SPUR: A SECURED PROTOCOL FOR UMTS REGISTRATION

Manel ABDELKADER and Noureddine BOUDRIGA
National Digital Certification Agency
3 bis rue d'Angleterre, Tunis RP 1000,Tunisia

Keywords: UMTS Release5, Registration, Authentication, IMS Security , SIP Security, Security Associations

Abstract: This paper presents a new scheme for mobile identification and registration in UMTS networks. Our approach attempts to alleviate different limitations observed with the current solutions (such as the 3GPP). It guarantees the protection of the data transmitted on the SIP messages during the registration procedure. Our method provides the authentication of the main entities involved in the registration procedure. It develops a mechanism for the management of relating security associations.

1 INTRODUCTION

Recently, the development of the Universal Mobile Telecommunications System (UMTS) architecture has known great evolutions as it can be noticed with the 3GPP specifications (Kaaranen et al., 2001). Since its release 5, the UMTS network has emerged to an all IP network leading to the introduction of new protocols and procedures (TS 23.228, 2003; TS 22.228, 2002). Among the most important subjects that have been discussed for the all IP network, one can find the problem of how to overcome the different threats applicable to the UMTS networks (TS 33.900, 2000; TS 33.120, 2000; TS 21.133, 2001).

The registration procedure of a mobile to a service provided by a UMTS network represents one of the critical phases that should be protected. During this phase, there is no fixed definition of the mechanism that allows to protect the integrity, confidentiality and authentication of the Signaling Initiation Protocol (SIP) messages involved with the Internet Multimedia Subsystem Authentication and Key Agreement (IMS AKA) process (TS 33.203, 2002; TS 24.229, 2002; Rosenberg et al., 2003).

Different proposals have been presented to provide registration ((S3-000689, 2000) and (S3z000010, 2000)). Authors of (S3-000689, 2000) have proposed that the Proxy Call Session Control Function (PCSCF) performs the IMS AKA with the Mobile Station (MS) and terminates integrity and confidentiality protection of the SIP messages transmitted by MS. However, the protection of the remaining segments of the communication toward the Serving CSCF (SCSCF) is based on the network domain features using Internet Protocol Security (IPsec). Therefore, the SCSCF may not be able to authenticate users at the service level. Authors of (S3z000010, 2000), on the other hand, have proposed that authentication and re-authentication procedures should be made by the Home Subscriber Server (HSS) using AKA process. The integrity and the confidentiality keys are then transmitted to the SCSCF and the PCSCF to insure the protection of the SIP messages. The main drawback of this approach is the important load added to the HSS. The 3GPP scheme allows to overcome some drawbacks of the previous two proposals by moving the authentication process to the SCSCF.

The IMS AKA (TS 33.203, 2002) presents itself other lacks of security, which include for example the following facts: (1) it transmits (in clear) the mobile private data; (2) it does not provide the authentication of the serving network to the user; and (3) it allows the SCSCF to attribute the user private keys to the PCSCF, which reduces the user's level of security. Limitations can be at the origin of different attacks such as masquerading and man in the middle.

In this paper, we propose a secured registration procedure, called *SPUR scheme*, in all IP UMTS networks that overcomes the previous mentioned limitations. We will mainly focus on the registration of a mobile to a service and provide protection schemes of the data transmitted on the SIP messages. Our method

Abdelkader M. and Boudriga N. (2004).
SPUR: A SECURED PROTOCOL FOR UMTS REGISTRATION.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 8-16
DOI: 10.5220/0001386800080016

is independent from the security mechanisms adopted in the lower layers. We also develop in this paper a proposition for a secured management of the security associations that we define for need of protecting the communication between the mobile and the IMS.

The remaining part of this paper is organized as follows: Section 2 develops the SPUR scheme and describes all its steps. It also presents a procedure for re-registration. Section 3 adapts the concept of security association to protect the security elements needed for the execution of SPUR. A secured model for security associations management is also defined. Section 4 analyzes SPUR's features and compares it to 3GPP. Section 5 develops a SPUR simulation, where the effects of message size on the error probability and the additional flow between nodes are estimated. Section 6 gives the conclusion of this paper.

2 THE SECURED PROTOCOL FOR UMTS REGISTRATION

The secured protocol for UMTS registration (SPUR) is designed to increase the security level of the registration process in the UMTS networks. It adds different security measures to the registration protocol as adopted by the 3GPP. It includes two procedures: the initial registration and the re-registration procedures. The following subsections develop these procedures.

2.1 Terms and notations

Nodes of the IMS subsystem contribute to the accomplishment of SPUR. However, for sake of simplification, the most important entities involved with SPUR are the following:

- The PCSCF: The Proxy Call Session Control Function behaves like a proxy. It accepts the MS requests, serves them internally or transfers them. In the case of registration, the PCSCF transfers the SIP REGISTER request of a user to an I-CSCF according to the home network domain name of the MS(TS 24.229, 2002).
- The ICSCF: The Interrogating Call Session Control Function is the contact point within an operator's network for all connections related to subscribers of this network. In the case of registration, upon the receipt of SIP REGISTER request, the ICSCF gets the address of the SCSCF from the HSS(TS 24.229, 2002).
- The SCSCF: The Serving Call Session Control Function acts as a SIP registrar. It provides services to the MS and controls the sessions of the users(TS 24.229, 2002).
- The HSS: The Home Subscriber Server is the master database for users containing their subscription related information(TS 23.228, 2003).

The terms used in the sequel by SPUR scheme are the following:

- IMPI, IMPU:the private and public identity of a user.
- K_{PX}, k_{pX}:the public key and the private key of X.
- $Cert_X$, $Cert_{HP}$, $Cert_{HS}$: the relative identity Certificate of X and of the PCSCF delivered by the HSS, and the attribute Certificate of the SCSCF delivered by the HSS.
- ID_X: the identifier of X(could be an IPv6 address).
- AK: authentication key shared between MS and HSS(TS 33.102, 2000).
- K_{si}: the session key established between the PCSCF and the MS.
- req_i, res_i: challenge and response used between the MS and the PCSCF during the establishment of K_{si}.
- AV_i: the authentication vector number i of a user as defined in(TS 33.102, 2000).

2.2 The Secured Registration Protocol

The registration procedure is initiated by a mobile when it wants to access a service, for the first time. The deployment of SPUR scheme supposes the satisfaction of the following assumptions:

- Every mobile MS possesses an identity certificate delivered by its home network.
- Every node of the Internet multimedia subsystem has an identity certificate. This includes the PCSCF, ICSCF, HSS, and SCSCF.
- The different Certification Authorities (CA) serving the function of publishing certificates of the above mentioned entities are linked to a Bridge Certification Authority (BCA)(Hastings and Polk, 2000) to ensure cross-certification.
- The signaling protocol used between the nodes of the IMS is assumed to be the SIP-EAP-TLS.

The registration protocol (as depicted by Figure 1) is a 15-step procedure defined as follows:

Step1. Mobile MS signs its private identity with its private key (k_{pMS}) and encrypts it with the public key of its HSS (K_{PHSS}). After that, the MS sends message M_1 to the related proxy PCSCF

$$M_1 = \{E = [(IMPI)\_k_{pMS}]\_K_{PHSS}, Cert_{MS}$$

$$, Cert_{HSS}, IMPU\}$$

(where (-)_k stems for the encryption function using key k). MS can obtain the address of the PCSCF from the Gateway GPRS Support Node after the success of a PDP ATTACH process (TS 23.060, 2002).

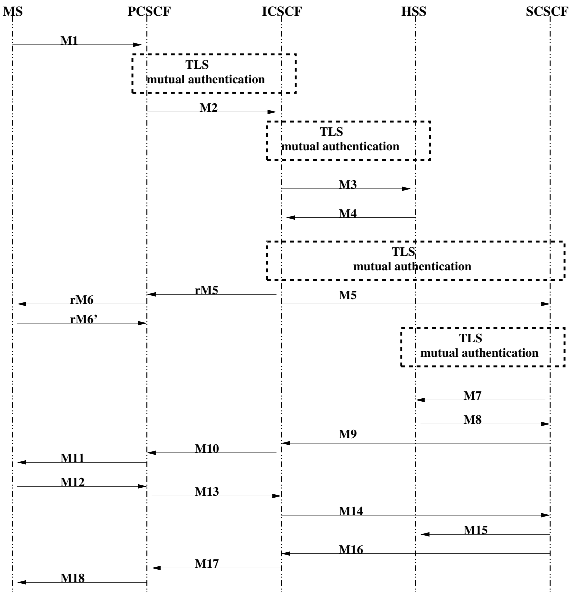

Figure 1: SPUR Architecture

Step 2. Upon receipt of M_1, the PCSCF checks the identity of the mobile home network to deduce the address of the ICSCF. Then, it initiates a secured session with the ICSCF based on TLS protocol. This process needs mutual certificates verification. Then, the Bridge Certification Authority (BCA) intervenes. The main purpose of the assumption on BCA is to facilitate the certificate verification process and to ensure inter-operability between the different operators.

Step 3. After the mutual authentication phase and the share of a symmetric session key, the PCSCF sends a message M_2 containing the information sent by the MS to the ICSCF.

Step 4. The ICSCF extracts the address of the HSS relative to MS from message M_2. Then, it initiates a secured session with this HSS based on TLS protocol. After that, the ICSCF retransmits to the HSS a message M_3 that includes the MS's information and the certificate of the current PCSCF.

Step 5. The HSS decrypts part E of message M_1 and verifies the signature of MS. Next, the HSS checks the private identity of MS and checks whether MS has the rights to accede the requested service. In the positive case, the HSS determines the address of the suitable SCSCF that is able to provide the service. On an other hand, the HSS verifies the validity of the PCSCF certificate and generates an identity certificate $Cert_{HP} = (K_{PPCSCF}, ID_{PCSCF}, \delta Cert_{HP})_{-}k_{pHSS}$ that will be transmitted to MS to verify the identity of the PCSCF. Variable $\delta Cert_{HP}$ defines the validity period of the certificate that we assume relatively short in order to avoid the verification of certificate revocation list at the MS level for this type of certificates. $Cert_{HP}$ is then sent to the ICSCF.

Step 6. On receipt, the ICSCF transmits certificate $Cert_{HP}$ and the public identity of MS to the PCSCF in message rM_5. rM_5 constitutes an implicit acknowledgment to the PCSCF, indicating that the identity of MS has been verified and that it should keep the connection until the accomplishment of the registration process. In the same time, the ICSCF establishes a secured session with the SCSCF based on the TLS protocol. Then, the ICSCF transmits message M_5 to the SCSCF which includes $\{E, Cert_{MS}, Cert_{HSS}, IMPU\}$.

Step 7. The PCSCF computes a symmetric session key K_{si} and signs it with private key k_{pPCSCF} and encrypts it with public key of MS K_{PMS}. Next, the PCSCF sends the $E' = [(K_{si})_{-}k_{pPCSCF}]_{-}K_{PMS}$, a challenge req_i and the certificate $Cert_{HP}$ delivered by the HSS to the MS in message rM_6.

Step 8. MS verifies the signature of the HSS on $Cert_{HP}$. It decrypts E' and verifies the signature of the PCSCF on the session key K_{si}. In the case of verification success, MS stores the session key to be used in its communications with the PCSCF. Furthermore, MS computes the response $res_i = (req_i)_{-}K_{si}$ and sends it to the PCSCF in the message rM'_6.

Step 9. When the SCSCF receives the message M_5, it extracts the address of the HSS, initiates a secured session with it based on the TLS protocol. Then, the SCSCF sends $E = [(IMPI)_{-}k_{pMS}]_{-}K_{PHSS}$ and the certificate $Cert_{MS}$ of the mobile.

Step 10. The HSS verifies the validity of mobile MS certificate and its private identity.

Step 11. The HSS extracts the authentication vectors relating MS. The structure and contents of these vectors are identical to those defined by the 3GPP in the IMS AKA (TS 33.203, 2002). The HSS extracts the different public identities of MS in order to give them to the SCSCF, to be used in the case where the same MS requests another access to a different service provided by the same SCSCF during the period of validity of the active registration. Then the vectors and the public identities are signed with the private key k_{pHSS} of the HSS and encrypted with the public key of the SCSCF. The HSS generates an attribute certificate in which it signs that the current SCSCF will offer the asked service to the MS $Cert_{HS} = (ID_{SCSCF}$,service,$\delta Cert_{HS})_{-}k_{pHSS}$, where $\delta Cert_{HS}$ is the validity period of the certificate, which is defined by the HSS in order to avoid the use of CRLs for MS. However, It should fulfill the following condition in order to guarantee service continuity:

$$\delta Cert_{HS} < \delta Cert_{HP}.$$

Step 12. The HSS sends the message $M_8 = \{E" = (\{AV_i, \{IMPU\}\}_{-}k_{pHSS})_{-}K_{PSCSCF}, Cert_{HS}\}$to the SCSCF. Moreover, it updates the mobile information (location, current request for registration, SCSCF concerned) and it is supposed to wait the end of the registration request to lunch the charging procedure.

Step 13. On the receipt of message M_8, the SCSCF decrypts E" and verifies the HSS signature. Then, the SCSCF selects a vector AV_i, extracts the values of $RAND_i$ and $AUTN_i$, which are sent with the $Cert_{HS}$ to the mobile MS.

Step 14. MS verifies the attribute certificate $Cert_{HS}$ and the freshness of the sequence number present in the $AUTN_i$. Next, it computes the response RES_i, the integrity key IK_i and the confidentiality key CK_i. Then, MS sends the response RES_i to the SCSCF.

Step 15. The SCSCF verifies the correspondence of RES_i and the value $XRES_i$ present in the AV_i. On success, the SCSCF sends a flag M_{15} to inform the HSS. It also sends a positive acknowledgment to the MS containing the period of time after which the mobile should proceed to a re-registration. This period is defined as $T - dt$ and is sent protected with the integrity key IK_i and the confidentiality key CK_i .

2.3 The Re-registration Protocol

When a mobile wants to extend an active registration, it proceeds as shown in Figure 2. For this, it attempts to perform the following steps:

- The MS sends its public identity and the last computed RES_i, for the current registration, protected with the integrity key IK_i to the SCSCF.
- When receiving this message, the SCSCF choses a new authentication vector AV_j and sends the corresponding $RAND_j$ and $AUTN_j$ to the MS.
- The MS computes the value RES_j and the new integrity and confidentiality keys (IK_j and CK_j). Then, it sends the RES_j to the SCSCF.
- After the verification process, the SCSCF starts the use of the new keys (IK_j and CK_j) and sends in an acknowledgment message to the MS the lifetime of the new registration.

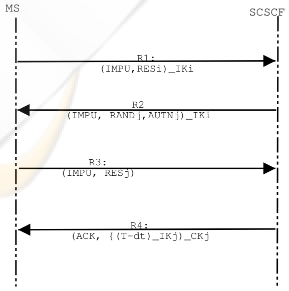

Figure 2: The re-registration procedure

3 MANAGING SECURITY ASSOCIATION IN UMTS ENVIRONMENT

In 3GPP, security associations (SA) were only defined between mobiles and the PCSCF (TS 33.203, 2002). The setup of these SAs is done during the registration process. A SA includes the following five major attributes: (1) a uniquely defined identifier of the SA; (2) the destination and the source address or identifier; (3) the authentication, integrity and encryption algorithms; (4) the keys lengths; and (5) the finite SA lifetime.

We have found that this kind of SAs cannot be adopted as they are, since PCSCF has no longer the same responsibilities as those defined in (TS 33.203, 2002). Our aim in this section is to provide an adaptation of this paradigm to provide a good management process and better security of the exchanged elements.

3.1 Defining security associations

Since the integrity and confidentiality keys would not be sent to the PCSCF, new SAs should be defined between the MS and the SCSCF. Other SAs should take place between the MS and the PCSCF. These associations allow the definition of security agreements between the different communicating entities.

Managing SAs between MS and PCSCF. SAs ensure the establishment of the security mode allowing the access to the IP network. In fact, they would guarantee confidentiality and integrity of the exchanged data between the MS and the PCSCF. The associations are characterized by the following aspects:

- the identifier of the mobile is no longer its private identity $IMPI$. It will be replaced by the public identity ($IMPU$) and the IP Address of the mobile,
- the keys defined between the PCSCF and the MS are symmetric session keys (and no longer the integrity and the confidentiality keys).

The setup of SAs starts when the mobile sends its first request for registration. In fact, message M_1 includes the necessary information to negotiate security parameters between the MS and the PCSCF and to authenticate MS. Those information specify the identity of the mobile, its supported algorithms, and its identity certificate. Upon receiving message M_1, the PCSCF verifies the security mechanisms presented by the MS. Then, it waits for message rM_5 to authenticate MS. This message implies the result of the check of the validity of the identity certificate of the mobile as well as its private identity in the HSS. In addition, the PCSCF receives its temporary identity certificate delivered by the HSS and the current valid Certificate Revocation List (CRL). The two certificates allow the

PCSCF to set up the lifetime of the SA. Therefore, the lifetime of SA should be smaller than the validity period of both $Cert_{HP}$ and the CRL. Otherwise, SA would be invalid when one of the two certificates becomes invalid. In this case, a request for a certificate renewal or a new CRL should be sent.

After the determination of the SA lifetime, the PCSCF computes a symmetric key, signs it and encrypts it with the public key of the MS. Then it sends message rM_6 to the MS in which it defines the SAs. rM_6 would include the chosen security mechanisms, the certificate $Cert_{HP}$, the lifetime of the SA and the symmetric session key. To ensure the security of the SA, the two latter parameters should be sent signed and encrypted. In addition, the PCSCF sends a request req_i to MS. When receiving rM_6, the MS authenticates the PCSCF with the verification of $Cert_{HP}$. Then, it stores the parameters of the SA to be used on the following messages. Furthermore, MS computes the response res_i and sends it to the PCSCF to accomplish the SA setup procedure.

Managing SAs between MS and SCSCF. To provide an end to end security between the MS and the SCSCF, new SA should be established between these two entities. The definition of these SAs allows the protection of all kinds of access to the services independently of the access network. Even if there is a security weakness on the communication links, the SCSCF could verify, and no longer delegate, the integrity and confidentiality of the messages sent by MS. In this case, SAs are defined between the MS, which is defined by its public identity $IMPU$ and by its IP address, and the SCSCF defined by its IP address. The selection of the security mechanisms (e.g., authentication, integrity and confidentiality) to be used/declared in SAs is done during the registration process. In fact, the MS sends with message M_1 the lists of its supported security mechanisms, the index of its security association, its identity certificate and its root certificate. Based on M_1, the SCSCF determines the mechanisms that it would deploy. Then, it authenticates the MS through the verification of its private identity and its identity certificate in the relative HSS. After that, the SCSCF use the CRL and the validity period of the $Cert_{HS}$ to deduce the lifetime of the security association such as it will have the smallest value. Next, the SCSCF chooses an authentication vector AV_i and extracts $RAND_i$ and $AUTN_i$. These parameters would allow the MS to compute the integrity and the confidentiality keys IK_i and CK_i. Finally, the SCSCF sends the previous indicated parameters to the MS in message M_9. On the other side, the MS would verify the freshness of the message and the identity of the SCSCF. Then, it computes RES_i, IK_i and CK_i. Next, the response of the MS (using message M_{12}) will confirm the choices indicated in the SA.

To resume, one can note that the keys and the parameters defined in each security association are those existing in the authentication vectors delivered by the HSS to the SCSCF. Therefore, every authentication vector contributes to the definition of a security association. The lifetime of the SAs defined both in the MS and in the SCSCF are specified to be longer than the lifetime of the registration. Thus, the request for re-registration is protected by the security association yet established. After the definition of the two SAs, the next sub-section will consider the mechanisms of protection of the SA databases.

3.2 The protection of the security associations

The security associations previously defined are stored in specific data bases (SADB). The protection of these databases needs in addition to a secured hard storage an enforcement of some appropriate protection. Thus, we propose the definition of two types of SADBs:

- the first contains the list of SAs established at a defined moment. It can include SAs established between the MS and the SCSCF:

SA#	Source Address	Destination Address	Encryption algo
Auth Algo	Integrity Algo	Ptr# rule#	

- the second contains the security policies defined between the different operators (e. g. between the SCSCF and the HSS).

Rule#	Source Address	Destination Address
Encryption algo	Authentication algo	Integrity Algo

The use of these databases ensures more protection of the SAs, since there is a continuous verification of the conformity of a security association to the rules defined between two different operators. Furthermore, this approach can offer security as a quality of service given to the subscribers according to the agreements defined between the HSS and the SCSCF.

4 SPUR ANALYSIS

In this section, the most important SPUR provisions are quoted. Furthermore, a comparison between the security mechanisms defined respectively in the 3GPP protocol and the SPUR is presented.

4.1 Security provisions

SPUR scheme presents different security provisions. More precisely, one can state the following:

• SPUR guarantees the protection of the integrity and confidentiality of the transmitted data between the different entities of the IMS at the SIP layer. It ensures two types of security mechanisms. The first is based on the use of TLS between the nodes of the IMS including PCSCF, SCSCF, ICSCF and HSS. The second uses the different SAs established between the MS, PCSCF, and SCSCF. So that every kind of transaction between the different participants in a communication is highly protected.

• SPUR allows the MS to authenticate the SCSCF and the PCSCF in addition to the home network. This is ensured by the use of certificates delivered by the HSS to each node. The MS can verify each time the signature of the HSS on the identities of the two nodes. If the verification is successful, the MS is sure that the HSS had authenticated the PCSCF and the SCSCF.

• SPUR provides end-to-end security for the private data of the MS. In fact, the use of SAs between the MS and the SCSCF allows to the server as well as to the MS to be sure that the integrity and the confidentiality of the exchanged data are protected during the validity of the security association.

• SPUR is independent from the protocols used in the lower layers, since all the presented mechanisms are implemented in the SIP messages without a need for lower protocols layers.

• SPUR exploits (or integrates) the 3GPP registration procedure. In fact, we have not changed the authentication vectors defined by the GPP standards. However, we have added other mechanisms to enforce the security of the exchanged data.

4.2 Comparing SPUR to 3GPP protocol

SPUR presents many enhancements comparing to the different propositions for UMTS registration. Siemens proposal has different drawbacks (S3-000689, 2000). First, there is no kind of authentication between the MS and the SCSCF. The MS only authenticates the HSS. This approach can induce different attacks such as masquerading and man in the middle attacks. Furthermore, the protection features used between the nodes of the IMS are based on the security mechanisms defined at the network layer. This means that the absence or the weakness of the security protocols implemented at the network layer could lead to an unprotected transmission of the private user data. This presents an important threat to the user security and does not respect the 3GPP requirements on SIP.

On an other hand, Ericsson proposal does not present a practical solution (S3z000010, 2000). In fact, it adds significant loads to the HSS, which must insure authentication and re-authentication each time a mobile accesses the IMS. Also, the performance of the HSS would decrease when sending the challenge and waiting for a response. Another drawback is related to the complexity of the re-authentication procedure, which is invoked by the HSS and induces the retransmission of the new integrity and confidentiality keys to the SCSCF and PCSCF.

3GPP has defined an other registration protocol that overcomes many drawbacks defined in previous proposals. It insures the authentication of the MS to the SCSCF, which receives the authentication vectors from the HSS. However, the PCSCF terminates the integrity and confidentiality protection using the appropriate keys defined by the authentication vectors. 3GPP protocol has also some drawbacks. First, the MS does not identify the SCSCF. Second, the private identity of the MS is clearly transmitted in the SIP layer for each authentication or re-authentication procedure. Third, the integrity and confidentiality keys of the user are transmitted from the SCSCF to the PCSCF using the network layer security mechanisms.

The following table summarizes the security enhancements provided by the SPUR scheme in comparison with the 3GPP registration procedure. The table shows in particular that SPUR provides at least six additional security services including SIP authentication and confidentiality.

Table 1: Comparison of the security provisions of the 3GPP and the SPUR

Criteria	3GPP	SPUR
SIP Authentication	1	1
SIP Confidentiality	0	1
SIP Integrity	0	1
IMPI Confidentiality	0	1
Establishment of the IK and the CK	1	1
Key Freshness	1	1
Serving Network Authentication	0	1
Certification use	0	1
Key Session Definition	0	1

5 SPUR SIMULATIONS

5.1 Simulation Environment

In this subsection, the impact of the addition of new processing in the IMS nodes is studied. Particularly, we will focus on the influence of the changing size of the signaling messages respectively on the error probability and on the data flows exchanged between the different nodes.

The simulation model we use is based on the studies defined in(Kist and Harris, 2002; Handlay et al., 1999). We have applied SPUR on four nodes which represents the MS, the PCSCF, the ICSCF and the SCSCF. The arrival process to IMS nodes is the Poisson process with a mean arrival rate of 1 session per second. IMS nodes have also a negative exponential service times with means of 20ms. We consider that the original size of a SIP message is varying between 170 bytes and 500 bytes(Rosenberg et al., 2003)(Sweeny et al., 2003). Also, cases where the additional size increased per each node is variable between 50 bytes and 200 bytes according to the type of the processing are studied. The first simulation considers the error probability defined for the transmitted messages depending on the Error Bit Rate (BER) and the size of messages. The error probability of a message is defined using the binomial distribution $P_E(M) = \sum_{k=1}^{8M} BER^k(1-BER)^{8M-k}$ where M is the size in bytes and k is the number of corrupted bits. The second study determines the additional flow defined on the links between the different nodes. Let's define n as the number of the links and l_i as the link on which the flow is calculated. The flow defined in one direction on link *li* is $F(l_i) = M(l_i)(1 + \sum_{m=l_i}^{n} \frac{P_E(m)}{\prod\limits_{j=l_i}^{m}(1-P_E(j))})$.

5.2 Analysis of the numerical results

We present in this subsection the results obtained by the execution of the previous model.

• **Error probability**

The following figures present the impact of the augmentation of the size of the messages on the error probability. Two cases are studied: the first considers the high error bit rates (shown in Figure 3) while the second presents the variation of the error probability for low values of BER (Figure 4). We notice that for low values of BER, the error probability is almost linear. Hence, to have reasonable error probabilities (i.e., less than 10^{-3}) the values of BER should be chosen lower than 10^{-6}. However, if BER$\geq 10^{-5}$, the error probability takes important values and grows exponentially toward the maximum probability even for small sizes.

Thus, we can conclude that we should choose the constraint (BER $<10^{-5}$) to have an acceptable error probability, and so have less message retransmission between the nodes.

• **Additional Flow**

The changing size of the transmitted messages induces additional flow between the network nodes, especially when the BER is not the same on the different links. In the following figures, three cases are considered: The first case considers the BER on the links between the nodes has high values (Figure 5). The second considers the same BER on all links (Figure 6), and the last addresses the case where BER has small values between links (Figure 7)e

The first figure shows the case where the radio link has a great value of BER. We can notice here that the additional flow on the link can reach 180% of the initial flow size which is unacceptable on the radio link since it adds unacceptable amounts of interference.

In the second case, we study the case where the BER is the same on all the links. This situation is not usually true since the radio link presents always the highest BER. Nevertheless, we notice that for a BER = 10^{-6} , the additional flow overheat has a maximum value of 8% .

The last studied case considers low values of BERs. We notice in this case that the additional flow does not take important values. It can be induced that the use of SPUR with low BERs on the links between the different nodes does not add high flows. The previous results demonstrate that the use of SPUR does not introduce large loads if the BER values are well chosen.

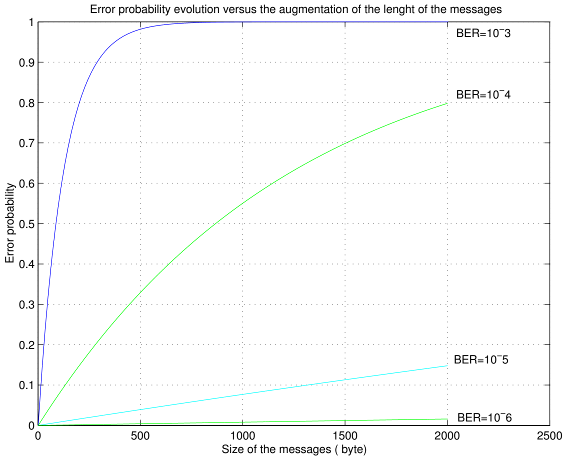

Figure 3: Error Probability in the case of high BER

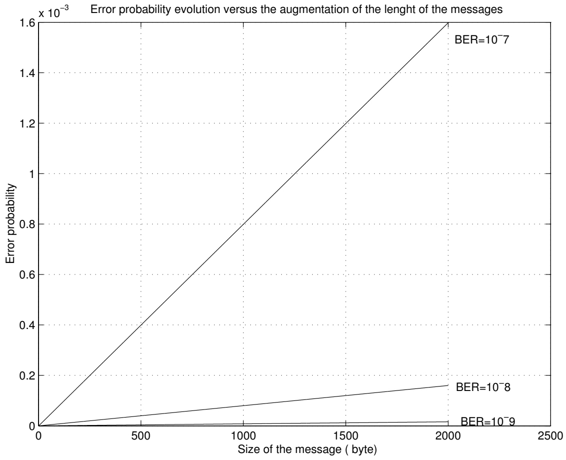

Figure 4: Error Probability in the case of low BER

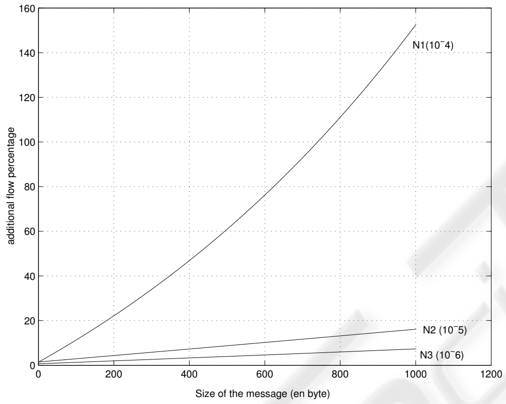

Figure 5: Additional flow for high BER

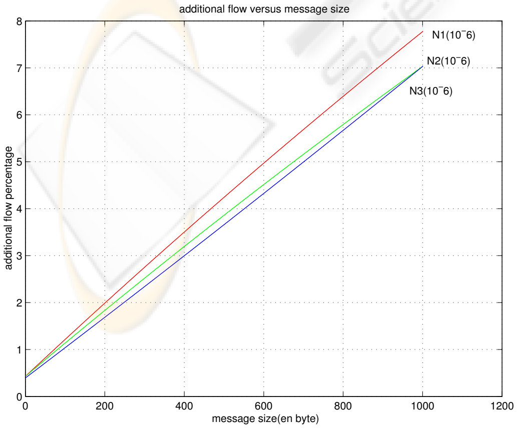

Figure 6: Additional flow for equal BER

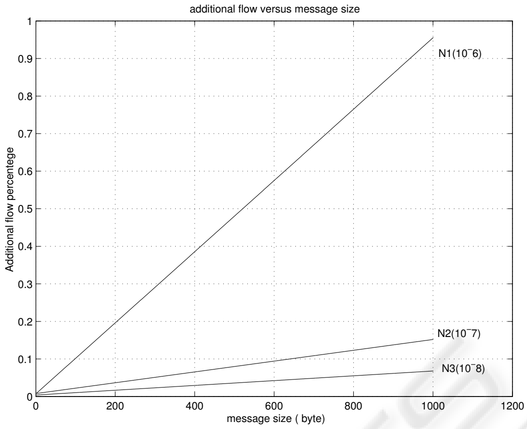

Figure 7: Additional flow for low BER

6 CONCLUSION

In this paper, we have presented a secure registration protocol for UMTS all IP networks. This protocol has added new security measures that provide mutual authentication, integrity and confidentiality between all entities involved in a communication process. In addition, it provides an end-to-end security service for the mobile privacy.

SPUR scheme is an extensible protocol that can define a comprehensive platform to integrate next generation networks (NGN), assuming that they are based on SIP-like protocols. The integration would assume that a bridge architecture of certification is made available in a way that any certificate provided can be checked efficiently.

REFERENCES

Kaaranen, H., Ahtiainen, A., Laitinen, L. , Naghian, S. ,Niemi, V. , (2001). *UMTS Networks : Architecture, Mobility and Services,* Weily, England,

TS 23.228 : IP Multimedia subsystem Stage 2. Retrieved March 3, 2003, from http ://www.3gpp.org

TS 22.228 : Service Requirements for the IP Multimedia Core Network. Retrieved June 6,2002, from http ://www.3gpp.org

TS 33.900 : A Guide to 3rd Generation Security. Retrieved January 1, 2000, from http ://www.3gpp.org

TS 33.120 : UMTS Security principals and objectives. Retrieved May 5, 2000, from http ://www.3gpp.org

TS 21.133 : Threats and attacks in UMTS, Retrieved December 12, 2001, from http ://www.3gpp.org

TS 33.203 : Access Security for IP-based services. Retrieved March 3, 2002, from http ://www.3gpp.org

TS 24.229 IP Multimedia Call Control Protocol based on SIP and SDP, V5.4.0 Retrieved March 3, 2002, from http ://www.3gpp.org

Rosenberg, J. , Schulzrinne, H. , Camarillo, A., Johnston, G., Peterson, R., Sparks, J., Handley, M., . Schooler, E,, (2002). *RFC 3261 : SIP. Session InitiationProtocol* Retrieved August 8, 2003, from IETF web site : http ://www.ietf.org/rfc/rfc3261.txt

3GPP TSG SA WG3 Security, S3-000689 : Access security for IP-based services . Retrieved November 11, 2000, from *www.3gpp.org/ftp/tsg_sa/WG3_Security/ 2001_meetings/TSGS3_17_Gothenberg/Docs/PDF*

3GPP TSG SA WG3 Security, S3z000010. 2000. Authentication and protection mechanisms for IM CN SS; Retrieved November 11, 2000, from *www.3gpp.org/ftp/tsg_sa/WG3_Security/ 2001_meetings/TSGS3_17_Gothenberg/Docs/PDF*

TS 33.102 : *3G Security, Security Architecture*, Retrieved September 9, 2000, from http ://www.3gpp.org

Hastings N.E. , Polk W. T. (2000), *Bridge Certification Authorities : Connecting B2B Public Key Infrastructures*. Retrived from csrc.nist.gov/pki/documents/B2B-article.pdf

TS 23.060 : General Packet Radio Service; Service Description. Retrieved March 3, 2002, from http ://www.3gpp.org

Kist, A. , and Harris, R.J.,(2002). A Simple Model for Calculating SIP Signaling Flows in 3GPP IP Multimedia Subsystems, *Lecture Notes in Computer Science,* 924-935

Handlay, M. , Schulzrinne, H., Schooler, E., and Rosenburg, J. D. , (1999). *RFC 2543* : SIP : Session Initiation Protoco*l* . Retrieved March 3, 2003, from IETF web site : http ://www.ietf.org/rfc/rfc3261.txt

Sweeny, J., Kenneally, V., Pesch, D., Purcell, G, (2003). *Efficient SIP based Presence and IM services with SIP message Compression in IST OPIUM.* Retrieved September 9, 2003, from http ://www.ist-opium.org/