M. Zitterbart (Hrsg.): Kommunikation in Verteilten Systemen (GI Fachtagung 19.-22.2.97 in Braunschweig), Informatik aktuell, Springer Heidelberg, 1997, Seite 77-91

Ein Vertraulichkeit gewährendes Erreichbarkeitsverfahren*

Schutz des Aufenthaltsortes in künftigen Mobilkommunikationssystemen

Hannes Federrath, Elke Franz, Anja Jerichow, Jan Müller, Andreas Pfitzmann

Technische Universität Dresden, Institut für Theoretische Informatik, 01062 Dresden
{federrath, ef1, jerichow, jm4, pfitza}@inf.tu-dresden.de

Zusammenfassung

Es wird ein Verfahren zur Verwaltung von Aufenthaltsinformationen in Mobilkommunikationssystemen vorgestellt. Dabei wird von dem in existierenden Netzen verwendeten Konzept der mehrstufigen Speicherung von Aufenthaltsinformationen ausgegangen. Das Verfahren erfüllt die Datenschutzforderung nach Vertraulichkeit des Aufenthaltsorts von Mobilkommunikationsteilnehmern. Es ermöglicht die Speicherung unterschiedlich granularer, geographischer Aufenthaltsinformationen unter Pseudonymen (statt der wahren Identität der Teilnehmer). Die Pseudonyme werden über Register unterschiedlicher Netzbetreiber miteinander verkettet. Somit ist die Erstellung von Bewegungsprofilen von mobilen Teilnehmern nicht möglich.

1 Motivation

Vertraulichkeit, Integrität und Verfügbarkeit sind grundsätzliche Forderungen an ein datenschutzgerechtes Kommunikationssystem. Dem Schutz des Aufenthaltsorts von Mobilkommunikationsteilnehmern als Teil von Vertraulichkeit wird in bestehenden Mobilkommunikationssystemen kaum Bedeutung beigemessen. Die Teilnehmer sind beobachtbar, da ihre Erreichbarkeit meist durch Speicherung der Aufenthaltsinformation gewährleistet wird. Zumindest dem Netzbetreiber ist so stets der aktuelle Aufenthaltsort jedes erreichbaren Teilnehmers bekannt.

1.1 Bestehende zellulare Funknetze

In einem zellularen Funknetz ist das Versorgungsgebiet gewöhnlich in Location Areas (LA) eingeteilt. Um einen mobilen Teilnehmer bei einem ankommenden Verbindungswunsch stets effizient erreichen zu können, muß dem Netz die aktuelle Location Area Identification (LAI) des Teilnehmers zur Signalisierung bekannt sein. Bewegt sich ein mobiler Teilnehmer von einem LA in ein anderes, löst seine Mobilstation (MS) *automatisch* ein Location Update (LUP) aus und meldet dem Netz so, vom Teilnehmer unbeeinflußt, seinen neuen Aufenthaltsort. Damit ist auch ein *passiver* Teilnehmer mit angemeldeter MS vom Netz stets verfolgbar, d.h. der Netzbetreiber kann *Bewegungsprofile* seiner Teilnehmer erstellen.

Im GSM (Global System for Mobile Communication) [GSM_93], einem zellularen Funknetz, werden die Aufenthaltsinformationen der Mobilteilnehmer aus Performancegründen *mehrstufig* im Home Location Register (HLR) und Visitor Location Register (VLR) gespeichert. So wird

* Wir danken der Deutschen Forschungsgemeinschaft (DFG) und der Gottlieb Daimler- und Karl Benz- Stiftung Ladenburg für die finanzielle Unterstützung. Für Anregungen, Diskussionen und Kritik geht unser Dank an Dagmar Schönfeld und Dogan Kesdogan.

im VLR die LAI des Teilnehmers hinterlegt, während im HLR die aktuelle VLR-Adresse gespeichert wird. Bild 1 veranschaulicht die Mehrstufigkeit der Speicherung in voller Allgemeinheit.

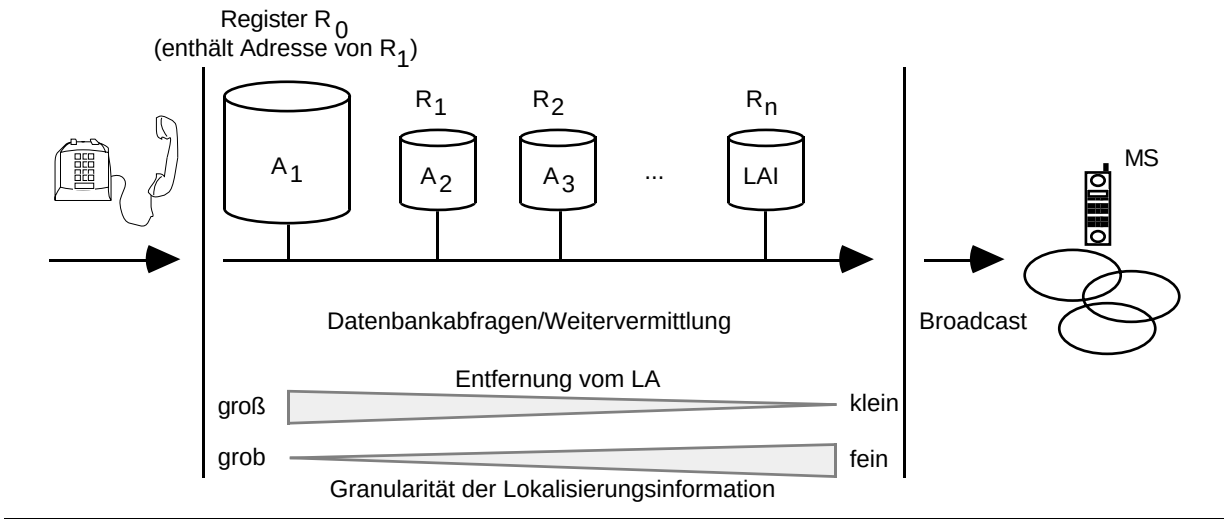

Bild 1: Mehrstufige Speicherung von Lokalisierungsinformation

Durch die Mehrstufigkeit sind in den einzelnen Ebenen des Netzes unterschiedlich genaue Lokalisierungsinformationen verfügbar. Das bringt beim LUP den Vorteil, daß stets nur die Register aktualisiert werden müssen, bei denen sich die Lokalisierungsinformation des Teilnehmers geändert hat. Dadurch erfolgt die LUP-Signalisierung meist nur über kurze Entfernungen im VLR-Bereich. Eine Signalisierung über große Entfernungen zum HLR ist nur selten erforderlich. Die Verteilung von Lokalisierungsinformationen führt dagegen zu einem aufwendigeren Verbindungsaufbau, da im Gegensatz zur zentralen Verwaltung zusätzliche Datenbankabfragen notwendig sind. Jedoch wird dieser Nachteil durch Einsparung an Bandbreite beim weitaus häufiger notwendigen LUP kompensiert.

Für den Datenschutz bedeutet diese Verteilung von Lokalisierungsinformation jedoch keine automatische Verbesserung. Zum einen hat ein Netzbetreiber in einem Mobilfunksystem wie GSM stets die globale Sicht auf alle Daten. Er kann also die verteilten Lokalisierungsinformationen verketten und Bewegungsprofile erstellen. Zum anderen wurden bisher noch keine Aussagen gemacht, unter welcher Identität die Datenbanken Lokalisierungsinformationen abspeichern. Im GSM-Netz erfolgt die Speicherung im HLR und VLR unter der Identität des Teilnehmers (der MSISDN, Mobile Subscriber ISDN Number bzw. der IMSI, International Mobile Subscriber Identity).

1.2 Künftige zellulare Funknetze

Ein künftiges System könnte verschiedene zellulare Funknetze integrieren. Das ist eine realistische Annahme. Z.B. ist bei UMTS (Universal Mobile Telecommunication System) [Mitt_94], einem in der Standardisierung befindlichen allgemeinen Mobilfunknetz, die Integration verschiedener Systeme geplant.

Das Eingliedern verschiedener Netze in ein Gesamtsystem erlaubt es, Daten unterschiedlich großer Versorgungsgebiete bei unterschiedlichen Betreibern zu speichern. Wir bezeichnen dies ebenfalls als mehrstufige Speicherung. Die Zellbereiche können sich dabei hierarchisch überlagern (siehe auch [FJKP_95]).

Im Bild 2 werden durch die verschiedenen Zellgrößen vier sich überlagernde Netze dargestellt, wobei das grau gezeichnete Netz einerseits ein separates, die anderen überlagerndes Netz darstellt. Andererseits übernimmt es auch Aufgaben als Gesamtsystem. Die drei schwarz dargestellten Netze versorgen Teilgebiete des alles überlagernden grauen Netzes. Jedem der Netze sind in den verschiedenen Ebenen Register R_i (i=0…3) zur Speicherung der Aufenthaltsinformationen zugeordnet. R_0 übernimmt ähnlich dem HLR in GSM eine zentrale Verwaltungsfunktion. In dem dargestellten Beispiel versorgt jeweils ein einzelnes Netz einen Bereich des Gesamtgebietes. Es ist jedoch wünschenswert, daß den Nutzern in jedem Bereich mehrere Netze bzw. Register verschiedener Betreiber zur Verfügung stehen, aus denen sie wählen können. Beispielsweise könnten neben R_2 noch die Register R_4 und R_5 existieren.

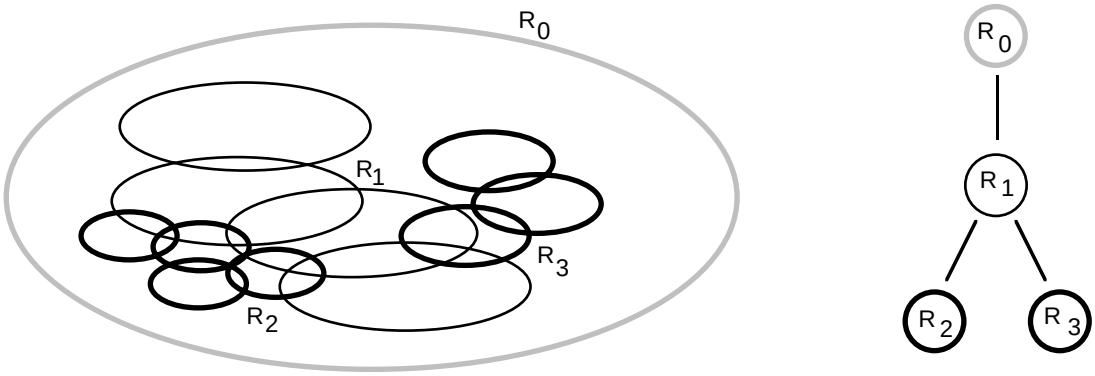

Bild 2: Integration verschiedener Netze

1.3 Mobilkommunikationssysteme der Zukunft

Ein in Zukunft vorstellbares System soll die Datenschutzforderung nach Anonymität, hier Erreichbarkeit ohne Verfolgbarkeit, gewährleisten und die Vorteile existierender Systeme nutzen. Eine Mobilstation muß häufiger ihren Aufenthaltsort zur Gewährleistung des Location Management signalisieren, als tatsächlich Verbindungen benötigt werden. Erreichbarkeit ohne Verfolgbarkeit bedeutet somit Schutz des Aufenthaltsortes während der Signalisierungsphase.

Folgendes ist von einem allgemeinen Mobilkommunikationssystem zu fordern.

- Mehrstufige Speicherung: Aufenthaltsdaten sollen verteilt in verschiedenen Registern R_i mit i=0…n gespeichert werden, wobei die Register *nicht* heimlich zusammenarbeiten. Das ist realistisch, wenn die Register mit Blick auf künftige Netze verschiedenen Betreibern unterstehen.
- Einsatz von Pseudonymen: Die Einträge der Teilnehmer in den Registern erfolgen unter Pseudonymen. Betreiber können die Identität eines Teilnehmers nicht mit seinem Pseudonym verketten. Ein Teilnehmer muß in der Lage sein, dem Netz seinen aktuellen Aufenthaltsort unter einem Pseudonym zu signalisieren.

In der Literatur [Hets_93, MüSt_95, Pfit_93, Walk_94] finden sich eine Reihe von Lösungen des Problems, die von einer vertrauenswürdigen Feststation ausgehen.

Im folgenden wird ein die Erreichbarkeit gewährleistendes Verfahren vorgestellt, das zum einen beim LUP effizient durch die mehrstufige Speicherung der Lokalisierungsinformation und zum anderen die Anonymität der mobilen Teilnehmer während der Signalisierungsphase gewährleistet. Die Verwendung von Kryptographie ist notwendig. Wir schlagen ein hybrides System vor, d.h. mittels asymmetrischer Verschlüsselung wird der Signalisierungspfad sehr aufwendig aufgebaut. Im Anschluß daran kann die Verbindung weniger aufwendig mittels symmetrischer

Kryptographie mehrfach genutzt werden, ohne den Schutz der Kommunikationsbeziehung aufzugeben.

2 Mehrstufige Speicherung mit Pseudonymen

Es wird die in [KeFo_95], [KFJP_96] und [FeJP_96] formulierte Idee aufgegriffen, Aufenthaltsinformationen mehrstufig und pseudonym zu speichern. Neue Ansätze bezüglich des Generierens der Pseudonyme werden vorgestellt.

2.1 Das allgemeine Prinzip

Gegeben sei ein Vermittlungsnetz. Die Knoten, hier Register genannt, speichern und verwalten die Lokalisierungsinformationen für die sich in bestimmten geographischen Bereichen befindlichen Teilnehmer. Teilnehmer am Kommunikationsverkehr sind unter einem definierten Namen, ihrer MSISDN, erreichbar. Ein Teilnehmer generiert mehrere Pseudonyme für seine Identität und hinterlegt in jedem Register ein Pseudonympaar. Nur das Register ist in der Lage, ein eingehendes Pseudonym mit einem ausgehenden zu verknüpfen. Diese Zuordnung wird im Text durch einen Pfeil $P_i \rightarrow P_{i+1}$ dargestellt. Im Wurzelregister R_0 ist der Teilnehmer unter seiner wahren Identität, der MSISDN, bekannt.

Jedes Register R_i muß also ein Pseudonym P_i sowie die Adresse A_{i+1} und das Folgepseudonym P_{i+1} des nächsten Registers R_{i+1} speichern. Das bedeutet, jeweils zwei Register teilen ein Geheimnis. Wenn man in der Lage ist, alle in den Registern gespeicherten Informationen zusammenzusetzen, so entsteht eine über Pseudonyme verkettete Liste, welche die Lokalisierungsinformation für die MS beschreibt.

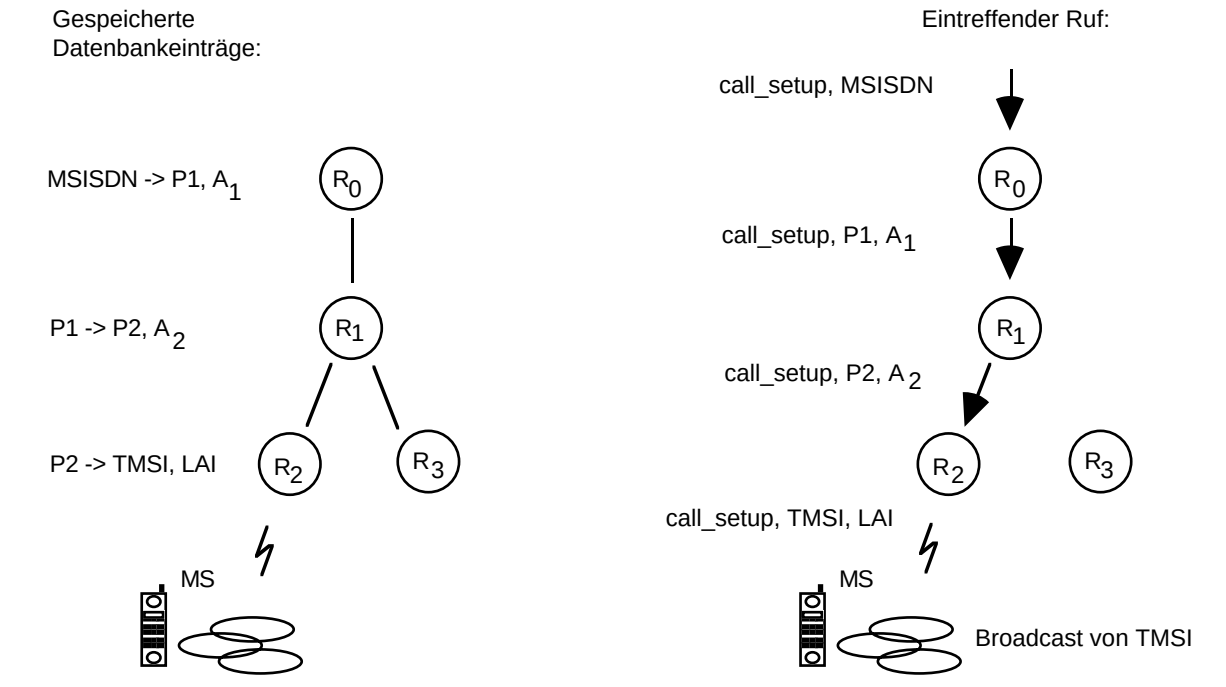

Bild 3: a) Beispiel für mehrstufige Verwaltung b) Erreichen einer MS

Bei einem ankommenden Ruf für MSISDN wird die Nachricht "call_setup" durch das Netz geschickt. Eine bei R_i ankommende Nachricht wird anhand des eingehenden Pseudonyms dem gespeicherten Folgepseudonym zugeordnet und an die Adresse von R_{i+1} weitergeleitet. Das

letzte Register der Kette speichert für sein Pseudonym die LAI und eine vom Teilnehmer generierte implizite Adresse TMSI (Temporary Mobile Subscriber Identity) für die Paging-Nachricht auf der Funkschnittstelle. Im Bild 3 kennt R_2 die Zuordnung P2 $\rightarrow$ TMSI, LAI.

Einem Register ist nur das gespeicherte Pseudonympaar P_i und P_{i+1} bekannt. In unserem Beispiel weiß der Betreiber des Registers R_1 nur, daß jemand mit dem Pseudonym P1 sich in dem durch A_2 beschriebenen geographischen Bereich aufhalten muß, an welchen es die Nachricht mit dem Pseudonym P2 weiterleitet. Selbst wenn ein Register korrumpiert ist, erhält es keine Information über die wahre Identität des Teilnehmers.

2.2 Angreifermodell

Wie in 1.2 und 1.3 beschrieben, ermöglicht die Eingliederung verschiedener unabhängiger Kommunikationssysteme in ein Gesamtsystem die Annahme, daß die Register der einzelnen Systeme zur Datenverwaltung nicht heimlich miteinander kooperieren. Aus dieser Annahme kann ein Angreifermodell abgeleitet werden. Ein Angreifermodell definiert die Stärke möglicher Angreifer. Ein System sollte möglichst starken Angriffen widerstehen können. Folgende Annahmen werden getroffen:

- Jegliche Kommunikation im Netz ist beobachtbar.
- In den Registern kann nicht gelesen werden, d.h. eingehende und ausgehende Pseudonyme sind nicht verkettbar.
- Die Register kooperieren nicht heimlich miteinander.
- Zwei benachbarte Register teilen ein Geheimnis, ein Pseudonym.

Um diese Forderungen zu erfüllen, sind an Register und Pseudonyme spezielle Anforderungen zu stellen. Kapitel 3 beschäftigt sich mit der Generierung der Pseudonyme.

Die Register empfangen und senden Nachrichten im Batch (auch Schub genannt), d.h. es werden entsprechend der Batchgröße Nachrichten erst gesammelt und dann *zu einem Zeittakt zusammen* weitergeleitet. Sonst wäre eine zeitliche Verkettung der Nachrichten möglich. Auch das Aussehen der Nachrichten muß sich ändern. Hierzu wird das den MIXen zugrundeliegende Konzept [Chau_81, PfPW_88, PfPW_91] genutzt: Ein MIX-Netz besteht aus mehreren MIXen und dient dem Schutz der Kommunikationsbeziehung zwischen Sender und Empfänger. Die Nachrichten werden im Batch von einem MIX zum anderen geschickt. In den MIXen erfolgt ein Umkodieren und Umsortieren der Nachrichten, so daß keine Rückschlüsse von den ein- auf die ausgehenden Nachrichten möglich sind. Aus diesem Grund wird auch die Länge der Nachrichten im gesamten Netz beibehalten, was als längentreue Umkodierung bezeichnet wird.

2.3 Verwaltung der Aufenthaltsinformation

Verwalten von Aufenthaltsinformationen (location management) bei der Signalisierung heißt Registrieren eines Teilnehmers, Aktualisieren seiner Aufenthaltsinformationen in den Registern und Abmelden.

2.3.1 Aufenthaltsregistrierung

Die Aufenthaltsregistrierung besteht darin, den Knoten R_i (i = 0...n) mitzuteilen, welchen Eintrag sie vorzunehmen haben. So kann später die Mobilstation effizient und mit geringem Signalisierungsaufwand erreicht werden.

Hierzu muß die Mobilstation jedoch wissen, welche R_i (i=0...n) für eine Registrierung in Frage kommen. Es ist außerdem wichtig, daß die MS zwischen vielen R_i unterschiedlicher Betreiber in jeder Ebene wählen kann (siehe 1.2). Dadurch wird die Vertrauenswürdigkeit verbessert. Die verfügbaren Register der verschiedenen Aufenthaltsgebiete können gebroadcastet oder durch die Teilnehmer aus einer Datenbasis abgefragt werden. Das Lesen aus dieser Datenbank muß natürlich so geschehen, daß nicht erkannt werden kann, welche Einträge für welche LAs gelesen wurden. Eine mögliche Lösung dieses Problems ist das in [CoBi_95] vorgestellte "Blinde Lesen". Bei diesem Verfahren wird gewährleistet, daß die Interessensdaten der Lesenden nicht offenbar werden.

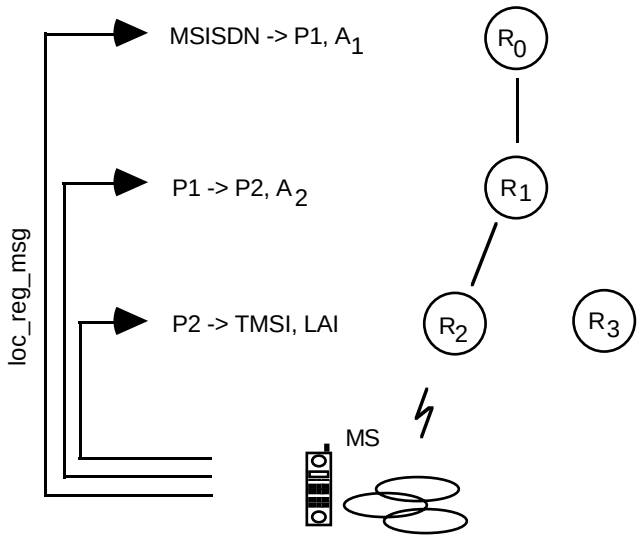

Bild 4: Location Registration

2.3.2 Aktualisieren der Register

Beim LUP erfragt die MS die für das Aufenthaltsgebiet verfügbaren Register (siehe 2.3.1), aus denen sie nach bestimmten Kriterien, wie z.B. Lastsituation im Netz oder Vertrauenswürdigkeit des Betreibers, auswählt. Daraus ermittelt sie, in welchen Registern Einträge vorzunehmen bzw. zu erneuern sind und berechnet die zu signalisierenden Nachrichten.

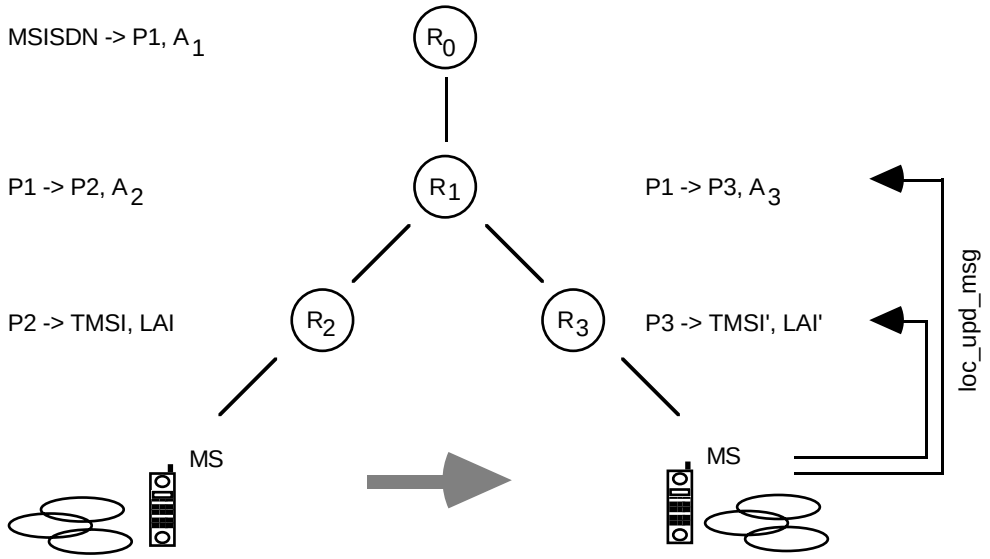

Bild 5: Location Update

Befinden sich die R_i mit wachsendem i näher beim LA, wird Signalisierungsaufwand im Fernbereich gespart, da nur die sich ändernden Lokalisierungsinformationen zu aktualisieren sind. Im Bild 5 bleibt z.B. der Eintrag von R_0 unverändert.

2.3.3 Abmelden

Die Daten der nicht mehr benutzten Register könnten nach einer bestimmten Zeit verfallen, oder es wird mittels einer Nachricht "Löschen" dies den entsprechenden Registern mitgeteilt.

Letzteres erscheint sinnvoll, da die Verbindung sonst auch dann aufgelöst werden könnte, wenn der Pfad längere Zeit nicht genutzt und die Zeitgrenze überschritten wird.

3 Pseudonymverwaltung

Einmal in den Registern hinterlegt, bilden die Pseudonyme einen *Signalisierungspfad*. Ziel der Verwendung der Pseudonyme als Kennzeichen ist es, einen einmal aufgebauten Pfad für die folgende Signalisierung (call setup, location update) effizient nutzen zu können. Ein Pfad wird mehrfach genutzt, ohne erneut den Registrierungsprozeß zu durchlaufen.

3.1 Forderungen an die Pseudonyme

- Das Hinterlegen der Pseudonyme in den verschiedenen Registern muß so erfolgen, daß nicht zugeordnet werden kann, welche MS die Nachricht gesendet hat. Sie müssen anonym hinterlegt werden.
- Um replay-Angriffe zu verhindern, darf ein Pseudonym nur einmal verwendet werden.
- Der Teilnehmer muß die Datensätze in den Registern aktualisieren können, da ein LUP immer von ihm initiiert wird.
- Die Gültigkeit der Pseudonyme ist zeitlich begrenzt.

Die Forderungen können durch die Verwendung eines "Zählers" (oder einer Zeitbasis) erfüllt werden, indem nach jeder Pseudonymverwendung (bzw. einer abgelaufenen Zeit) ein neues Pseudonym über einen Pseudozufallszahlengenerator generiert wird. Es wäre auch möglich,

über eine global einheitliche Zeitbasis T die Pseudonyme synchron weiterzuschalten. Die Weiterschaltung wäre dann unabhängig von den zu übermittelnden Nachrichten. Wenn das Schalten über eine global bekannte Funktion f erfolgt, muß die Mobilstation beim Einbuchen bzw. LUP einen Initialwert[1] $P_{i,init}$ senden, über den die Pseudonyme nach der Vorschrift $P_i' := f(T,P_{i,init})$ gebildet werden. Das Hinterlegen der Pseudonyme könnte durch MIXe erfolgen. Das bedeutet, jedes Register ist Empfänger einer Nachricht $[P_i \rightarrow P_{i+1},A_{i+1}]$. Diese wird unter Wahrung der Anonymität der MS von ihr über das MIX-Netz an die Registerknoten übermittelt.

Statt jedes Pseudonym separat zu hinterlegen, könnten die Register zusätzliche Funktionen übernehmen. Ähnlich zu den MIXen sammeln die Register bereits die ankommenden Verbindungswünsche und schicken sie im Batch weiter. Die MS könnte denselben Weg nutzen, um von ihr generierte Pseudonyme in den entsprechenden Registern zu hinterlegen.

Im Gegensatz zu den MIXen sind die Register an geographische Bereiche gebunden. Durch Batchbetrieb und längentreue Umkodierung der Nachrichten kann jedoch keine Zuordnung erfolgen, vorausgesetzt die Anzahl der übermittelten Nachrichten ist groß genug. Gegebenenfalls müssen in den Registern bedeutungslose Nachrichten generiert werden, um diese Bedingung zu gewährleisten. Die Register kennen nur die Adresse des jeweils nächsten Registers. Eine Verkettung der Lokalisierungsinformation ist nur dann möglich, wenn die Register verdeckt zusammenarbeiten. Dies widerspricht aber dem Angreifermodell.

3.2 Generieren der Pseudonyme

3.2.1 Aufenthaltsregistrierung

Die Pseudonyme werden von der MS generiert und bei der Aufenthaltsregistrierung hinterlegt. In den Registern soll jeweils ein Datensatz $[k_i,P_i \rightarrow P_{i+1},A_{i+1}]$ gespeichert werden. Hierzu wird an ein Register R_i jeweils eine Nachricht $m_i := c_i(A_{i-1},k_i,P_i \rightarrow P_{i+1},A_{i+1},m_{i-1})$ geschickt. A_{i-1} ist die Adresse des Registers, an welches "loc_reg_msg,m_{i-1}" weitergeleitet wird. k_i ist der zum späteren Umkodieren der Nachrichten notwendige symmetrische Schlüssel. P_i und P_{i+1} sind die in den Registern gespeicherten Pseudonyme. A_{i+1} ist die für die Signalisierung eines Verbindungswunsches (call_setup) notwendige nächste Zieladresse.

[1] z.B. eine Zufallszahl, entspricht dem beim Einbuchen hinterlegten Pseudonym

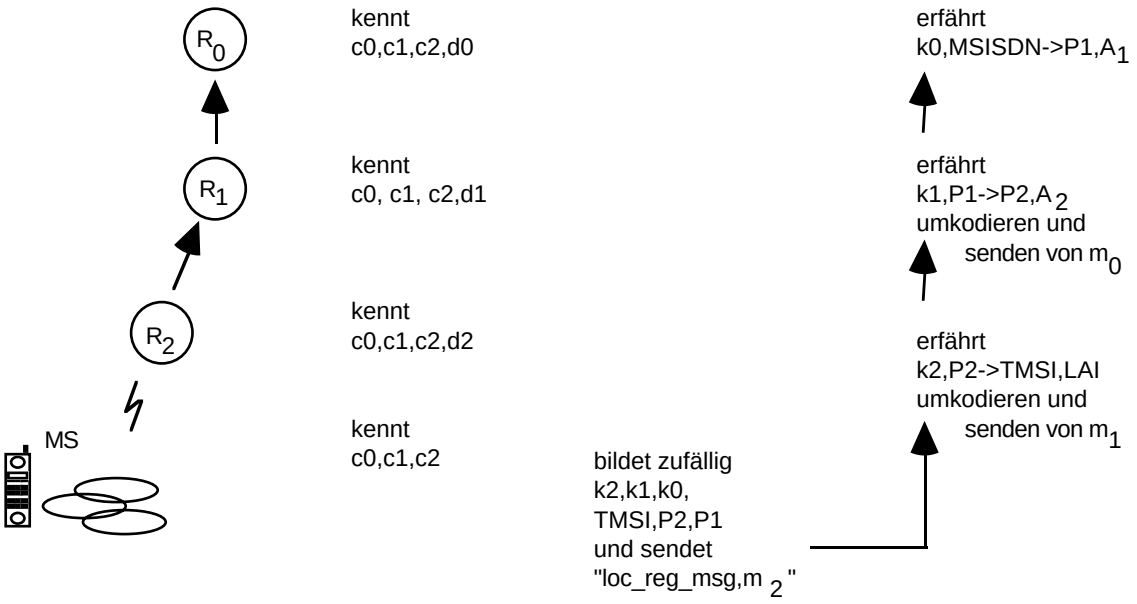

Bild 6: Veranschaulichung des Einbuchens

Der Teilnehmer benötigt ein Kennzeichen, um die Datensätze im Register zur Pseudonymberechnung bzw. -hinterlegung nach einer Signalisierung ansprechen zu können. Solche Registerkennzeichen müssen deshalb vom Teilnehmer generiert werden bzw. dem Teilnehmer bekannt sein. Es bietet sich an, den symmetrischen Schlüssel, der im Datensatz enthalten ist, hierfür zu nutzen (siehe auch 3.3).

Will eine MS einbuchen, wird nach Auswahl der zu durchlaufenden R_i mit i=0…n sowie dem Generieren der Pseudonyme für die R_i eine Nachricht m_n folgendermaßen gebildet.

$$m_0 := c_0(k_0,\text{MSISDN}\rightarrow P_1,A_1)$$

$$m_i := c_i(A_{i-1},k_i,P_i\rightarrow P_{i+1},A_{i+1},m_{i-1}) \qquad \text{für } i=1\ldots n$$

MS schickt die Nachricht N := "loc_reg_msg,m_n" an das erste, ihr zugängliche Register R_n, wobei A_{n+1} der eigenen Ortsinformation, der LAI, und P_{n+1} der TMSI entspricht.

Kommt also m_i bei R_i an, so wird m_i mit dem privaten Schlüssel d_i (passend zu c_i) des Registers entschlüsselt. Die in m_i mitgeschickten Pseudonyme P_i und P_{i+1} werden gemeinsam mit k_i und A_{i+1} als Datensatz in R_i gespeichert. A_{i+1} ist die Adresse, an die später ein bei R_i anliegender Verbindungswunsch weitergeleitet werden soll. Der Rest der Nachricht wird an die beim Entschlüsseln gefundene Folgeadresse A_{i-1} mit dem Vermerk "loc_reg_msg" weitergeschickt.

R_0 erkennt sich als Empfänger, da keine Adresse angegeben ist, an die die angekommene Nachricht weiterzuleiten ist. In R_0 werden die MSISDN, die Abbildung auf das erste Pseudonym P_1 und die beim "call_setup" notwendige erste Zieladresse A_1 gespeichert.

3.2.2 Aufenthaltsaktualisierung

Die MS bewegt sich von einem LA in ein anderes. Um am neuen Aufenthaltsort erreichbar zu sein, muß der Signalisierungspfad aktualisiert, also teilweise neu aufgebaut werden. Die MS generiert für die neuen Register die relevanten Daten. Entsprechend dem Einbuchen werden

diese Informationen in der Nachricht "loc_update,m_m" kodiert, die an das Register R'$_m$ im neuen LA geschickt wird[2].

Ein Vorteil der mehrstufigen Speicherung ist, daß nicht mehr der gesamte Pfad neu aufgebaut werden muß. In den neuen Registern erfolgt im Prinzip eine Aufenthaltsregistrierung, wirklich aktualisiert wird nur das tiefste, für alten und neuen Signalisierungspfad gleichgebliebene Register R_k. In R_k wird ein neuer Datensatz (z.B. in Bild 7 [k1,P1→P3,A3]) eingetragen.

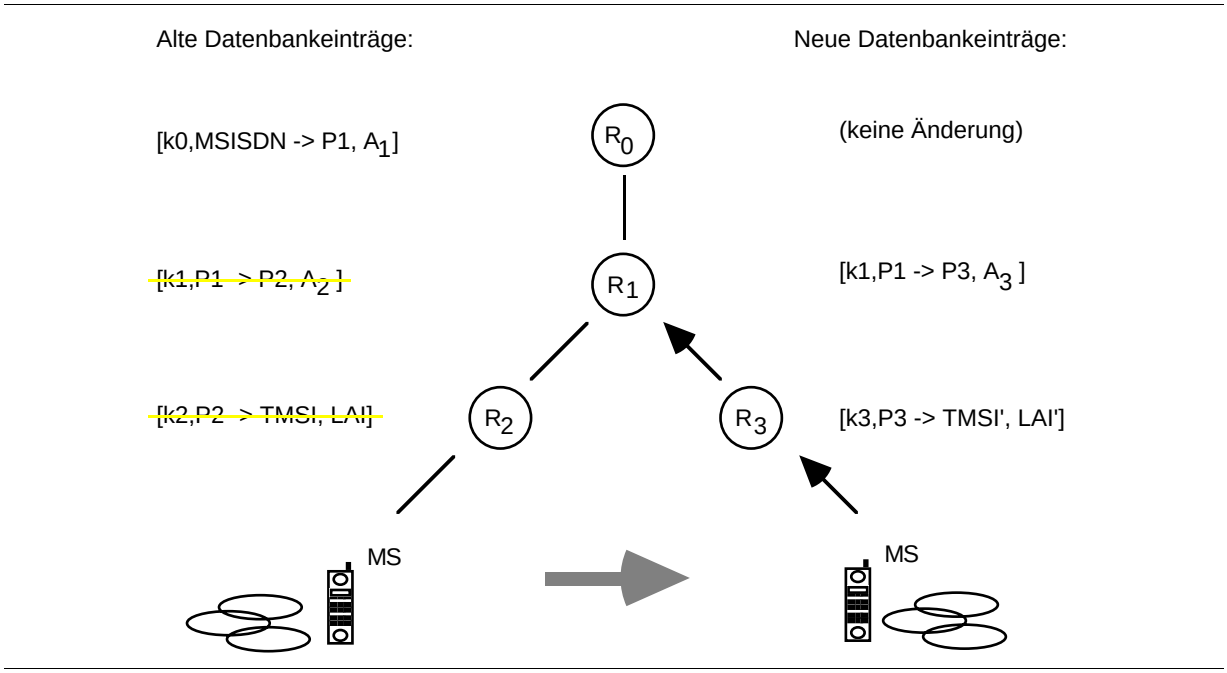

Bild 7: Beispiel für konkretisiertes Location Update

Der Pfad wird umgelenkt. Am mitgesendeten Vermerk "loc_update" erkennt das Register im Umlenkpunkt die ankommende Nachricht. Um die symmetrisch verschlüsselte Nachricht entschlüsseln zu können, muß es alle gespeicherten Schlüssel durchprobieren. Am gleichbleibenden k_k bzw. P_k wird beim Signalisieren eines Verbindungswunsches der neue Signalisierungspfad zu R'$_{k+1}$ mit A'$_{k+1}$ erkannt. In R_k wird die Nachricht mit der neuen Folgeadresse A'$_{k+1}$ und dem zugehörigen neuen Initialwert P'$_{k+1}$ für das nächste Register eingetragen. Die Nachricht m_m wird wie folgt gebildet:

$$m_k := k'_k(P_k \rightarrow P'_{k+1}, A'_{k+1})$$

$$m_i := c'_i(A'_{i-1}, k'_i, P'_i \rightarrow P'_{i+1}, A'_{i+1}, m_{i-1}) \quad \text{für } i=k+1\ldots m$$

wobei P'$_{m+1}$ der neuen TMSI' und A'$_{m+1}$ der neuen LAI' entspricht. Die Datensätze der Register des alten, nicht mehr benötigten Teils des Signalisierungspfades, also der Register R_i (mit i=k+1…n), können wiederum durch eine Löschmeldung freigegeben werden, bzw. sie verfallen nach einer bestimmten Zeit.

Da die Pseudonyme nur einmal verwendet werden, entsteht für die MS zusätzlicher Aufwand. Sie muß die an die Register geschickten Pseudonyme speichern und bei jeder Neuberechnung der Pseudonyme den gespeicherten Stand aktualisieren. Es bietet sich also die oben beschriebene Variante der global einheitlichen Zeitbasis an. Dann braucht erst bei einer Aufenthaltsaktualisierung die in 3.1 erwähnte Vorschrift zur Berechnung von P_i angewendet zu werden. Eine andere Möglichkeit wird im folgenden Abschnitt beschrieben.

---

[2] Als Index wird hier "m" verwendet, da die Anzahl der Register im neuen Signalisierungspfad nicht zwingend gleich der Anzahl "n" im alten Pfad ist. Es kann auch m>n oder m<n gelten.

3.3 Effizientes Generieren der Pseudonyme

Wenn der Teilnehmer alle Pseudonyme generieren muß, so entsteht beträchtlicher Übertragungsaufwand, da bei der Aufenthaltsregistrierung asymmetrisch verschlüsselt werden und die Längentreue gewährleistet sein muß.

Der Aufwand läßt sich möglicherweise senken, indem die Pseudonyme in den Registern gebildet werden. Der Teilnehmer generiert nur den Startwert für das erste Register. Auf die Bildung der Pseudonyme in den Registern hat er keinen Einfluß mehr. Damit ein Outsider aus den von Register zu Register übertragenen Pseudonymen kein Wissen erlangt, haben die Register jeweils ein Geheimnis miteinander ausgetauscht, z.B. eine Zufallszahl (oder besser einen kryptographischen Schlüssel). Somit kann ein Outsider keine Folgepseudonyme berechnen und auch Pseudonyme untereinander nicht verketten.

Um den in 3.2.2 beschriebenen Prozeß der Aufenthaltsaktualisierung durchzuführen, muß jedoch auf die Register zugegriffen werden können. Der MS sind nur die Adressen der Register und die von ihr generierten symmetrischen Schlüssel bekannt. Wie bereits in 3.2.1 erwähnt, ist k_i als ein eindeutiges Kennzeichen dafür geeignet. Statt Einführung eines neuen Merkmals kann dieser Schlüssel als Registerkennzeichen genutzt werden.

Das Wissen wird im Netz verteilt gespeichert. Die Pseudonyme zur Nutzung des Signalisierungspfades bleiben der MS verborgen. Der Teilnehmer kann in den Prozeß nur über die Schlüssel und die Auswahl der Register eingreifen. Die Verwaltung der Pseudonyme obliegt dem Netz.

3.3.1 Aufenthaltsregistrierung

Will sich eine MS im Netz einbuchen, werden die zu durchlaufenden Register R_i (i=0...n) ausgewählt. Die MS schickt die Nachricht "loc_reg_msg,m_n,T_{init}" an das erste Register R_n. T_{init} ist der Initialwert für die Pseudonymbildung.

$$m_0 := c_0(k_0,\text{MSISDN},A_1)$$

$$m_i := c_i(A_{i-1},k_i,A_{i+1},m_{i-1}) \qquad \text{für } i=1\ldots n$$

wobei A_{n+1} der LAI entspricht. Aus T_{init} wird das erste Pseudonym für R_n gebildet und als Pseudonympaar $P_n \rightarrow T_{init}$ gespeichert.

Vom Register R_i wird m_i sowie ein in R_{i+1} gebildetes Pseudonym P_{i+1} empfangen. Als erstes wird mittels privatem Schlüssel d_i die Nachricht entschlüsselt. Die Entschlüsselung $d_i(c_i(A_{i-1},k_i,A_{i+1},m_{i-1})$ ergibt die nächste Registeradresse A_{i-1}, den symmetrischen Schlüssel bzw. das Registerkennzeichen k_i, die Rückadresse A_{i+1} für das call_setup und die Restnachricht m_{i-1}.

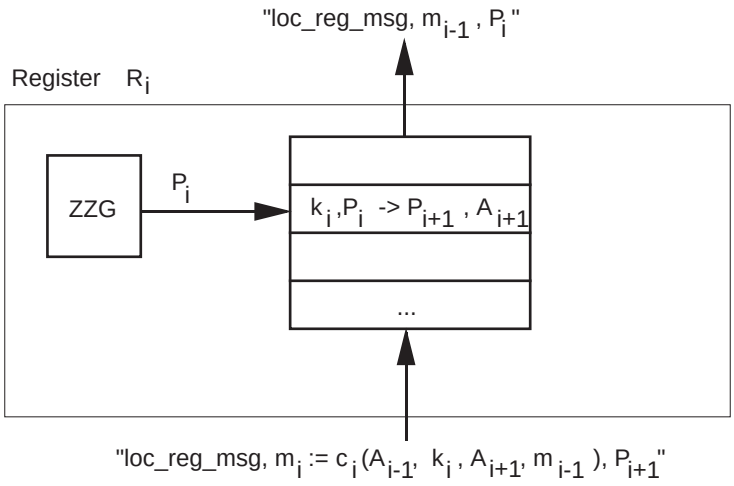

Bild 8: Allgemeines Schema zur Generierung der Startwerte bei der Registrierung

Durch "loc_reg_msg" initiiert, generiert das Register R_i unabhängig vom empfangenen P_{i+1} ein Pseudonym P_i mittels eines Zufallszahlengenerators (ZZG). Der Teilnehmer hat also keinen Einfluß auf die Pseudonymbildung. Nur R_i kann P_i und P_{i+1} miteinander verketten, beide Pseudonyme sowie Schlüssel und Rückadresse werden als Datensatz gespeichert. Die Restnachricht m_{i-1}, der Vermerk "loc_reg_msg" und das im Register gebildete P_i werden an das nächste Register übermittelt.

3.3.2 Aufenthaltsaktualisierung

Der Teilnehmer kennt die von ihm in den Registern hinterlegten k_i. Bei Änderung des Signalisierungspfades wird über die neuen Register R'_i mit i=m…k+1 bis zum k-ten Register R_k eine Aktualisierungsnachricht übermittelt.

An R'_m wird dabei die folgende Nachricht N := loc_update,m_m,T'_{init} geschickt, mit

$m_k := c_k(k_k,A_k)$

$m_i := c'_i(A'_{i-1},k'_i,A'_{i+1},m_{i-1})$ für i=k+1…m

Das Bilden der Pseudonyme erfolgt entsprechend dem Einbuchen.

3.3.3 Signalisieren eines Verbindungswunsches

Bei der Nutzung des Pfades zum Signalisieren (call_setup) werden eventuell nicht öffentliche Signalisierungsdaten (z.B. die Nummer eines ihn rufenden Teilnehmers oder spezielle Gebühreninformationen) übertragen. Diese werden mittels der in den Registern enthaltenen Schlüssel k_i von jedem Register verschlüsselt. Nur der Teilnehmer selbst, der alle k_i kennt, kann wieder entschlüsseln und somit die Daten lesen.

Nach einmaliger Nutzung des Pfades müssen wiederum neue Pseudonyme generiert werden. Das bedeutet, der Datensatz ist zu aktualisieren. Wie bereits erwähnt, darf der Algorithmus zum Generieren der Pseudonyme nur den jeweils beteiligten Registern bekannt sein. Wird wie im Bild 9 hierfür ein Pseudozufallszahlengenerator (PZZG) verwendet, so besteht das Geheimnis zwischen den Registern R_{i-1} und R_i im Zufallszahlenanteil zz1, und zwischen R_i und R_{i+1} ist es entsprechend zz2.

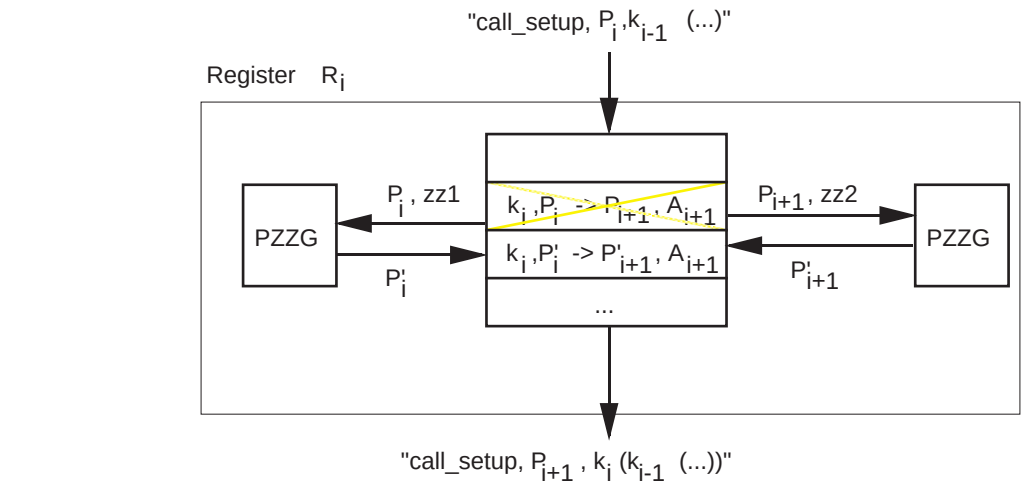

Bild 9: Bilden der neuen Pseudonyme beim call_setup

Das Problem von Replay-Angriffen wurde bereits erwähnt. Ein Angreifer könnte eine Verbindungswunschnachricht abfangen und erneut senden. Würden die Pseudonyme nach einmaligem Zugriff nicht wechseln, könnte ein Angreifer eine Nachricht mehrmals schicken und würde aufgrund derselben Ausgabenachricht Kenntnisse über den Signalisierungspfad und somit auch über den Aufenthaltsort der MS erlangen.

3.3.4 Einsparen von Übertragungsaufwand

Beim Übertragen von Daten wird Bandbreite benötigt. Dem Register ist das Vorgängerregister sowie das nachfolgende Register bekannt, da alle Kommunikation im Netz abhörbar ist. Deshalb ist das Mitschicken der Rückadressen nicht zwingend erforderlich. Ein Register R_i kann anhand des Senders R_{i+1} selbständig die Adresse A_{i+1} des späteren Empfängers speichern.

Eine weitere Einsparung kann darin bestehen, daß der Teilnehmer statt der Schlüssel und Pseudonyme nur jeweils eine kurze Zufallsbitfolge schickt, aus der dann die relevanten Daten von den Registern selbst generiert werden. Natürlich muß hier ein solcher Algorithmus verfügbar sein, der keinem Outsider bzw. anderen Registern das Nachvollziehen der Berechnungen ermöglicht.

4 Diskussion des Angreifermodells

4.1 Bisheriges Angreifermodell

Bisher wurde bei der Diskussion der Sicherheit des vorgeschlagenen Verfahrens das in Kapitel 2.2 aufgestellte Angreifermodell benutzt. Die grundlegende Annahme in diesem Modell lautet, daß die Register R_i nicht kooperieren. Damit ist der stärkste Angreifer ein Register, denn es kann, wie jeder außenstehende Angreifer, den Netzverkehr beobachten und besitzt zusätzlich noch Informationen für die Pseudonymverkettung im eigenen Register. Der dadurch entstehende Informationsgewinn ist gering. Das Register R_0 kann als Angreifer ermitteln, in welchem Register der Ebene 1 der Teilnehmer angemeldet ist. Ein anderes Register R_i kann 2 Pseudonyme verketten, aber keiner Identität zuordnen. Das Verfahren ist demzufolge unter den getroffenen Festlegungen sicher. In diesem Kapitel wird ein schärferes Angreifermodell betrachtet und diskutiert, inwieweit das vorgestellte Verfahren diesem standhält.

4.2 Ein schärferes Angreifermodell

4.2.1 Angreifermodell

Das in 4.1 beschriebene Angreifermodell setzt ein wenig korrumpiertes System voraus. Durch das Angreifermodell des MIX-Netzes angeregt, wird dem Kommunikationsnetz im folgenden ein schärferes Angreifermodell zugrundegelegt.

- Jegliche Kommunikation im Netz ist beobachtbar.
- Von n Registern kooperieren maximal n-1 Register.

Die folgenden Überlegungen werden zeigen, daß unter diesen schärferen Annahmen das vorgeschlagene Verfahren gebrochen werden kann. Es existieren jedoch Möglichkeiten, den Angriff zu erschweren!

4.2.2 Ein Angriff

Unter dem Angreifermodell aus 4.2.1 ist folgender Angriff denkbar und erfolgreich: Ein Register, z.B. R_k soll überbrückt werden. Man nehme an, R_k sei das einzige vertrauenswürdige Register auf dem Signalisierungspfad des Teilnehmers. Der Angreifer kennt durch seine Mächtigkeit bereits alle Pseudonymumsetzungen außerhalb von R_k und natürlich das zwischen R_{k-1} und R_k bzw. R_k und R_{k+1} ausgetauschte Geheimnis.

Wird dem angegriffenen Teilnehmer signalisiert, so kann der Angreifer den Ausgabebatch B1 von R_k beobachten und speichern. Er kann aber die in R_k gespeicherten P_k und P_{k+1} nicht verketten. Nach dem Weiterleiten der Nachricht generiert R_k neue Pseudonyme P'_k und P'_{k+1} (entsprechend 3.3.3). Wird dem angegriffenen Teilnehmer *erneut* signalisiert, speichert der Angreifer wiederum den Ausgabebatch B2. Da R_{k+1} aufgrund des mit R_k ausgetauschten Geheimnisses die Pseudonyme P_{k+1} und P'_{k+1} ebenfalls verketten kann, kann jetzt das Register R_{k+1} prüfen, wie oft P_{k+1} in B1 und P'_{k+1} in B2 enthalten ist. Ist diese Zuordnung nur für ein Paar erfolgreich, so hat der Angreifer damit die Pseudonyme P_k und P_{k+1} verkettet und somit R_k überbrückt.

Der gesamte Signalisierungspfad läßt sich vom ersten bis zum letzten Register nachvollziehen. Mit diesem Angriff ist ein Teilnehmer somit lokalisierbar und verfolgbar, wenn nur ihm in zwei Batchen B1 und B2 signalisiert wird.

Dieser Angriff ist derart verallgemeinerbar, daß bereits die Kooperation zweier beliebig weit auseinanderliegender Register genügt, um den Aufenthaltsort eines Teilnehmers bei erneuter Signalisierung offenzulegen.

4.2.3 Erschweren des Angriffs

Man kann den oben beschriebenen Angriff erschweren, wenn man die Register im Pool- statt Batchbetrieb verwendet. Beim Poolbetrieb werden im Register Nachrichten gesammelt, bis eine vorher definierte Poolgröße erreicht worden ist. Danach wird für jede eingehende Nachricht eine zufällig gewählte freigegeben. Der Angreifer kann dadurch den Ausgabezeitpunkt der Nachrichten nicht berechnen. Sein Aufwand steigt. Außerdem ist es möglich, daß die zweite Signalisierungsnachricht vor der ersten ausgegeben wird. Die Wahrscheinlichkeit steigt, daß während des Angriffs noch mindestens einem anderen Teilnehmer zweimal signalisiert wird.

Der Nachteil des Poolbetriebs liegt in der Dienstqualität, da keine maximale Durchlaufverzögerung der Signalisierung garantiert werden kann.

Betrachtet man die in den Registern gespeicherten Teilnehmer als Anonymitätsgruppe, läßt sich der in 4.2.2 beschriebene Angriff bereits im Batchbetrieb erschweren, wenn für jeden

Teilnehmer der Gruppe eine Signalisierungsnachricht in jedem Batch enthalten ist. Dies wird beispielsweise beim Verfahren der ISDN-MIXe [PfPW_91] angewendet. Unter Anonymitätsgruppe versteht man eine Gruppe, deren Zusammensetzung sich während des bestehenden Signalisierungspfades nicht ändert. Durch diese Forderungen ist der Einsatz in einem Mobilkommunikationsnetz mit Terminal Mobility jedoch nicht mehr effektiv möglich. In Situationen mit geringer Teilnehmermobilität ist ein statischer Signalisierpfad vorteilhalft, da er dann potentiell mehrfach genutzt wird. Solche Mobilitätsmuster findet man z.B. im Bereich Personal Mobility, wenn sich ein Teilnehmer (etwa an seinem Arbeitsplatz) für längere Zeit an einem Ort aufhält. Da hier die Abstände zwischen zwei Aufenthaltsaktualisierungen meist größer sind, bleiben auch die Anonymitätsgruppen über einen längeren Zeitraum bestehen.

5 Schlußbemerkungen

Ein Mobilkommunikationssystem wurde beschrieben, das bei der Verwaltung von Aufenthaltsinformationen die Anonymität der Teilnehmer in der Signalisierungsphase gewährleistet, jedoch die Erreichbarkeit nicht einschränkt.

Eine Abschätzung der Leistung des Verfahrens zeigt folgendes:

Durch die Pseudonymverwaltung erhöht sich der Speicheraufwand gegenüber existierenden Systemen. Die Datenschutzforderung nach Vertraulichkeit des Aufenthaltsortes wird erfüllt, natürlich ist damit höherer Realisierungsaufwand des Kommunikationssystems verbunden.

Der Managementaufwand für die Mobilstation soll möglichst gering gehalten werden. Unter 3.3 wird eine Möglichkeit dazu durch effizientes Generieren der Pseudonyme vorgestellt.

Es wird angestrebt, daß auf jeder Ebene zu jeder Zeit immer genügend Register unterschiedlicher Betreiber zur Auswahl stehen. Erst dadurch wird die Vertrauenswürdigkeit gewährleistet. Durch diese Auswahlmöglichkeit kann außerdem auf unterschiedliche Lastsituationen im Netz reagiert werden.

Die Aufenthaltsinformationen werden pseudonym und mehrstufig verwaltet. Sind die Teilnehmer mobil, so erfolgt aufgrund der mehrstufigen Speicherung die Aufenthaltsaktualisierung in der Regel nur innerhalb eines Teilnetzes. Dann muß nicht im gesamten Netz signalisiert werden.

Die Verwendung hybrider kryptographischer Systeme ermöglicht nach einmaligem Aufbau eines Signalisierungspfades dessen mehrmalige effiziente Nutzung. Im ersten Schritt werden symmetrische Schlüssel in den Vermittlungsknoten (Registern) mittels eines asymmetrischen Verfahrens hinterlegt. In den folgenden Schritten können dann die symmetrischen Schlüssel genutzt werden. Beim Location Update kann Aufwand gespart werden, da nur ein Teil des Signalisierungspfades erneuert werden muß. Im Umlenkpunkt kann sogar symmetrisch gearbeitet werden. Durch hybride Systeme werden die Vorteile von asymmetrischer und symmetrischer Kryptographie miteinander verknüpft. Die Verwendung kryptographischer Funktionen erhöht jedoch den Signalisierungsaufwand.

Die Diskussion eines schärferen Angreifermodells zeigt, daß Modifikationen ursprünglicher Annahmen auch Veränderungen im Verfahren nach sich ziehen. Je mehr Stärke den Angreifern zugestanden wird, desto mehr Forderungen werden an das Verfahren gestellt. Bei nicht miteinander kooperierenden Registern werden keine besonderen Annahmen über die Teilnehmer getroffen. Wird das Angreifermodell jedoch modifiziert (siehe Kapitel 4), hält das Verfahren Angriffen nur stand, wenn die Teilnehmer Anonymitätsgruppen zugeordnet werden. Eine andere Variante wird in [FeJP_96] aufgezeigt, wo die Unverkettbarkeit der Registerinformationen durch zwischengeschaltete Mixe gewährleistet wird. Aufgrund verschiedener Einsatzmöglichkeiten ist die Betrachtung verschiedener Szenarien wichtig.

6 Literatur

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

CoBi_95 David A. Cooper, Kenneth 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.

FeJP_96 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: location management with privacy, Proc. of the Workshop on Information Hiding, Cambridge (UK), Univ.of Cambridge, Isaac Newton Institute, 30.5.-1.6.96.

FJKP_95 Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas 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 Thomas Hetschold: Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes; GMD-Studien no. 222, Oktober 1993.

KeFo_95 Dogan Kesdogan, Xavier Fouletier: Secure Location Information Management in Cellular Radio Systems; IEEE Wireless Communication System Symposium 95, Proceedings, Long Island (1995) 35-46.

KFJP_96 Dogan Kesdogan, Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Location management strategies increasing privacy in mobile communication; 12th IFIP International Conference on Information Security (IFIP/Sec '96), Chapman & Hall, London 1996, 37-38.

Mitt_94 H. Mitts: Universal Mobile Telecommunication Systems - Mobile access to Broadband ISDN; in Broadland Islands '94: Connecting with the End-User, W. Bauerfeld, O. Spaniol, F. Williams (Editors) 1994, 203-209.

MüSt_95 Günter Müller, Frank Stoll: Der Freiburger Kommunikationsassistent - Sicherheit in multimedialen Kommunikationsnetzen durch nutzerbezogene Dezentralisation. Dokumentation zum Symposium "Multimedia und Datenschutz" des Berliner Datenschutzbeauftragen, Internationale Funkausstellung Berlin, August 1995, 1-16.

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

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze; Informatik-Spektrum 11/3 (1988) 118-142.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead; Proc. Kommunikation in verteilten Systemen, IFB 267, Springer-Verlag, Heidelberg 1991, 451-463.

Walk_94 Bernhard Walke: Technik-Akzeptanz und -Verträglichkeit von mobilen Kommunikationsnetzen; ITG-Fachtagung "Herausforderung Informationstechnik", VDE-Verlag, München, 18.-20.Oktober 1994.