A network-assisted mobile VPN for securing users data in UMTS

Christos Xenakis[1], Christoforos Ntantogian[2] Ioannis Stavrakakis[2]

[1]Department of Technology Education and Digital Systems, University of Piraeus, Greece

[1]Department of Informatics and Telecommunications, University of Athens, Greece

e-mail: xenakis@unipi.gr, ntantogian@di.uoa.gr, ioannis@di.uoa.gr

Abstract

This paper proposes a network-assisted mobile Virtual Private Network (mVPN) security scheme that provides secure remote access to corporate resources over the Universal Mobile Telecommunication System (UMTS). The proposed scheme, which is based on IPsec, distributes the required security functionality for deploying a VPN between the involved user's device and the mobile network limiting the configuration, computation and communication overheads associated with the user and its device. The network-assisted mVPN addresses the security weaknesses of the UMTS technology in protecting users' data and satisfies the security requirements of the mobile users. It can be integrated into the UMTS network infrastructure requiring only some limited enhancements to the existing mobile network architecture, and without disrupting the network operation. For the initialization of a network-assisted mVPN and the related key agreement an extension of Internet Key Exchange version 2 (IKEv2) is proposed. The proposed network-assisted mVPN can operate seamlessly and provide security services continuously while the mobile user moves and roams as it binds the UMTS mobility management with the VPN deployment. The deployment cost of the proposed scheme is evaluated analytically and via simulations and is compared to that of the end-to-end (e2e) VPN scheme that protects the data exchanged between the mobile user and the remote server, and a scheme that does not include any additional security mechanism. The proposed scheme increases the cumulative VPN deployment cost compared to the e2e scheme, but on the other hand it limits considerably the VPN deployment cost of the involved MS, which is important due to it resource limitation. Moreover, it does not considerably affect the capacity of the UMTS network. Finally, the deployed network-assisted mVPN hardly has an impact on the total delay of the transmitted user's packets.

1. Introduction

The Universal Mobile Telecommunication System (UMTS) [1] is a realization of third generation (3G) networks, which intends to establish a single integrated system that supports a wide spectrum of operating environments. The mobile users of UMTS have seamless access to a wide range of multimedia services that are already available to non-mobile users and provided by fixed networking, independently of their location. Therefore, the UMTS comprises an extension of the wired Internet towards the mobile computing world, materializing the mobile Internet.

Similarly to non-mobile Internet users, the mobile users of UMTS require dynamic, client-initiated security mechanisms that are available anywhere – anytime, providing secure remote access to corporate resources and ensuring any-to-any connectivity in an ad hoc fashion. These mechanisms should provide customized security services to data traffic, taking into account the users' mobility and the mobile network characteristics. Specifically, the mobile users require security solutions of low configuration, computation and communication overhead since: (i) the mobile devices are characterized by limited power and processing capabilities; (ii) the mobile users usually do not have specialized knowledge on security issues; and (iii) the radio interface has limited bandwidth resources.

Virtual Private Networks (VPNs) are used for authentication and authorization of users' access to corporate resources, the establishment of secure tunnels between the communicating parties and the encapsulation and protection of the data transmitted by the network. Traditionally, VPNs were established in a static manner, without any consideration for mobility support. However, the rapid evolution of the wireless technologies has enabled mobility that has become one of the most imperative requirements of users, which desire to connect with their enterprise network from external mobile networks and at the same time maintain their VPN connection as they move from one access network to another.

To address the aforementioned requirements, this paper proposes a network-assisted mobile VPN (mVPN) security scheme for secure remote access to corporate resources over UMTS. The proposed scheme, which is based on IPsec, distributes the required security functionality for deploying a VPN between the involved user's device and the mobile network, limiting the configuration, computation and communication overheads associated with the user and its device. The network-assisted mVPN protects user's data by employing the UMTS ciphering over the radio access network and establishing a mVPN over the UMTS backbone network and the public Internet according to the user's needs. The functional differences of this scheme compared to existing mVPN schemes can be summarized as follows: (i) the proposed solution does not involve the mobile user's device in executing complex and resource consuming authentication, key negotiation and mobility management protocols for maintaining the established mVPN [8]; (ii) the mobile user's device does not perform duplicated security transformations to the transmitted data [8]; (iii) the transferred data over the radio access network are not encrypted twice; and (iv) the proposed scheme is compatible with the legal interception option that requires access to the traversing data within the mobile/wireless network. For the initialization of a network-assisted mVPN an extension of the Internet Key Exchange version 2 (IKEv2) [21] is proposed. This extension enables the mobile user to initiate, dynamically, a VPN establishment, while outsourcing the negotiation and the generation of keys to the network infrastructure. The established network-assisted mVPN can operate seamlessly and provide security services continuously while the mobile user moves and roams as it binds the UMTS mobility management with the VPN deployment. Based on the analysis of the proposed security scheme, the VPN deployment cost associated with the peers' authentication and the VPN establishment and which occurs once for each deployed mVPN is estimated. In addition, the operation cost of the deployed network-assisted mVPN, which is related to the protection of the transmitted data, is

considered. To evaluate this cost we have developed a simulation model and compared the performance of the proposed security scheme to this of the end-to-end (e2e) VPN scheme that protects the data exchanged between a mobile user and a remote server, and a scheme that does not include any additional security mechanism.

The rest of this paper is organized as follows. Section 2 briefly presents the UMTS technology and the related work on mVPNs. Section 3 describes and analyses the proposed network-assisted mVPN security scheme. Section 4 evaluates the performance of the proposed security scheme and finally, Section 5 contains the conclusions.

2. Background

2.1 UMTS

The UMTS network architecture includes the core network (CN), the radio access network and the user equipment, as shown in Fig. 1. This division provides the necessary flexibility by allowing the coexistence of different access techniques and different core network technologies, thus facilitating the migration form second generation (2G) to 3G networks. The fundamental difference between the Global System for Mobile Communications (GSM)/ General Packet Radio Services (GPRS) [1] and the UMTS release 1999 (R99) [2] is that the latter supports higher bit rates (up to 2Mbps). This is achieved by employing a new wideband code division multiple access (WCDMA) radio interface for the land based communication system, named UMTS terrestrial radio access network (UTRAN) [3]. UTRAN consists of two distinct elements: Node Bs, and a Radio Network Controller (RNC). A Node B converts data flows between the lu-b and Uu interfaces, which connect it to the RNC and the user equipment, respectively. The RNC owns and controls the radio resources of the Nodes Bs connected to it. The user equipment comprises a mobile station (MS) that is usually characterized by limited processing, memory and power capabilities.

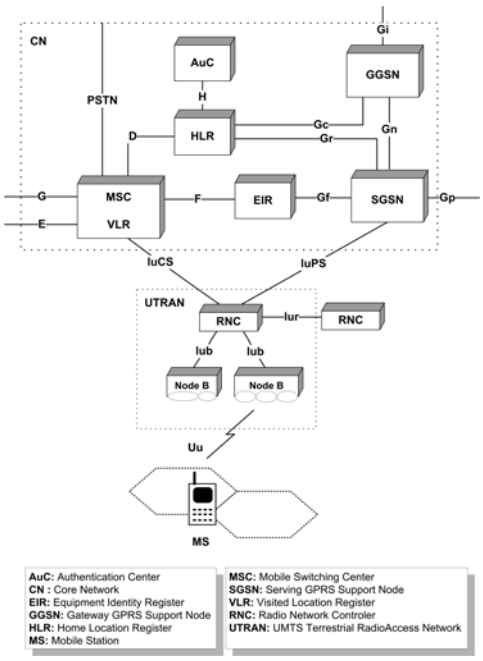

Fig. 1: UMTS network architecture (release 99)

The CN of the UMTS R99 uses the network elements of GSM/GPRS such as the Home Location Register (HLR), the Visitor Location Register (VLR), the Authentication Centre (AuC), the Equipment Identity Register (EIR), the Mobile Service Switching Centre (MSC), the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN) [1]. HLR is a database used for the management of the permanent data of mobile users. VLR is a database of the service area visited by an MS and contains all the related information required for the MS service handling. AuC maintains security information related to subscribers' identity, while the EIR maintains information related to mobile equipments' identity. MSC provides circuit-switched services (e.g., voice call), and the SGSN and GGSN handle packet-based traffic between MSs and external packet data networks (PDNs). More specifically, the SGSN is responsible for the delivery of data packets from and to a MS within its service area. Its tasks include packet routing and transfer, mobility management, logical link management, and authentication and charging functions. Finally, the GGSN acts as an interface between the UMTS CN and an external PDN (e.g., Internet). It converts the UMTS packets coming from the SGSN into the appropriate packet data protocol (PDP)

format (e.g., IP) and forwards them to the corresponding PDN. Similar is the functionality of the GGSN in the opposite direction. The communication between the SGSN and the GGSN is based on IP tunnels through the use of the GPRS Tunneling Protocol (GTP) [4].

User's data transmitted over the radio interface (i.e., between the MS and the RNC) of UMTS are subject to ciphering using the function f8. F8 is a symmetric synchronous stream cipher algorithm used for encrypting frames of variable length [19]. However, this security mechanism does not extend far enough towards the CN of UMTS, resulting in the clear-text transmission of the user's data within it (i.e., CN) [5]. The UMTS CN transports the user's data using the GTP protocol, which does not support any security measure. GTP establishes unencrypted tunnels between an SGSN and a GGSN using the IP protocol stack, which provides open and easily accessible network architectures. Thus, the user's data conveyed over the UMTS CN are exposed to all security threats (e.g., IP spoofing, compromise of confidentiality and privacy, denial of service attacks, etc.) that the public Internet is subject to, which degrade the level of security supported by the UMTS [6].

2.2 Mobile VPNs

Recently, several solutions have been proposed that support seamless mVPN deployment. The Internet Engineering Task Force (IETF) [9] proposes an approach that uses two instances of mobile IP (MIP) to support seamless and secure mVPN deployment between a user and an associated enterprise network. When the user moves to an external network, the first instance of MIP ensures that the established VPN tunnel is not broken due to the change of the user's IP address. The second instance of MIP guarantees that packets sent to the user are forwarded to it through the VPN tunnel. The key advantage of this scheme is that it uses existing IETF protocols and does not require any modifications to them. However, the multiple encapsulations of data packets (i.e., internal MIP, VPN tunnel, and external MIP) reduce the overall performance, especially over bandwidth-constrained wireless networks. A. Dutta et al.

[10] has evaluated the performance of the IETF's mVPN scheme in terms of packet transmission delay, variation delay and packet loss.

The deployment of the above mVPN scheme requires the incorporation of two different Home Agents (HA): an internal HA (i-HA) in the enterprise network and an external HA (x-HA) in the external network. This fact raises two questions: (i) where should the x-HA be resided, since the placement of x-HA impacts the handoff and the end-to-end latency, and (ii) how should the x-HA be trusted, since the x-HA is outside the private network and might not be under the control of the private network. Jyh-Cheng Chen et al. [11] address the above issues by assigning dynamically the x-HA [12] in a secure manner using the Diameter MIP application [13]. Thus, they manage to minimize the handoff and end-to-end latency and at the same time to establish secure and trusted relations between the mobile user, the x-HA and the i-HA.

Shun-Chao Huang et al. [14] propose a Session Initiation Protocol (SIP) based mVPN scheme that supports real-time applications, which require relatively small delays. SIP is an application layer signaling protocol that supports both user and terminal mobility. The authors have conducted various experiments to measure the bandwidth consumption, the end-to-end delay and the handoff latency of the proposed mVPN solution. Their results indicate that the SIP based mVPN has better behavior than the IETF's mobile VPN solution.

IETF has also proposed a mVPN solution that combines a new mechanism called Mobility and Multihoming IKE (MOBIKE) [15][16] with MIP [17]. To achieve VPN mobility the user employs MIP when moving within the enterprise network and Mobike when moving outside it (i.e., external network). The main advantage of Mobike is that it can modify the IPsec security associations (SAs) without re-establishing the IPsec tunnel in cases that the user changes its IP address. Thus, it does not use either MIP or SIP for VPN mobility, therefore reducing the mobility management overhead.

Finally, an implementation of mVPN in UMTS, [8], integrates the security functionality into the communicating peers, which negotiate and apply security providing e2e VPNs. A MS and a remote Security Gateway (SG) of a corporate private network establish a pair of IPsec SAs between them, which are extended over the entire communication path. Thus, sensitive data are secured as they leave the originator site (MS or SG) and remain protected while they are conveyed over the radio interface, the UMTS CN and the public Internet. The deployed e2e VPN has no interrelation with the underlying network operation and the provided network connectivity. It supports user mobility and roaming, and operates transparently to the MS movement, since the security parameters, which are contained in the IPsec SAs, are not affected by the UMTS mobility management procedures, [18].

A common characteristic of the existing mVPN solutions is that they deploy e2e VPNs between the communicating peers. Thus, they do not consider the fact that mobile devices are usually characterized by limited energy and processing capabilities, which may increase the processing latency of the transmitted data. In addition, the execution of cryptographic algorithms, key negotiation protocols (IKE or IKEv2) for the establishment of VPN tunnels and mobility management protocols (i.e., MIP or SIP) may cause energy consumption issues for the mobile devices. The current mVPN solutions duplicate encryption over the scarce radio interface, since the mobile/wireless networks (e.g. WLAN, UMTS) employ optimized ciphering for packet data transmission over it. This increases the overall communication cost and decreases the access network capacity. Finally, the existing e2e mVPN solutions are not compatible with the legal interception option. Legal interception enables mobile/wireless operators to monitor traversed data lawfully, in order to curb malicious activities such as terrorism [28] [29]. In all the aforementioned e2e mVPN solutions the mobile/wireless network is not involved in the establishment of the mVPN and thus it is not aware of the employed security keys and algorithms. Therefore, the operator

cannot have access to the traversing data within the mobile/wireless network, as required by the authorities.

3. Proposed network-assisted mVPN

This paper proposes a network-assisted mVPN security scheme over UMTS. The proposed scheme differs from the existing mVPN solutions in several ways: (i) it copes with the energy consumption issues at the level of mobile devices; (ii) it improves the network efficiency by optimizing the usage of the scarce radio resources, without compromising the provided level of security; (iii) it is compatible with the legal interception option. In the following, the necessary enhancements for the deployment of the proposed security scheme as well as the establishment and operation of a network-assisted mVPN are presented and analysed.

3.1 Network enhancements

For the deployment of the proposed security scheme, the MS and the RNC must be enhanced with specific security modules. Specifically, the MS must integrate a lightweight security client (SecC), which is used to request VPN services and express the user's preferences. On the other hand, the RNC must incorporate a security server (SecS) that establishes, controls and manages network-assisted mVPNs between itself and remote SGs, on behalf of mobile users (see Fig. 2).

SecS comprises an IPsec implementation modified to provide the network-assisted mVPN scheme and operate in the UMTS environment. It consists of six components including: (i) the security manager, (ii) the IKEv2, (iii) the policy manager, (iv) the security policy database (SPD), (v) the security association database (SADB), and (vi) the IPsec base protocol. The security manager is the central functional component of the SecS that manages the latter's submodules and facilitates the configuration of VPNs. In addition, it maintains the SPD, handles the users' requests and reports on errors. IKEv2 authenticates the peers,

negotiates security services and generates shared keys, dynamically. The policy manager contains the network security policy that specifies the set of users that are allowed to have security services and the type of the offered services. It communicates with the HLR to acquire the users' profile and its 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, etc. 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. SADB maintains the contents of all active SAs used by the SecS for IPsec. An IPsec_SA is a management feature used to enforce a security policy. It contains all the necessary parameters (including protocols, modes, algorithms, etc.) that have been agreed between the security peers. The security manager is responsible for filling out the contents of each entry in the SADB. Finally, the IPsec base protocol performs the authentication and encryption transformations defined in the IPsec SAs. It handles all the network layer functions (i.e., fragmentation, path maximum transfer unit, etc.) and ensures that all the traffic passing through the RNC is secure and authorized providing firewall capabilities.

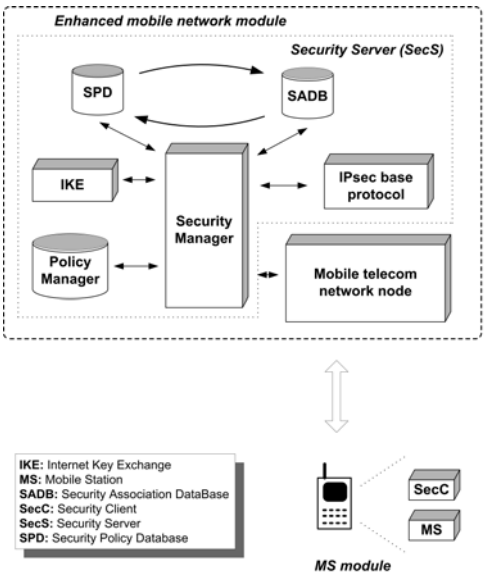

Fig. 2: Security Client (SecC) and Security Server (SecS) modules

3.2 Security management

For the initialization of a network-assisted mVPN and the related key agreement an extension of the IKEv2 [21] is proposed. The extension mainly refers to the incorporation of new messages that are exchanged between the SecC and the SecS, as well as between the SecS and the SGSN. The new messages exchanged between the SecC and the SecS enable the user to initiate, dynamically, a VPN establishment, while outsourcing the negotiation and the generation of keys to the network infrastructure. On the other hand, the new messages exchanged between the SecS and the SGSN carry security related information that is used for VPN mobility, in cases that the mobile user moves and roams.

When the user wants to establish a secure remote connection towards a SG with which it shares a pre-shared key (PSKEY), it uses the SecC to request an IPsec_SA from the corporate SecS. This phase is called request phase. The SecS negotiates the IPsec_SA, on behalf of the SecC, by using the IKEv2 protocol [21]. IKEv2 supports two separate phases (i.e., phase 1 and phase 2). The IKEv2 phase 1 creates two distinct SAs: (a) an IKE_SA that protects the messages of phase 1 and phase 2; and (b) an IPsec_SA that protects the user's data. In addition, the execution of phase 1 consists of two subphases: (i) the IKE_SA_INIT exchange of messages, which negotiates cryptographic algorithms, exchanges nonces, detects the presence of NAT [22], does a Diffie-Hellman exchange and creates the IKE_SA; and (ii) the IKE_AUTH Request - Reply exchange, which authenticates the previous messages, exchanges identities and certificates, negotiates the NAT traversal technique [23] and establishes the IPsec_SA. On the other hand, the IKEv2 phase 2 consists of the Create_Child_SA exchange of messages, which either generates new keying material for the IPsec_SA that was created in the phase 1 or establishes a new IPsec_SA. In the following, the proposed request phase, as well as the IKEv2 phase 1 and phase 2 for the establishment of a network-assisted mVPN are elaborated.

3.2.1 Request phase

To initiate the IPsec_SA negotiation (see Fig. 3), the SecC forwards a VPN-Request message (message 1) to the SecS that includes the IP address of the remote SG (IP_{SG}), the IPsec_SA request (SA_{MS}), the mobile user identity (ID_{MS}) and an authentication value ($AUTH_{MS}$). The latter is produced by applying a hashed Message Authentication Code (MAC) using the pre-shared key (PSKEY) (between the mobile user and the remote SG) over the ID_{MS} and the IP_{SG}. Upon receiving the request, the SecS verifies the user's privileges and the mobile network's capabilities in providing the requested VPN services, by asking the policy manager. Additionally, it looks for an already active IKE_SA between the SecS and the SG on behalf of the specific user. If such an SA exists, then the SecS proceeds to the IKEv2 phase 2. If not, the SecS starts with the IKEv2 phase 1 and the IKE_SA_INIT exchange. It is worth noting that both the MS and the UMTS network have been authenticated each other when the former is connected to the latter (i.e., UMTS authentication). Moreover, the data exchanged between the MS and the RNC of the UMTS network are encrypted and integrity protected using the UMTS ciphering [5].

3.2.2 IKEv2 phase 1

At the beginning of the IKEv2 phase 1 (i.e., IKE_SA_INIT exchange) (message 2 in Fig. 3), the SecS sends to the remote SG the *SAi1* payload, which denotes the set of cryptographic algorithms that it supports for the IKE_SA, the *KEi* payload, which is the Diffie-Hellman value, a *Ni* value that represents the nonce, and the NAT discovery payload (NAT-Di), which detects the presence of NAT between the security endpoints [23]. The SG answers with a message (message 3 in Fig. 3) that contains its choice from the set of cryptographic algorithms for the IKE_SA (*SAr1*), its value to complete the Diffie-Hellman exchange (*KEr*), its nonce (*Nr*), the NAT discovery payload (NAT-Dr), and a list of the Certificate Authorities

(*CAs*), whose public keys it trusts (*CERTREQr*). At this point, both the SecS and the SG can calculate the *SKEYSEED* value as follows:

$$SKEYSEED = prf((Ni \mid Nr), g^{ir}),$$

where *prf* is the pseudorandom function negotiated in the previous messages, | means string concatenation and *g^ir* is the shared secret key that derives from the Diffie-Hellman exchange. The *SKEYSEED* value is used to calculate various secret keys. The most important are: the *SK_d* used for providing the keying material for the IPsec_SA; *SK_ei* and *SK_ai* used for encrypting and providing integrity services, respectively, to the IKEv2 messages from the SecS to the remote SG (IKE_SA); and, finally, *SK_er* and *SK_ar* that provide security services in the opposite direction (IKE_SA).

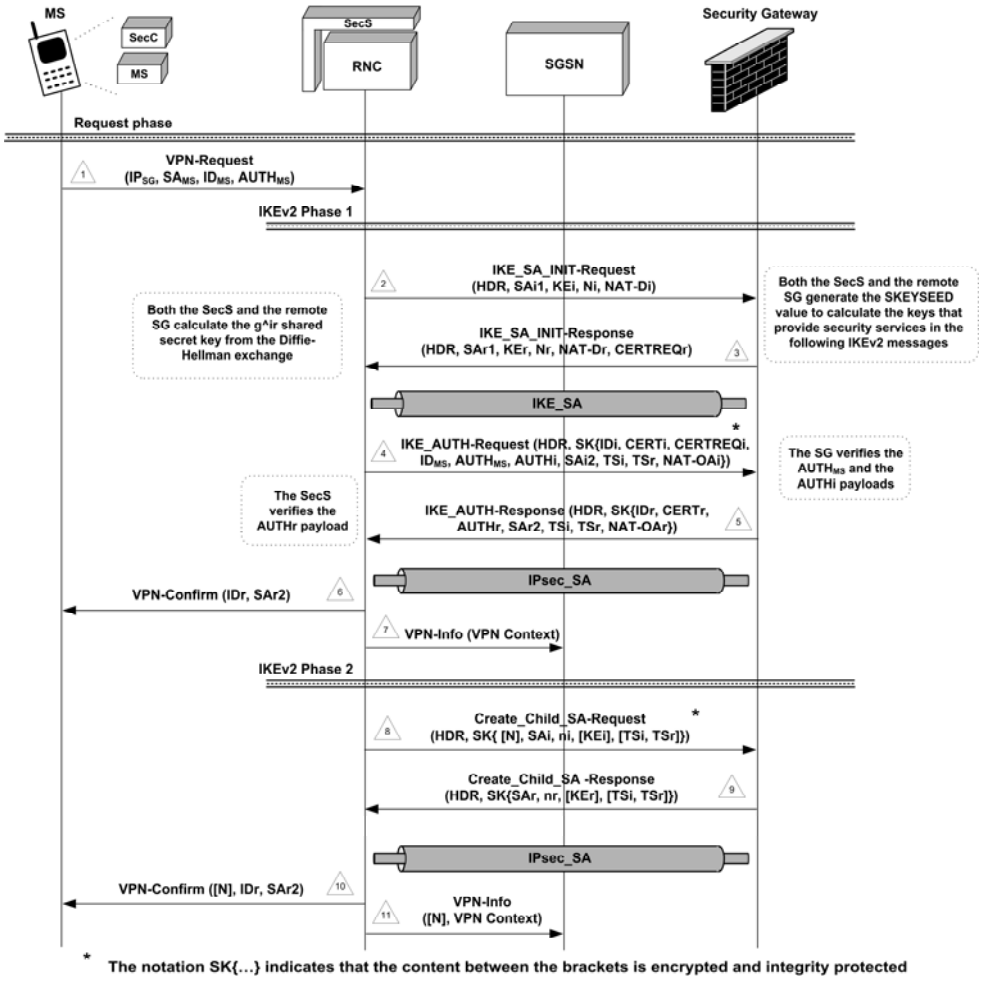

Fig. 3: VPN establishment

After the completion of the IKE_SA_INIT exchange, the IKE_AUTH exchange starts. It is worth noting that from this point all the payloads of the following IKEv2 messages, excluding the message header (*HDR* payload), are encrypted and integrity protected using the IKE_SA, as shown in Fig. 3. The IKE_AUTH exchange of messages starts when the SecS sends to the SG a message (message 4 in Fig. 3) that includes its certificate *CERTi*, the mobile user identity ID_{MS}, the authentication value of the mobile user $AUTH_{MS}$, the *CERTREQi* payload, which is a list of the CAs whose public keys the SecS trusts, the *SAi2* payload, which denotes the set of cryptographic algorithms that the SecS supports for the IPsec_SA, the traffic selectors (i.e., *TSi* and *TSr*), which allow the peers to identify the packet flows that require processing by IPsec, and the NAT Original Address (NAT-OAi), which indicates that the SecS proposes user data protocol (UDP) encapsulation as a NAT-Traversal technique [24]. The SecS also includes in this message the *AUTHi* payload, which is used for authentication purposes and produced by signing the IKE_SA_INIT-Request message (i.e., previous message) using the private key of the SecS.

Upon receiving the previous message, the SG verifies the *AUTHi* and the $AUTH_{MS}$ fields by using the public key of the SecS included in the *CERTi* payload and the pre-shared key *PSKEY*, respectively. If the verifications succeed, the SG forwards to the SecS (message 5) its identity *IDr*, its certificate *CERTr,* the traffic selectors *TSi* and *TSr*, its choice from the supported set of cryptographic algorithms that will be used in the IPsec_SA (*SAr2* payload), the NAT-OAr (if the SG agrees in using the UDP encapsulation as a NAT-Traversal technique) [24], and the *AUTHr* payload. The latter is computed by signing the IKE_SA_INIT-Response message using the SG's private key, similarly to the *AUTHi* payload. After receiving the IKE_AUTH-Response message, the SecS verifies the *AUTHr* field using the public key of the SG (included in the *CERTr* payload). If the verification succeeds, then the IKEv2 phase 1 is completed and consequently a one-way IPsec_SA

between the SecS and the remote SG has been established. At this point, both the security endpoints must generate the keying material for the established IPsec_SA as follows:

$$KEYMAT = prf(SK\_d, Ni \mid Nr)$$

where *Ni* and *Nr* are the nonces from the IKE_SA_INIT exchange and *SK_d* is the key calculated from *SKEYSEED*. The *KEYMAT* is used to extract the keys employed by IPsec for security purposes.

After the generation of keys, the SecS sends two messages (i.e., one to the SecC and one to the SGSN) that are not included in the IKEv2 negotiation. Specifically, the SecS (i.e., RNC) informs the SecC (i.e., MS) that the IPsec_SA has been established by sending to it a VPN-Confirm message, which includes the identity of the remote SG (*IDr*) and the set of algorithms that will be used in the IPsec_SA (*SAr2* payload). In addition, the SecS forwards to the SGSN, which handles the requesting MS, the security and routing parameters that characterize the established IPsec_SA (i.e., VPN-Info message). We define this set of parameters as VPN context. The VPN context includes the SADB and SPD contents for the deployed IPsec_SA [20]. This information is necessary for the SGSN to support mobility of the established IPsec_SA and VPN, in case that the MS moves and roams. It is worth noting that for bidirectional secure communication between the MS and the remote SG, two IPsec_SAs need to be established (one in each direction) [20].

3.2.3 IKEv2 Phase 2

The IKEv2 phase 2 either establishes a new IPsec_SA and the associated keying material or re-keys the existing IPsec_SA, depending on the needs. If the Perfect Forward Secrecy (PFS) feature [21] is enabled, then this phase exchanges new Diffie-Hellman values. Similarly to the IKE_AUTH exchange of messages (i.e., phase 1), all the payloads of the messages of this phase, except for the message header (HDR payload), are encrypted using the *SK_ei* and *SK_er* keys and integrity protected using the *SK_ai* and *SK_ar* keys. It is worth noting that

both the SecS and the remote SG can start the execution of phase 2. However, in the current analysis we consider that the SecS starts this execution for simplicity reasons.

At the beginning of the IKEv2 phase 2 (message 8 in Fig. 3), the SecS sends to the SG the *N* payload (optional), which is included only in case that re-keying takes place and used for identifying the existing IPsec_SA, the set of cryptographic algorithms that the SecS supports for the IPsec_SA (*SAi* payload), a new nonce (*ni* payload), a Diffie-Hellman value (*KEi* payload) (optional, in case that PFS is enabled), and the proposed traffic selectors (*TSi* and *TSr*) (optional, in case that a new IPsec_SA is established). The SG ends this phase by replying (message 9) with the chosen cryptographic suite (from the initial set stated by the SecS) (*SAr* payload), its traffic selectors (*TSi* and *TSr*) (optional, in case that a new IPsec_SA is established), the new nonce (*nr*), and a Diffie-Hellman value (*KEr* payload) (optional, in case that PFS is enabled). Ending this phase, both the SecS and the remote SG generate new keying material (*KEYMAT*). In case that PFS is disabled, KEYMAT is calculated as follows:

$$KEYMAT = prf(SK\_d, ni \mid nr),$$

where *ni* and *nr* are the new nonces exchanged in the phase 2 and *SK_d* is the key calculated from *SKEYSEED* (phase 1). Otherwise, *KEYMAT* is calculated as:

$$KEYMAT = prf(SK\_d, g\text{^}ir(new) \mid ni \mid nr),$$

where *g^ir* is the new shared secret key that derives from the Diffie-Hellman exchange.

After the generation of keys, the SecS sends another two messages (i.e., one to the SecC and one to the SGSN) that are not included in the IKEv2 negotiation. Specifically, the SecS sends to the SecC a VPN-Confirm message indicating the completion of the re-keying procedure or the establishment of a new IPsec_SA. This message contains the *N* payload (optional, only in case that re-keying takes place), which is used for identifying the existing IPsec_SA, the identity of the remote SG (*IDr*), and the set of algorithms that will be used in the IPsec_SA (*SAr2* payload). In addition, the SecS forwards to the SGSN a VPN-Info

message, which contains the VPN context of the established IPsec_SAs used for the VPN mobility management.

3.3 VPN deployment and mobility

When the MS is set on, it searches for a suitable cell in the UTRAN that provides services and tunes to its control channel. Then, it performs a packet International Mobile Subscriber Identity (IMSI) attach that creates valid routing information for the packet switched (PS) connection and a PDP context activation procedure that negotiates the desired connection characteristics between the MS and the network. In addition, the SGSN performs a radio access bearer (RAB) allocation over the UTRAN and establishes a CN bearer between itself and the GGSN. As a result two types of bi-directional tunnels are set up: *(a)* one between the MS and the RNC by employing the Medium Access Control protocol over the WCDMA radio access interface (see Fig. 4), which supports security protection; and *(b)* one tunnel between the RNC and the GGSN by employing the GTP without any security precaution. The second tunnel consists of two parts: the Iu bearer over the Iu interface and the PS domain backbone bearer between the SGSN and GGSN (see Fig. 4).

After the related user's request and the establishment of a network-assisted mVPN between the SecS and a remote corporate SG (see section 3.3), the MS may communicate with the latter, securely. The data packets protected by the UMTS ciphering are tunneled and forwarded to the serving RNC using the established RAB. In this part of the network, the identification of the MS flows is achieved by using a temporary identity, which can be either the cell radio network temporary identities (C-RNTI) or the UTRAN radio network temporary identity (U-RNTI). In addition, the network service access point identifier (NSAPI) identifies uniquely the RAB of the specific MS in the service network and binds data streams from the access stratum and the non-access stratum [4]. Due to the presence of the SecS (see Fig. 4), 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 execution of IPsec in the RNC and the deployment of the proposed network-assisted mVPN, the default set of IPsec selectors [20] that facilitate the interaction with the SPD should be enhanced. The enhanced set includes the UMTS routing parameters such as the NSAPI, the IP address of the involved SGSN and the tunnel endpoint identifier (TEID) (identifies the employed GTP tunnel), which facilitate the mapping of a data flow originated from a specific MS to the appropriated network-assisted mVPN.

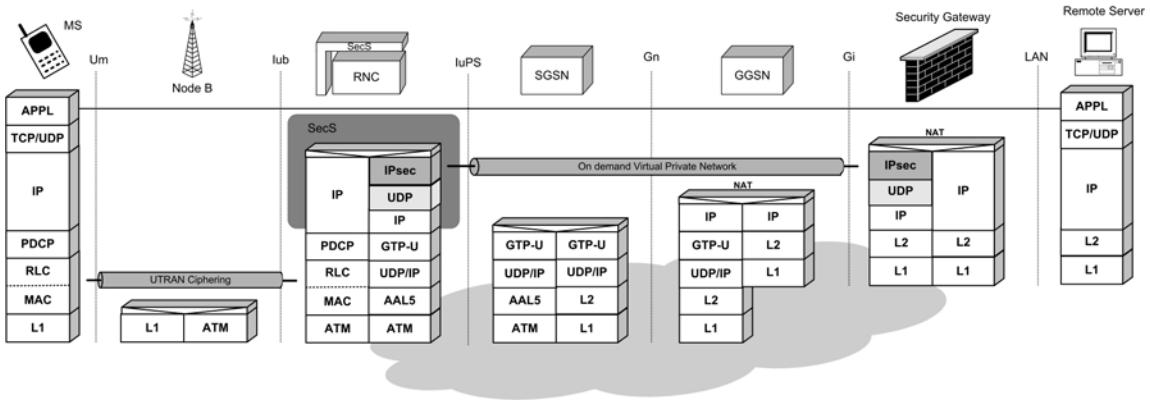

Fig. 4: Protocol stack for network-wide VPN scenario

The proposed network-assisted mVPN can seamlessly operate and continuously provide security services while the mobile user moves and roams. VPN mobility is achieved by making a binding between the UMTS mobility management and the VPN deployment. This requires some changes to the procedures of the UMTS mobility management, which must incorporate and carry the VPN context. As a VPN context we define the set of parameters that characterize the established IPsec SAs (incoming and outgoing) of the specific user over the UMTS network, such as the SPD entries and the SADB entries.

In case that the user moves to an adjacent cell, which is served by the same RNC, it performs a cell update procedure to inform the RNC about the new cell. This procedure may reallocate the C-RNTI when the MS accesses the new cell, but since none of the UMTS routing parameters that are also involved in the operation of the proposed scheme (i.e.,

NSAPI and TEID) is changed, the network-assisted mVPN between the RNC and the SG remains the same. In case that the MS enters a new service area, which is controlled by a different RNC, it has to perform an update procedure depending on the change of SGSN or not. If the new service area is controlled by the same SGSN, the procedure is referred to as intra-SGSN routing area update, which corresponds to the relocation of the Iu interface. Otherwise, if the new service area is controlled by a different SGSN, then the procedure is referred to as inter-SGSN routing area update [4][25].

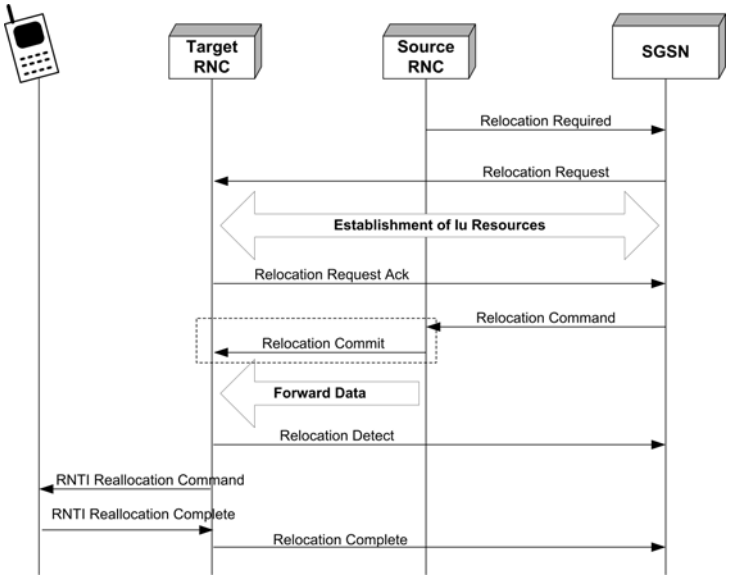

Fig. 5: Enhanced Intra-SGSN relocation

Fig. 5 illustrates the message sequence diagram of the slightly modified intra-SGSN relocation procedure that preserves the established network-assisted mVPNs of the moving MS. The relocation begins when the source RNC sends a *Relocation Required* message to the SGSN. The latter receives this and tries to allocate the appropriate Iu resources towards the target RNC. For this reason, the SGSN sends a *Relocation Request* message to the target RNC, which contains the information required to build the same RAB configuration as the one that exists for the MS before the relocation. 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 a *Relocation Command* to the source RNC. The source RNC requests from the target RNC to proceed with the relocation by sending a *Relocation Commit* message. The purpose of this message is to transfer the servicing 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 that are to be transmitted in the uplink and downlink directions. The *Relocation Commit* message (i.e., message in a dashed box in Fig. 5) should be enhanced to incorporate also the VPN context of the moving user. This facilitates the target RNC to construct a copy of the security relationships that exist between the source RNC and remote SGs ensuring mobility. It is important to note that before sending the *Relocation Commit message*, both the uplink and downlink data transfer at the source RNC are suspended. After having sent this message, the source RNC begins the forwarding of data for each related RAB to the target RNC and the relocation procedure proceeds normally by exchanging the last messages (i.e., *Relocation Detect, RNTI Reallocation* and *Relocation Complete*).

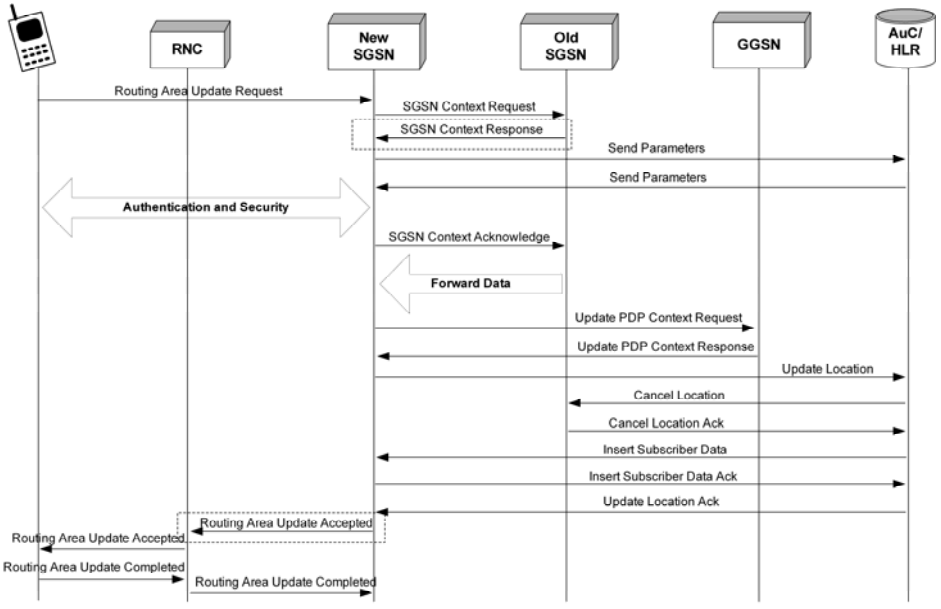

Fig. 6: Enhanced Inter-SGSN routing area update procedure

In case of inter-SGSN routing area update (see Fig. 6), the MS first sends a *Routing Area Update Request* message to the new SGSN that contains the old and the new routing area identifiers. Based on this information, the new SGSN determines the old SGSN and requests for 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 (i.e., message in a dashed box in Fig. 6), which includes the active PDP context, the mobility management (MM) context and the VPN context. The latter contains all the security and routing parameters that characterize the established IPsec_SAs for the moving user. The new SGSN acknowledges the contexts' transfer (*SGSN Context Acknowledge*), stores them and sends an enhanced *Routing Area Update Accepted* message (i.e., message in a dashed box in Fig. 6) to the target RNC, which also contains the VPN context of the moving user. The RNC stores the VPN context values and verifies its availability in providing VPN services. Then, updates its SPD and SADB with the relative IPsec_SAs contents and sends a *Routing Area Update Accepted* message to the MS. The latter generates and forwards a *Routing Area Update Complete message,* which ends the update procedure.

4. Evaluation and performance analysis

The proposed network-assisted mVPN security scheme is beneficial for both mobile users and network operators as mentioned below and further analyzed in sections 4.1 & 4.2. First it conserves energy at the level of mobile devices as the latter are not involved in the execution of complex authentication, key negotiation (i.e., IKEv2) and mobility management protocols (i.e., MIP, SIP) for maintaining the established mVPN, and they do not perform duplicated security transformation (i.e., UMTS ciphering & IPsec) [30]. Moreover, the proposed scheme does not degrade the efficiency of the network over the scarce radio interface since it avoids the execution of resource consuming protocols (i.e., IKEv2) over the access network and the

protected data transferred over the radio interface are not encrypted twice (i.e., UMTS ciphering & IPsec). Finally, the proposed solution is compatible with the legal interception option because the mobile network infrastructure undertakes the responsibility to generate and store the security keys of the deployed mVPN. Thus, if it is required by the authorities, the 3G mobile operator can monitor the traversed data of malicious users for legal purposes.

To evaluate the proposed security scheme, we assess and estimate the related communication cost. This cost can be divided into the VPN deployment cost, which is related to the peers' authentication and the VPN establishment and occurs once for each deployed VPN, and the operation cost, which is related to the protection of the transmitted data. Finally, we compare the performance the proposed network-assisted mVPN to that of the e2e mVPN over UMTS [8]. The e2e mVPN over UMTS is the lighter version of the existing mVPNs schemes described in section 2.2, since it does not employ any additional mobility management procedure for maintaining the established mVPN.

4.1 Deployment cost

The VPN deployment cost can be reasonably well estimated by taking into consideration the basic and most resource consuming communication and security functions. These functions concern: (i) the message transmission and reception, (ii) the calculation of an authentication value using no keys or a pre-shared key for providing or verifying a MAC, (iii) the calculation of an authentication value using PKI for providing or verifying MAC, (iv) the calculation of keys, and (v) the encryption or decryption of a message. The notation of the cost of these functions is presented in Table 1.

Symbol	Description
C_{MAC}	The cost of providing or verifying a MAC using no keys or a pre-shared key
$C_{MAC\text{-}PKI}$	The cost of providing or verifying a MAC using PKI
C_{M}	The cost of transmitting or receiving a message
C_{KEY}	The cost of keys calculation
C_{ENC}	The cost of message encryption or decryption

Table 1: VPN deployment cost parameters

The cumulative VPN deployment cost consists of the sum of the partial costs of the involved entities (i.e., SecC, SecS, SG and SGSN) in the proposed security scheme. The SecC, which is integrated in the MS, sends one message (i.e., VPN-Request), receives two messages (i.e., VPN-Confirm) and produces one authentication value using a pre-shared key (i.e., $AUTH_{MS}$). Therefore, the partial VPN deployment cost of the SecC for the proposed network-assisted mVPN is computed as:

$$C_{SecC\text{-}mVPN} = 3 \times C_{M} + C_{MAC} \quad (1)$$

The SecS, which is integrated in the RNC, is involved in the transmission and reception of 11 messages, the calculation of a MAC (i.e., NAT-Di) and the verification of another (i.e., NAT-Dr) without using any key, the calculation of a MAC (i.e., AUTHi) and the verification of another (i.e., AUTHr) using PKI, the generation of three groups of secret keys, and the exchange of four encrypted message, which require encryption – decryption. Thus, the partial VPN deployment cost of the SecS for the network-assisted mVPN is:

$$C_{SecS\text{-}mVPN} = 11 \times C_{M} + 2 \times C_{MAC} + 2 \times C_{MAC\text{-}PKI} + 3 \times C_{KEY} + 4 \times C_{ENC} \quad (2)$$

Similarly, we calculate the partial costs of the SG and the SGSN:

$$C_{SG\text{-}mVPN} = 6 \times C_{M} + 3 \times C_{MAC} + 2 \times C_{MAC\text{-}PKI} + 3 \times C_{KEY} + 4 \times C_{ENC} \quad (3)$$

$$C_{SGSN\text{-}mVPN} = 2 \times C_{M} \quad (4)$$

Therefore, the cumulative VPN deployment cost for the proposed security scheme is:

$$C_{CUM\text{-}mVPN} = 22 \times C_{M} + 6 \times C_{MAC} + 4 \times C_{MAC\text{-}PKI} + 6 \times C_{KEY} + 8 \times C_{ENC} \quad (5)$$

On the other hand, the e2e VPN scheme involves only the MS and the remote SG that execute the standard IKEv2 [21]. Therefore, the partial VPN deployment costs for this scheme are related to these nodes and calculated as:

$$C_{MS\text{-}e2eVPN} = 6 \times C_M + 2 \times C_{MAC} + 2 \times C_{MAC\text{-}PKI} + 3 \times C_{KEY} + 4 \times C_{ENC} \quad (6)$$

$$C_{SG\text{-}e2eVPN} = 6 \times C_M + 2 \times C_{MAC} + 2 \times C_{MAC\text{-}PKI} + 3 \times C_{KEY} + 4 \times C_{ENC} \quad (7),$$

The cumulative VPN deployment cost for the e2e VPN scheme is:

$$C_{CUM\text{-}e2eVPN} = 12 \times C_M + 4 \times C_{MAC} + 4 \times C_{MAC\text{-}PKI} + 6 \times C_{KEY} + 8 \times C_{ENC} \quad (8)$$

From eq. (5) and (8), it can be perceived that the proposed network-assisted scheme increases the cumulative VPN deployment cost, compared to the e2e scheme. This is because the proposed security scheme involves four networks entities (i.e., SecC, SecS, SGSN, SG), in contrast to the e2e scheme that involves only two (i.e., MS and SG). This fact necessitates the exchange of 5 more messages among the involved nodes in the proposed security scheme and the employment of an extra authentication value (i.e., $AUTH_{MS}$), which facilitates the authentication of the mobile user to the remote SG. These two factors increase the cumulative VPN deployment cost of the proposed security scheme compared to the e2e scheme that employs the standard IKEv2 for VPN deployment.

On the other hand, one of the basic advantages of the proposed scheme compared to the e2e is that it limits considerably the partial VPN deployment cost of the involved MS (see eq (1) and (6)). By employing the SecC module, the mobile users can initiate dynamically a network-assisted mVPN between itself and a corporate LAN's SG, while outsourcing authentication, key negotiation and encryption/decryption functionality to the mobile network infrastructure. This minimizes the configuration and computation overheads associated with the mobile user and its device, and reduces the relevant cost. Considering also the constraints imposed by the nature of mobile devices (i.e., low processing power and memory

capabilities), it can be argued that the mobile user can benefit significantly from outsourcing the management and operation of his VPNs to the network operator.

From eq. (1) and (6) which refer to the partial VPN deployment cost of the involved MS for the proposed mVPN and the legacy e2e VPN scheme respectively, we can deduce that the proposed scheme conserves energy at the level of MS and does not considerably affects the network efficiency over the scarce radio interface. More specifically, for the deployment of the mVPN (see eq. (1)), the MS is involved only in the generation of a MAC value using a pre-shared key. On the other hand, in the e2e VPN (see eq. (6)) the MS is involved in the calculation of a MAC value (i.e., NAT-Di) and the verification of another (i.e., NAT-Dr) without using any key, the calculation of a MAC (i.e., AUTHi) and the verification of another (i.e., AUTHr) using PKI, the generation of three groups of secret keys, and the encryption/decryption of four messages. Therefore, it is evident that the proposed solution copes with energy consumption issues at the level of mobile devices. In addition, it requires the exchange of three messages over the scarce radio access network, while the legacy e2e VPN requires the exchange of six messages. Thus, the proposed solution improves the network efficiency by optimizing the usage of radio resources.

4.2 Operation cost

The operation cost of the proposed security scheme is mainly related to the processing and space overheads of the security protocols and algorithms employed to provide security services. More specifically, the processing overhead considers the computational complexity of the applied security algorithms that transform users' data in the framework of IPsec, while the space overhead considers the increase of the final size of the protected data packets transmitted. To analyze the operation cost of the proposed network-assisted mVPN scheme, we use the quantification of the processing and space overheads of IPsec presented in [26]. A

simulation model has been developed to evaluate this cost and compare the performance of the proposed security scheme to that of the e2e scheme as well as to that of a scheme that does not include any additional security mechanism.

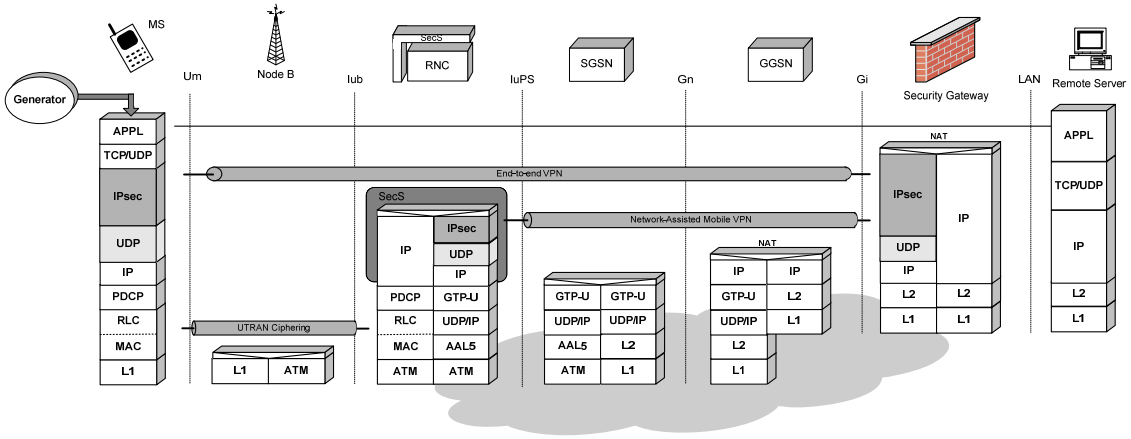

Fig. 7: Block diagram of the simulation model

Fig. 7 depicts a block diagram of the simulation model used in this study. The model consists of the following components: (i) a traffic generator for the creation of non-real time traffic at the application layer according to the parameters defined bellow; (ii) a MS that includes the protocol stack of the UMTS radio access network, transmits the generated traffic over the latter, and applies IPsec in case that the e2e VPN scheme is simulated; (iii) a Node B that connects the MS with an RNC; (iv) the RNC, which terminates the protocol stack of the radio access network, includes a SecS that applies security transformations to the transmitted data packets in cases that the network-assisted mVPN is simulated, and relays the protected data packets to the UMTS backbone network; (v) an SGSN that is a central component of the UMTS backbone network; (vi) a GGSN that connects the UMTS backbone to the public Internet; (vii) an SG, which terminates the deployed VPN (i.e., e2e or network-assisted) and connects a remote corporate private network to the public Internet; and finally, (viii) a remote server, which represents the destination of the data flow and provides the statistics.

The traffic generator represents a user, which generates packet sessions (i.e., non-real time traffic) and each session involves bursty sequences of packets. The mean user data rate

(i.e., denoted by λ_{data}) ranges from 128 Kbit/s to 1.2 Mbit/s and packet inter-arrival times between subsequent user packets in a session are exponentially distributed. The sizes of user packets are modeled by an i.i.d. random variable S_d that follows the truncated Pareto distribution $f_{Sd}(x)$:

$$f_{S_d}(x) = \begin{cases} \dfrac{ak^a}{x^{a+1}}, k \le x < m \\ \left(\dfrac{k}{m}\right)^a, x = m \end{cases} \qquad (9)$$

The parameters m and k define the maximum and the minimum user data packets, respectively (i.e., the default values are m=66666 bytes and k=81.5 bytes). The parameter α defines the skewness of the distribution (i.e., the default value is a=1.1). The average packet size is μ_n=480 bytes and the radio channel capacity is 2 Mbps (total rate including all the management and control information). The packet error rate (PER), which specifies the percentage of retransmissions at the link layer, is 2%. It is important to note that the aforementioned values are taken from the reference 3G traffic model defined by the 3GPP in [27]. Finally, the processing speed of the MS (i.e., denoted by C_p) ranges from 50 - 200 Millions of Instructions Per Second (MIPS) [26].

Simulation parameters	
Mean data rate λ_{data}	128 Kbit/s – 1.2 Mbps
Packet inter-arrival times	Exponentially distributed
The sizes of user packets	Truncated Pareto distribution
Average size of datagram μ_n	480 bytes
Radio channel capacity	2 Mbps
Packet error rate (PER)	2%
MS processing speed C_p	50 – 200 MIPS

Table 2: Simulation parameters setting

The simulation study considers nine (9) different scenarios. The first scenario, also called as no-security scenario, does not apply any additional security mechanism on the user's data and thus, it conveys them in clear-text over the UMTS backbone network and the

public Internet. From the remaining scenarios, four of them study the e2e VPN deployment scheme and the other four the proposed network-assisted mVPN scheme. Each security scenario employs the Advanced Encryption Standard (AES) algorithm with a different configuration for providing confidentiality services, (i.e., AES with 128 bit key, AES with 192 bit key and AES with 256 bit key) and combined confidentiality and integrity services (i.e., AES with 256 bit key plus the Message Digest (MD5) algorithm). IPsec is configured to operate in transport mode. The evaluation of the different scenarios is based on the system's throughput and the packet's latency. The parameters that are varied in the simulations include: the offered traffic load and the processing capabilities of the MS.

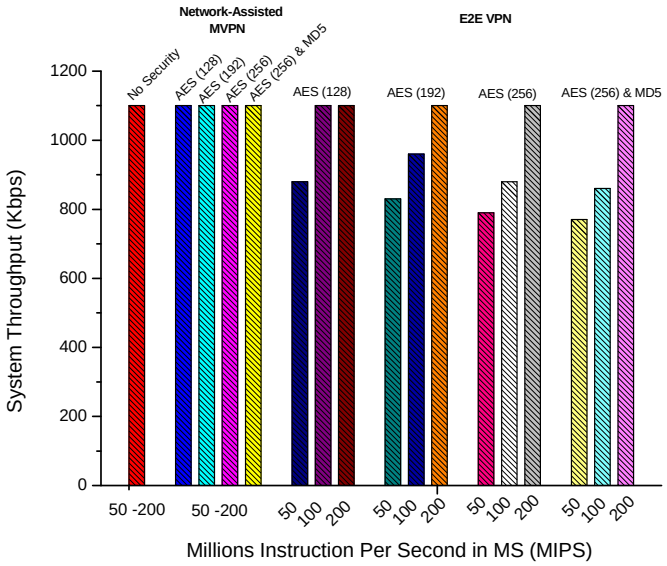

Fig. 8: System's throughput as a function of the processing speed of the MS for the three different security schemes (no-security, network-assisted mVPN and e2e VPN)

Fig. 8 depicts the system's throughput as a function of the processing speed of the MS. One may observe that the four security scenarios that implement the proposed network-assisted mVPN scheme (i.e., AES(128), AES(192), AES(256) and AES(256) & MD5) present the same throughput with the one that implements the no-security scenario. On the other hand, the e2e VPN scheme decreases noticeably the system throughput, especially in

cases that the MS is equipped with a processor that has limited processing capabilities (i.e., less than 200 MIPS). This means that the proposed network-assisted mVPN does not considerably affects the efficiency of the UMTS network and more precisely the efficiency of the radio access network that offers limited bandwidth resource. This occurs because in the proposed scheme the deployed mVPN is not extended over the UMTS radio access network. Thus, the proposed solution does not duplicate encryption (i.e., UMTS ciphering & IPsec) over the radio interface optimizing the usage of scarce radio resources. In addition, the proposed scheme does not involve the MS, which is characterized by limited processing capabilities, in any extra security transformation processing (i.e., IPsec) except for the standard UMTS ciphering. On the contrary, it utilizes the UMTS ciphering for data protection over the UMTS radio access network and delegates to the UMTS network infrastructure (i.e., RNC), which has more resources compared to the MS, the deployment of a mVPN for a specific mobile user. Therefore, the proposed scheme conserves the limited processing capabilities of the MSs and the available energy, addressing performance and energy consumption issues.

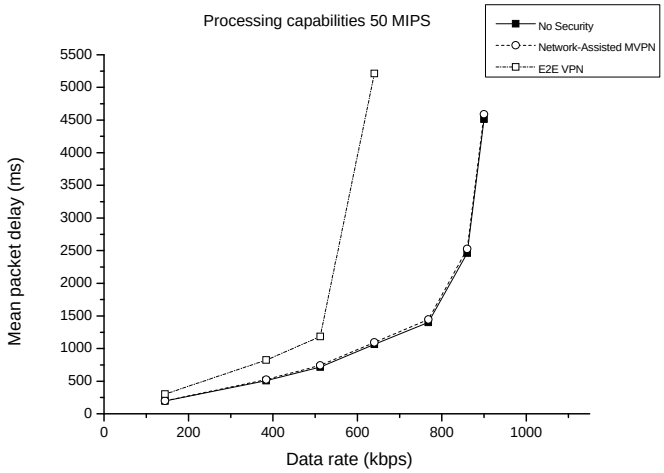

Fig. 9: Mean total delay as a function of mean data rate for 50 MIPS processing rate at the MS and the different security schemes

Except for the impact on the system's throughput, the application of VPN-based security services may increase the total delay of the transmitted user's packets. Fig. 9 presents the total delay as a function of the user's data rate for the deployed security schemes and an MS processing rate of 50 MIPS. The different security algorithms (i.e., AES(128), AES(192), AES(256) and AES(256) & MD5) that are employed to protect the user's data in the two security schemes (i.e., network-assisted and e2e) do not considerably differentiate the observed delay values. Therefore, the depicted delay values represent the mean packet delay from the simulation of the entire set of the security algorithms for each security scheme.

The proposed network-assisted security scheme presents mean delay values very close to those of the no-security scheme, meaning that the deployed network-assisted mVPN hardly has an impact on the total delay. From the depicted values we can deduce that the involved user will not realize the deployment of the network-assisted mVPN, even if he holds a MS that has limited processing capabilities (i.e., 50 MIPS). On the other hand, the e2e VPN scheme increases considerably the mean packet delay values, if the MS processing rate is about 50 MIPS. Moreover, this security scheme under sufficiently high user data rates lead to excessive delay values, which point to the fact that the user data rate has exceeded the maximum capacity of the MS.

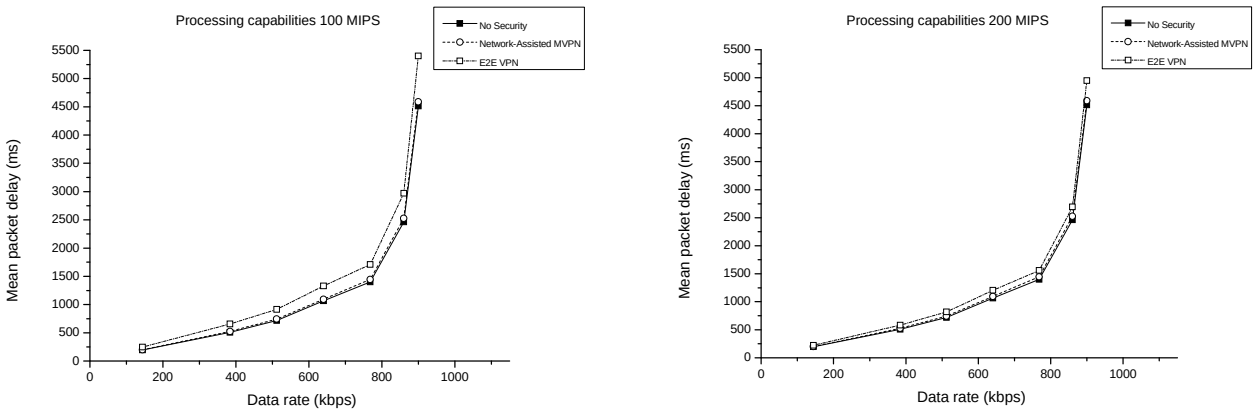

Fig. 10: Mean total delay as a function of mean data rate for (a) 100 MIPS and (b) 200 MIPS processing rate at the MS and the different security schemes

For a greater MS processing rate of 100 MIPS (see Fig. 10 (a)), the mean packet delay values for the no-security and the proposed network-assisted mVPN schemes remain unchanged; since both schemes are mainly independent from the processing speed of the MS. In these two schemes the processing capabilities of the MS do not significantly affect the system's performance, as the MS does not carry out any additional resource consuming security operation for data transfer. On the other hand, the e2e security scheme presents a similar qualitative behavior with the one described in the abovementioned scenario of 50 MIPS processing rate at the level of MS. However, the absolute delay values become smaller, owing to the fact that the transmitted data spent less time within the MS for security (i.e., IPsec) processing. Increasing the MS processing rate further to 200 MIPS (see Fig. 10 (b)) pushes the delay curve of the e2e security scheme closer to those of the network-assisted and the no-security scenarios.

5. Conclusions

This paper has proposed a network-assisted mVPN security scheme for secure remote access to corporate resources over UMTS. The proposed scheme, which is based on IPsec, distributes the required security functionality for deploying a VPN between the involved user's device and the mobile network, limiting the configuration, computation and communication overheads associated with the user and its device. The network-assisted mVPN protects the conveyed user's data by employing the UMTS ciphering over the radio access network and establishing a mVPN over the UMTS backbone network and the public Internet according to the user's needs. It differs from the existing mVPN solutions for the following reasons: (i) it copes with the energy consumption issues at the level of mobile devices; (ii) it improves the network efficiency by optimizing the usage of the scarce radio resources and without compromising the provided level of security; (iii) it is compatible with

the legal interception option. The proposed network-assisted mVPN can operate seamlessly and provide security services continuously while the mobile user moves and roams. VPN mobility is achieved by making a binding between the UMTS mobility management and the VPN deployment. To evaluate the proposed network-assisted mVPN, we have estimated the VPN deployment cost and compared its performance to that of the e2e mVPN over UMTS. In our study, the e2e mVPN scheme is a representative of the existing mVPNs schemes, since each of them establishes a VPN between the communicating peers and involves the MS in the establishment and operation of it. The proposed network-assisted mVPN increases the cumulative VPN deployment cost compared to the e2e scheme, but on the other hand it limits considerably the VPN deployment cost of the involved MS, which is important due to it resource limitation. Moreover, it does not considerably affect the capacity of the UMTS network, as happens with the e2e scheme. Finally, the deployed network-assisted mVPN hardly has an impact on the total delay of the transmitted user's packets.

Acknowledgement

This work has been supported by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission.

References

[1] 3GPP TS 03.6 (v7.9.0), "GPRS Service Description, Stage 2," Sept. 2002.

[2] 3GPP TS 23.002 (v3.6.0) "Network Architecture," release '99, Sept 2002.

[3] 3GPP TS 25.401 (v3.10.0) "UTRAN Overall Description," release '99, Sept. 2002.

[4] 3GPP TS 23.060 (v3.16.0) "GPRS Tunneling Protocol (GTP) across the Gn and Gp interface," release '99, March 2003.

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

[6] C. Xenakis, “Malicious actions against the GPRS technology,” Computer Virology, Springer, Vol. 2, No. 2, Nov. 2006, pp. 121-133.

[7] C. Xenakis, L. Merakos, “Vulnerabilities and Possible Attacks against the GPRS Backbone Network,” In Proc. International Workshop on Critical Information Infrastructures Security, (CRITIS’06), LNCS 4347, Springer, 2006, pp. 262 – 272.

[8] C. Xenakis, L. Merakos, “IPsec-based end-to-end VPN deployment over UMTS,” Computer Communications, Elsevier Science, Vol. 27, No. 17, Nov. 2004, pp. 1693-1708.

[9] S. Vaarala, E. Klovning, “Mobile IPv4 Traversal Across IPsec based VPN Gateways”, IETF Internet Draft, <draft-ietf-mobile-IP4-vpn-problem-solution-02>, Nov. 2005.

[10] A. Dutta et al., “Secure Universal Mobility for Wireless Internet”, ACM International Workshop on Wireless Mobile Applications and Services on WLAN hotspots (WMASH) Philadelphia, USA, Oct 2004.

[11] Jyh-Cheng Chen, Yi-Wen Liu, Li-Wei Lin, “Mobile virtual private networks with dynamic MOBILE IP home agent assignment,” Wiley Wireless Communications & Mobile Computing Vol. 6, No. 5 pp: 601 - 616, Aug. 2006.

[12] M. Kulkarni, A. Patel, K. Leung, “Mobile IPv4 Dynamic Home Agent Assignment,” RFC 4433, Mar. 2006.

[13] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, P. McCann, “Diameter Mobile IPv4 Application,” IETF RFC 4004, August 2005.

[14] Shun-Chao Huang, Zong-Hua Liu, Jyh-Cheng Chen, “SIP Based Mobile VPN for Real-Time Applications,” IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, USA, Mar. 2005.

[15] T.Kivinen, H, Tschofenig, “Design of the Mobike Protocol,” RFC 4621, Aug.2006.

[16] P.Eronen, “IKEv2 Mobility and Multihoming Protocol (MOBIKE),” RFC 4555, Jun 2006.

[17] V. Devarapalli, P. Eronen, “Secure Connectivity and Mobility using Mobile IPv4 and MOBIKE,” draft-ietf-mobile IP4-mobike-connectivity-02, Jan. 2007.

[18] C. Xenakis, L. Merakos, “Alternative Schemes for Dynamic Secure VPN Deployment over UMTS,” Wireless Personal Communications, Springer, Vol. 36, No. 2, Jan. 2006, pp. 163-194.

[19] 3GPP TR 33.908 (v3.0.0) “3G Security; General report on the Design, Specification and Evaluation of 3GPP Standards Confidentiality and Integrity Algorithms,” release ’99, March 2000.

[20] S. Kent, “Security Architecture for Internet Protocol,” RFC 4301, Dec 2005.

[21] C. Kaufman, “The Internet Key Exchange (IKEv2) Protocol,” RFC 4306, Dec 2005.

[22] B. Aboda, W. Dixon, “IPsec-Network Address Translation (NAT) Compatibility Requirements,” RFC 3715, March 2004.

[23] T. Kivinen et al., “Negotiation of NAT-Traversal in the IKE,” RFC 3947, Jan. 2005.

[24] A. Huttunen et al., “UDP Encapsulation of IPsec ESP Packets,” RFC 3948, Jan. 2005.

[25] 3GPP TS 24.008 (v3.15.0) “Mobile Radio Interface Layer 3 specification; Core Network Protocols – Stage 3”, release ’99, March 2003.

[26] C. Xenakis, N. Laoutaris, L. Merakos, I. Stavrakakis, “A Generic Characterization of the Overheads Imposed by IPsec and Associated Cryptographic Algorithms,” Computer Networks, Elsevier Science, Vol. 50, No. 17, Dec 2006, pp. 3225-3241.

[27] ETSI, Universal Mobile Telecommunication System (UMTS);Selection Procedures for the Choice of Radio Transmission Technologies of the UMTS, Technical Report TR 101 112 v3.2.0,1998.

[28] 3GPP TS 33.107 (v8.3.0) “3G security; Lawful interception architecture and functions”, release 8, March. 2008.

[29] 3GPP TS 33.106 (v8.1.0) “3G security; Lawful interception requirements”, release 8, March 2008.

[30] N. R. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols”, IEEE Transactions on Mobile Computing“, Vo. 5, No 2, pp:128-143, Feb. 2006.