in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 169-180.

Mobilkommunikation ohne Bewegungsprofile_

Hannes Federrath*, Anja Jerichow*, Dogan Kesdogan◊, Andreas Pfitzmann*, Otto Spaniol◊

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

◊RWTH Aachen, Informatik 4 (Kommunikationssysteme), Ahornstr.55, 52074 Aachen, {dogan, spaniol}@informatik.rwth-aachen.de

Zusammenfassung

Mobilkommunikation bietet viele neue Möglichkeiten. Durch den Mobilitätsaspekt verschärfen sich jedoch Datenschutzprobleme.

Unser Ziel ist es, Informationen über den Aufenthaltsort einer Mobilstation vertraulich zu verwalten. Die vorgeschlagene Verwaltung dieser Informationen dient der Anonymisierung der Teilnehmer und erfüllt somit deren Wunsch nach Privatsphäre.

1 Einführung

Der Standard GSM [1] bildet eine Grundlage für digitale Mobilfunknetze. Der Verbindungsaufbau zur Mobilstation (MS) eines Teilnehmers erfolgt mit vorheriger Anfrage an eine *zentrale* Datenbank (Home Location Register, HLR).

GSM-Netze haben eine verteilte Netzstruktur. Das Versorgungsgebiet wird in Lokalisierungsgebiete (Location Areas, LA) aufgeteilt. Diese Gebiete werden durch Vermittlungsstellen

---

– Nachdruck eines in it+ti 38. Jg. Heft 4 (1996) S.24-29 erschienenen Artikels.

(Mobile Switching Centres, MSC) mit zugehörigen *lokalen* Datenbanken (Visitor Location Registers, VLR) verwaltet. Eine MSC kann für mehrere LAs zuständig sein.

Das MSC ist für einen oder mehrere Base Station Controller (BSC) verantwortlich. Ein BSC wiederum verwaltet eine oder mehrere Base Transceiver Stations (BTS), die für eine oder mehrere Zellen zuständig sind. Die konkrete Anzahl der Zellen innerhalb eines LA läßt sich optimieren aus der Betrachtung der Teilnehmermobilität, der Anzahl der mobilen Teilnehmer im LA und dem Nachrichtenverkehr im LA. BSC und BTSs werden als Base Station System (BSS) bezeichnet.

Aufgrund der Mobilität der Teilnehmer hat die Verwaltung von Aufenthaltsinformationen, das sogenannte Location Management, eine besondere Bedeutung. Zu den Verwaltungsfunktionen gehören das Einbuchen einer MS, der Verbindungsaufbau von einer MS (mobile originated call, moc) und zu einer MS (mobile terminated call, mtc) sowie das Aktualisieren der Aufenthaltsinformationen (Location Update, LUP).

Um die Erreichbarkeit eines Teilnehmers im zellularen Funknetz zu gewährleisten, sind Aufenthaltsinformationen über den Teilnehmer bzw. seine Mobilstation (MS) notwendig. In existierenden Zellnetzen erfolgt die Speicherung dieser Informationen (z.B. des augenblicklichen Aufenthaltsgebietes) in zentral organisierten Datenbanken, die zumindest durch den Netzbetreiber mißbräuchlich verwendet werden können, um Bewegungsprofile zu erstellen.

Die mögliche Verfolgung der Mobilstation eines Teilnehmers im Netz sehen wir als einen Verstoß gegen die Datenschutzforderung Vertraulichkeit: Der *momentane Ort* einer Mobilstation bzw. des sie benutzenden Teilnehmers soll ohne dessen Einwilligung weder durch potentielle Kommunikationspartner noch Unbeteiligte (inkl. Netzbetreiber) ermittelt werden können. Dieses Problem verschärft sich, da aufgrund begrenzter Frequenzressourcen im Mobilfunk eine immer feinere Aufteilung in Zellen notwendig ist. Die zur Weitervermittlung ankommender Rufe notwendigen Informationen über den augenblicklichen Aufenthaltsort des mobilen Teilnehmers werden immer detaillierter.

Ansätze zum Entschärfen dieses Datenschutzproblems existieren in der Literatur [2, 3, 4, 5, 6, 7]. Unsere hier vorgestellten neuen Konzepte zeichnen sich durch ihre Datensparsamkeit bei der Verwaltung der Informationen über die mobilen Teilnehmer sowie durch die weitgehende Beibehaltung existierender Netzstrukturen aus.

2 Datenschutzforderungen und Umsetzungsmöglichkeiten

2.1 Forderungen

Unbefugter Informationsgewinn, unerkannte Änderung von Informationen und Beeinträchtigung der Funktionalität durch Unbefugte sollen in einem Kommunikationsnetz verhindert werden. Die daraus resultierenden Schutzziele können unter den Begriffen *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* zusammengefaßt werden.

Verfügbarkeit bedeutet, daß das Netz die Kommunikationswünsche der Teilnehmer erfüllt, soweit sie nicht verboten sind.

Integrität steht für Richtigkeit, Vollständigkeit und Aktualität von Daten sowie für Sender- und Empfängernachweis. Technisch umgesetzt wird Integrität hauptsächlich durch Anwendung kryptographischer Methoden wie Authentikationscodes und digitale Signaturen.

Vertraulichkeit heißt, daß Daten nur Berechtigten verfügbar werden. Hierunter fällt der Schutz des momentanen Orts des mobilen Teilnehmers gegenüber dem Netzbetreiber, also die Verwaltung von Aufenthaltsinformationen.

In [4] wird hierzu das Konzept der Funk-MIXe[1] geschlagen. Kryptographische Techniken alleine genügen für Vertraulichkeit nicht, da die Schutzforderungen auch die Vermittlungsdaten betreffen (Bild 1).

---

[1] Funk-MIXe = Grundkonzept zum Schutz von Sender, Empfänger und momentanem Ort des Teilnehmers in Funknetzen, das mehrere Maßnahmen kombiniert (Ende-zu-Ende-Verschlüsselung, Verbindungs-Verschlüsselung zwischen mobiler und ortsfester Teilnehmerstation, ortsfeste umkodierte MIXe und Verteilung gefilterter Verbindungswünsche) [3].

Schutzziel Vertraulichkeit	***Umsetzungsmöglichkeiten***
Nachrichteninhalte	Ende-zu-Ende-Verschlüsselung (Konzelation)
Sender- und/oder Empfängeranonymität	Dummy Traffic MIXe
momentaner Aufenthaltsort • *Location Management* • *Adressierung* • *Schutz vor Peil- und Identifizierbarkeit sendender MS (siehe auch [8])*	Verteilung (Broadcast) neue Strategien zur Verwaltung von Aufenthaltsinformationen Bandspreizverfahren/CDMA (Direct Sequence Spread Spectrum)

Bild 1: *Technische Umsetzungsmöglichkeiten für das Schutzziel Vertraulichkeit in Funknetzen*

Sicherheit wurde bisher üblicherweise nur einseitig betrachtet. Beispielsweise muß sich der Benutzer eines Kommunikationssystems wie GSM gegenüber dem Netzbetreiber authentisieren. Der umgekehrte Vorgang ist jedoch nicht vorgesehen.

Wir fordern *mehrseitige Sicherheit* in Netzen. Hierunter verstehen wir die Garantie der oben genannten Schutzziele für jeden, selbst wenn andere an der Kommunikation oder Dienster-bringung Beteiligte angreifen[2]. Vor allem soll Vertraulichkeit für den individuellen Nutzer, für seinen Kommunikationspartner und je nach Anwendung auch für Dritte sowie die Dienstanbieter und Netzbetreiber gewährleistet werden.

2.2 Einige Ansätze zur Umsetzung

Zur Realisierung der Unbeobachtbarkeit des Aufenthaltsorts eines Teilnehmers existieren Lösungsvorschläge (z.B. [4, 5]). Die Datenbanken, die zur Speicherung der Informationen zum Aufenthaltsort des mobilen Teilnehmers nötig waren, werden in diesen Vorschlägen an einen vertrauenswürdigen Ort ausgelagert. Die Verwaltung erfolgt in [4] und [5] unter Nutzung eines persönlichen digitalen Assistenten oder Kommunikationsleibwächters beispielsweise in Form einer ortsfesten Teilnehmerstation HPC (Home Personal Computer), die je einem Teilnehmer zugeordnet ist.

---

[2] Unter "angreifen" verstehen wir Verhalten, das den Schutzinteressen (von anderen) zuwiderläuft.

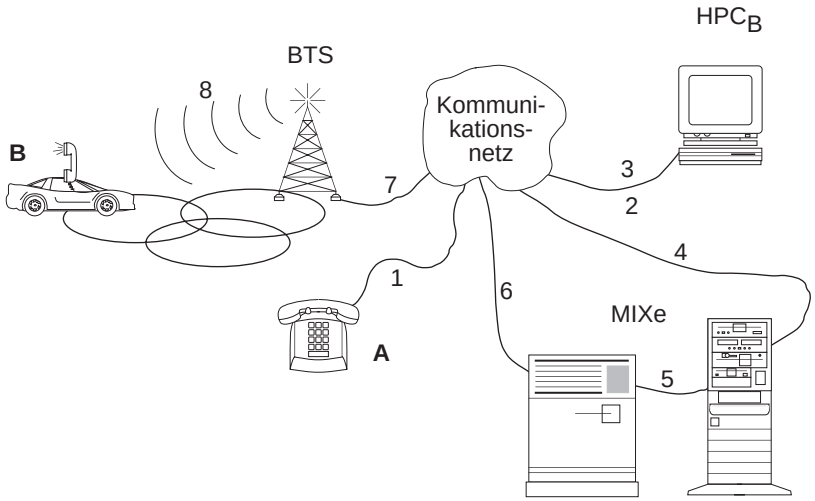

Bild 2: *Vertrauenswürdige Speicherung von Aufenthaltsinformationen im HPC*

Wechselt die MS das LA, so erfolgt eine Aktualisierung der Lokalisierungsinformation im HPC. In [4] wird aus Anonymitätsgründen weiterhin gefordert, daß hierbei die Verbindung zwischen MS und HPC durch MIX-Kaskaden[3] zu schützen ist. Durch die Verwendung von MIX-Kaskaden können die Wege der Nachrichten weder anhand ihres äußeren Erscheinungsbildes (also ihrer Länge und Codierung) noch anhand zeitlicher oder räumlicher Zusammenhänge verfolgt werden.

Erfolgt bei jedem Wechsel des Aufenthaltsgebietes eine Aktualisierung der Information im HPC, so kann bei häufigem Wechsel des Aufenthaltsbereiches beträchtlicher Signalisieraufwand entstehen. Dies kann abgeschwächt werden, indem statt ständiger Signalisierung zur Aktualisierung des gegenwärtigen Aufenthaltsorts erst in folgendem Fall signalisiert wird:

Bei einem beim HPC ankommenden Kommunikationswunsch soll die MS durch den HPC mittels Broadcast im gesamten Versorgungsbereich gesucht werden. Im HPC müssen demnach keine detaillierten Aufenthaltsinformationen verwaltet werden. Bei dieser Art der Anonymisierung wird das Konzept der offenen impliziten Adressen angewandt.

Implizite Adressen kennzeichnen im Gegensatz zu expliziten weder einen Ort im Netz noch eine Station. Sie sind nur ein Merkmal für den Empfänger, das ansonsten bedeutungslos und mit

---

[3] Ein MIX puffert Nachrichten gleicher Länge von vielen Sendern, codiert sie um und gibt sie umsortiert aus. Das Umcodieren erfolgt durch Ent- oder Verschlüsseln mittels eines Kryptosystems. Bei Verwendung mehrerer MIXe, sog. MIX-Kaskaden, sind Sender und Empfänger nicht miteinander verkettbar [7].

nichts anderem in Beziehung zu setzen ist. Der Empfänger kann daran erkennen, ob eine Nachricht für ihn bestimmt ist. Offene implizite Adressen können von Unbeteiligten auf Gleichheit getestet werden.

Eine geeignete Realisierung sind Zufallszahlen, die vom Empfänger mittels eines Assoziativspeichers, in den alle für die Station gerade gültigen offenen impliziten Adressen geschrieben werden, sehr effizient erkannt werden können. Hingegen können verdeckte implizite Adressen von niemandem außer vom Adressaten auf Gleichheit getestet werden. Dieser Test stellt eine kryptographische Operation dar und ist deshalb auch für den Adressaten deutlich aufwendiger als bei offenen impliziten Adressen.

Hat der HPC die Funktionalität eines Erreichbarkeitsmanagers [7], so können ankommende Kommunikationswünsche gefiltert werden. Dadurch ist u.U. weniger Broadcast-Signalisierung notwendig. Der HPC könnte vom Teilnehmer auch so eingestellt werden, daß ein bestimmtes Broadcast-Gebiet in Abhängigkeit des wahrscheinlichen Aufenthaltsbereiches des mobilen Teilnehmers vorgegeben ist.

[6] schlägt die Ausnutzung hierarchischer Zellüberlagerungen für einen datensparsamen Verbindungsaufbau vor. Durch die geplante Integration gegenwärtig existierender und künftiger Kommunikationssysteme in UMTS (Universal Mobile Telecommunication System) sind die Zellen verschiedener Systeme verschieden groß und damit zumindest teilweise überlagernd. Bei der Verteilung von Broadcast-Nachrichten im Versorgungsgebiet ist klar: Je größer ein Broadcast-Gebiet, d.h. ein oder mehrere Zellen, gewählt wird, um so größer ist auch die Anonymität des Einzelnen.

Erfolgt die Verteilung einer Nachricht in einem möglichst großen Zellbereich, d.h. einem System, dessen Zellen die Aufenthaltszelle der MS in ihrem Netz großflächig überlagern, so kann die notwendige Aufenthaltsinformation viel ungenauer sein [6]. Man wird also versuchen, je nach Netzeffizienz und gewünschtem Anonymitätsgrad den Kommunikationswunsch in einem möglichst großen Zellbereich mittels Broadcast zu signalisieren.

3 Pseudonymisierung der Teilnehmer im Netz

Datenschutzkonforme Vorschläge zur Verwaltung von Aufenthaltsinformationen hatten bisher das Ziel, die Erhebung solcher Daten durch den Netzbetreiber völlig zu unterbinden. Der Netzbetreiber sollte keine Datenbanken mehr haben, in denen er die Aufenthaltsinformation des mobilen Teilnehmers verwaltet.

Im folgenden steht das Verbergen der Identität (hier speziell die Pseudonymisierung) des mobilen Teilnehmers gegenüber dem Netzbetreiber im Vordergrund. Von einem pseudonymisierten Teilnehmer darf der Netzbetreiber die Aufenthaltsinformation dann registrieren und effizient verwalten, wenn durch die Art der Pseudonymisierung und der Mobilitätsverwaltung nichts oder zumindest nur sehr wenig über seine Identität zu erfahren ist.

Abrechnungsverfahren werden in dieser Abhandlung nicht betrachtet. Eine Modifikation der Verfahren, beispielsweise durch Nutzung anonymer Zahlungssysteme, wird jedoch notwendig. [9] stellt Konzepte hierfür vor.

3.1 Temporäre Pseudonyme für einzelne Teilnehmer

Der Netzbetreiber soll in seinen Datenbanken genaue Aufenthaltsinformationen verwalten dürfen, wenn diese *nicht* teilnehmerbezogen sind, sondern sich auf wechselnde Pseudonyme beziehen. Das Netzwerk ist zeitsynchronisiert und erhält zu entsprechenden Synchronisationszeitpunkten t_i von seinen Teilnehmern in den jeweiligen LAs eine relativ lange offene implizite Adresse (z.B. 50 bis 100 Bits), welche als Pseudonym verwendet wird. Das Pseudonym wird mittels parametrisiertem Zufallszahlengenerator (ZZG) zeitgleich im mobilen Endgerät und im dem Teilnehmer vertrauenswürdigen HPC mittels des vorher ausgetauschten, geheimen Schlüssels k_B erzeugt. Nach Ablauf einer bestimmten Zeit muß ein neues Pseudonym erzeugt werden.

3.1.1 Einbuchen, Ausbuchen und Aktualisieren

Der Teilnehmer B hat durch $ZZG(k_B,t_i)$ ein Pseudonym ID_B erzeugt, welches beim Einbuchen im HPC von B und im Netzwerk (HLR) mit dem zugehörigen VLR registriert und aktualisiert wird.

Alle LUP Prozeduren von GSM arbeiten jetzt unter dem Pseudonym, keine Modifikationen sind notwendig.

3.1.2 Verbindungsaufbau zur MS

Versucht ein Teilnehmer A den mobilen Teilnehmer B zu erreichen, muß das momentane Pseudonym ID_B durch das Gateway MSC (GMSC) im vertrauenswürdigen HPC abgefragt werden. Durch Speicherung des Abfragezeitpunkts von GMSC an HPC im HPC kann ein Mißbrauch des Pseudonyms durch mehrmalige Abfrage verhindert werden.

Mit Hilfe des Eintrags "ID_B,VLR" im HLR erfolgt der Verbindungsaufbau (gemäß GSM), d.h. das Weiterleiten des Rufes zum entsprechenden MSC/VLR (Bild 3).

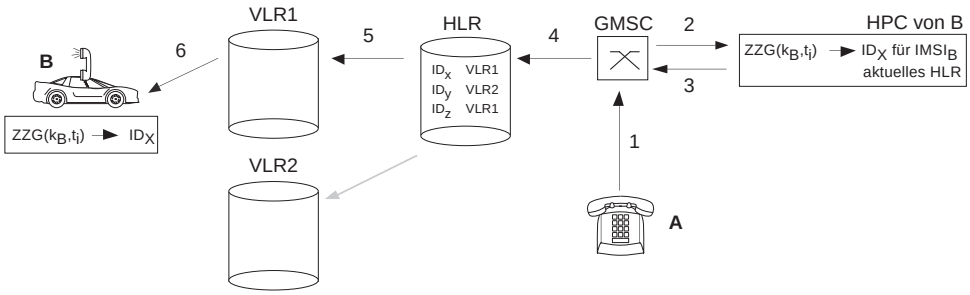

Bild 3: *Pseudonymisierung des Teilnehmers und Adressierung im HPC*

Die Synchronisationsanforderungen an das vorgestellte System können entschärft werden, indem die Netzdatenbanken die alte ID erst nach Ablauf einer Verfallszeit, die länger als die Synchronisationszeit ist, löschen. Da jede ID autonom vom Netzbetreiber behandelt wird und ohne Kenntnis von k_B kein Zusammenhang zwischen den erzeugten IDs existiert, besteht keine Möglichkeit der Verkettung der IDs.

Ein Vorteil dieser Lösung besteht in der weitgehenden Beibehaltung von bestehenden Netzstrukturen in GSM. Nachteilig ist die im Vergleich zu GSM längere Bitkette zum Adressieren des Nutzers. Der Signalisieraufwand bleibt ähnlich hoch wie im HPC-Ansatz in 2.2.

3.2 Dynamische Gruppenpseudonyme – Verwaltung unter Beibehaltung der logischen GSM-Struktur

Bisherige Betrachtungen setzten die Existenz eines HPCs voraus. Der Einsatz eines solchen Gerätes bringt uns unserem Wunsch nach mehrseitiger Sicherheit deutlich näher, erfordert andererseits jedoch technischen Mehraufwand, ist ineffizient und gefährdet u.U. die Verfügbarkeit von Diensten (z.B. Stromausfall zu Hause beim mobilen Teilnehmer).

Erfolgt die Durchführung datenschutzkritischer Aufgaben organisierter und zentraler, so können oben genannte Nachteile des Einsatzes von vertraulichen Endgeräten kompensiert werden.

Der in diesem Abschnitt vorgestellte Ansatz geht von folgender Annahme aus: Wenn es möglich ist, Teilmengen von Teilnehmern in Gruppen zusammenzufassen, sind die Aufenthaltsorte einzelner Teilnehmer innerhalb einer Gruppe unbekannt, also anonym. Den Teilnehmern einer Gruppe wird ein sog. Gruppenpseudonym zugeordnet.

Für jeden Teilnehmer wird aus der fest vorgegebenen IMSI (International Mobile Subscriber Identity) mittels einer allgemein bekannten Hashfunktion *h* eine verkürzte IMSI' gebildet. Der Hashwert IMSI'=*h*(IMSI) ist ein Gruppenpseudonym für eine Menge von Teilnehmern, da mehrere IMSIs auf eine IMSI' abgebildet werden.

Die Netzstruktur des GSM soll weitgehend beibehalten werden. Deshalb verwenden wir für die Datenbanken des GSM die Bezeichner HLR* und VLR* (s. Bild 4).

3.2.1 Einbuchen und Ausbuchen

Mit dem Einbuchen von Teilnehmer B in ein Netz ist ein Registrieren des Aufenthaltsorts verbunden. B hört den Broadcast-Kanal ab und meldet dem für sein LA zuständigen VLR* den Hashwert seiner $IMSI_B$, also $IMSI'_B$.

Meldet sich ein Teilnehmer aus einer noch nicht im VLR* registrierten Anonymitätsgruppe (z.B. $IMSI'_B$), wird dort ein neuer Datensatz "$IMSI'_B$,*n*" mit *n*:=1 angelegt und an HLR* die Meldung gegeben, daß ein Teilnehmer der Anonymitätsgruppe $IMSI'_B$ registriert wurde.

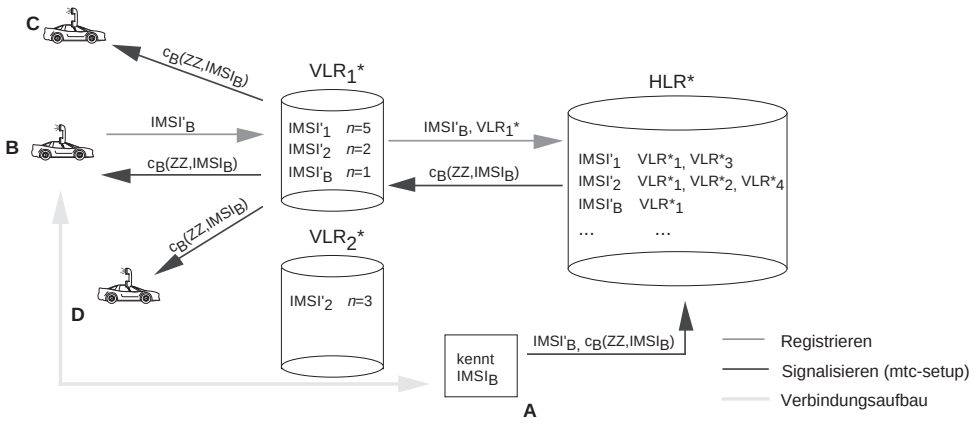

Bild 4: *Registrieren, Signalisieren und Verbindung aufbauen*

Meldet sich ein weiterer Teilnehmer einer bereits im VLR* registrierten Anonymitätsgruppe, so erfolgt eine Aktualisierung des Datensatzes "$IMSI'_B$,*n*:=*n*+1". Eine Meldung an HLR* erfolgt nicht.

Über den Zähler *n* kann das VLR* feststellen, wieviele Teilnehmer der gleichen Anonymitätsgruppe sich zu einem Zeitpunkt im VLR* aufhalten.

Meldet sich der letzte registrierte Teilnehmer einer Anonymitätsgruppe im VLR* ab, wird dies dem HLR* entsprechend mitgeteilt.

Im HLR* werden zu jeder Anonymitätsgruppe die VLRs* gespeichert, in denen sich Teilnehmer der jeweiligen Anonymitätsgruppe aufhalten.

3.2.2 Verbindungsaufbau zur MS

Will ein Teilnehmer A eine Verbindung zu B aufbauen (mtc-setup), so bildet A aus der ihm bekannten $IMSI_B$ den Hashwert $IMSI'_B$ und meldet mit Senden von $IMSI'_B$ dem Netz seinen Verbindungswunsch.

Zusätzlich sendet A die mit dem öffentlichen Schlüssel[4] c_B von B verschlüsselte $IMSI_B$ in Form der verdeckten impliziten Adresse $c_B(ZZ,IMSI_B)$. Durch die Zufallszahl ZZ wird sichergestellt, daß der Teilnehmer nicht durch das Netz identifiziert werden kann. Um Angriffe gegen Replay von $c_B(ZZ,IMSI_B)$ zu verhindern, könnte der verdeckten impliziten Adresse ein Zeitstempel T mitgegeben werden: $c_B(ZZ,IMSI_B,T)$.

HLR* sendet $c_B(ZZ,IMSI_B)$ an alle zu diesem Gruppenpseudonym registrierten VLRs* (in Bild 4 nur VLR_1*). Diese verteilen den Verbindungswunsch in den LAs (Broadcast).

Alle Teilnehmer hören den Broadcast-Kanal ab, aber nur B kann die Nachricht positiv auswerten, d.h. entschlüsseln. Indem er mit d_B, seinem geheimen Schlüssel, $d_B(c_B(ZZ,IMSI_B))$ berechnet, kann er feststellen, daß er adressiert ist.

3.2.3 Aktualisieren der Aufenthaltsinformation

Beim Wechseln in ein anderes LA erfolgt ein LUP. Dazu hört B ständig den Broadcast-Kanal ab. Stellt B fest, daß ein neues VLR* zuständig ist (bzw. besseren Empfang bietet), so meldet B seine $IMSI'_B$ an das jetzt zuständige $VLR*_{neu}$. Aufgrund dessen wird der Zähler in $VLR*_{alt}$ um 1 verringert und in $VLR*_{neu}$ erhöht.

Bei Bedarf (siehe die Bemerkungen zum Ein- und Ausbuchen) melden $VLR*_{alt}$ und $VLR*_{neu}$ die Veränderungen an HLR*.

Das hier vorgestellte Verfahren verwendet die logische Struktur des GSM-Netzes weitgehend unverändert. Ein wesentlicher Unterschied zu GSM besteht jedoch darin, daß zum Erreichen eines bestimmten mobilen Teilnehmers jetzt in mehreren LAs signalisiert werden muß. Dies führt zu einer Erhöhung des Signalisieraufwandes.

Der kritische Parameter dieses Verfahrens ist offenbar die Anzahl der Teilnehmer, die man unter einem Gruppenpseudonym zusammenfaßt. Wählt man die Anonymitätsgruppe zu groß, so ist zwar die Gefahr der Verfolgung einzelner Teilnehmer gering, aber dafür der Signalisier-Overhead durch Broadcast stark erhöht und umgekehrt.

Ein weiterer Unterschied ist die notwendige Bandbreite zur Signalisierung eines Verbindungswunsches.

---

[4] Ein asymmetrisches Kryptosystem sei vorausgesetzt.

Bei Verwendung von asymmetrischer Kryptographie müssen sicherheitsabhängig derzeit mindestens 500 Bit zur Adressierung übertragen werden. Gleichzeitig ist dann jedoch der mögliche erweiterte "Klartextraum" der impliziten Adresse zur Signalisierung von Zusatzinformationen (z.B. Angaben über die Abrechnungsart, Übertragung der Challenge-Information für die Authentikation) nutzbar. So lassen sich u.U. weitere Protokollschritte einsparen bzw. effizienter als bei GSM gestalten.

Bei Verwendung eines symmetrischen Verschlüsselungssystems wird zwar das Bandbreiteproblem pro Signalisierung innerhalb eines LAs entschärft, gleichzeitig dürfte jedoch das Schlüsselmanagement erheblich problematischer zu realisieren sein als bei asymmetrischer Kryptographie. Schließlich muß mit *jedem* potentiellen Kommunikationspartner vorher ein symmetrischer Schlüssel ausgetauscht sein.

4 Ausblick

Die beschriebenen Verfahren zur Verwaltung von Aufenthaltsinformation erreichen, daß selbst der Netzbetreiber keine Bewegungsprofile von Teilnehmern erstellen kann.

Zukünftigen Untersuchungen vorbehalten, bleibt zu klären, wie sich der *Aufwand* der beschriebenen Strategien im Vergleich zu den bisher angewandten, entwickelten Verfahren, die nicht den Schutz des Aufenthaltsortes von mobilen Teilnehmern zum Ziel hatten, verhält. Weitere interessante Fragen sind: Wie sind die beschriebenen Verfahren zu *verbessern*? Können die verschiedenen beschriebenen Verfahren sinnvoll *kombiniert* werden? Wie genau könnte und sollte die Abrechnung der Dienstnutzung erfolgen. Grundkonzepte für die Abrechnung bei Pseudonymisierung sind bekannt [4, 9].

Wir hoffen, daß zumindest die wesentlichen Fragen so rechtzeitig beantwortet werden, so daß bei der Konkretisierung von UMTS die hier aufgeworfenen Probleme und Lösungen berücksichtigt werden.

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

5 Literatur

[1] ETSI: GSM Recommendations: GSM 01.02 - 12.21. February 1993, Release 92.

[2] M. Spreitzer, M. Theimer: Scalable, Secure, Mobile Computing with Location Information. Communications of the ACM 36/7 (1993).

[3] M. Spreitzer, M. Theimer: Architectural Considerations for Scalable, Secure, Mobile Computing with Location Information. Proceedings of the 14th International Conference on Distributed Systems, IEEE 1994.

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

[5] Thomas Hetschold: Aufbewahrbarkeit von Erreichbarkeits- und Schlüsselinformation im Gewahrsam des Endbenutzers unter Erhaltung der GSM-Funktionalität eines Funknetzes. GMD-Studien Nr. 222, Oktober 1993.

[6] 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.

[7] Hannes Federrath, Dogan Kesdogan, Andreas Pfitzmann, Otto Spaniol: Erreichbarkeits-management und Notrufdienst auf der Basis datensparsamer Adressierung. Arbeitspapier zum Kolleg "Sicherheit in der Kommunikationstechnik" der Gottlieb Daimler - und Karl Benz - Stiftung Ladenburg, April 1994.

[8] Jürgen Thees, Hannes Federrath: Methoden zum Schutz von Verkehrsdaten in Funknetzen. Proc. Verläßliche Informationssysteme (VIS'95), Vieweg 1995, 181-192.

[9] Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüber-prüfbarem Datenschutz. IFB 234, Springer-Verlag, Heidelberg 1990.

Seit dem Erscheinen dieses Artikels sind folgende Arbeiten entstanden:

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

Andreas Fasbender, Dogan Kesdogan, Olaf Kubitz: Analysis of Security and Privacy in Mobile IP. Proc. 4th International Conference on Telecommunication Systems, Modelling and Analysis, Nashville, March 21-24, 1996, 363 - 370.

S.Hoff, K.Jakobs, D.Kesdogan: Anonymous Mobility Management for Third Generation Mobile Networks. IFIP TC11 and TC 6 working conference on Communications and Multimedia Security, Chapmann & Hall, London 1996, 72 - 83.

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, 39-48.

Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy. Information Hiding, First International Workshop, Cambridge, UK, May/June 1996, LNCS 1174, Springer-Verlag, Heidelberg 1996, 121-135.

Hannes Federrath, Elke Franz, Anja Jerichow, Jan Müller, Andreas Pfitzmann: Ein Vertraulichkeit gewährendes Erreichbarkeitsverfahren – Schutz des Aufenthaltsortes in künftigen Mobilkommunikationssystemen. Kommunikation in Verteilten Systemen (KiVS) 97, Informatik aktuell, Springer-Verlag, Heidelberg 1997, 77-91.

Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann, Dirk Trossen: Minimizing the Average Cost of Paging on the Air Interface – An Approach Considering Privacy. Proc. IEEE 47th Annual International Vehicular Technology Conference (VTC 97).