DYNAMIC NETWORK-BASED SECURE VPN DEPLOYMENT IN GPRS

Christos Xenakis and Lazaros Merakos

Department of Informatics & Telecommunications, University of Athens, 15784 Athens, Greece
{xenakis,merakos}@di.uoa.gr

Abstract – A dynamic network-based Virtual Private Network (VPN) deployment, which is established between the General Packet Radio Services (GPRS) border gateway and a corporate Intranet gateway, is presented and analyzed. By relying on a sequence of concatenated protection mechanisms (GPRS ciphering and VPN deployment), it is possible to provide secure remote access to mobile users without requiring an extra tunnel overhead on the radio link or the implementation of computationally intense encryption algorithms in the mobile station. The VPN functionality is based on IPsec. For VPN initialization and key agreement procedures an Internet Key Exchange (IKE) protocol proxy scheme is proposed, which enables the mobile user to initiate a VPN, while shifting complex key negotiation to the network infrastructure. The required enhancements for security service provision can be integrated in the existing network infrastructure, and therefore, the proposed security scheme can be used as an add-on feature of the GPRS.

Keywords – Security, VPN, GPRS, IPsec, IKE.

I. INTRODUCTION

Recently, there has been an explosive growth in the popularity and availability of handheld mobile devices that can be wirelessly connected to the Internet. Wireless carriers foresee that one of the main uses of cellular data networks is the remote access to private networks by a mobile workforce. In such an IP-based hybrid environment, where clients are connecting to ever growing networks in an ad-hoc fashion, security is considered paramount.

The most widely deployed public cellular data network, which enables the integration of IP world with mobile networks, is the General Packet Radio Services (GPRS) [1]. Many GPRS providers have recognized the need to offer companies dedicated wireless Virtual Private Network (VPN) [11] access to the corporate Intranets, enabling employees to easily and securely retrieve up-to-date company information remotely. However, these VPNs are established in a static manner between the Gateway GPRS Support Node (GGSN) and the corporate security gateway. Thus, if the static VPN parameters or the VPN topology have to be changed, then the network administrators in both ends must reconfigure it. Furthermore, the aforementioned security scheme can provide VPN service neither to individual mobile users, who may require on demand VPN establishment, nor to enterprise users that may roam internationally. In these cases, the only way to accomplish secure access to a remote server is either to make an expensive phone call, or to establish an end-to-end security scheme [5], which requires from the mobile device to have full security functionality.

However, the mobile devices are designed to be portable with small screen size, limited input capabilities, and limited battery power and energy. The computing power of the processor is typically small, and the operating system's capabilities limited, thus, demanding computations will be slow. In order to conserve energy, processing speeds need to be slower, and processor cycles and data transmissions must be reduced. These constraints impose limits on a potential deployment of full IP security functionality at the mobile device level, due to the computational complexity of the encryption algorithms, and the number of messages exchanged in the involved security protocols [2].

In this paper, a dynamic network-based VPN deployment, which is established between the GGSN and a corporate Local Area Network (LAN) security gateway, is presented and analyzed. Dynamic, client-initiated VPN services are well suited to mobile users who require access to remote networks, "anywhere – anytime". By relying on a sequence of concatenated protection mechanisms (GPRS ciphering and VPN deployment), it is possible to provide secure remote access to mobile users without requiring an extra tunnel overhead on the radio link, or the implementation of computationally intense encryption algorithms in the Mobile Station (MS). The deployed VPN is based on the IPsec [3] security framework, which facilitates transparent security services to any application using the network. For VPN initialization and key agreement procedures an Internet Key Exchange (IKE) [4] protocol proxy scheme is proposed, which enables the mobile user to initiate a VPN, while shifting complex key negotiation to the network infrastructure. Thus, on-demand VPN services are available for all GPRS subscribers and roaming users. The required enhancements for security service provision can be integrated in the existing network infrastructure, and therefore, the proposed security scheme can be used as an add-on feature of the GPRS.

The rest of the paper is organized as follows. Section 2 describes the network architecture, analyses the required network enhancements, proposes an IKE protocol proxy scheme for VPN initialization and key agreement, elaborates on the VPN operation, and presents the mobility implications on the deployed network-based VPN. Section 3 outlines a qualitative evaluation of the proposed VPN scenario, as well as a brief comparison to the conventional end-to-end scheme [5]. Finally, section 4 presents the conclusions.

II. VPN DEPLOYMENT

A. Architecture

Consider a mobile network subscriber with a MS attempting to establish a secure remote connection to a corporate LAN and access a remote server through a GPRS infrastructure, as shown in Fig. 1. The GPRS network is connected to the public Internet through the GGSN. On the other side, the corporate LAN uses the Security Gateway (SG) as a gatekeeper between itself and the Internet. The SG functions as a proxy device providing security services to nodes in the private network it protects.

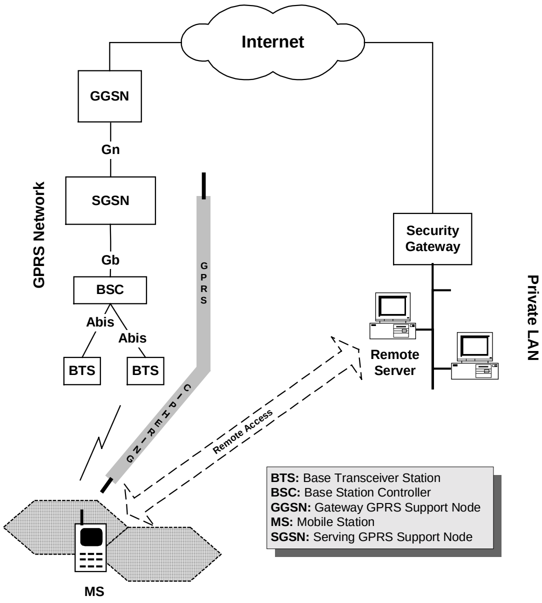

Fig. 1: Network architecture

The standard GPRS network itself does not offer an adequate solution for providing dynamic secure mobile access to a corporate LAN. Despite that the air interface ciphering [1], which extends up to the SGSN, is secure, in the basic scenario, the IP traffic goes unencrypted all the way from the SGSN to the SG. The GPRS backbone network also utilizes firewall and private IP addressing to restrict unauthorized access to it.

Therefore, for secure data exchange between the MS and the remote server, a VPN realization over the public Internet is recommended. For VPN establishment, a client-initiated model, which is well suited to mobile users, is being used. It is assumed that the Internet and the GPRS backbone are based on IPv4. Additionally, both the GGSN and the SG use Network Address Translation (NAT) [6].

B. GPRS network enhancements

The proposed network-based VPN deployment places the IPsec functionality both at the MS and the GGSN, and consequently, requires enhancements of the existing infrastructure, as shown in Fig. 2. The MS must be enhanced with a Security Client (SecC) module, which is used to request VPN services and express the user preferences. Moreover, the GGSN must incorporate a Security Server (SecS) module that establishes, controls, and manages the VPN between the GGSN and the SG at the corporate Intranet on behalf of the mobile user.

SecS comprises an IPsec framework implementation modified to adapt to the client-initiated VPN scheme, and the security service provision in a mobile GPRS environment. The main functional component of the SecS is the Security Manager (SM), which plays the central role in providing VPN service by managing the SecS submodules and facilitating the VPN configuration. The SM 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 Diffie-Hellman [7] exchanges.

The Policy Manager (PM) contains the network security policy that specifies the set of users allowed to have security services, as well as the type of the offered services. It communicates with the Home Location Register (HLR) in order to acquire the users profile. The PM contents are used to configure the Security Policy Database (SPD), and the Security Association Database (SADB).

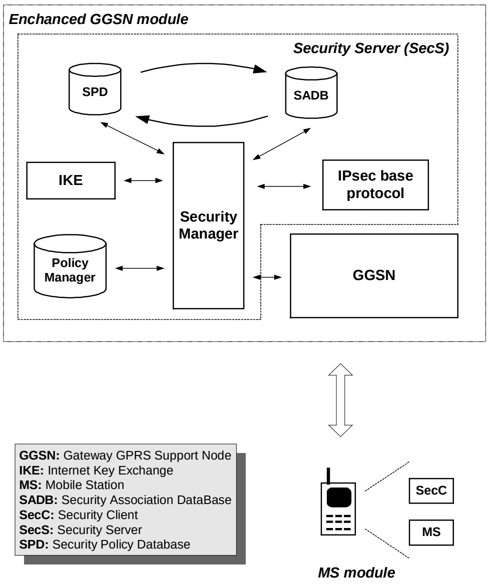

Fig. 2: GPRS enhancements

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]. SM is responsible for filling out the contents of this database, and sharing them with the other SecS submodules.

The SADB maintains the contents of all active Security Associations (SA) [3] 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. SM is responsible for filling out the content 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 GGSN is secure and authorized, providing firewall capabilities.

C. Security management

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) [8] SA negotiation in Aggressive Mode (AM) [4] takes place. 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.

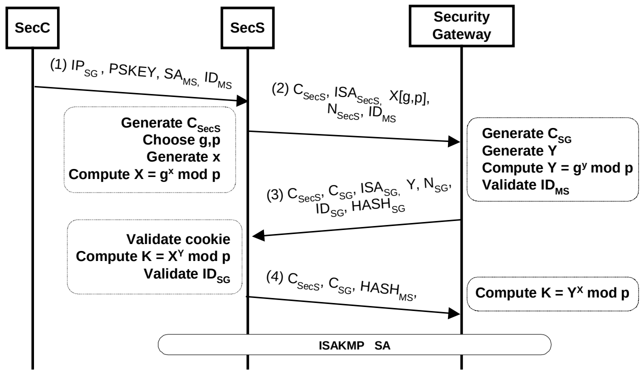
SecC
SecS
Security Gateway
(1) IP_{SG} , PSKEY, $SA_{MS,}$ ID_{MS}
(2) C_{SecS}, $ISA_{SecS,}$ X[g,p], N_{SecS}, ID_{MS}
Generate C_{SecS}
Choose g,p
Generate x
Compute $X = g^x \bmod p$
Generate C_{SG}
Generate Y
Compute $Y = g^y \bmod p$
Validate ID_{MS}
(3) C_{SecS}, C_{SG}, $ISA_{SG,}$ Y, N_{SG}, ID_{SG}, $HASH_{SG}$
Validate cookie
Compute $K = X^Y \bmod p$
Validate ID_{SG}
(4) C_{SecS}, C_{SG}, $HASH_{MS}$,
Compute $K = Y^X \bmod p$
ISAKMP SA

Fig. 3: ISAKMP SA negotiation in aggressive mode

The authentication of endpoints is based on a pre-shared key method, since it is considered the simplest form of authentication, compared to digital signature and public key encryption authentication methods, and fits better in the mobile network-based VPN scenario. The authentication computation is based on the Identification Data (ID) field, which is static, rather than on the IP address, which may vary.

To initiate the IPsec SA negotiation (see Fig. 3) the SecC forwards message (1) destined for the SecS that includes the IP address (IP_{SG}) of the remote SG, the IPsec SA request (SA_{MS}), the pre-shared key (PSKEY) and the Identification data (ID_{MS}) of the mobile subscriber. Upon receiving the request, the SecS verifies the mobile subscriber's privileges and mobile network capabilities in providing VPN services by asking the PM. Additionally, it 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 first generates a cookie (C_{SecS}), the Diffie-Helman (DH) half key and a nonce (N_{SecS}), and then, sends them together with the ISAKMP SA data (ISA_{SecS}) and the identification data (ID_{MS}) to the SG (message 2). The SG replies with message (3), which contains the cookie pair, as well as its ISAKMP SA response, the DH half-key, a nonce, its identity and the $HASH_{SG,}$ which contains SG's authentication information. Finally, the SecS with message (4) transmits the MS's authentication information ($HASH_{MS}$) to the SG together with the cookie pair.

Having established the ISAKMP SA between the SecS and the SG, on behalf of the MS, the communicating parties have agreed on [4]:

- the encryption algorithm,
- the hash algorithm for signing,
- the authentication method for signing,
- the Diffie-Hellman exchange.

Following the successful completion of phase 1, the IKE phase 2 is performed to establish the IPsec SA (see Fig. 4). All packets pertaining to phase 2 are encrypted using the pre-established ISAKMP SA. In message (1), the SecS transmits the cookies (C_{SecS} , C_{SG}), the IPsec SA request (SA_{MS}), its nonce (N_{SecS}), the DH half key and the identities of the MS and SG (ID_{MS} , ID_{SG}) respectively. Additionally, the SecS authenticates the message with HASH(1), which is computed as follows:

$$\mathrm{HASH(1)}=hashfunc(SKEYID_a\ ,\ M_{ID}\ |\ SA_{MS}\ \ |N_{SecS}\ \ |X\ |ID_{MS}\ |ID_{SG}\ )$$

$SKEYID_a$ is a key derived from SKEYID and is used as an authentication key. SKEYID is derived differently for each authentication method. Using the preshared key authentication method the SKEYID is computed as follows:

$\mathrm{SKEYID}=hashfunc(PSKEY,\ N_{SecS}\ |N_{SG})$, where PSKEY is the preshared key.

$$\mathrm{SKEYID_a}=hashfunc(SKEYID,\ SKEYID_d\ |k\ |C_{SecS}\ |C_{SG}\ |1\ )$$

Similarly, $\mathrm{SKEYID_d}=hashfunc(SKEYID,\ k\ \ |C_{SecS}\ \ |C_{SG}\ \ |0)$ where k is the key resulting from the DH exchange. $SKEYID_d$ is used to derive more keying material. Finally,

M_{ID} is the value of the message identifier, which is a generic part of ISAKMP header and is included in all IKE packets.

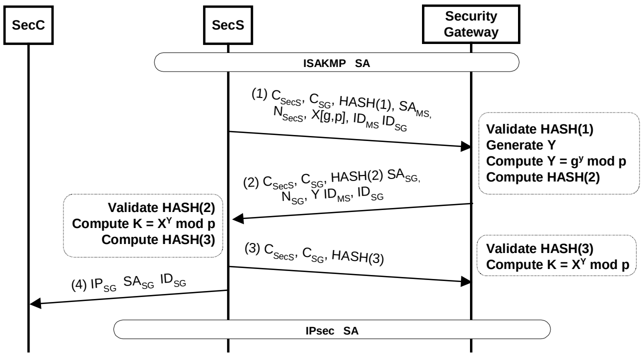
SecC
SecS
Security Gateway
ISAKMP SA
(1) C_{SecS}, C_{SG}, HASH(1), $SA_{MS,}$ N_{SecS}, X[g,p], ID_{MS} ID_{SG}
Validate HASH(1)
Generate Y
Compute Y = g^y mod p
Compute HASH(2)
(2) C_{SecS}, C_{SG}, HASH(2) $SA_{SG,}$ N_{SG}, Y ID_{MS}, ID_{SG}
Validate HASH(2)
Compute K = X^Y mod p
Compute HASH(3)
(3) C_{SecS}, C_{SG}, HASH(3)
Validate HASH(3)
Compute K = X^Y mod p
(4) IP_{SG} SA_{SG} ID_{SG}
IPsec SA

Fig. 4: IPsec SA negotiation

In message (2) the SG transmits the cookies, its IPsec SA response, its nonce, the DH half key, and the (MS & SG) identities. The security gateway also authenticates the message with HASH(2), which is computed as follows:

$\mathrm{HASH(2)}=\mathit{hashfunc}(SKEYID_a\ ,\ M_{ID}\ |SA_{SG}\ |N_{SG}\ |Y\ |\ ID_{MS}\ |ID_{SG}\ )$

In message (3), the SecS replies with the cookie pair and authenticates the transaction with HASH(3), which is computed as follows:

$\mathrm{HASH(3)}=\mathit{hashfunc}(SKEYID_a\ ,\ 0\ |M_{ID}\ |N_{SecS}\ |N_{SG}\ )$

Finalizing this dialog, the SecS with message (4) informs the SecC about the successful completion of the IPsec SA. As an IPsec SA is used only in one direction, for bi-directional communications between the SecS and the SG, two SAs are required.

D. VPN operation

Having established a pair of IPsec SAs between the SecS and the SG, a bi-directional private channel that allows for secure data exchange over the public Internet has been set up (see Fig. 5). The IPsec protocol is configured in tunnel mode, since both security ends (GGSN and SG) in this particular scenario are gateways. Furthermore, the Encapsulation Security Payload (ESP) [9] protocol employment is considered more advantageous in this architecture, given that ESP can provide confidentiality and integrity protection as well.

Every outbound packet is subject to processing by the IPsec base protocol, which determines whether it will apply IPsec protection or not. Furthermore, the IPsec base protocol ensures that the IP datagram is authorized to pass, or is to be rejected, providing firewall services. In order to decide on what service is to be afforded, the IPsec base protocol interacts with the SPD. The outbound processing at the SPD compares the values of the selectors fields against the SPD to find a matching SPD entry. In effect, these selectors are used to filter outgoing traffic in order to map it into a particular SA. Each SA has an entry in the SADB that defines the security parameters associated with it. Note that if an SPD entry does not currently point to an active SA, then the SecS creates one and links this to the SPD entry.

In case that IPsec processing is to be applied, the original IP packets are encrypted and authenticated. Tunnel mode permits encryption and authentication of the upper layer protocols (e.g., TCP segments) including the original IP header.

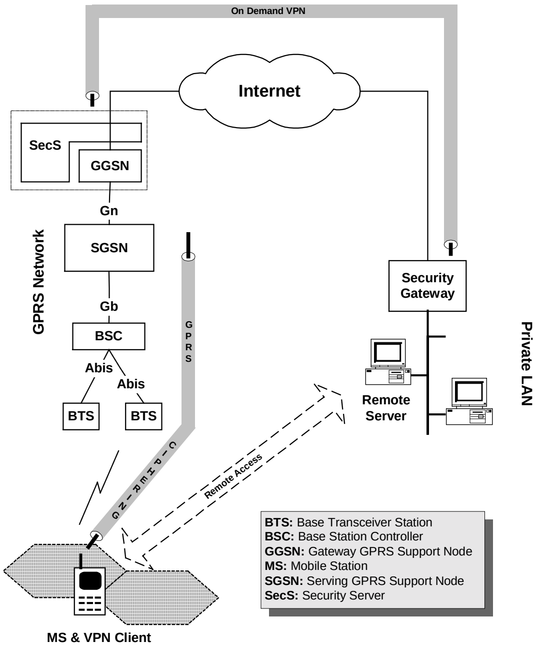

Fig. 5: Dynamic network-based VPN scheme

For inbound traffic, prior to performing any IPsec processing, the IP fragments are reassembled. 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 SADB is performed. If the SA lookup fails, then the packet is dropped, and the error is reported. Otherwise, based on the SA found, the IPsec base protocol does the IPsec processing (decapsulates, authenticates and decrypts the packet). Then, it matches the inner packet's selectors to those 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 the destination.

E. Mobility implication

The MS may freely move within the GPRS coverage area maintaining network connectivity thanks to the mobility management procedures [1]. As long as the MS remains under the same GGSN, its movement has no impact on the deployed network-based VPN. Otherwise, the VPN cannot be used, and another VPN from the new GGSN should be established.

III. VPN SCENARIO EVALUATION

A. Advantages

The main advantage of the proposed security scheme derives from the fact that a mobile subscriber initiates a VPN establishment between the GGSN and a corporate LAN SG, outsourcing complex key negotiation and encryption/decryption functionality to the mobile network infrastructure. Dynamic, client-initiated VPN services are well suited to mobile users who require access to remote networks, “anywhere – anytime”. The end-user decides when and where to establish a VPN across a vulnerable public network protecting sensitive data transfer. Furthermore, the proposed security scheme is compatible with the legal interception option, which requires access to the traversing data within the mobile network.

An additional goal is to minimize the configuration and the computation cost associated with the mobile devices, compared to the conventional end-to-end scheme [5]. More specifically, the use of IPsec imposes computational costs on the hosts that implement these protocols. These costs are associated with the memory needed for IPsec code and data structures, the number of messages that are exchanged for security negotiation, and the computation of integrity check, encryption and decryption, which is added in a per-packet fashion [3]. Considering the constraints imposed by the nature of the mobile devices (low CPU processing power, limited battery power, and limited memory capabilities), with the proposed scheme mobile subscribers can reap significant advantages from outsourcing the operation and the management of their VPNs to the network operator.

Network operators have solid network management expertise, and better resources to effectively create, deploy, and manage VPN services that originate from the mobile subscribers. They can offer security services at a lower cost, by consolidating them over a common infrastructure. This enables the utilization of specific hardware accelerator modules for faster and more efficient IPsec deployment. Furthermore, the network-based implementation can continuously evolve in order to cater for the new emerging end-user requirements, and allows network operators to develop integrated security strategies.

The required network enhancements for the security service provision can be integrated in the existing GGSN, supporting collaboration with existing GPRS network functionality. The network-based VPN operates transparently to the GPRS network management, mobility management and routing functions, and therefore, it can be used as an add-on feature of the GPRS standard. By providing dynamically initiated network-based VPN services, the mobile network operator has the opportunity to attract new subscribers. Reducing the operational and maintenance cost enables faster and more efficient VPN services, and eliminates the specialized technical knowledge required by the end user. The end station simply initiates the VPN establishment, and it is not required by the end-user to have any security skills. Generally, in this scenario, the SA configuration is transparent to the mobile user.

Additionally, GPRS uses specific authentication and ciphering procedures, which are optimized for packet data transmission over radio interface, between the MS and the SGSN. In contrast to the end-to-end scenario, the proposed scheme utilizes the security services provided by the GPRS standard, and avoids applying duplicate encryption (packet encapsulation) over the scarce and expensive radio interface resources. Therefore, the network-based VPN deployment has no impact on the radio access network efficiency.

Finally, compared to the static VPN deployment scheme that is currently supported by GPRS, the proposed scheme provides on-demand VPN services, which are available to the entire set of mobile subscribers. It is also compatible with border gateway firewall, which is responsible for packet filtering, access control, and NAT use. The NAT employment at the GGSN has no impact on the VPN operation, since IPsec is located at the public address space, and, thus, the combination of IPsec with NAT is feasible without any compatibility problem [10].

B. Drawbacks

The biggest consideration in the proposed scheme is that the VPN establishment and operation is not directly under the end-user control. This security scheme, which is already used in wired terrestrial networks, assumes that the corporate mobile subscribers trust the mobile network operator.

In order to effectively provide VPN services, the existing GPRS network infrastructure must be enhanced. Specifically, the MS requires the introduction of the lightweight module (SecC) that initiates the VPN establishment and expresses the end-user preferences. Furthermore, the GGSN requires the SecS incorporation, which is responsible for the VPN establishment and operation. However, the enhancements referring to the GPRS core network require an additional investment from the mobile operator, and their functionality is expected to increase the signaling and the workload burden on the network.

Finally, when a MS moves to a new routing area, which is assigned to a new GGSN, the network-based VPN that has been established by the old GGSN is not operational any more. In this case, the MS has to initiate a new VPN establishment from the new GGSN.

C. Comparison with the conventional end-to-end approach

Based on the analysis presented above, as well as on the analysis presented in [5], we can deduce that both the end-to-end approach and the network-based approach support dynamic client-initiated VPN deployment. However, the end-to-end scheme provides the best security services from the customer's point of view, minimizes the required network enhancement as well as the signaling burden on the network, and does not require the communicating parties to trust the mobile network operator. On the other hand, the network-based approach minimizes the involvement of the mobile user and his mobile terminal in the VPN deployment, has no impact on the scarce radio resources, is compatible with the NAT presence and the legal interception option, and finally, provides more efficient security services at a lower cost. In table 1, the comparison of the two VPN schemes is presented in a tabular form.

Table 1 End-to-end and network-based schemes comparison

	End-to-end scenario	Network-based scenario
Dynamic client-initiated VPN services	√	√
End to end security	√	
Minimize the network enhancements and burden	√	
No third party trust	√	
Legal interception compatibility		√
Minimize the impact on the MS		√
Transparent SA configuration to the end-user		√
Negligible implications on the radio interface		√
NAT compatible		√
Lower VPN cost		√

IV. CONCLUSIONS

In this paper, a dynamic network-based VPN deployment, which is established between the GGSN and a corporate LAN security, has been presented and analyzed. Dynamic, client-initiated VPN services are well suited to mobile users who require access to remote networks, "anywhere – anytime". By relying on a sequence of concatenated protection mechanisms (GPRS ciphering and VPN deployment), it is possible to provide secure remote access to mobile users, without requiring an extra tunnel overhead on the radio link or the implementation of computationally intense encryption algorithms on the MS. The deployed VPN is based on the IPsec security framework, which facilitates transparent security services to any application using the network. For VPN initialization and key agreement procedures, an IKE protocol proxy scheme is proposed, which enables the mobile user to initiate a VPN, while shifting complex key negotiation to the network infrastructure. Thus, on-demand VPN services are available for all GPRS subscribers and roaming users. The required enhancements for security service provision can be integrated in the existing network infrastructure, and therefore, the proposed security scheme can be used as an add-on feature of the GPRS.

REFERENCES

[1] GSM 03.60, GPRS, Service Description, Stage 2, 1998.

[2] Samantha Donovan, Peter Drabwell and Rae Harbird, "VPN and lightweight clients", *Elsevier Science, Information Security Technical Report*, Vol. 6, No. 1, pp. 49-64, March 2000.

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

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

[5] Ch. Xenakis, E. Gazis and L. Merakos "Secure VPN Deployment in GPRS Mobile Network", *European Wireless* 2002, Florence Italy, Feb 2002.

[6] Egevang, K. and Francis, P., "The IP Network Address Translator (NAT)", RFC 1631, May 1994.

[7] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Info. Theor*y, Vol. 22, Nov. 1976.

[8] D. Maughan et al., "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, Nov 1998.

[9] S. Kent and R. Atkinson, "IP Encapsulation Security Payload (ESP)", RFC 2404, Nov. 1998.

[10] L. Phifer, "The Trouble with NAT", *Cisco publications*, *The Internet Protocol Journal*, Vol. 4, Dec. 2000.

[11] B. Gleeson, A. Lin, J. Heinanen, G. Armitage and A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, Feb. 2000.