

need for any standardization effort for defining any new specific header for this purpose.

[0199] The SIP Content-Type header specifies the message body content. In this case it will indicate that is carrying Presence information using TID or any other XML based format (Example: "Content-Type: presence /TID").

[0200] There are many possibilities:

[0201] Content-Type: presence/TID. As shown in FIG. 2, the user provides the location information following the TID format (Appendix 3).

[0202] Content-Type: presence/GML-GIS. The user is using another format that follows the GIS structure.

[0203] Content-Type: presence. In this case the user is indicating that he desires to make his presence publicly available and the Server will fill his information based on his service profile. This is meant for small devices where one cannot implement a complete system for calculating the positioning (GPS) and the Server will do it for them. The Server can use any available system (Cell-ID) to figure out the user location and fulfil the user data.

[0204] Presence Message Flow Examples

[0205] The following describes various user cases and the message flows for illustrating the Presence Service according to the present invention.

[0206] When a new call arrives to the Session Manager it will strip off the packet to check the SIP headers. In the case that it is a REGISTER message it will be notified to the Mobility Manager. The MM will check if the Content-Type is equal to "presence/???". In this case the MM will get the SIP packet and will check if it contains the attribute defined herein (TID, GML-GIS, or it is void). If that is the case, those values will be stored or updated in the HSS for further transactions.

[0207] For later transactions, the MM will access that information stored in the HSS if it is required for managing incoming sessions based on user profile. Otherwise, the CSCF is handling a new call set-up and the SIP packet does not contain these new attributes. Based on the SIP headers Content-type the LS will update the User Register data stored in the Home Location Register. The user profile is updated with the SDP information and stored according to the legacy networks format. The legacy networks will download directly the information required from the HLR.

[0208] FIG. 9 presents an example of call flow during a Presence service transaction. The first step is the Registration and Authentication of the SIP Terminal and the utilization of the SIP payload packet for providing User Identification Information within the Registration.

[0209] In this case we are dealing with a mobile terminal using UMTS. The user needs a small lunch break and does not have enough knowledge about the services available in the surroundings. For obtaining a service suited to his actual location he needs to register his situation as shown. Afterwards, the user requests a specific service and he receives the response with the service adapted to his physical situation.

[0210] Referring back to FIG. 3, the SIP Terminal will encrypt the User Identity & System location for sending it in

the REGISTER Request. The REGISTER request may be encrypted or not based on the user requirements. If the user does not mind that everyone knows his location the Request will be in plain text. Otherwise, the SIP contains the Authorization field (e.g. it is after a 401 Authentication Required response) and the Location Information (TID) is encrypted.

[0211] The CSCF (with SIP Proxy/Registrar capabilities) will accept the user registration. Furthermore, the CSSF sends the User Information either to the HSS (Signalling Interface Cx) or the Presence Server if such an entity exists, as shown. After this the user is registered and his situation is available for other services. If the Presence Server does not exist, then the HSS will behave like a similar Presence Server. At this point is a matter or re-using or not overloading existing entities.

[0212] At this point the user Requests the specific service mentioned above, which in order to be fulfilled, it will be essential for the Location-based service center to have the knowledge of his location that is already available at the HSS. Thus, the user issues an INVITE for opening a session where he ask for some information. It is necessary to define an attribute to indicate the nature of this Request. Hence, at the Content-Type will be defined the attribute "Service-Request" as shown in FIG. 4.

[0213] The CSCF receives the message and checks the information of that user either in the HSS or in the Presence Server. If the user has the location information stored, the CSCF makes a query to the Location Based Services server without revealing the identity of the user that needs the information. The CSCF just make a request for a concrete service at a specific place.

[0214] The LBS server will respond with the information according only to the requirements indicated in the query by the CSCF (location-service). Thus, the user's privacy is kept secure in the CSCF.

[0215] Finally, once the CSCF receives the response from the LBS, it is forwarded to the user. The format is similar to the request but in this case the information is carried in the 200_OK response. After that the user will translate the information and give back the ACK to the CSCF that will close the session.

[0216] Instant Messaging (IM)

[0217] Embodiments of an Instant Messaging service will now be described in a few examples.

[0218] The functionality is based on the SUBSCRIBE/NOTIFY methods of SIP for sending a notification to the user when a new message arrives.

[0219] Consider a first example where a user does not want to be disturbed during a period of time but he wants to be aware of any event in case something abnormal occurs.

[0220] The advantage of this approach is that the user can be informed constantly without establishing a complete session. Again, it is emphasized that the important feature is that it does not require any new SIP method, it just uses the existing framework and defines new attributes for SIP headers.