Building Mobile Intranets Over The UMTS

Constantinos F. Grecas, Sotirios I. Maniatis and Iakovos S. Venieris
National Technical University of Athens, Dep. of Electrical and Computer Engineering,
9 Heroon Polytechniou str, 157 73, Athens, Greece,
Telephone: (+ 30 - 1) 77 22 551, *FAX:* (+ 30 - 1) 77 22 534,
Email: {cgrecas,sotos} @ telecom.ntua.gr, ivenieri@cc.ece.ntua.gr

Abstract: The GPRS and UMTS specifications define the procedures supporting the mobility and the data sessions of a mobile user moving within the area of the corresponding PLMNs. For the case, though, of mobile users working in group, using a PLMN infrastructure, the aforementioned networks foresee no special treatment. However, services tightly related to a specific geographic area, like for example security or surveillance services, could be implemented by a group of collaborating Mobile Nodes forming a mobile intranet that uses the facilities of a PLMN. In this paper, after a description of what the specifications provide, methods are proposed for the deployment of intranets over the GPRS or the UMTS infrastructure. At this aim, the concept of the GIP is introduced regarding a frame of interconnected SGSNs, within the GPRS/UMTS environment. This frame supports, without the intervention of the GGSN, the mobility of a number of Mobile Nodes belonging to the same group, as well as the data traffic between them. Moreover, the additional tasks to be undertaken by the SGSNs forming the frame are described.

1. INTRODUCTION

The steadily increasing demands for services' offer, even when the user is in motion, has led to the evolution of the circuit switched cellular mobile telephone networks to high bit-rate systems, offering packet switched type services to mobile users, connected to the Internet. As a matter of fact, the General Packet Radio Services (GPRS) and the Universal Mobile Telecommunication System (UMTS) are the wireless packet Public Land Mobile Network (PLMN) technologies defined by the European Telecommunications Standards Institute (ETSI) and destined to dominate the

telecommunication market, at least in Europe, in the next years. They are expected to provide transmission speeds not only comparable to the currently offered by the wired networks, but even higher, while their deployment will facilitate connections characterized not only by the user's mobility but also by the machine's portability.

The introduction, though, of these high speed wireless data networks will not only upgrade the connection profile of the isolated machines, but will trigger their exploitation for services demanding group work, as well. Nevertheless, these systems by themselves, as described in the specifications, do not foresee special procedures for the deployment of networked structures running in the GPRS or the UMTS environment. According to the currently proposed situation, the users should define the collaborating nodes forming a group, while the system remaining unaware of the Mobile Nodes' (MN) grouping. In such a case and because of the way the data is routed in the PLMNs under consideration, the whole data traffic between the nodes belonging to the group must pass through the Gateway GPRS Support Node (GGSN), the PLMNs' Gateway. Such a fact implies additional burden to the GGSN and waste of resources, which otherwise could be used for communication with machines outside the PLMN.

Recalling, at this point, services like security and surveillance, as they are offered by e.g. municipality police, private security companies charged with the guarding of a specific area, fire service responsible for an urban or a rural area, etc., it is obvious that they can be supported by mobile Virtual Private Networks (VPN) or intranets, running Internet protocols and applications. Moreover, the main load of information, which their nodes mutually exchange, remains within the intranet, especially if the node responsible for the coordination and the control of the entire group is a mobile one moving in the area of charge.

The candidacy of the GPRS or the UMTS as bearers of networks of this nature seems quite reasonable. Nevertheless, the endowment with routing abilities of the PLMNs' Serving GPRS Support Node (SGSN) is necessary. Supplying the SGSNs with routing abilities permits the operator to interconnect them in platforms, within the Core network (CN) of the PLMN. Each such a platform, we propose here with the name GPRS Intranet Platform (GIP), having its nodes properly set up, will be able to support the mobility of groups of collaborating MNs, within the area the platform covers, without the intervention of the GGSN.

With such a configuration, possible overloading of the GGSN is avoided, while at the same time resources on the Gateway are liberated for communication with the external networks. The main advantage, though, of the scheme is the decentralization of the control of the intranet connections, since it is distributed among the framed SGSNs. As a matter of fact, not

having all the traffic between the collaborating Mobile Nodes passing through the GGSN, the disadvantage of the concentrated control of the connections is avoided, since even if the GGSN fails, the mobile intranet's connections remain intact. Obviously this is a critical point for services that support security applications. Moreover, excluding the GGSN from the data communication protects the intranet's MNs from possible attacks from external sources, as the latter must pass through the GGSN.

In the analysis that follows, proposals are made about the way the implementation of mobile intranets running over the UMTS infrastructure can be realized. Actually, the remaining of the paper is structured as follows: In section 2, the UMTS Network Architecture, as well as the MN's location and the data transfer main procedures are described, as they are given by the specifications. In section 3, our proposals and the necessary modifications and procedures, about how a mobile intranet in a UMTS environment can be built, are exposed. Finally, our conclusions are given in section 4.

2. THE UMTS NETWORK ARCHITECTURE AND PROCESSES

The wireless packet PLMNs, namely the UMTS [1] as well as the GPRS, are modular systems constituted by network elements grouped in the Radio Access Network (RAN), the Core Network (CN) and the Mobile Nodes (MN). From a specification point of view, the already deployed GPRS is a direct descendant of the GSM, regarding its RAN part, consisting of the well-known Base Station System (BSS). On the other hand, the third generation UMTS disposes the UMTS Terrestrial RAN (UTRAN), standardized over new specifications, as the new interfaces show in Figure 1.

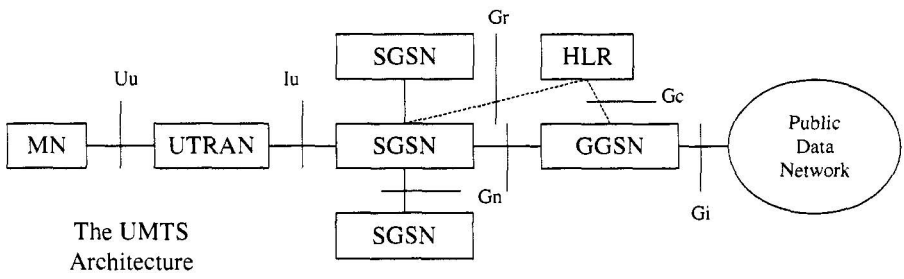

Figure 1. The UMTS Network Architecture

Both systems, though, retain similar CN architectures, based on the GSM's [2] philosophy, although specific differences in internal functionality

can be recognized. The Serving SGSN, the GGSN and the Home Location Register (HLR) are met in both architectures. Moreover, within the CN, the processes taking place over the common interfaces remained unchanged for the GPRS and the UMTS.

2.1 Location and Traffic Related Processes

Being interested in the packet modes of the networks mentioned above, for the needs of the present paper, we examine the procedures defined for UMTS. Similar techniques can be equally applied to the GPRS as well, but are not further addressed in the paper.

2.1.1 Mobile Node Location Management

According to the specifications [1] the MNs inform the infrastructure about their point of presence when initially powered–up, when they enter a new area (cell or routing area), and periodically, in order to refresh the infrastructure's information about their position.

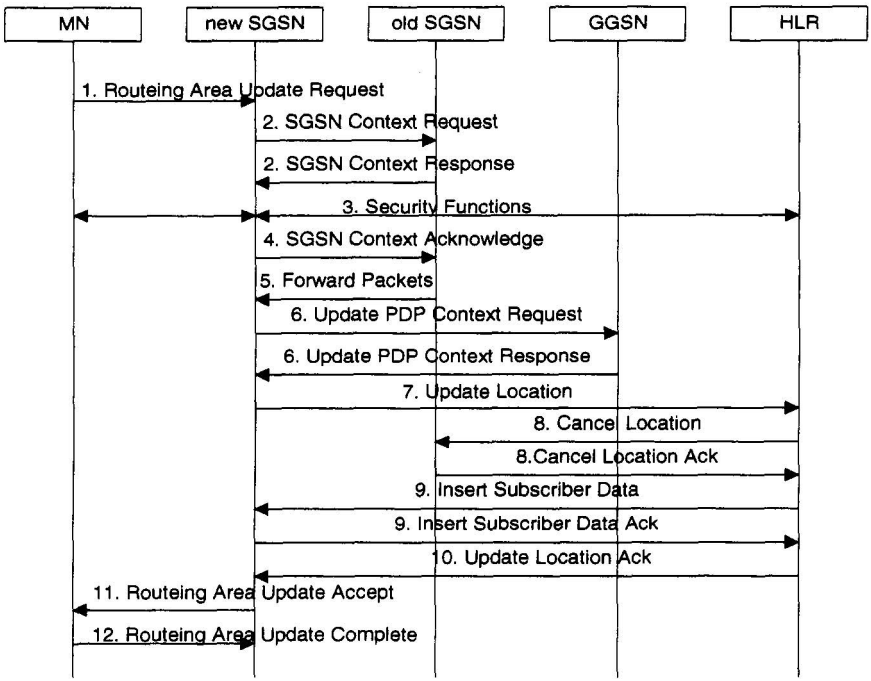

Figure 2. Inter SGSN Routing Area Update Procedure

The update can be an intra-SGSN or inter-SGSN one. The former, realized by transactions between each MN and the SGSN currently serving it, is transparent to the rest of the system, while the latter, concerning our analysis, is depicted in Figure 2. Actually, Figure 2 describes the handover of an MN from the Routing Area (RA), a group of cells, of the old SGSN to a Routing Area of the new SGSN, during a packet session.

2.1.2 Packet Routing and Transfer

The packet transfer in PLMN, as in every Packet Network, is a process regarding directions uplink, from the MN to the GGSN, and downlink, from the GGSN to MN. In GPRS three nodes participate in the packet transfer, the MN the SSGN and the GGSN, while two processes are activated for the set up of the route between the MN and the GGSN. So, the Packet Data Protocol (PDP) Context Activation Transfer procedure is called to set up a route for uplink data transfer, and the Network-Requested PDP Activation procedure is employed for route set up in the case downlink data transfer is asked.

The messages exchanged during the former of the above procedures are shown in Figure 3. Now the route for the PDP Context, that is the packet session, has been set up, and packets between the MN and the GGSN can be sent.

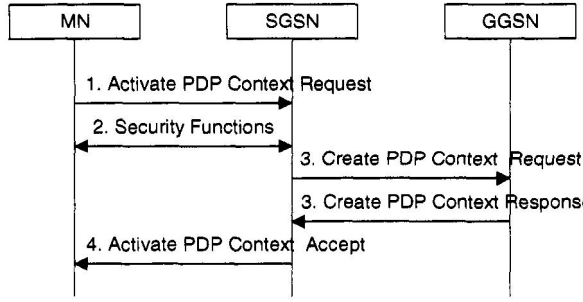

Figure 3. The PDP Context Activation Procedure

On the other hand, Figure 4 depicts the messages exchanged for route set up in a PDP Context Activation procedure triggered by the network.

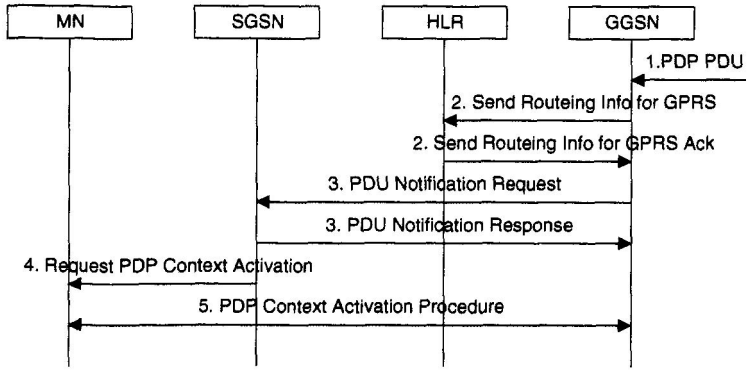

Figure 4. The Network-Requested PDP Context Activation Procedure

2.2 Intra-PLMN Paths and Traffic

The aforementioned procedures render obvious the following characteristics of the system:

- Every time an MN migrates from the area of one's SGSN to the area of another's, the GGSN is correspondingly updated.
- In order for a session to take place, the participation of the GGSN is indispensable.

This role of the GGSN facilitates the communication of the MNs with the external networks, since the mobile packet networks have been designed as the wireless extension of a user's connection to a Packet Data Network (PDN), and mainly to the Internet.

In the case, though, two mobile users, belonging to the same PLMN, have to communicate, their connection has to be realized, again, by the intervention of the GGSN, see Figure 5. This means that data, originating from one of them and destined for the other, will travel uplink to the GGSN and pinged back by it into the PLMN to the final destination. If more than two MNs is necessary to form a group of collaborating mobile machines, the same methodology is followed in setting up the connection paths between them, since the system is able to only treat single nodes, leaving to the users the determination of the MNs that are going to collaborate in group. Consequently, resources of the GGSN over the Gn interface should be allocated even for this kind of internal traffic and signalling as well.

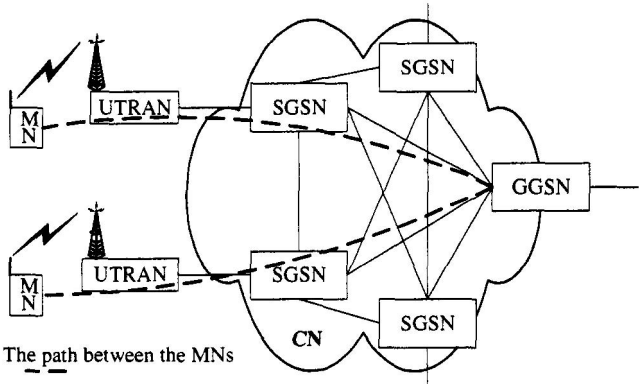

Figure 5. The path for internal connection between two MNs

Let us consider, for example, the case of security and surveillance services, as they are offered by a group of MNs, serving a metropolitan area and employing the services offered by a GPRS network. Following the way the GPRS sets up the links between the communicating nodes, all the traffic is to pass through the GGSN. In the case the GGSN fails, all the nodes belonging to the group lose their contact, since there are no alternative paths to support connections between them. As a consequence, the security and surveillance service, which the group of the MNs is expected to offer, fails. On the other hand, although the traffic of the nodes under consideration remains within the service area of the PLMN, resources are disposed to them, which otherwise could be allocated to users communicating with an external network.

In the subsequent section, based on the above observations, we propose methods about how alternative paths serving the intra-PLMN traffic between collaborating MNs of a group of users in motion can be set up. This is an additional way of building an intranet over the UMTS infrastructure, with actually no change in the system's configuration, and with the minimal possible extensions of the system's software.

3. EXTENDING THE ROUTING ABILITIES WITHIN THE UMTS

According to the system functionality currently proposed in the standards [1], the nodes of the CN, that is the SGSNs and the GGSN, are supplied with some kind of restricted range routing abilities, based on information stored in the HLR, in order for the MNs to be located. Actually, at the SGSNs level,

solely the SGSN to which the MN has migrated is aware of the mobile's position, and only in the case of a handoff two SGSNs, the old and the new one, interfere in routing the packets to the MN. On the other hand, the GGSN, updated of the MN's inter-SGSN transfers, is able to route the packet to the proper SGSN for delivery to the MN. So, for a given MN, no other node in the CN, except the ones mentioned above, retains any information about the MN's position within the PLMN.

To be noted at this point, and before going any further, that the analysis that follows deals exclusively with adding routing abilities in the SGSNs of the CN. That is the procedures we propose are transparent to the GGSN and to the MNs.

3.1 A Platform for Mobile Intranet over UMTS

Considering group activities, implemented by means of collaborating mobile terminals, we introduce, here, the concept of the GPRS Intranet Platform (GP). The term denotes a set of SGSNs, each of them able to:

- Hold information about the position of a predetermined number of MNs, as long as these MNs are present in the area covered by the SGSNs.
- Route user traffic between the MNs constituting the mobile intranet, without the intervention of the GGSN, as long as this traffic remains within the GIP, that is none of the communicating intranet's MN has migrated outside the GIP.

The fact that user data has to be transferred within the GIP without the intervention of the GGSN implies that the SGSNs, forming the GIP, should be supplied with routing abilities. Having in mind the exploitation of the IP network running in the CN, we propose the enhancement of the SGSN's protocol stack, currently specified in the standards [1], by the accretion of an IP network layer on top of it, see Figure 6. This additional IP layer is destined to serve exclusively the MNs of the mobile intranet, built over the GIP.

The resulting architecture, see Figure 7, can be considered as an additional option of the user plane in the UMTS. Its function, in combination with the signaling concerning the sessions of the mobile intranet's MNs, is described in the followings.

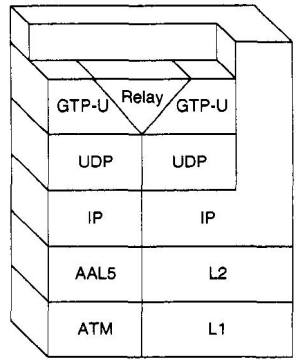

Figure 6. The enhanced protocol stack of the GIP's SGSN

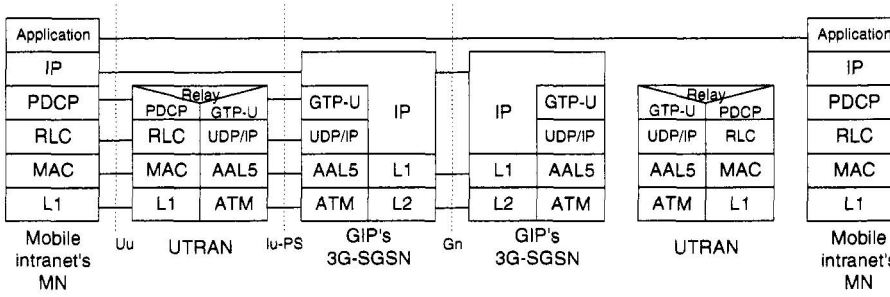

Figure 7. User Plane for the GIP

3.2 Procedures within the GIP

3.2.1 Mobile Intranet's MN Attach and Authorization Procedures

The initial attach and authorization procedure remains unchanged and is executed as the standards specify [3] for each of the mobile group's MN, the process being transparent to the GP.

3.2.2 Packet Routing and Transfer within the GIP

As has been mentioned above, the GP concept is transparent to the MNs of the intranet served by the SGSNs platform. This means that the messages exchanged between these MNs and the infrastructure remain unchanged. In Figure 3, the messages necessary for the establishment of a packet session originated by an MN are shown. In the following analysis we describe the way these messages are interpreted by a GIP's SGSN, when they are

transmitted by an MN participating to a mobile intranet served by the GIP under consideration. For the case we refer to Figure 8.
The <Activate PDP Context Request> message [1] [4] originated by the MN contains two important parameters for the GIP. The first one is the PDP Address. As we will explain below, for the MNs belonging to the GIP, the GGSN does not participate in the Activate PDP Context procedure. Thus, we assume that each MN belonging to the GIP must have a statically allocated PDP Address, initialised in this message by the MN. The second parameter is the Access Point Name (APN) that is the logical name of the target network the destination node belongs to. Here, we assume that each GIP's MN, whenever activates a PDP context to be used for intranet purposes, inserts a pre-defined APN, so that the SGSN that receives the <Activate PDP Context Request> message can identify that the target network is the intranet one. Moreover, from the Mobility Management, the SGSN knows which MN sent the message.
Let us now examine the way the GIP's SGSN treats the <Activate PDP Context Request> message. If the source of the message is not an MN participating to the mobile intranet the request message is obviously rejected. Otherwise, the SGSN replies immediately with an <Activate PDP Context Accept> message, containing the same parameters specified in the standards [1] [4]. No <Create PDP Context Request> message is sent to the GGSN.

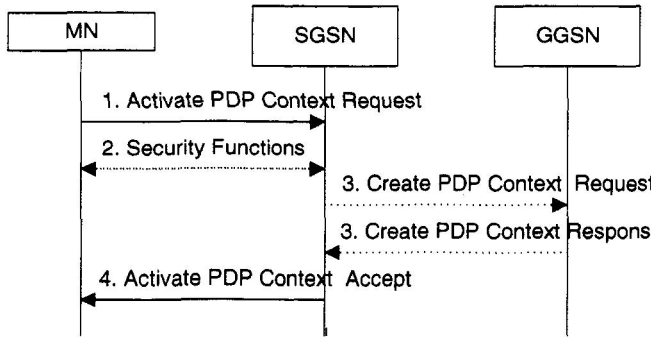

Figure 8. Treatment of PDP context establishment messages by the GIP

In the case, though, the SGSN is informed, through the appropriate system maintenance signalling, that some of the links connecting it with the other SGSNs of the GIP is crashed, then it proceeds with the establishment of a PDP context, as the specifications describe. Actually, the SGSN forwards to the GGSN the request of the MN by the means of <Create PDP Context Request> message [5], dashed lines in Figure 8, bypassing the GIP's

functionality. In such a case the < Create PDP Context Response> is expected from the GGSN.

To the GGSN are forwarded, as well, requests corning from an intranet's MN containing an APN corresponding to an external network. Obviously, the SGSN should reject such requests, if the MN is not authorized to communicate with nodes not participating to the same mobile intranet.

As a matter of fact, the processes regarding resources' allocation between the MN and the SGSN, triggered by the context activation procedures, remain unchanged no matter if they concern MNs belonging to a mobile intranet or not.

The receipt of the <Activate PDP Context Accept> by the mobile intranet's MN enables it to start transmitting packets, over the resources disposed to it. At the SGSN these packets arrive at the exit of a deliberately created tunnel at the GTP-U layer on the Iu-PS interface, see Figure 7. Such an exit, characterized by a Tunnelling Endpoint Identifier (TEID) [5], is corresponded by the SGSN, during the resources' allocation procedures triggered by the PDP Context Activation messages, to a specific session on the specific MN. So, packets, coming out of TEIDs allocated to serve traffic destined for nodes outside the mobile intranet, are relayed to the GTP-U layer on the Gn interface, see Figure 6, in order to be forwarded to the GGSN. On the other hand, packets, coming out of TEIDs corresponded to sessions between mobile intranet's MNs, are delivered to the overlaying IP layer, added for the purposes of GIP.

At the IP layer, from the routing table and on the base of the packet's destination IP address, the IP address of the SGSN, currently hosting the destination MN, is located. So, the packet is delivered to the destination's SGSN, by means of the data link layer (Ll) over the Gn interface, see Figure 7. At the IP layer of the destination's SGSN, on the base of the routing table, the destination MN is sought. Actually, the SGSN finds out the TEID that is associated with the PDP Context of the destination MN for the GIP traffic and sends the IP PDU according to the standard UMTS user-plane routeing procedures. However, there is also the possibility that the MN has migrated to another SGSN of the GIP. In this case, the IP PDU is sent to the SGSN the MN has migrated, as explained below, see Figure 9.

Upon the receipt of the first packet destined for the target MN the hosting SGSN sends it a <Request PDP Context Activation> message, described in [4], containing only the network assigned Transaction Identifier (TI). The MN receiving the <Request PDP Context Activation> responds with a <Activate PDP Context Request> message containing the static PDP Address, the PDP type and the GIP's APN, as well as the TI requested by the network, and the procedures of Figure 8, shown as number 3 in Figure 9, are carried on. In the case the <Request PDP Context Activation> message is not

rejected, rejection reasons are described in [4], the packets between the MNs of the mobile intranet are exchanged without the intervention of the GGSN.

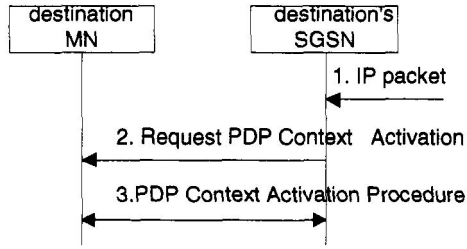

Figure 9. PDP Context Request Activation from a GIP's SGSN to a mobile intranet's MN

3.2.3 Mobile Intranet's MN Location Management within the GIP

In order the concepts of the GIP and the group of the collaborating mobiles to be realized, the SGSNs constituting the intranet platform must be equipped with routing tables, containing the position of every MN belonging to the mobile intranet served by the specific GIP. The messages, though, exchanged between the SGSNs and the MNs should remain in tact, since the functionality of the GIP, to be said once more, is transparent to the MNs.

First of all, each SGSN of the GIP, by means of a set up procedure, is supplied with a list containing the mobile intranet identities and the statically assigned IP addresses of the MNs forming the mobile intranet. In addition, the system numbers (and the corresponding IP addresses) of all the SGSN participating to the GIP are contained in the list as well. No location information about the exact point of presence of the served intranet MNs' is provided during this set up process, since normally is not available. This information, initially obtained through the attach procedure of the corresponding MNs, is stored locally by the SGSN, and forwarded to all the other SGSNs forming the GP.

From this point on, the Location Update within the GIP Procedure, see Figure 10, takes over every time the mobile intranet's MNs enter a new SGSN's area or refresh their location information. As a matter of fact, the <Routeing Area Update Request> [1] [4] message triggers actions in the GIP according to whether a packet transfer is in progress or not.

So, in the case the MN is attached to the network and migrates between the GIP's SGSNs without being involved in any user data transfer, the message sequence constituted of the messages from 3 to 8 is executed. Otherwise, that is if a handover takes place while the MN participates in a packet transfer session, the above message sequence is preceded by the messages number 2.

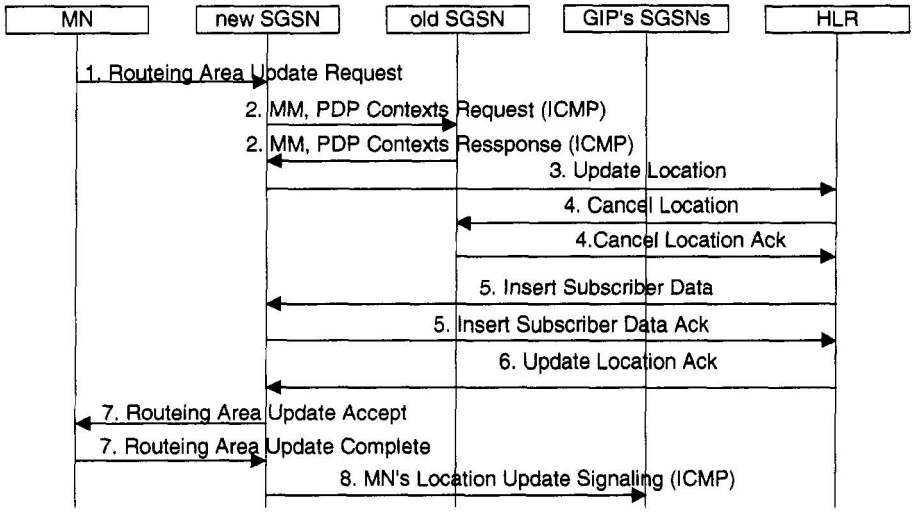

Figure 10. Location Update signalling for migration within the GIP

Of the messages shown in Figure 10, the ones dealing with transactions with the HLR remain unchanged and are executed as the standards determine. Moreover, the messages 2 and 8 are introduced for use within the GIP. Apparently, message 8 should contain the system and IP addresses of the visited SGSN as well as the MN's system and IP addresses. On the other hand, the messages 2 concerning the seamless continuation of a packet session contain the Mobility Management Context, regarding ciphering and authorization information, and the PDP Contexts, which are the Sessions Management parameters. As a matter of fact the PDP Contexts regarding intra-GIP transactions do not include any GGSN related information, being for this reason lighter than the ones described in the standards.

Both these message types are encapsulated in Internet Control Message Protocol (ICMP) packets and delivered to the GIP's nodes they concern. The structure of these ICMP packets could be similar to the one used to transfer addresses in the routing advertisement case of fixed networks [6]. So, all the SGSNs under consideration are able to update continuously their routing tables about the position of each MN belonging to the mobile intranet.

3.2.3.1 Location Management for intranet MNs migrating outside the GIP

An interesting case that should be examined, relates to a session started within the GIP between two mobile intranet's MNs, but for some reason one of them migrates outside the GIP, while the session is still in progress.

Referring to Figure 11, two such MNs, the MN A and the MN B, have to continue their data transactions, while the MN B has left the GIP's area

migrated to some SGSN3 out of it. According to what has already been described above, the <Routeing Area Update Request > message, which MN B sends to the new SGSN3, should be treated according to the standard process of Figure 2. Actually, the corresponding message sequence starts. With the receipt, though, of the <SGSN Context Response> and because of lack of parameters related to some GGSN, the new SGSN3 concludes that the newcomer has a session with another MN within their familiar GIP.

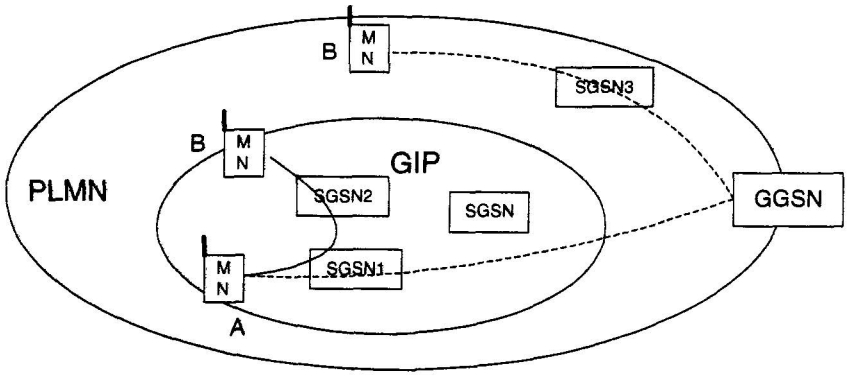

Figure 11. Session Deviation

To be noted at this point, and it will be explained below, that the <SGSN Context Response> messages sent in such a case should contain the identity of the SGSNI, hosting MN A. Obviously, no PDP Context update messages are exchanged with the GGSN and the message sequence of Figure 2 is modified for the case to the one shown in Figure 12.

In addition, the <Session Deviation> message, containing the new SGSN3 address is sent to the SGSNI. So, at the end of the message sequence of Figure 12, the SGSNl knows that MN B, although one of the mobile intranet's MNs, has migrated outside the GIP's area. Moreover, the SGSN3 knows the address of the SGSN1, hosting the MN A, the MN B has a session with.

In order MN B and MN A to continue exchanging traffic, SGSNI, upon the receipt of the <Session Deviation> message, starts towards the GGSN a PDP Context activation procedure, messages 3 and 4 of Figure 3, based on the PDP Context ruling the MN A – MN B session before the handover. In the corresponding <Create PDP Context Request> message the address of the SGSN3 may be included, so that the GGSN, saving time, will not have to search for the SGSN, currently hosting B. To be mentioned, here, that the inclusion of the SGSN address violates the transparency, to the GGSN, of the GIP's functionality.

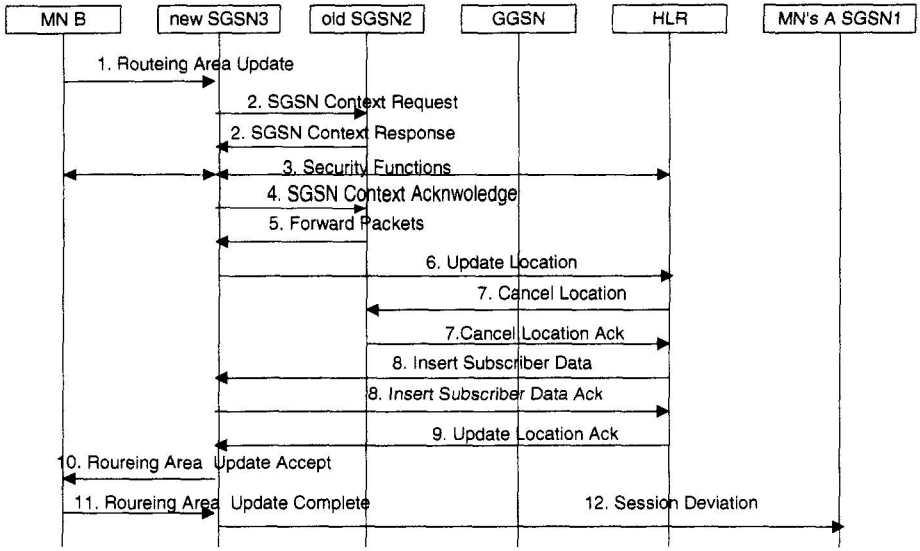

Figure 12. Message Sequence in Session Deviation

On the other hand, the receipt of the <SGSN Context Response> message without any GGSN related parameter triggers, per se, in the SGSN3 the procedure towards the GGSN for the creation of a PDP Context, based on the session management parameters received in the message <SGSN Context Response>, see Figure 12. For time saving reasons, the address of the SGSNl can also be contained in the <Create PDP Context Request> message, sent in this case.

In both cases, the <Create PDP Context Response> message, see Figure 3, coming from the GGSN and verifying the establishment of a PDP Context, is consumed by the SGSN receiving it. Consumed by these SGSNs is, as well, the message <Request PDP Context Activation>, see Figure 4. In this way the whole process renders transparent to MN A and MN B, and the session carries on through the GGSN, see Figure 11.

3.2.4 Mobile Intranet's MN Detach Procedures

Three detach procedures are currently specified in the standards [1], namely the MN-initiated, the SGSN-initiated and the HLR-initiated detach procedures. All the three of them as well the reasoning which they might triggered for are preserved for the mobile intranet's MNs. Apparently, in this case these processes remain transparent to the GGSN as far as it does not participate to the establishment of the session. Consequently, the

transactions, regarding the signaling for the PDP Contexts deletion, between the SGSN and the GGSN do not take place.

3.3 Transactions with Nodes outside the GIP

The GIP functionality, related to a certain number of MNs, ignores entirely MNs not belonging to the intranet served by it. In other words, an SGSN participating to the GIP does not recognize any peculiarity to MNs migrated to its area of coverage, if the MNs are not served by the relative GIP. So, packet sessions having as source or destination "foreign" MNs are carried out with participation of the GGSN, as typical isolated mobile terminals.

On the other hand, packet sessions originated from mobile or fixed nodes outside the GIP, or even outside the PLMN, can be directed to one of the GIP's internal MNs. Nevertheless, the MNs of the mobile intranet can originate transactions with terminals outside the GIP. However, it is intranet's administrator responsibility to decide whether and which of the collaborating MNs, normally residing in the GIP area, will be allowed to communicate with machines outside it. Besides possible intranet's functional reasons, e.g. information concealment, the mobile intranet concept aims at supporting services, which been related to a specific area, are for this reason "introvert". Consequently, it may not be necessary all the nodes to have access to the "outside" world. The ban on forwarding user traffic, coming from these MNs, outside the mobile intranet should be controlled by the hosting SGSN on the basis of the APN parameter, included in the messages related to the PDP Context activation, as well as the MN's system address, known from the Mobility Management.

4. CONCLUSIONS

The UMTS specifications describe procedures supporting the user mobility and the data sessions to and from a mobile user. No special method has been defined in them regarding the treatment of Mobile Nodes joined together in a group residing within an area and using the infrastructure of any of the aforementioned networks.

Extending the facilities of the PLMN under consideration, we have proposed in this paper the introduction of the GPRS Intranet Platform (GIP), so that collaborating Mobile Nodes charged with special tasks, e.g. security, fire service etc., within specific areas are treated in a special way by the SGSNs forming the platform. According to our proposals, the set of the MNs constitutes a mobile intranet, running in the UMTS environment, whose

nodes can mutually establish data sessions without the intervention of the GGSN. As a consequence, the overloading of the GGSN, now discharged of the corresponding traffic, is avoided. Moreover, the control of the sessions within the intranet is decentralized, since it is passed to the SGSNs forming the GIP, which at this aim are enriched with routing abilities regarding the location of the nodes of the intranet served. The concept of the GIP is opaque to the GGSN and to the MNs of the mobile group, since all the main procedures remain unchanged.

Our future research efforts will be focused on the support of charging capabilities and QoS provision by the GIP's SGSNs, originally offered by the GGSN. For the GIP, as proposed in this paper, we have made the assumption that these cannot be negotiated dynamically but are predetermined, according to service level agreements between the PLMN operator and the users of the mobile intranet.

REFERENCES

[1] ETSI TS 123 060 v3.5.0 (2000-10); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2.

[2] M. Mouly, M. B. Pautet, The GSM System for Mobile Communications, 1992.

[3] ETSI TS 133 102 v3.5.0 (2000-07); Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture (3GPP TS 33.102 3.6.0 Release 1999).

[4] ETSI TS 124 008 v3.5.0 (2000-09); Universal Mobile Telecommunications System (UMTS); Mobile radio interface layer 3 specification; Core Network Protocols-Stage 3; (3GPP TS 24 008 3.5.0 Release 1999).

[5] ETSI TS 129 060 v3.6.0 (2000-09); Universal Mobile Telecommunications System (UMTS); General Packet Radio Services (GPRS); GPRS Tunnelling Protocol (GTF') across the Gn and the Gp Interface (3GPP TS 29.060 3.6.0 Release 1999).

[6] W. Richard Stevens, TCPAP Illustrated, Volume1 , The Protocols, Addison-Wesley, 1994.