Perfect Identity Concealment in UMTS over Radio Access Links

Michel Barbeau and Jean-Marc Robert

***Abstract*—** Identity concealment is viewed as a standard identity privacy feature. UMTS provides partial concealment. This work extends the UMTS mutual authentication protocol such that the true identity of a mobile equipment cannot be discovered by an attacker eavesdropping over the radio access link interface. Three different solutions using aliases are proposed. Each of them provides perfect identity concealment to mobile equipment over the radio access link part of an UMTS connection.

***Index Terms*—** *Mobile networking, Wireless Networks Standards and Protocols, Architectures and Protocols or Mobile Networks, Security, Privacy and Authentication in Mobile Environments.*

I. Introduction

IN wireless access networks, attackers may passively monitor the traffic to uncover identities of subscribers. Identity concealment is viewed as a standard privacy/security feature [1]. It is relevant for several reasons. For example, if the identity is not protected, the location of a wireless device (and by association, the location of its user) can be tracked simply by eavesdropping the communications. This can lead to attacks directed towards selected users. It is also an enabler for location based mobile spam, which consists of spamming users with location related advertising. Thus, the absence of identity confidentiality is a factor that may compromise the acceptance of a technology by the potential users.

Universal Mobile Telecommunications System (UMTS) provides a partial form of identity concealment [2]. The goal of this work is to extend the mutual authentication protocol of UMTS such that the true identity of mobile equipment (ME) cannot be discovered by radio access link eavesdroppers.

The concealment of the ME identity can be addressed through the use of one-time aliases. The real identity shall never be divulgated over the radio access link interface, only aliases may. This approach requires that the ME can generate new aliases on the fly. These aliases (1) must be hard to associate to a given user identity and (2) must be difficult to link to any related previously used alias.

This paper addresses the problem of providing *perfect identity concealment* to UMTS ME over the radio access link interface. Three different solutions using one-time aliases are proposed: a *coupon-based* solution, a *PKI-based* solution, and a *anonymous number-based* solution. Each solution provides perfect identity concealment against a attacker (1) which can only eavesdrop over the radio access link of an UMTS connection – a *passive* attacker – or (2) which can eavesdrop and inject messages over the radio access link – an *active* attacker.

The rest of the paper is structured as follows. Related work is discussed in Section II. The UMTS architecture and the various kinds of identity it contains are reviewed in Section III. The UMTS mutual authentication protocol, which this work extends, is described in Section IV. Finally, the new protocol extensions providing perfect identity concealment over the radio access link in UMTS are presented in Section V. Section VI discusses future work. We conclude with Section VII.

II. Related work

The protection of the *identity* and the *anonymity* of a user becomes an essential requirement for many E-Commerce applications such as E-cash, E-Banking, E-Trading, and E-Auctions. New proposals for E-Voting put obviously even more emphasis on these confidentiality issues.

There are several forms of identity concealment: *sender anonymity* (the most asked on the Internet and the subject of this paper), *receiver anonymity*, *mutual anonymity* and *unlinkability-of-sender-and-receiver*. In [3], Guan *et al.* gives a good introduction on this topic and presents one of the first quantitative analysis of the main proposals.

At the protocol level, there is two ways to achieve sender anonymity: *rerouting-based* techniques and *non rerouting-based* techniques. Rerouting-based techniques use intermediate nodes on a rerouting path to obfuscate the source of a message. Examples of this approach are numerous: *Anonymizer Server*, *Anonymizer Remailer, Onion-Routing* (see [3], for an excellent presentation of these techniques).

This work has been done while the first author was visiting the Security Group of Alcatel Research and Innovation.

Michel Barbeau is with the School of Computer Science, Carleton University, 1125 Colonel By Drive, Ottawa, Canada, K1S 5B6 (email: michel.barbeau@scs.carleton.ca).

Jean-Marc Robert is with Alcatel, Research and Innovation, Security Group, 600 March Rd, Ottawa, Canada, K2K 2E6 (email: jean-marc.robert@alcatel.com).

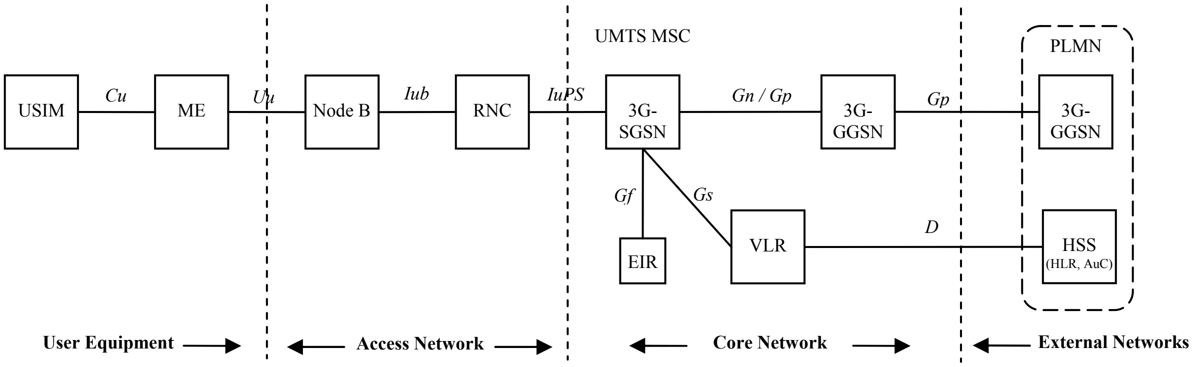

Figure 1: UMTS high-level architecture for packet based networks. AuC = Authentication Center; **EIR** = Equipment Identity Register; **HLR** = Home Location Register; **HSS** = Home Subscriber Server; **ME** = Mobile Equipment; **Node B** = Base Station; **PLMN** = Public Land Mobile Network; **RNC** = Radio Network Control; **UMTS MSC** = UMTS Mobile Switching Center; **USIM** = Universal Subscriber Identity Module; **VLR** = Visitor Location Registor; **3G-GGSN** = 3G Gateway GPRS Support Node; **3G-SGSN** = 3G Serving GPRS Support Node.

A similar approach has been used to hide the caller identity in Session Initiation Protocol (SIP). In this case, a SIP Anonymizer agent is used to remove all the original information related to the caller [4]. Using such a tool, a client and server can establish a communication through a intermediate proxy translating the original identities to anonymous identities.

Finally, the DC-Net [5] seems to be the only example of a non rerouting-based technique to hide the identity of the sender of a message. However, no application uses this solution due to its scalability issues.

III. Identities in UMTS architecture

The UMTS architecture is depicted in Figure 1. In an architecture of such a complexity (see also Refs. [6] and [7]), information regarding user identity may leak at different places. Protection of user privacy is an important and challenging issue.

Numerous forms of identity are defined in UMTS [8] [9]:

- *MSISDN* (Mobile Subscriber Integrated Services Digital Network) representing the user phone number.
- *IMEI* (International Mobile Equipment Identity) representing the ME serial number and which can be used for fraud prevention.
- *IMEISV* (International Mobile Station Equipment Identity and Software Number) is simlar to the IMEI and addresses both hardware and software indentity.
- *IMSI* (International Mobile Station Identity) representing the permanent *user identity* which is stored in the Universal Subscriber Identity Module (USIM) secure component, i.e. smart card.
- [*P*-]*TMSI* ([Packet-]Temporary Mobile Subscriber Identity) which is a temporary identifier in the local network in which a user is registered.

These various identities are used by the different components of the UMTS architecture as shown in the following table.

Table 1: UMTS Identities in the UMTS components

Parameter	Type	HLR	VLR	SGSN	GGSN
MSISDN	T	M	M	M	M
IMEI	T	-	-	C	-
IMSI	P	M	M	M	M
P-TMSI (signature)	T	-	-	C	-

Legend: M = mandatory; C = conditional; T = temporary; P = permanent.

The UMTS security architecture [2] specifies the following security features:

- ***user identity confidentiality:*** *the property that the permanent identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;*
- ***user location confidentiality:*** *the property that the presence or arrival of a user in a given area access link;*
- ***user untraceability:*** *the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.*

Unfortunately, the UMTS specification falls short to perfectly achieve these requirements. When a ME and a base station establish an initial Radio Resource Control (RRC) connection, the IMSI of the ME is sent to the base station in clear over the radio access link interface. This violates the *user identity confidentiality* and *user location confidentiality* properties.

Once a ME has been registered into a given UMTS network, it may use its temporary identity TSMI to establish a RRC connection. If the TMSI is not updated after each RRC connection (i.e. each time the TMSI is sent in clear over the radio access link), the *user location confidentiality* and *user untraceability* properties are not fully achieved. An eavesdropper is able to link the different connections established under a given TMSI.

This paper addresses these problems of identity leakage occurring during the RRC connection establishment. The objective is to insure that the three properties, specified in the UMTS security architecture [2], are fully achieved without any exception.

IV. MUTUAL AUTHENTICATION IN UMTS

The UMTS mutual authentication protocol relies on a challenge-response mechanism. The goal of this protocol has two-fold: (1) allow the base station/VLR to authenticate the ME/USIM for billing purpose, and (2) allow the ME/USIM to authenticate the base station, avoiding eavesdropping or another fraud from a rogue base station.

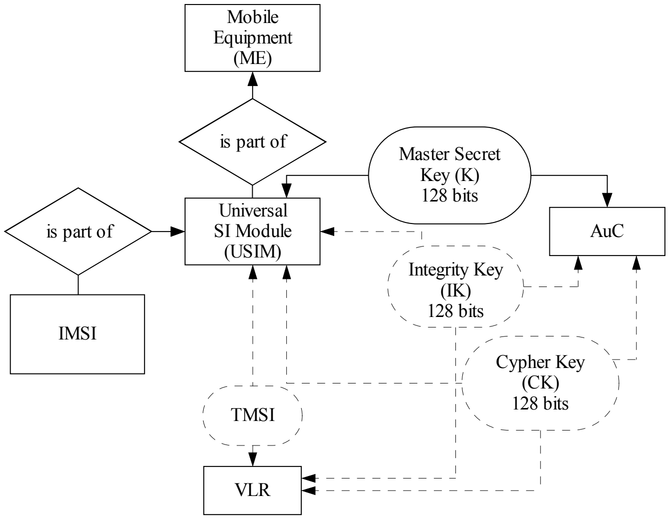
Mobile Equipment (ME)
is part of
Master Secret Key (K) 128 bits
Universal SI Module (USIM)
AuC
is part of
IMSI
Integrity Key (IK) 128 bits
Cypher Key (CK) 128 bits
TMSI
VLR

Figure 2: Security associations in UMTS.

A model of the security associations in UMTS is pictured in Figure 2. Static elements are represented as solid line shapes, dynamic elements as dotted line shapes. The ME contains a USIM. It is a tamper resistant smart card embedding cryptographic algorithms and a master secret key (K), shared with the authentication center (AuC). The USIM embeds as well the permanent identity IMSI of the ME. During the authentication procedure of a ME, the AuC generates for the ME an integrity key (IK), for message authentication, and a cipher key (CK), for message encryption. The VLR generates for the ME a TMSI.

The mutual authentication and key agreement procedure is pictured in Figure 3 . The ME discovers a VLR. It sends to the VLR its old TMSI, i.e. acquired in a previous authentication procedure execution. If the VLR fails to retrieve the IMSI associated to that TMSI, it asks to ME to submit the permanent identity.

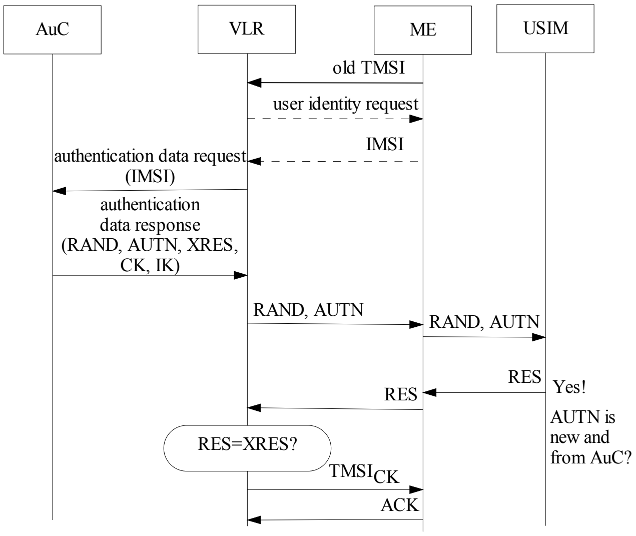
AuC
VLR
ME
USIM
old TMSI
user identity request
IMSI
authentication data request (IMSI)
authentication data response (RAND, AUTN, XRES, CK, IK)
RAND, AUTN
RAND, AUTN
RES
Yes!
RES
AUTN is new and from AuC?
RES=XRES?
TMSI$_{CK}$
ACK

Figure 3: Mutual authentication and key agreement in UMTS.

Once the VLR has identified the ME, it requests authentication data from the AuC of the ME home network. From the IMSI, the AuC retrieves the corresponding master secret key K and generates a challenge for the ME. To avoid replay attacks, the freshness of the challenge relies on a sequence number SQN and a random number RAND. Based on this information, the AuC computes an authentication token AUTN, an expected response XRES, an authentication key AK, a cipher key CK and an integrity key IK. The values RAND, AUTN, XRES, CK and IK collectively constitute the authentication vector sent back to the local VLR.

Once the local VLR has received the authentication vector, it can challenge the ME with the values RAND and AUTN. From its master secret key K and RAND, the USIM component of the ME can authenticate the challenge through AUTN. Then, the USIM computes the response RES to the challenge, the cipher key CK, the integrity key IK, and the authentication key AK. The response RES is returned to the local VLR, which compares it with the expected response XRES. If they match, the keys CK and IK are transferred to the RNC which can establish a secure communication channel with the ME.

Once both parties have been authenticated and a secure channel has been established, the VLR attributes to the ME a temporary identity TMSI, which identifies uniquely the ME in the local network. This identity can be used for the future connection establishments in the same network.

Finally, as mentioned earlier, the RRC connection establishment does not provide perfect identity concealment since the permanent identity IMSI (or the temporary identity TMSI) is sent before the establishment of any secure channel between the ME and the base station.

V. Identity concealment extensions

This section presents novel techniques to provide perfect identity concealment over the radio access link. They rely upon the use of one-time aliases which are hard to link with the IMSIs. Three different implementations are presented in the following sections. Each of these extensions to the UMTS protocols has its advantages and its limitations.

In all the solutions, an implicit assumption is made: the aliases are prefixed with the *Mobile Country Code* (MCC) and *Mobile Network Code* (MNC), which identify the subscriber's service provider [8]. With this information, a local VLR knows who can authenticate a given ME.

A. Coupon-based technique

The first solution is based on one-time coupons generated by the home AuC and provided to the ME.

For each new RRC connection, a ME uses a new one-time coupon to communicate with a local VLR. This coupon is sent to the appropriate AuC which makes the association with a given ME. The mutual authentication proceeds as described in Section IV, but the one-time coupon is used instead of the IMSI (or the TMSI).

Along with the authentication vector, the AuC must send to a given ME a set of new coupons $C_1, \ldots, C_n$ for future connections. This solution raises the following questions:

1. How many coupons need to be sent?
2. Do coupons need to be protected? Against whom?

Under the assumption that a VLR authenticates a ME for each RRC connection, one new coupon is sufficient. At the end of the mutual authentication process, the ME obtains a coupon to be used for the next RRC connection. Thus, the amount of information maintained by the HLR is minimal.

The answer to the second question is not as obvious. The coupons have to be protected on the radio access link interface. However, a number of constraints have to be considered:

- minimize the risk of desynchronization between AuC and ME;
- avoid dependency on the VLR to transmit the coupon after a secure communication channel has been established between the RNC and a ME;
- conceal the coupon from the VLR.

The last point is to avoid that the local access and core networks can link different connections through the ME aliases (see Section VI on future research for more details).

In accordance with these requirements, we propose that the AuC encrypts the coupon and authenticates it through the message authentication code (MAC) of the authentication vector. The coupon can be encrypted as $Coupon \oplus f(AK)$, for some appropriate function f to be defined.[1] Once decrypted, the value *Coupon* can be fed to the function f_1, which computes the MAC value (see the definition of the security architecture and the different building blocks [12]). This last step authenticates the value *Coupon* for the ME.

The main drawback of this solution is the modification of message formats, between the VLR–AuC and the VLR–SGSN–RNC–ME.

B. PKI-based technique

In order to avoid too substantial modification of the mutual authentication process as well as the format of the messages between the different components, this second solution proposes a method allowing a ME to generate its own one-time coupons.

This second solution relies on the use of public-key cryptography [11]. A ME has to know the public key of its AuC – say a RSA public key. Thus, the ME generates a random value and builds the following bit-sequence:

00001 <random value> 00 <IMSI>

This corresponds to the PKCS #1 encoding [11] of the IMSI which is encrypted with the AuC public key.

The encrypted value of the IMSI is used as an alias. Each time the alias needs to be renewed, a new random value is generated and the aforementioned procedure is applied. When the AuC receives such an alias, it can recover the value of the IMSI. The mutual authentication process proceeds as described in Section IV, but the one-time alias is used instead of the IMSI (or the TMSI).

This solution has one major drawback. For each connection, it requires more expensive computation and longer identifications due to the use of RSA encryption – with most likely 1024-bit keys. Elliptic Curve Cryptography (ECC) [11] may represent an interesting alternative. However, it still requires extensive resources.

C. Anonymous number-based technique

The third solution is an attempt to overcome the drawbacks of the previous two methods. It is based on one-time aliases which can be derived independently by both the AuC and the ME. This new identifier is called the International Mobile Anonymous Number (IMAN).

In this solution, a ME must respect the following rules:

- Never use the IMSI for the RRC connections;
- Use one IMAN per successful connection;
- Derive the new IMAN once the current one has been used.

The IMAN is derived during the mutual authentication process between a AuC and a ME. The IMAN is obtained from the anonymity key (AK). The choice of AK is not

[1] The choice of f has to be done carefully. For example, if f corresponds to the identity function, one can retrieve the value of Coupon$\oplus SQN$.

arbitrary. This key is known to the AuC and not to the VLR. Thus, another requirement for this perfect identity concealment problem can be stated as follow:

- Only the AuC and the ME must be able to derive the new IMAN.

The last point is to avoid the linkability of the different connections by the local access and core networks through the ME aliases, as mentioned earlier.

The IMAN is obtained as follow: during the authentication procedure, a AuC and a ME compute the value MD5 (AK | SEQN | RND) where MD5 is the well-known cryptographic hashing function [11] hard to inverse. The concatenation of the values SEQN and RND insures the freshness of the result. This is not the only possibility and this solution is given as a representative example. The main aspect is the fact that the function is hard to inverse and that its image is large enough to avoid frequent collisions.

This third solution has small impacts compared to the other solutions. The IMSI (or the TMSI) is replaced by the IMAN which adds seven extra bytes to the messages[2]. Furthermore, the solution is not computationally expensive if the one-way function is chosen properly.

In the remaining of this section, a thorough analysis of our preferred solution to the perfect identity concealment problem in UMTS is presented.

The first impact of this solution is on the database maintained by the AuC. This database has to be indexed by the three following values:

<IMSI, IMAN, Old IMAN>

The Old IMAN has to be kept to insure the continuous synchronization between the AuC and a ME (Lemma 3).

The IMAN becomes the unique element used in the different components to identify a given ME. Only the AuC must know the relationship between an IMAN and an IMSI.

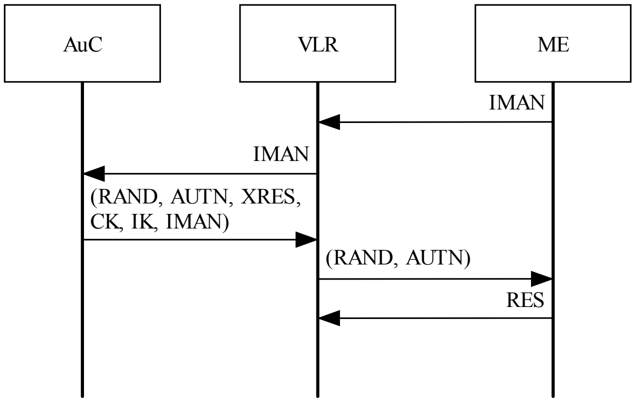

Figure 4: Establishment of a new IMAN.

The procedure for establishing a new IMAN is pictured in Figure 4. Initially, the ME and the AuC share an initial IMAN. A new IMAN is generated when the ME and the AuC proceed to the mutual authentication process.

The ME sends its current IMAN to the VLR. The VLR builds and forwards an authentication data request to the AuC. Using the IMAN, the AuC extracts the master secret key K and produces the authentication vector and a new IMAN'. The AuC has to make sure that the new IMAN' does not collide with other IMANs (current and new). If such a collision occurs, the AuC has the freedom to choose another random value RAND and recomputes the authentication vector.

From now on, the mutual authentication process proceeds as described in Section IV. The authentication vector is returned to the VLR. The VLR challenges the ME. The ME verifies the consistency of the AUTN, produces and returns the response to the challenge. It also calculates the authentication key AK and new IMAN'. The challenge response is verified by the VLR.

At the end of a successful mutual authentication process, the ME updates its identity. The current IMAN becomes the old IMAN and the new IMAN' becomes the current IMAN.

The correctness of this identity concealment protocol extension relies on the following assumptions:

A. The ME's master secret key K is known only by the ME and the AuC;
B. The functions $f_1, \ldots, f_5$ defined in the security architecture are secure one-way functions [13].

A theoretical analysis of this protocol is conducted hereafter.

Lemma 1 (confidentiality). *The AuC and the ME believe that they secretly share the link between an IMAN and an IMSI.*

Proof. The confidentiality of the link between the IMAN and IMSI follows from Assumptions A and B which implies that the anonymity key AK is a secret shared between the AuC and the ME. •

Lemma 2 (unlinkability). *A current IMAN and a new IMAN' are unlikable over the VLR-ME channel.*

Proof. The unlinkability of an IMAN-IMAN' pair over the VLR-ME channel follows from the following facts: (1) the IMAN-IMAN' pair are never transmitted together, (2) the assumption that the channel between the AuC and VLR is secure and (3) each IMAN is fresh. The last point follows from the assumption that the AK is fresh due to the SQN and the RAND values. •

Lemma 3 (self synchronization). *The AuC and a ME cannot loose synchronization with respect to the current IMAN.*

Proof. The desynchronization of the IMAN between the AuC and a ME can be achieved in two different ways.

[2] Those extra bytes can even be discarded at the price of having more potential collisions. This may require more expensive computation by the AuC if it has to discard some random values RAND producing collisions.

Firstly, an attacker can impersonate the ME and can send a forged IMAN to the VLR, which sends to the AuC. The attack will fail because the attacker will fail to provide a valid response to the challenge.

Secondly, an attacker can impersonate the VLR and can send a forged IMAN to the ME. The attack will also fail because the impersonator will fail to provide a valid authentication token to the ME. Both the AuC and ME save the old IMAN while attempting to establish a new IMAN. The old IMAN can always be used to recover from a failure to establish a new IMAN. •

D. More powerful attackers

For the sake of completeness, we conclude this section by presenting a type of attacks against which our new solutions are vulnerable.

A new type of radio frequency signal analysis has been presented in [14]. Radio Frequency Fingerprinting (RFF) is a technique with which each radio transmitter can be uniquely identified by extracting a digital signature from the signal.

The unlinkability can be compromised using a RFF attack. Links can be established between IMANs by cross linking them with their radio frequency fingerprints. Currently, RFF requires advanced hardware and is doable by very sophisticated attackers.

VI. Future Work

Protecting the identity at the radio access link interface is a first step towards a total identity concealment. The next step is to see if identity concealment can be done at the interface between the RNC and the SGSN. Ultimately, the concealment could be pushed up to the interface between the visited local network GGSN and home network GGSN. In such a case, only the subscriber's service provider would be able to track all the calls of a subscriber.

In this context, the different identities presented in the Section III have to be considered. The real challenge is to see if the VLR – and by extension the visited UMTS network – really needs the MSISDN (i.e. phone number) of the roaming ME for some essential functionality.[3] Obviously, the HLR has to know where each ME is located since it is involved in the call forwarding process. Therefore, the objective of the perfect identity concealment problem in this broad context can be the impossibility of linking phone calls from two different RRC connections, leaving to the ME itself the choice of establishing new RRC connections for each new call.

Finally, any new proposition to conceal the identity will have to respect the strict lawful interception requirements [15] to be accepted and deployable.

VII. Conclusion

This paper has presented three solutions to provide perfect identity concealment in UMTS to MEs over the radio access link: the coupon-based, PKI-based and anonymous number-based techniques. In the coupon-based technique, aliases are generated off-line by the AuC and pre-configuration of the ME is required. In the PKI-based technique, the aliases are generated by the ME. They consist of values encrypted using the public key of the AuC. The results of encryption are used as the aliases. When the AuC receives such an alias, it can recover the IMSI by decrypting the alias using its private key. Finally, in the anonymous number-based technique, the aliases are generated by both the ME and AuC using the same material and hence resulting in identical values. The ME must be pre-configured with an initial IMAN. Afterwards, the new IMANs are generated by both the AuC and ME. The technique has the confidentiality, unlinkability and self synchronization properties.

References

[1] V. Niemi and K. Nyberg, *UMTS Security*, Wiley, 2003.

[2] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects, 3G Security, Security Architecture (Release 5)." 3GPP TS 33.102 v5.5.0, 2004.

[3] Y. Guan, X. Fu, R. Bittati and W. Zhao, "A Quantitative Analysis of Anonymous Communications," *IEEE Transactions on Reliability*, vol. 52, no. 1, pp. 103-115, 2004.

[4] M. Castleman, SIPANON: A SIP Anonymizer, Course Report (CS W3998), 2001.

[5] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Receiver Untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65-75, 1988.

[6] 3rd Generation Partnership Project, "Technical Specification Group Services and Systems Aspects: Network architecture, Release 6." 3GPP TS 23.002 v6.5.0, 2004.

[7] 3rd Generation Partnership Project, "Technical Specification Group Services and Systems Aspects: General UMTS architecture, Release 5." 3GPP TS 23.101 v5.0.1, 2003.

[8] 3rd Generation Partnership Project, "Technical Specification Group Services and Systems Aspects: Numbering, addressing and identification, Release 6." 3GPP TS 23.003 v6.4.0, 2004.

[9] 3rd Generation Partnership Project, "Technical Specification Group Services and Systems Aspects: Organization of subscriber data, Release 6." 3GPP TS 23.008 v6.3.0, 2004.

[10] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.

[11] A. Menezes, P. van Ooorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[12] 3rd Generation Partnership Project, "Security Architecture (Release 6)." 3GPP TS 33.102 V6.2.0, 2004.

[13] 3rd Generation Partnership Project, "Cryptographic algorithm requirements (Release 6)." 3GPP TS 33.105 V6.0.0, 2004.

[14] J. Hall, M. Barbeau and E. Kranakis, "Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting", in *Proc. of Communications, Internet and Information Technology (CIIT)*, 2004.

[15] 3rd Generation Partnership Project, "Lawful interception architecture and functions (Release 6)." 3GPP TS 33.107 V6.3.0, 2004.

[3] One non-essential functionality may be listed: displaying the caller phone number on the callee phone display.