A Secure Mobile VPN Scheme for UMTS

Christos Xenakis, Nikos Loukas and Lazaros Merakos

Communication Networks Laboratory, Department of Informatics & Telecommunications,
University of Athens, Greece
{xenakis, loukas, merakos}@di.uoa.gr

Abstract - **In this paper, a mobile Virtual Private Network (VPN) scheme for the Universal Mobile Telecommunication System (UMTS) is proposed and analyzed from a security point of view. The proposed scheme improves the level of protection for data transfer that is currently supported in UMTS and facilitates the realization of Mobile Internet. The security functionality, which is based on the IPsec framework, is integrated to the mobile network infrastructure so as to eliminate the potential computational overhead on mobile devices. The proposed VPN scheme operates transparently to the mobile subscribers' movement. Moreover, the required enhancements can be integrated in the existing network infrastructure, and, therefore, the proposed security scheme can be employed as an add-on feature to the UMTS standard.**

1. Introduction

The Universal Mobile Telecommunication System (UMTS) [1] is a realization of 3G networks, which intend to establish a single integrated system that supports a wide spectrum of operating environments. Users have seamless access to a wide range of new telecommunication services, such as high data rate transmission for high-speed Internet/Intranet applications, independently of their location. Thus, mobile networks comprise a natural extension of the wired Internet computing world, enabling access for mobile users to multimedia services that already exist for non-mobile users and fixed networking.

For the success of these applications over mobile systems, security is considered as an essential feature. In order to meet security objectives, UMTS incorporates a specific security architecture, which aims at protecting network operation and data transfer through the radio access network. In addition to this, the involved parties (network operator and mobile users) can employ traditional security technologies used in terrestrial networking, such as: *(a)* firewalls that protect UMTS core network from external (Internet) attacks; *(b)* application layer security which mainly protects web-based application data between the communicating peers; and *(c)* pre-configured IPsec-based Virtual Private Networks (VPNs) that protect data transfer over the public Internet for specific mobile subscribers and remote Internet sites [2]. However, the firewall technology cannot adequately ensure data transfer within the UMTS core network, pre-configured IPsec-based VPNs cannot be applied in any mobile scenario, and application layer security solutions cannot be employed in any type of potential services.

Thus, data communications over the UMTS network may experience security threats. The reason is that there is a lack of a general-purpose, application independent security mechanism that provides advanced security services to user data traffic according to the particular end-user needs, inside and outside the mobile core network [2]. To address this, the current article proposes and analyses a secure mobile VPN scheme for the UMTS network architecture. The proposed security scheme integrates the VPN functionality into the mobile network infrastructure, minimizing the administrative and the computational overheads for end-users. It utilizes the encryption mechanism over the radio interface and deploys an IPsec-based [3] VPN over the UMTS backbone and the pubic Internet. For VPN initialization and key agreement procedures, an IKE protocol proxy scheme [4] is employed, which enables the mobile user to establish a VPN, while outsourcing complex key negotiation to the network infrastructure. The proposed scheme operates transparently to the mobile subscribers' movement. Moreover, the required enhancements can be integrated in the existing network infrastructure, and, therefore, the proposed security scheme can be employed as an add-on feature to the UMTS standard.

The rest of this paper is organized as follows. Section 2 introduces the network architecture. Section 3 presents the proposed mobile VPN scheme. Section 4 elaborates on the impact of mobility to the proposed security scheme. Finally, section 5 contains the conclusions.

2. Network Architecture

Consider a mobile subscriber using a mobile station (MS) and attempting to establish a secure remote connection to a corporate Local Area Network (LAN), and access a remote server through the UMTS infrastructure, as shown in Fig. 1. The security gateway (SG) that resides between the LAN and the public Internet functions as a proxy device providing security services to the private network nodes. It is assumed that the Internet and the UMTS backbone are based on IPv4. Both the Gateway GPRS Support Node (GGSN) and the SG use Network Address translation NAT [4].

After power-on, the MS searches for a suitable cell in the UMTS Terrestrial Radio Access Network (UTRAN) to provide services, and tunes to its control channel. Then, it performs the packet International Mobile Subscriber Identity (IMSI) attach procedure, which creates valid routing information for the packet switched (PS) connection in every node involved, and transferring the subscriber profile from the Home Location Register (HLR). When the IMSI has been

attached, the MS initiates a Packet Data Protocol (PDP) context activation procedure, which negotiates the desired packet connection characteristics between the MS and the network [5]. The employed protocol for PS data transport in the UMTS R99 backbone network is the GPRS Tunneling Protocol (GTP) [6]. To be able to convey data packets from and to the MS, the Serving GPRS Support Node (SGSN) starts a radio access bearer (RAB) allocation procedure over the UTRAN, and a core network (CN) bearer is established between itself and the GGSN [5] [7].

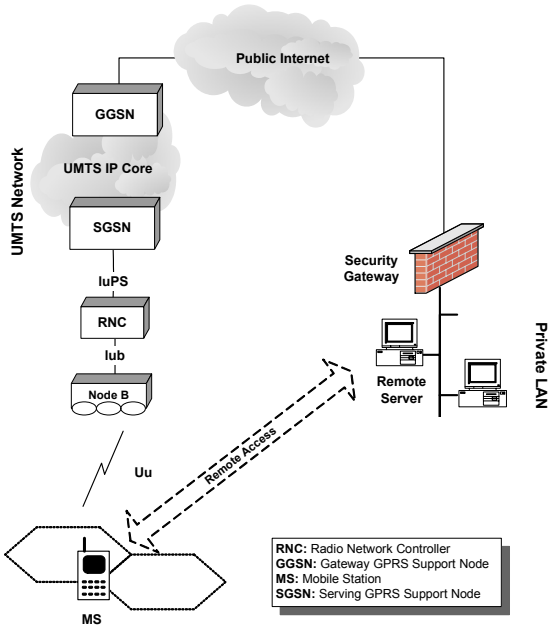

Figure 1: Network architecture

The result of these procedures is that two types of bi-directional tunnels are set up: *a)* one tunnel between the MS and the Radio Network Controller (RNC) employing the Medium Access Control (MAC) [8] protocol over the WCDMA radio access interface, which also supports security protection; and *b)* one tunnel between the RNC and the GGSN employing the GTP without any security precaution. The latter consist of two parts: the Iu bearer over the Iu interface, and the PS domain backbone bearer between the SGSN and GGSN.

Despite the ciphering over the air interface, the IP traffic goes unencrypted all the way from the RNC to the corporate LAN SG, and vice-versa. Given that the GTP protocol operates over IP, and the UMTS is connected to the public Internet, the UMTS backbone may be considered as a vulnerable and easily accessible network segment. Firewall technology is inadequate against attacks that originate from malicious mobile subscribers, as well as from network operator personnel, or from any other third-party who gets access to the UMTS core network. Application layer solutions, such as SSL and WAP security can be used to secure the communication of any application, but they must be integrated into the application, and, thus, to a large extent they are used for web-based applications. Moreover, the current static VPN scheme supported by the UMTS involves the predefined establishment of security associations between the UMTS border and remote sites, failing to provide the necessary flexibility required by typical mobile users and ad hoc services [2].

3. Secure Mobile VPN Scheme

The proposed model integrates the VPN functionality into the UMTS network infrastructure. The network operators provide the security aggregation facilities, which are shared amongst the network subscribers, as a complementary service granting added value. They have solid network management expertise and more resources to effectively create, deploy, and manage VPN services originating from mobile subscribers. However, the proposed security model involves two separate security domains (i.e., mobile subscriber – mobile operator, and mobile operator – remote site), and, thus, requires an explicit level of trusted relationships between them.

3.1 UMTS Network Enhancements

For the deployment of the security scheme the MS must be enhanced with a security client (SecC), which is used to request for VPN services and express the end-user preferences. Moreover, the RNC of the UMTS architecture should incorporate a security server (SecS) that establishes, controls, and manages VPNs between itself and remote SGs at corporate LANs on behalf of the mobile users (see Fig. 2). SecS comprises an IPsec implementation modified to adapt to the client-initiated VPN scheme, and the security service provision in a mobile UMTS environment. It consists of six components including: security manager, Internet Key Exchange (IKE), policy manager, security policy database (SPD), security association database (SADB) and IPsec base protocol.

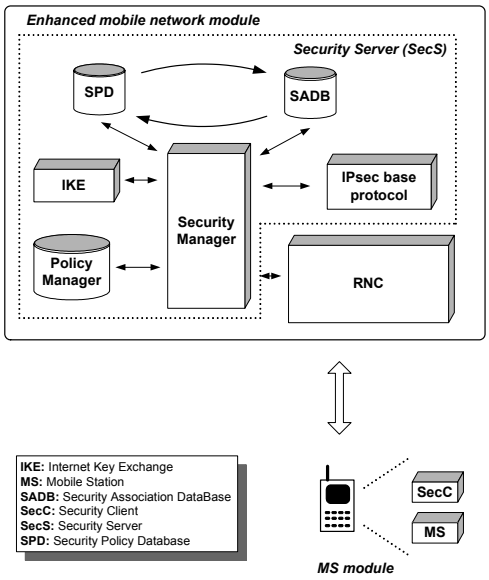

Figure 2: Security Client (SecC) and Security Server (SecS) modules

The main functional component of the SecS is the security manager, which manages the SecS submodules, and facilitates the VPNs configuration. The security manager maintains the security policy databases, handles the user requests, and reports on errors.

IKE authenticates IPsec peers, negotiates security services, and generates shared keys dynamically. It provides secure key determination via DH exchanges.

The policy manager contains the network security policy that specifies the set of users that are allowed to have security services, as well as the type of the offered services. It communicates with the HLR in order to acquire the users profile. The policy manager contents are used to configure the SPD and the SADB.

SPD is the primary policy database used by the SecS to decide on network traffic handling, such as encryption, decryption, authentication, discarding, passing through and modification. SPD contains an ordered list of policy entries, each of which defines the set of IP traffic encompassed by this policy entry, and is keyed by one or more selectors [3].

SADB maintains the contents of all active SAs used by the SecS for IPsec formatting. An SA is a management feature used to enforce a security policy. It represents all the necessary parameters (including protocols, modes, algorithms, etc.) that have been agreed between the IPsec peers. The security manager is responsible for filling out the contents of each entry in SADB.

Finally, the IPsec base protocol processes the authentication and encryption transformation defined in the IPsec framework. It handles all the network layer functions, such as fragmentation and path maximum transfer unit, and ensures that all traffic passing through the UMTS node is secure and authorized, providing firewall capabilities.

3.2 VPN Establishment

VPN initialization and key agreement procedures are based on an IKE-proxy scheme [4]. When a mobile user wants to establish a secure remote connection towards a SG, it uses the SecC to request for an IPsec SA from the corporate SecS. The SecS negotiates the IPsec SA by using the IKE protocol on behalf of the SecC. During phase 1, an Internet Security Association and Key Management Protocol (ISAKMP) SA negotiation in Aggressive Mode (AM) takes place [9]. The AM of the IKE negotiation is an option defined to speed up the IKE transaction at the cost of slightly less security. Moreover, the authentication method used in AM does not involve the IP address of the initiator. Thus, the IKE protocol is operational in a proxy-based scheme, where the VPN is not directly established by the initiator, and in a mobile network environment where dynamic (not static) IP addresses may be used.

To initiate an IPsec SA negotiation, the SecC forwards a message destined for the SecS that includes the IP address of the remote SG, the IPsec SA request, and the Identification Data of the mobile subscriber. Upon receiving the request, the SecS verifies the mobile subscriber privileges and the mobile network capabilities in providing VPN services by asking the policy manager. Additionally, looks for an already active ISAKMP SA between the SecS and the SG on behalf of the particular user. If such an SA exists, then, the SecS proceeds to phase 2. If not, the SecS negotiates an IPsec SA using the IKE protocol.

Although the coexistence of NAT and IPsec is quite troublesome, both mechanisms can be configured to co-operate in the particular scenario for VPN deployment. The NAT employment in the GGSN requires special consideration for the proposed mobile VPN deployment. For that reason, the ESP is proposed for security services, given that it allows NAT to modify the protected IP packets header without experiencing integrity failure. Moreover, the complementary UDP encapsulation is used to overcome the incompatibilities arising from the TCP and NAT coexistence [4].

3.3 VPN Operation

After the VPN establishment between the SecS and the corporate SG (see Fig. 3), the MS may communicate with the remote server securely. Before transmitted over the radio interface the IP packets, which are destined for the remote server, are processed by the Packet Data Convergence Protocol (PDCP) [10] the Radio Link Control (RLC) protocol [11] and the MAC sublayer.

The PDCP compresses the headers of the payload protocol in order to be carried over the WCDMA radio interface. The RLC performs link layer functions, such as segmentation and reassembly, flow control, sequence number check, ciphering, etc. The UTRAN ciphering is performed either in the RLC, if the radio bearer uses the non-transparent RLC mode, or in the MAC, if the radio bearer uses the transparent RLC mode.

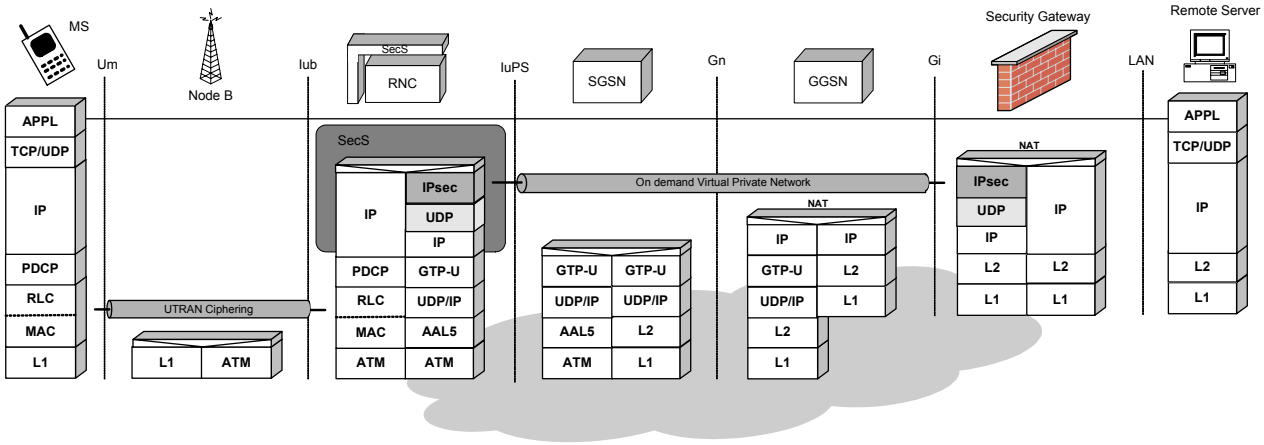

Figure 3: Protocol stack for the proposed mobile VPN scheme

The MAC layer multiplexes protocol data units from higher layer into transport block sets carried over common transport channels. Protected data packets (by UMTS ciphering) are tunneled and forwarded to the serving RNC using the established RAB. The identification of MSs on the common transport channel is performed by a temporary identity, which can be either the Cell Radio Network Temporary Identities (C-RNTI), or the UTRAN Radio Network Temporary Identity (U-RNTI). The RAB ID identifies uniquely the RAB for the particular MS and the specific core network domain. It includes a binary representation of the Network Service Access Point Identifier (NSAPI), which binds data streams from the access stratum and the non-access stratum [5] [12].

In the RNC, the corresponding protocols terminate the MAC tunneling, decipher the packets and acquire the active PDP context based on the RAB ID, the RNTI and the NSAPI values. A GTP tunnel, which is identified by the Tunnel Endpoint Identifier (TEID) and the IP address of the involved SGSN, corresponds to each PDP context [12]. Because of the presence of the SecS, every packet that is going through the RNC is subject to processing by the IPsec base protocol, which determines whether it will apply IPsec protection or not. For the specific mobile VPN scheme, the default set of selectors [3] that facilitates the interaction with the SPD should be enhanced to incorporate UMTS routing parameters, such as the NSAPI, the TEID and the involved SGSN IP address.

In case that IPsec processing is to be applied, the original IP packets are encrypted and authenticated. The IPsec is configured in transport mode avoiding multiple encapsulations within the UMTS backbone. After the application of IPsec, the protected data packets are wrapped within UDP/IP headers for NAT traversal [4]. The wrapped packets are then tunneled between the RNC and the GGSN using the GTP protocol. The TEID, which is presented in the GTP header, indicates which tunnel a particular protocol data unit belongs to.

The GTP tunnel is terminated at the GGSN, which removes the GTP header and applies NAT on the encrypted IP packets. The packets are then forwarded to the public Internet and the latter delivers them to the SG located at the private LAN. Upon receiving protected data packets, the SG discards the UDP header, terminates the IPsec tunnel, decrypts the packets and forwards them to the inner LAN destination. Because of NAT application, the SG changes the destination address in the IP header. However, the NAT employment within the SG does not have any impact on the IPsec operation, since the IPsec tunnel has been terminated. In Fig. 4, the protected data flow from the MS to the corporate remote server over the UMTS network and the public Internet is presented.

Whenever the remote server sends IP datagrams to the MS, the SG receives these packets, changes their source IP address (NAT), maps them to the appropriate SA, and, then, wraps the encrypted packets with UDP/IP header for NAT traversal. The encrypted packets are forwarded through the Internet, and are routed to the GGSN. The latter inquires the HLR to obtain the MS current location, and tunnels the packet through the UMTS backbone to the appropriate SGSN and RNC.

Within the RNC, prior to performing any IPsec processing, the UDP header and the GTP encapsulation are removed. Each IPsec-protected datagram is identified by the appearance of the ESP value in the IP next protocol field. In order to determine the IPsec SA that is to be applied, a look up in the SADB is performed. If the SA lookup fails, then, the packet is dropped and an error is reported. Otherwise, based on the SA found, the IPsec base protocol performs the IPsec processing (authenticates and decrypts the packet). In the sequel, it matches the packet selectors to these encompassed within the SA and finds the incoming policy within the SPD. Finally, it checks whether the required IPsec processing has been applied and forwards the original IP packet to its destination.

4. Mobility Implications

The RNC partially handles the MS movement within the radio access network using the radio resource control (RRC) procedures [7]. The location information in PS transactions is distributed in such a way that the core network domain is aware of the location of the MS within the accuracy of routing area and the RNC knows the location of the MS with the accuracy of cell. When the MS moves to an adjacent cell, which is served by the same RNC, it performs an RRC cell update procedure to inform the RNC about the current cell. The C-RNTI may be reallocated when the MS accesses the new cell, but since none of the UMTS routing parameters that are also involved in the VPN operation (NSAPI and TEID) is changed, the VPN between the RNC and the SG remains the same.

Every time the MS enters a new UTRAN registration area and owns an RRC connection, it has also to perform an update procedure. In case this area is controlled by a different RNC but the same SGSN, the procedure is referred to as intra-SGSN routing area update, which corresponds to the relocation of the Iu interface.

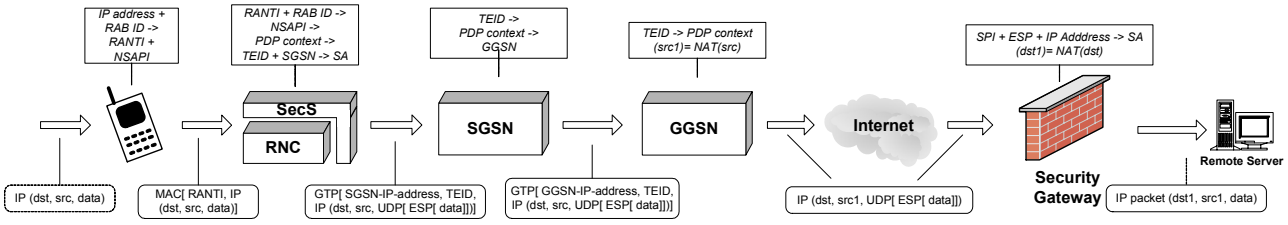

Figure 4: Protected data flow from the MS to the remote server in the proposed VPN scheme

On the other hand, when the mobile enters an area, which is controlled by a different RNC and a different SGSN, then, it is referred to as inter-SGSN routing area update procedure [5] [6].

Fig. 5 illustrates the message sequence diagram of the intra-SGSN relocation procedure, which attempts to preserve the established network-wide VPN for the moving MS. Relocation procedure begins when the source RNC sends a *Relocation Required* message to the SGSN. The SGSN receives this and tries to allocate the appropriate Iu resources towards the target RNC. It sends the *Relocation Request* message to the target RNC, which contains the information required to build the same RAB configuration as the one existing for the MS before the relocation.

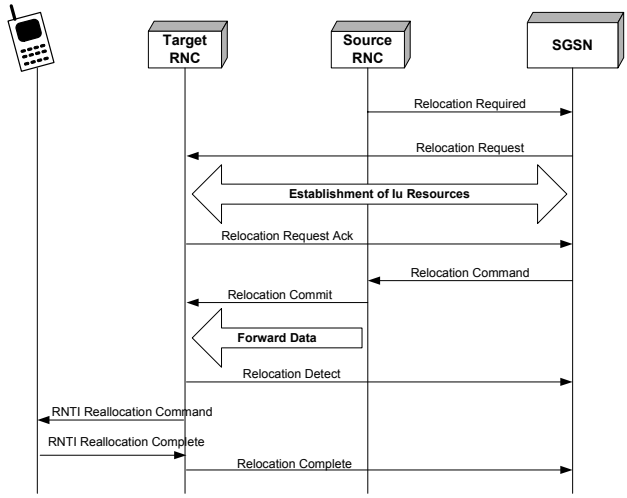

Figure 5: Intra-SGSN relocation procedure

When the appropriate Iu resources are allocated, the target RNC responds with a *Relocation Request Acknowledge* message. The SGSN informs the source RNC that the preparation of the relocation is over and, therefore, the appropriate actions may take place to perform the actual relocation of the serving RNC. For this purpose, the SGSN sends the *Relocation Command* to the source RNC. The source RNC requests from the target RNC to proceed with the relocation by sending *Relocation Commit* message. The purpose of this message is to transfer the serving contexts from the source RNC to the target RNC. These contexts are sent for each RAB and mainly contain the appropriate sequence numbers of the user-plane messages to be subsequently transmitted in the uplink, and downlink directions. The *Relocation Commit* message should be enhanced to incorporate the status of the active SAs that the moving MS has established. It should contain the VPN context, which includes the SPD entries and the SADB entries referring to the involved MS SAs (incoming and outgoing). The VPN context transfer facilitates the target RNC to construct a copy of the security relations that exist between the source RNC and remote SGs for the particular MS and thus, it guarantees network-wide VPN service continuity as the user moves.

It is important to note that before sending the *Relocation Commit*, uplink and downlink data transfer at the source RNC is suspended. After having sent the *Relocation Commit* message, the source RNC begins the forwarding of data for each concerned RAB to the target RNC and the target RNC sends *Relocation Detect* message to indicate to the SGSN that the execution of the serving RNS relocation has been detected. Then, the target RNC allocates a new RNTI to the MS and forwards this value to the mobile with *RNTI Reallocation* message. When the MS acknowledges the correct reception of the RNTI, the target RNC considers that the relocation procedure has been completed, and responds to the CN with a *Relocation Complete* message.

In case of inter-SGSN routing area update (see Fig. 6 in next page), the MS first sends a *Routing Area Update Request* message, which contains the old and the new routing area identifier values to the new SGSN. Based on this information the new SGSN is able to determine the old SGSN and it requests information about the subscriber contexts by sending an *SGSN Context Request* message. The old SGSN validates the presence of the MS and responds with an enhanced *SGSN Context Response* message, which includes the active PDP context, the mobility management (MM) context, as well as the involved VPN context. Therefore, a copy of the current VPN context, which resides at the RNC and describes the active SAs between the RNC and remote SGs for the particular user, must also exist in the SGSN. This facilitates the VPN reconstruction and the VPN service continuation in case that a moving MS handoffs to a different RNC or SGSN.

The new SGSN requests the subscriber Authentication Center (AuC) to provide authentication vectors, which returns them within a *Send Parameters* message. Now, the new SGSN is able to start authentication and security control for the moving MS. Furthermore, it acknowledges the contexts transfer and informs the old SGSN that is ready to receive data packets belonging to the conveyed PDP contexts. When authentication activities have been successfully completed, the new SGSN informs the GGSN that the SGSN has now been changed and the PDP context information has been changed accordingly. The new SGSN updates location information in the HLR, which in turns cancels the old location of the MS from the old SGSN. Then, the HLR starts to transfer the subscriber profile to the new SGSN, which sends a *Routing Area Update Accepted* message to the target RNC. The RNC receives and stores the VPN context values in order to reconstruct the security relations that exist between the source RNC and remote SGs for the moving MS. The target RNC verifies its availability in providing VPN services, updates its SPD and SADB with the relative IPsec SAs contents and finally, sends a *Routing Area Update Accepted* message to the MS. The latter stores the new temporary identity on its USIM and acknowledges the receipt by sending a *Routing Area Update Complete*.

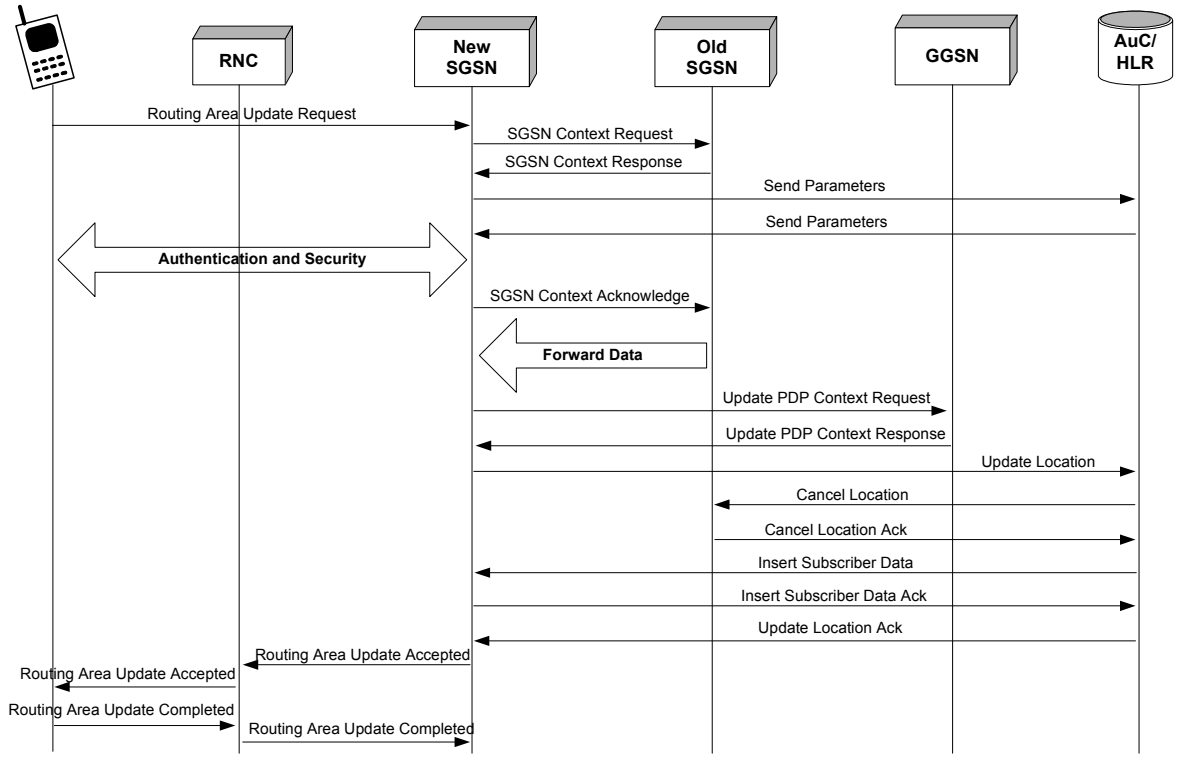

Figure 6. Inter-SGSN routing area update procedure

5. Conclusions

In this paper, a secure mobile VPN scheme for UMTS has been presented. The proposed scheme improves the level of protection that is currently supported in UMTS and facilitates the Mobile Internet realization. It can be deployed in a dynamic manner, enabling on-demand VPN services for all UMTS network subscribers and roaming users. It secures data transmission over the entire network route (from the mobile user to the remote connected server) by utilizing the default UMTS ciphering over the radio interface and by deploying an IP VPN over the UMTS core and the public Internet. The VPN functionality, which is based on the IPsec framework, is outsourced to the network infrastructure so as to eliminate the potential computational overhead on the mobile devices. Finally, the required enhancements can be integrated in the existing SGSN and thus, the proposed security scheme can be employed as an add-on feature to the UMTS standard.

REFERENCES

[1] 3GPP TS 23.002 (v3.6.0) "*Network Architecture*", release '99, Sept 2002.

[2] C. Xenakis, L. Merakos, "*Security in third Generation Mobile Networks*", Computer Communications, Elsevier Science, Vol. 27, No. 7, May 2004, pp. 638-650.

[3] S. Kent and R. Atkinson, "*Security Architecture for the Internet Protocol*", RFC 2401, Nov. 1998.

[4] C. Xenakis and L. Merakos, "*On Demand Network-wide VPN Deployment in GPRS*", IEEE Network, Vol. 16, No. 6, Nov/Dec. 2002, pp. 28-37.

[5] 3GPP TS 24.008 (v3.15.0) "*Mobile Radio Interface Layer 3 specification; Core Network Protocols – Stage 3*", release '99, March 2003.

[6] 3GPP TS 23.060 (v3.16.0) "*GPRS Tunneling Protocol (GTP) across the Gn and Gp interface*", release '99, March 2003.

[7] 3GPP TS 25.331 (v3.14.0) "*Radio Resource Control (RRC) protocol specification*", release '99, March 2003.

[8] 3GPP TS 25.321 (v3.15.0) "*Medium Access Control (MAC) protocol specification*", release '99, March 2003.

[9] D. Harkins and D. Carrel, "*The Internet Key Exchange (IKE)*", RFC 2409, Nov. 1998.

[10] 3GPP TS 25.323 (v3.10.0) "*Packet Data Convergence Protocol (PDCP) Specification*", release '99, Sept 2002.

[11] 3GPP TS 25.322 (v3.15.0) "*Radio Link Control (RLC) protocol specification*", release '99, Dec 2002.

[12] 3GPP TS 25.301 (v3.11.0) "*Radio Interface Protocol Architecture*", release '99, Sept 2002.