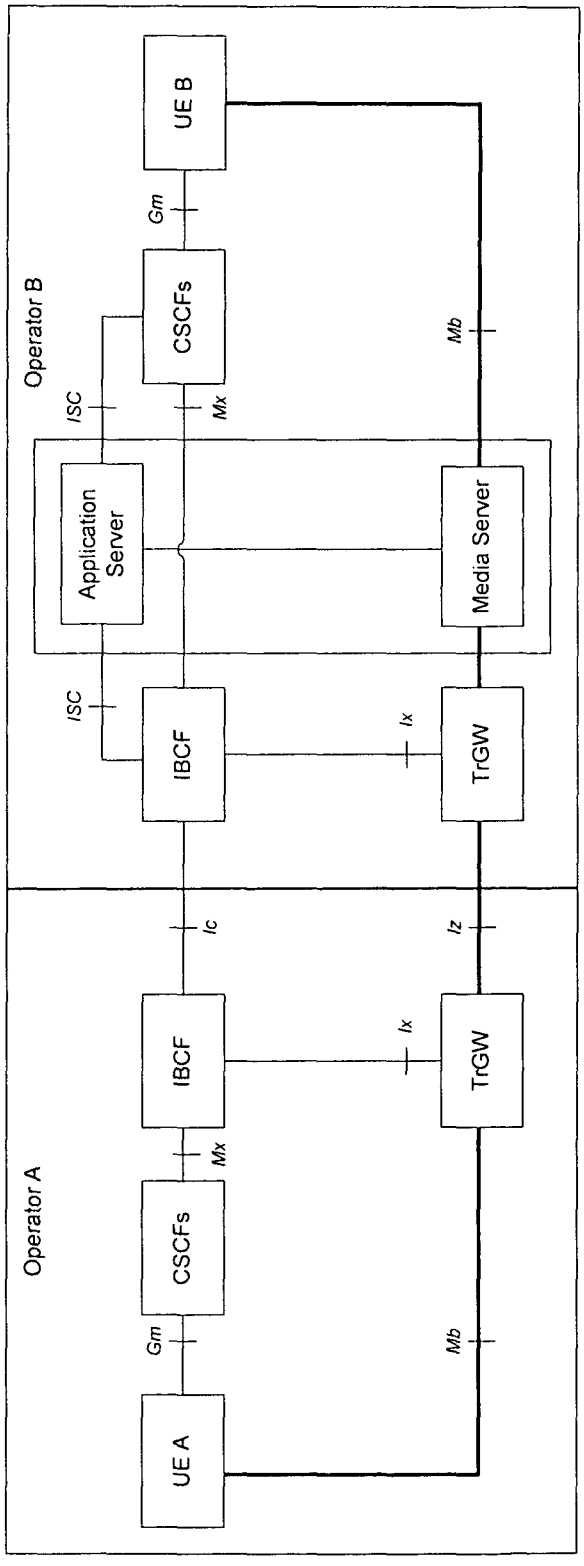

Operator A
Operator B
UE A
UE B
Gm
Gm
CSCFs
CSCFs
Mx
Mx
IBCF
IBCF
Ic
Iz
Ix
Ix
TrGW
TrGW
Mb
Mb
ISC
ISC
Application Server
Media Server

Fig. 2

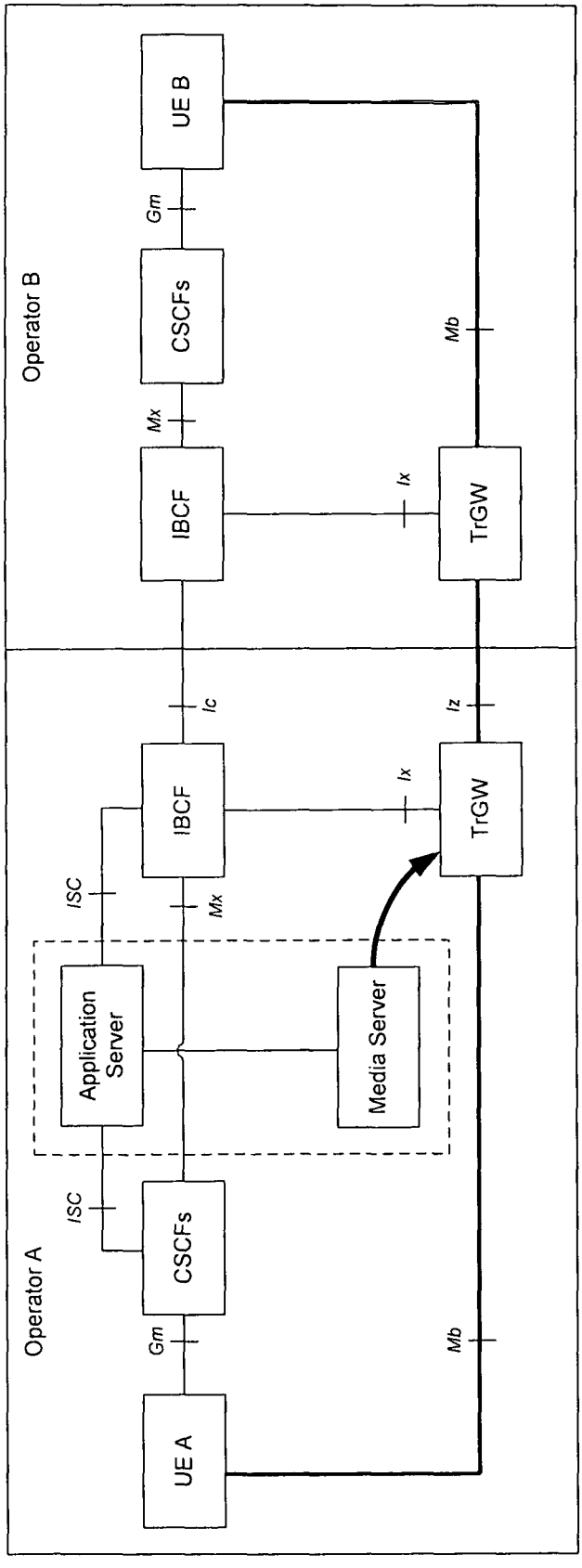

Operator B
UE B
Gm
CSCFs
Mx
IBCF
Ix
TrGW
Mb
Ic
Iz
Operator A
ISC
Application Server
Media Server
UE A

Fig. 3

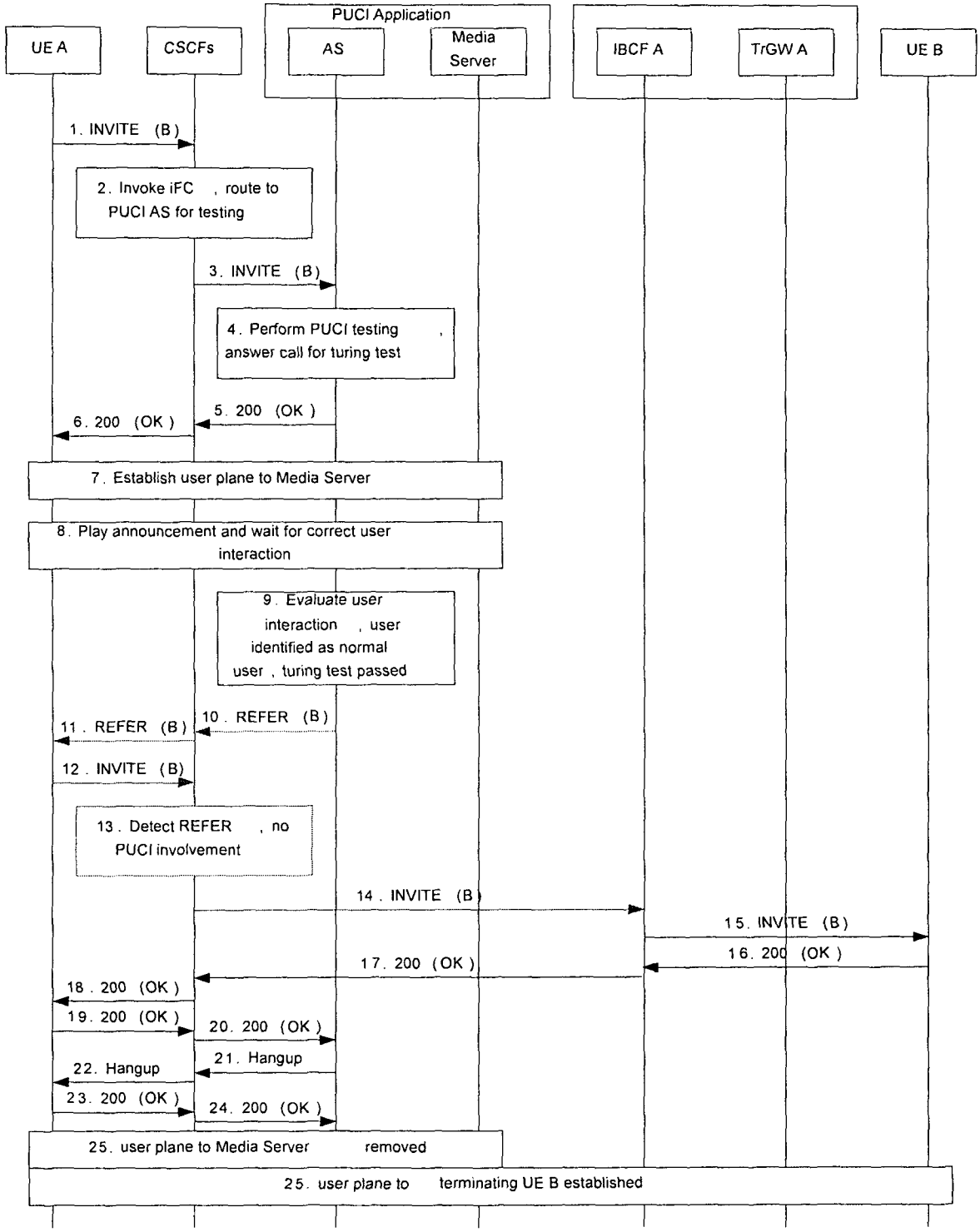

PUCI Application
UE A
CSCFs
AS
Media Server
IBCF A
TrGW A
UE B
1. INVITE (B)
2. Invoke iFC , route to PUCI AS for testing
3. INVITE (B)
4. Perform PUCI testing , answer call for turing test
5. 200 (OK)
6. 200 (OK)
7. Establish user plane to Media Server
8. Play announcement and wait for correct user interaction
9. Evaluate user interaction , user identified as normal user , turing test passed
10. REFER (B)
11. REFER (B)
12. INVITE (B)
13. Detect REFER , no PUCI involvement
14. INVITE (B)
15. INVITE (B)
16. 200 (OK)
17. 200 (OK)
18. 200 (OK)
19. 200 (OK)
20. 200 (OK)
21. Hangup
22. Hangup
23. 200 (OK)
24. 200 (OK)
25. user plane to Media Server removed
25. user plane to terminating UE B established

Fig. 4

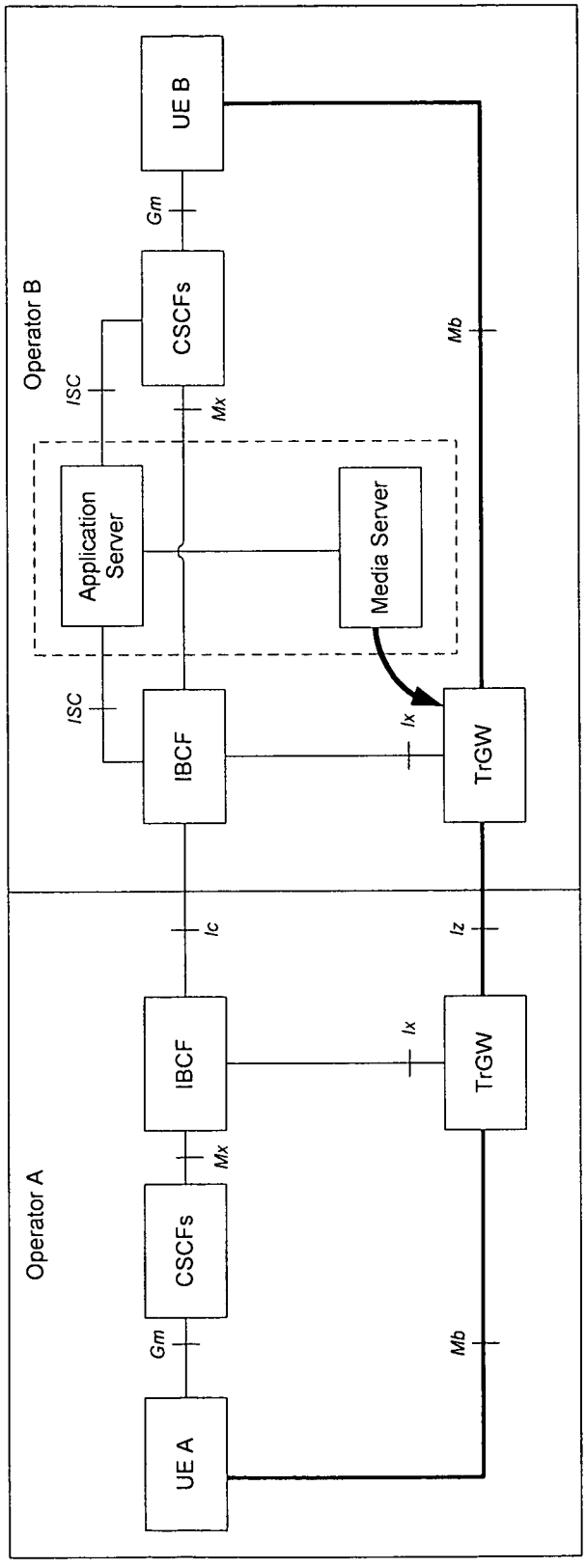

Operator B
UE B
Gm
CSCFs
ISC
Mx
Mb
Application Server
Media Server
ISC
IBCF
Ix
TrGW
Ic
Iz
Operator A
IBCF
Ix
TrGW
Mx
CSCFs
Gm
Mb
UE A

Fig. 5

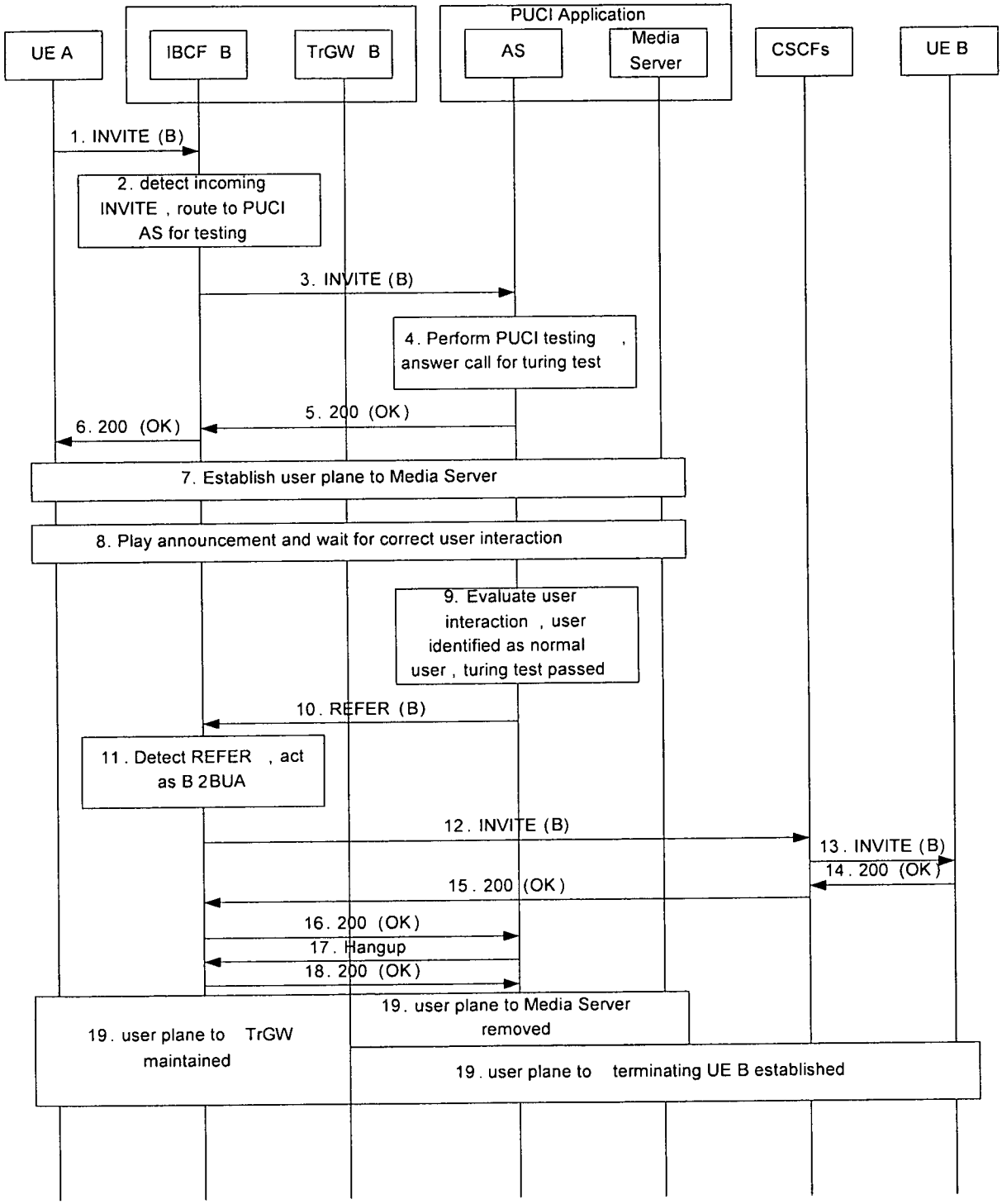

UE A
IBCF B
TrGW B
PUCI Application
AS
Media Server
CSCFs
UE B
1. INVITE (B)
2. detect incoming INVITE , route to PUCI AS for testing
3. INVITE (B)
4. Perform PUCI testing , answer call for turing test
5. 200 (OK)
6. 200 (OK)
7. Establish user plane to Media Server
8. Play announcement and wait for correct user interaction
9. Evaluate user interaction , user identified as normal user , turing test passed
10. REFER (B)
11. Detect REFER , act as B 2BUA
12. INVITE (B)
13. INVITE (B)
14. 200 (OK)
15. 200 (OK)
16. 200 (OK)
17. Hangup
18. 200 (OK)
19. user plane to Media Server removed
19. user plane to TrGW maintained
19. user plane to terminating UE B established

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/001667

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04M3/436
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)
H04L H04M

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 practical, search terms used)
EPO-Internal, INSPEC, 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	WAITING D ET AL: "The Threat of Unsolicited Sessions in the 3GPP IP Multimedia Subsystem" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 45, no. 7, 1 July 2007 (2007-07-01), pages 100-106, XP011187093 ISSN: 0163-6804 page 103, line 16 ("TURING TESTS") - page 105, line 35	1-20
X	US 2007/071200 A1 (BROUWER SANDER [NL]) 29 March 2007 (2007-03-29) page 2, paragraph 41 - page 3, paragraph 52 figures 1,3	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 document 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
22 June 2010	29/06/2010

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	Karavassilis, N

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/001667

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	3GPP: "3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI) (Release 9)" 3GPP DRAFT; S3-081577-PUCI-TRV0.1.0, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. Kyoto; 20081114, 14 November 2008 (2008-11-14), XP050334658 [retrieved on 2008-11-14] the whole document ----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2010/001667

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007071200 A1	29-03-2007	NONE	