Proc. Workshop on Information Hiding, Cambridge (UK), Univ.of Cambridge, Isaac Newton Institute, 30.5.-1.6.96

MIXes in Mobile Communication Systems: Location Management with Privacy*

Hannes Federrath, Anja Jerichow, Andreas Pfitzmann

University of Dresden,
Institute of Theoretical Computer Science, D-01062 Dresden, Germany

{feder, jerichow, pfitza}@inf.tu-dresden.de

Summary. This paper introduces a new technique for location management in cellular networks. It avoids the recording of moving tracks of mobile subscribers. The described procedures are derived from the well known untraceable MIX network and the distributed storage of location information according to GSM networks.

1 Terminology

The served area of a cellular radio network is usually divided into location areas. Location areas are comprised of one or several radio cells. The mark (address) of a location area is the Location Area Identification (LAI).

To address a Mobile Station (MS) in the case of an incoming call, the mobile network needs to know the current location area in order to broadcast the connection request.[1]

The location management is comprised of the procedures location update and handover.

The location update consists of all procedures for location management in the stand-by state of an MS, whereas the handover handles an MS moving during a call.

2 Storage of Location Information

To register the location of an MS, the network operator can maintain a Home Location Register (HLR) at a *central place* in the network. The HLR keeps track of the actual LAI of the MS.

In the case of a (mobile terminated) call the subscriber A calls the Mobile Subscriber Integrated Services Digital Network Number (MSISDN) of the mobile subscriber B. The mobile network reads the current LAI and routes the call to the responsible Base Transceiver Station (BTS). Then the BTS broadcasts a connection request in all cells of the location area (see Fig. 1).

---

* We thank the Gottlieb-Daimler - and Karl-Benz Foundation, Ladenburg (Germany) and the German Science Foundation (DFG) for their financial support. For suggestions and discussions, we thank Elke Franz, Ulrich Hensel, Dogan Kesdogan, Jan Müller, Leslie & Christian "ChriRo" Rook and Ivonne Voigt.

1 The technique "broadcast over the whole served area" is not discussed in this paper! In 3rd generation mobile networks (Universal Mobile Telecommunication System, UMTS and Future Public Land Mobile Telecommunication Network, FPLMTN) the globally covered area does not allow broadcast. However, broadcasts in some parts of the globe require location management again.

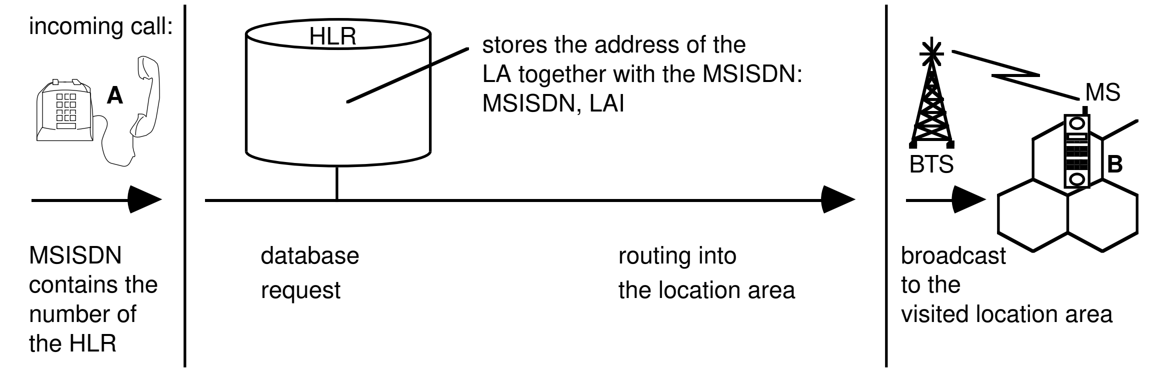

Fig. 1: Call setup with central storage of location information

If the MS is moving into another location area, the HLR is addressed and informed of the new LAI. This location update causes a signalling load on the air-interface and the fixed mobile network. In case of long distances between the visited location area and the HLR, the load in the fixed mobile network is immense.

The solution of this problem is *two-stage storage*: The additional Visitor Location Register (VLR) stores the actual LAI while the HLR (hierarchically) holds the address of the VLR (A_{VLR}).

If the location area changes without leaving the VLR area, only the VLR record has to be updated. If the MS moves to a new VLR area, the HLR record has to be updated. The signalling load in the fixed mobile network is reduced by this technique. However, the complexity of the network management increases. The location management described above is used in the Global System for Mobile Communication (GSM) [GSM_93] (see Fig. 2).

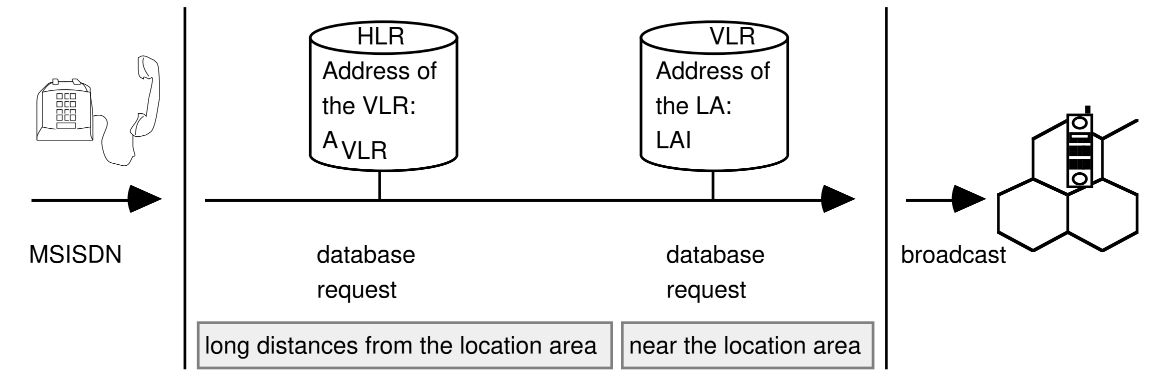

Fig. 2: Call setup with two-stage storage of location information in HLR and VLR

A generalized form of the two-stage storage is the *multi-stage storage* of location information (see Fig. 3). The registers Ri (with i=1..n) store hierarchical location information.

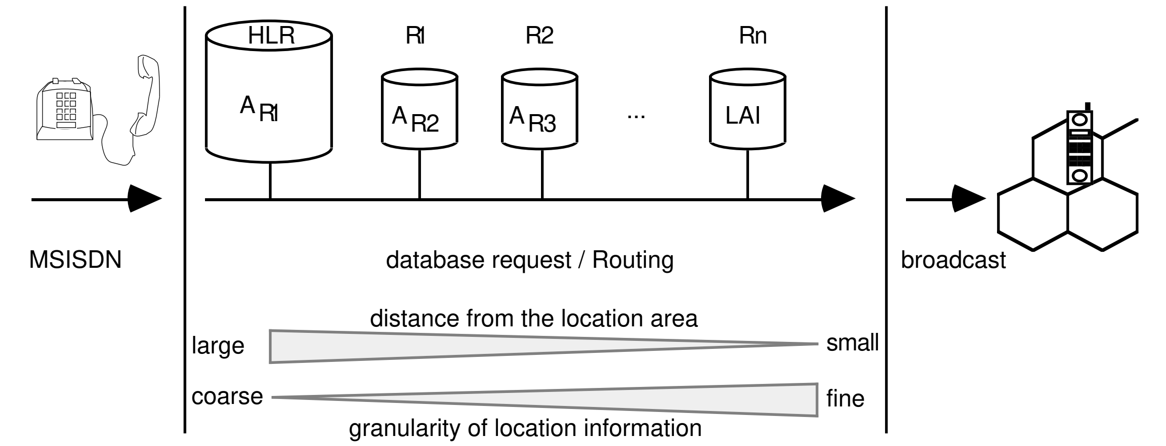

Fig. 3: Generalized multi-stage storage of location information

Consequently, the additional database requests require an even more expensive call setup. The costs for database updates in the case of long distances from the location area are decreased and the signalling load may be reduced.

3 Recording Moving Tracks of Mobile Subscribers

Unfortunately, the above mentioned measures do not prevent the ability of the network operator to record moving tracks. There are two reasons for this problem:

Firstly, the operators of the registers (HLR, VLR, Ri) cooperate with one another. This cooperation is necessary for call setup but implies the hazards of an easier linkability of the distributed location information.

Secondly, it is yet unclear under which identity the registers store the location information. Clearly, the stored identity in the HLR is the publicly known MSISDN.[2] However, for the VLR and the Ri respectively, this is not necessary. There, the records may be stored pseudonymously.[3] Changing the pseudonym periodically, e.g. each time a location update is performed on the stage Ri, complicates considerably the recording of moving tracks.

The use of pseudonyms for the storage of location information, however, creates new problems:

Each incoming call requires a link between the pseudonymous records.

Changing the pseudonym should lead to the unlinkability between the old and the new pseudonym of the same MS.

---

2 For internal purposes, the MS has another number, the International Mobile Subscriber Identity (IMSI). In the procedures described in this paper, we assume that MSISDN and IMSI are equivalent identities. For a uniform presentation of all described procedures, we use only the MSISDN!

3 If they are not stored under a pseudonym, but under the identity of the mobile subscriber (MSISDN), the MS is traceable by the VLR (and the Ri respectively). The moving track will become more detailed with increasing i. Otherwise, only a pseudonym is traceable.

4 Measures that Prevent the Creation of Moving Tracks

Generally, the "creation of moving tracks in mobile communication" can be prevented as follows:

1) *Avoidance of location information* and broadcast covering the entire served area (see [FJKP_95]),

2) *Trustworthy maintenance of location information* (see [Pfit_93, Hets_93, FJKP_95]), e.g. in a trusted Fixed Station (trusted FS, e.g. the fixed telephone of the mobile subscriber in the fixed network),

3) *"covered" storage of location information* — the scope of this paper.

In particular, the solutions 2) and 3), however, require further measures depending on the varying strength of an attacker. These measures are:

i) Protection of the communication relations between the components of the fixed network (see [PfWa_87, PfPW_91]),

ii) Protection against locating by means of electromagnetic radio waves (see [FeTh_95, FJKP_95]).

The measure *i*) works against a strong attacker who can observe all communications in the network, e.g. transactions between BTS', VLRs and HLR. Since the BTS' serve particular areas, indirect locating is possible. In order to achieve protection against observation, the untraceable MIX network [Chau_81, PfWa_87, PfPW_91] and special addressing attributes, "implicit addresses", can be used.

Measure *ii*) is important because the source of the waves corresponds to the location of the sending mobile station. Special modulation methods, e.g. Direct Sequence Spread Spectrum (DS/SS) and Code Division Multiple Access (CDMA) reduce the abilities for locating.

5 A New Centralized Procedure for Location Management with Privacy

In the following sections we are going to describe a new "covered" form of the location information (LAI) stored in the HLR database. The new procedure is firstly described for the centralized storage of location information and will afterwards be generalized to the multi-stage storage.

The situation without protection can be described as follows. In the HLR, a database record «MSISDN, LAI» is stored. For each incoming call, the mobile network routes the connection request to the responsible Mobile Switching Centre (MSC) which arranges to broadcast the call setup message to the location area.

Before a MS can recognize its call setup message (in Fig. 4 call_setup_msg[4]), it must be addressed using an implicit address concealing the MS' identity.

This method is similarly applied in GSM networks. A frequently changing pseudonym – the Temporary Mobile Subscriber Identity (TMSI) – ensures the privacy on the air-interface against outsider attacks. The TMSIs are assigned by the network.

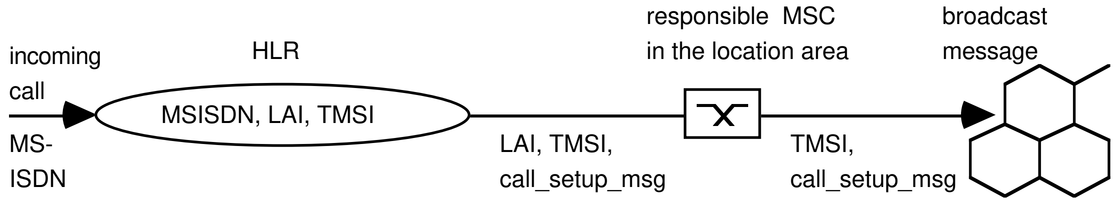

Fig. 4: Call setup with centralized storage of location information (more detailed than Fig. 1)

Below, we describe the new procedures for location registration and call setup with covered LAI. The LAI is *stored not in its plain form, but in its covered form instead*, denoted by {LAI}.

5.1 Premises and Assumptions

Throughout this paper, an MIX network [Chau_81, PfWa_87, PfPW_91] is assumed. Consequently, all statements in the literature concerning the organization, operation and efficiency of MIXes are to be applied to the new procedures.

For clarification, we assume that an encryption key has been exchanged between the MS and the fixed part of the mobile network to encrypt *all* messages on the air-interface. This encryption is omitted in the following formulas.

In asymmetric (public key) cryptosystems we assume an *indeterministic cryptosystem*, i.e. equal plaintext blocks are encrypted to different ciphertext blocks!

Furthermore, we only describe the most necessary messages in the following “protocols”. For better comprehension we use characteristic examples instead of the general formal notation.

5.2 Location Registration and Location Update

Whereas before the network has taken the routing information from the LAI, now the MS needs to create the routing information itself.

4 Provided that all messages (e.g. call_setup_msg and location_registration_msg) are unique and network wide standardized messages – a kind of service primitives – used by all subscribers for a service request.

For the covered location registration, the MS formulates for the {LAI} a so called *untraceable return address* (example for a cascade of three MIXes M1, M2 and M3):

$\{LAI\} := A_{M1}, c_{M1}(k_{M1}, A_{M2}, c_{M2}(k_{M2}, A_{M3}, c_{M3}(k_{M3}, TMSI)))$.[5]

A_{M1}, A_{M2} and A_{M3} denote the addresses of the MIXes M1, M2 and M3; their public keys are denoted by c_{M1}, c_{M2} and c_{M3}, respectively. The sending in every MIX, i.e. call_setup_msg, is encoded by the (symmetric) keys k_{M1}, k_{M2} and k_{M3}.

The implicit address for the broadcast on the air-interface is denoted by TMSI. Our algorithms allow only the MS to create the TMSI. In the following section, additional properties of the TMSI are required.

The location registration message LR to the Home Location Register is

LR := MSISDN, {LAI}, location_registration_msg.

The MS uses the MIX network to protect the LR message (and consequently its source):

$\{LR\} := A_{M3}, c_{M3}(A_{M2}, c_{M2}(A_{M1}, c_{M1}(A_{HLR}, LR)))$.

Since an *indeterministic* cryptosystem was assumed, there is no need to encode random bits into {LR}. The indeterministic encryption is necessary to prevent the following attack to a MIX network: The attacker could simply encrypt the outgoing messages of a MIX Mi using its public key c_{Mi} and matching it to the incoming messages!

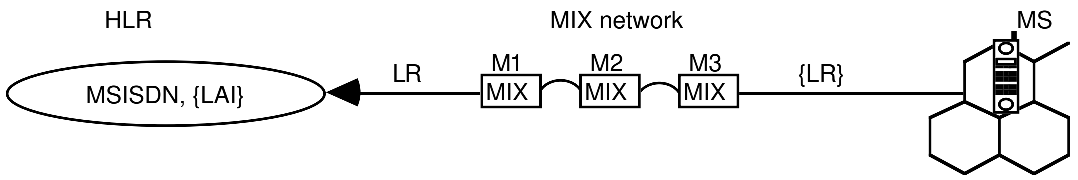

Fig. 5: Location registration with central and covered storage of the location information

The HLR stores the covered return address {LAI} instead of the plain LAI.

Because the TMSI is encoded in the {LAI}, it does not need to be stored explicitly.

In case of a location update, the HLR is informed of the new {LAI}, and the old {LAI} expires.

It is important to know that (according to the MIX functionality "ignore repeats of messages") each {LAI} can only be used once.[6] This means that after a transaction caused by the HLR a new {LAI} is needed. For permanent reachability of the MS, it transmits a new {LAI} after each transaction or a set of {LAI}s for more sophisticated interactions.

---

5 The symbol k_x with some subscript x will always denote a key of the symmetric cryptosystem, c_x and d_x public and private keys of the asymmetric cryptosystem; encryptions and decryptions of a message N are denoted by $k_x(N)$, $k_x^{-1}(N)$, $c_x(N)$, and $d_x(N)$, resp. The subscript denotes the owner of the key.

6 The MIX ignores repetitions of sent messages in order to prevent replay attacks. The deterministic decryption of these messages would "uncover" the relation between the incoming and outgoing messages.

5.3 Call Setup (mobile terminated)

In the case of an incoming call, the stored record of the MSISDN is read. The {LAI} contains the address A_{M1} of the first MIX. Beyond this point, the HLR has no routing information for the message call_setup_msg!

MIX M1 finds the address A_{M2} and k_{M1} to encode the call_setup_msg. The encoding of the message is the (symmetric) encryption k_{M1}(call_setup_msg).

Through the MIXes M1, M2 and M3, the encoded message

{call_setup_msg} := $k_{M3}(k_{M2}(k_{M1}($call_setup_msg$)))$

is generated. It is addressed with the TMSI and broadcasted to the location area.

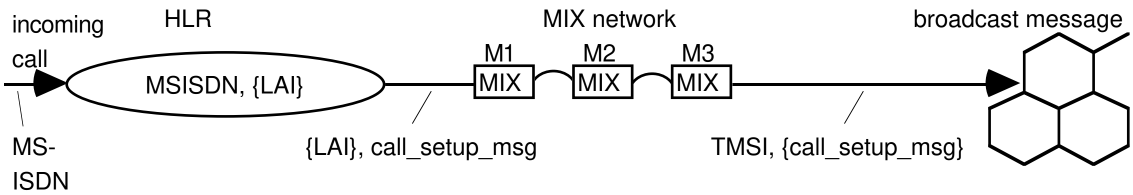

Fig. 6: Call setup with central and covered storage of the location information

The MS decodes the message {call_setup_msg} by decrypting with k_{M3}, k_{M2} and k_{M1}. Therefore, it must store or reconstruct these keys. The TMSI indicates the relation to an {LAI}. This means that the MS does not store the {LAI} but the TMSI instead and derives the k_{Mi} (i=1..3) directly from the TMSI as suggested in this paper.

6 Efficiency

The use of asymmetric cryptography in MIX networks leads to a message expansion. However, the bandwidth on the air-interface is limited. The following section proposes optimizations of the ideas described above.

6.1 Trusted Base Transceiver Station (trusted BTS)

Because of the small bandwidth on the air-interface, the BTS could act as an extension of the MS, and it could generate and transmit the {LAI}s. In this case, the BTS must be trustworthy to the MS, i.e. it is identified and authenticated as a trusted BTS.

To reduce the ability of locating (by means of the radio waves), this organizational condition is possibly acceptable. Consequently, the MIX functionality works only in the fixed network.

6.2 Generating {LAI} Sets

As mentioned above, each {LAI} can only be used once. Therefore, it is desirable to hold a set of {LAI}s in the HLR.

A further measure for reducing the bandwidth on the air-interface in location update situations is to reference existing[7] {LAI}s of different location areas with a short index. Of course, the transfer of the {LAI}s to the HLR requires more bandwidth than plain method described above. Moreover, additional memory capacity is needed in the HLR.

The problem of limited bandwidth does not exist if the MS is roaming in an area with low traffic or if the MS is "connected" to the fixed network.[8] In these situations the MS can transmit {LAI} sets to the HLR. A similar situation is given by the end of an existing connection (e.g. a normal call). The existing radio channel could be used to transmit some {LAI}s.[9]

The following types of {LAI} sets can be distinguished:

a) {LAI} sets of the present roaming area. This variant is restricted to the MS staying within a single location area. These {LAI} sets can be transmitted at the end of a call connection.

b) {LAI} sets of different roaming areas previously visited by the MS. In this variant, it is assumed that an MS revisits these areas.

c) {LAI} sets of different areas preferred by the MS to be visited. This variant requires intelligent mobility analysis strategies in the MS.

In particular, b) and c) may increase the efficiency of the location management (especially location update).

It is not necessary to transmit the short indices while transmitting the {LAI} sets. With the help of a globally known hash function h, the index (i.e. the hash value) of a {LAI} is calculated by $h(\{LAI\})$ and stored together with the {LAI}. The hash value must be sufficiently long to avoid collisions of indices.

The MS must also store the hash value $h(\{LAI\})$. It is not necessary to store the {LAI} itself, but the relation to the location area must be stored. Furthermore, the MS must store the accompanying TMSI (and possibly the k_{Mi}).

If the {LAI} is already stored in the HLR while a location is being updated, the MS transmits only the index of the {LAI}.

---

7 stored in the HLR

8 The mobile networks of the 3rd generation (Universal Mobile Telecommunication System, UMTS, and Future Public Land Mobile Telecommunication Network, FPLMTN) distinguish between home, business, and public environments with different mobility levels and bandwidths.

9 In this way, another problem may be solved. The disconnection of several MS' occurs simultaneously if discrete time slots (e.g. the full minute and the 30th second of a minute) are used. Thereby the linkability of subscriber actions is reduced.

6.3 Trusted Fixed Station (trusted FS)

If a trusted Fixed Station (trusted FS) is installed instead of, or in addition to, a telephone in the fixed network, the short "plain" LAI can be transmitted to the trusted FS. The covered {LAI}s can be generated in the trusted FS and transmitted to the HLR. Of course, the MS must know the TMSIs and the k_{Mi}!

However, the strength of the proposed procedures is that a trusted FS is unnecessary, at least from the security and privacy point of view.[10] This offers new opportunities to "decentralize" the procedures which will be demonstrated in the following sections.

7 Multi-staged Storage of Location Information with Pseudonyms but without MIXes

The following measures reduce the signalling load during the location update process under central storage of location information if the distance between the HLR and the location area is large.

We put the situation described in Fig. 3 into a concrete form in terms of privacy aspects. For example, we use a 3-stage storage (Ri with i=0..2) of location information (see Fig. 7).

7.1 Call Setup (mobile terminated)

For a mobile subscriber with a MSISDN, the HLR (also denoted as R0) stores the address of the next register (A_{R1}) which, in turn, stores the location information of the mobile subscriber. The HLR also stores a pseudonym P1 which is not linkable to anything.[11]

The register R1 uses the pseudonym P1 to store the address of the next register (here A_{R2}) and a pseudonym P2.

The register R2 uses the pseudonym P2 to store the LAI and the implicit address TMSI for the broadcast message on the air-interface.

This system results in a pseudonymously chained list which describes the location information for the MS. When a call comes in, the chaining is processed.

For the security of the described procedure, we assume that not all Ri conspire together as one attacker. The HLR plays a special role in that. Without cooperation from anyone it can assign coarse location information to the MSISDN, provided the address of R1 represents a location (respectively a served area similar to the VLR in GSM networks).

The message call_setup_msg is unique in the whole network. As a result, no linkability is possible via call_setup_msg! In this way, we can take advantage of this "small (signalling) message space".

---

[10] There are other proposals using a trusted FS that may be more efficient than our procedures (see [KFJP_95, FJKP_95]). However, in this proposals the trusted FS is *necessary for security and privacy*!

[11] It can be computed by a true random generator.

Replay attacks are another problem. An attacker who does not control all Ri can intercept a connection request message and send it to the Ri again. Because of the deterministic process, the Ri would create the same output message, and the "path" of the message would be recognizable. Therefore, each pseudonym may only be used once (similar to a {LAI} in the previous sections).

A solution for this problem is a modification of the pseudonyms, either after each use or periodically.

If a global time base T is used, the pseudonyms switch forward at each time step. In this case the switching does not depend on the transactions. If the switching is processed by a globally known cryptographic function *f*, the MS must send an initial value P_{init} for the location update, or location registration where P_{init} can be a random number. The pseudonyms are calculated according to the rule $Pi := f(T, P_{init})$.

Alternatively, the switch of the pseudonyms is calculated by the successor function $Pi' := f(Pi, k_{Pi})$ from the current pseudonym Pi. The required "secrets" (keys) k_{Pi} are only known to the two Ri, which use a common pseudonym (e.g. R0 and R1 regarding P1; R1 and R2 regarding P2).

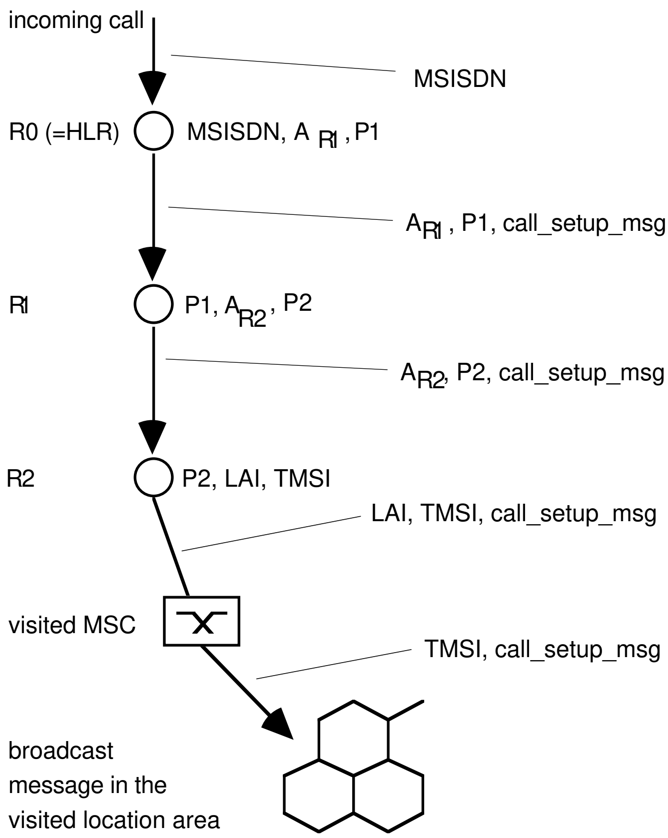

Fig. 7: Call setup with 3-staged pseudonymous location management without MIXes

7.2 Location Registration and Location Update

The terms “location registration” and “location update” are used in this paper for the process through which the registers Ri are informed of the records they must store. If the distance to the location area decreases with increasing i, the signalling load will be reduced.

For location registration and location update, the MS must know the potentially usable Ri. It is desired that the MS can them select from many Ri on all stages. This diversity achieves the independence of the Ri. An anonymous directory service – e.g. the “blinded read operation” described in [CoBi_95] – could be a proper solution for gathering information about favorable Ri. Using this service, the MS can read the directory entries for the visited area in an anonymous and unobservable manner.

For a location update, only the MS decides which records must be updated in which Ri. The MS decides when it must change to another register.

An MIX network (sender anonymity scheme) is also used for the unlinkability between the sender (i.e. the MS) and recipient (i.e. the registers Ri).

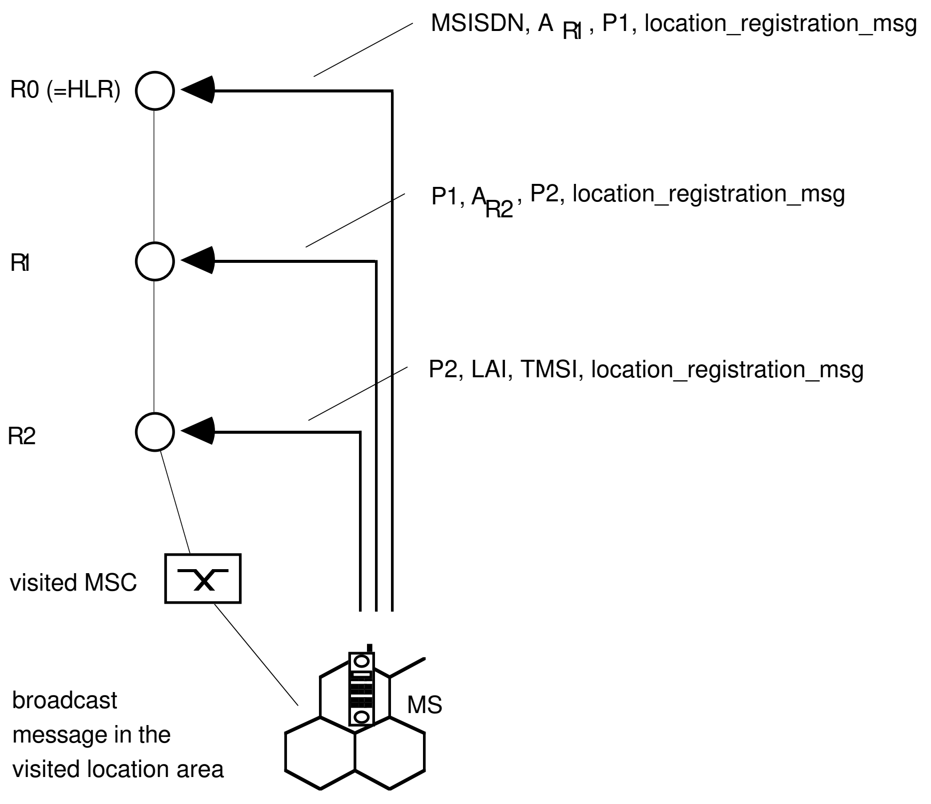

Fig. 8: Location registration with 3-staged pseudonymous location management without MIXes

8 Multi-staged Location Management with Pseudonyms and MIXes

So far, we have assumed that the Ri do not conspire (work together) as one attacker. In reality, this would be too hard to achieve because many available registers can belong to one network operator.

If an attacker can observe all communication in the entire network, he can moreover recognize all communication relations if no untraceable network is used.

The registers store the signalling messages, wait until other connection messages are received, and then sends them out in one batch. This system reduces the linkability of signalling messages.

The use of an MIX network makes multi-staged location management applicable without the above mentioned limitations of security.

Here, each Ri stores an untraceable return address {Ri+1} generated by the MS. Ri+1 and Pi+1 are included in {Ri+1}. Thus, neither Ri+1 nor Pi+1 is recognizable by the register Ri. Even if all Ri conspire, they are not in a position to uncover the location of the MS.[12]

8.1 Call Setup (mobile terminated)

An incoming call is processed in the following way (example for the three registers R0, R1 and R2, see Fig. 9).

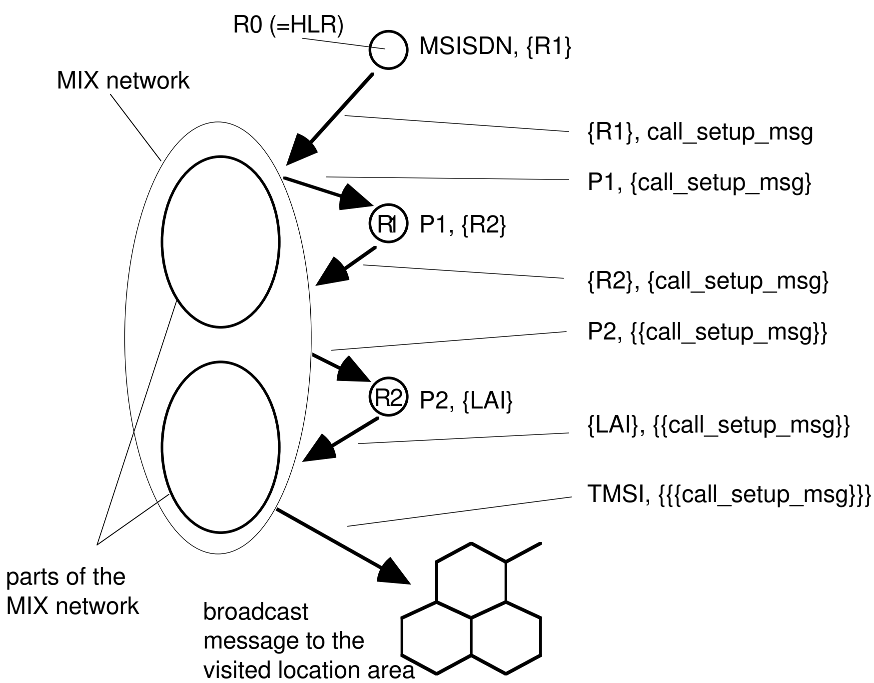

Fig. 9: Call setup with multi-staged pseudonymous location management with MIXes

12 Untraceable return addresses *force* the registers Ri to use the MIX network.

The HLR (R0) sends a connection request message call_setup_msg – "addressed" with covered {R1} into the MIX network.

The register R1 receives P1 and the encoded message {call_setup_msg} and passes the message {call_setup_msg} to the MIX network – prefixed with the untraceable return address {R2}.

The register R2 receives P2, and the "re-encoded" message {{call_setup_msg}} sends {{call_setup_msg}} into the MIX network again – addressed with the covered {LAI}.

Finally, the MS receives the TMSI and the three times covered connection request message {{{call_setup_msg}}}.

The MS must decode this message with all k_{Mi} used "along" its path through the MIX network.

The procedure is described assuming a "classic" MIX network[13]. If no linkable information is contained in the (signalling) messages, as is assumed in the above sections, the expensive change of encoding in the MIXes is unnecessary. Passing the messages (without encoding) through the MIXes would be sufficient to ensure security. However, the MIXes need to know that the incoming messages are signalling messages without any linkability. For the use of a common classic MIX network, the described form with encoding is useful.

8.2 Security and Efficiency

Even if all registers would conspire as one attacker, they would not even be able to trace the messages they send to themselves, because of the use of untraceable return addresses generated by the MS.

The security of our procedures – that is the privacy of the location information – depends on the security of the MIX network. The only purpose of using the registers is to increase the efficiency of the location management (similar to GSMs functional division of the location management between the HLR and the VLR).

The use of MIXes geographically close to the Ri is recommended to prevent an unnecessary reduction of efficiency.

9 Conclusions

The outlined procedures do not require a trustworthy fixed station for location management without recordable moving tracks of mobile subscribers. The security of the procedures is based on the security of asymmetric (public key) cryptography, whereas the procedures at best are complexity theoretically secure. The design principle "diversity" – realized in the multi-stage storage of the location information – was used to increase the security.

[13] Store incoming messages, discard repeats, change encodings and reorder them, and put them out as a single batch.

It is interesting to note that the recipient anonymity scheme (i.e. untraceable return addresses) is not directly used to hold the recipient (the MS) anonymously. After all, the HLR "knows" the identity of the mobile subscriber – the MSISDN. The untraceable return addresses are only used to hide the routing information and thereby the location of the MS in cellular networks.

It is worth stating at this point that the use of MIXes in this paper refers only to signalling processes in mobile communications. The efficient use of MIX networks to protect the communication relations (and the exchange of user data) between fixed stations in fixed networks is described in the literature (e.g. in [PfPW_91]); however, its use in mobile communications corresponds to these measures to a great extend.

Finally, the small bandwidth on the air-interface conflicts with the increasing signalling overhead of the new procedures. The construction and use of a trusted BTS (see section 6.1) may be the remedial action.

The application of the procedures to mobile networks using only personal mobility – i.e., the mobile subscriber has no mobile station but can use his personal communication environment at all fixed terminals – however, seems possible because a broadband network (but no air-interface) is used.

10 References

Chau_81 D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

CoBi_95 D. A. Cooper, K. P. Birman: Preserving Privacy in a Network of Mobile Computers; 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

FeTh_95 H. Federrath, Jürgen Thees: Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern; Datenschutz und Datensicherung, DuD 6/95, 338-348.

FJKP_95 H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann: Security in Public Mobile Communication Networks; Proc. of the IFIP TC 6 International Workshop on Personal Wireless Communications, Verlag der Augustinus Buchhandlung Aachen, 1995, 105-116.

GSM_93 ETSI: GSM Recommendations: GSM 01.02 - 12.21; February 1993, Release 92.

Hets_93 T. Hetschold: Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes; GMD-Studien Nr. 222, Oktober 1993.

KFJP_96 D. Kesdogan, H. Federrath, A. Jerichow, A. Pfitzmann: Location Management Strategies increasing Privacy in Mobile Communication Systems; in: Information Systems Security. Facing the information society of the 21st century. Proc. of the IFIP SEC '96 12th International Information Security

Conference 21 - 24 May, 1996, Island of Samos, Greece, Chapman & Hall, 1996.

Pfit_93 A. Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung, DuD 17/8 (1993), 451-463.

PfPW_91 A. Pfitzmann, B. Pfitzmann, M. Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead; Proc. IFIP/Sec'91, May 1991, Brighton, North-Holland, Amsterdam 1991, 245-258.

PfWa_87 A. Pfitzmann, M. Waidner: Networks without user observability; Computers & Security 6/2 (1987) 158-166.