UNIVERSITÄT KARLSRUHE
FAKULTÄT FÜR INFORMATIK
Postfach 63 80, D 7500 Karlsruhe 1

Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes

Andreas Pfitzmann

Institut für Informatik IV, Universität Karlsruhe,
Postfach 6380, D-7500 Karlsruhe 1

Interner Bericht Nr. 18/83 Dezember 1983

Abstract

In practically all proposed or realized public two way communication networks user stations can be easily identified at the Physical-, Data Link- or Network Layer. Therefore the public network (or an intruder) could easily monitor when, how much and with which other instance a user of the public network is communicating, even if end-to-end encryption is used. This is called the traffic analysis problem.

When more and more human-human or human-computer communication uses public networks, the possibility of monitoring becomes unacceptable. Hence a switching/broadcast network structure (SBNS) is derived, which decreases user observability.

The SBNS proposal is

1. physically based on cheap and powerful microelectronics (e. g. personal computers) and on the enormous bandwidth and inherent broadcast facility of local networks and
2. logically based on the generation of random numbers and keys of a public key cryptosystems.

The backbone of the SBNS proposal is a conventional circuit- or packet switched ISDN. The terminals of the switched ISDN are gateways. Each gateway masters a local two-way broadcast network. Each two-way broadcast network connects the user stations of a user group. All services offered by the backbone ISDN are available at the user stations. Implementations of local two-way broadcast networks are discussed and protocols derived, which together can hide the sender and addressee of a message but enable the generation of untraceable return addresses, digital signatures and billing.

Fault tolerance and protection against fraud are discussed.

A cost model shows, that user groups of 10 to 700 users are economically feasible.

After patterns in space of the message traffic are substantially reduced using broadcast it is shown, how patterns in time can be reduced using large local memories. Otherwise, patterns in time could be used to monitor user behavior, too.

The SBNS is compared with the only other known solution to the traffic analysis problem. The other solution is found to be too costly in terms of required bandwidth.

Finally, the connection of a SBNS with other networks is discussed.

Zusammenfassung

In praktisch allen vorgeschlagenen oder realisierten öffentlichen Netzen zur Zweiwegkommunikation können Teilnehmerstationen leicht auf der Physikalischen Ebene, Verbindungs- oder Netzwerkebene identifiziert werden. Deshalb könnte das öffentliche Netz oder ein Eindringling leicht beobachten, wann, wie viel und mit welcher anderen Instanz ein Teilnehmer kommuniziert. Dieses Verkehrsanalyseproblem kann auch durch Ende-zu-Ende-Verschlüsselung nicht verhindert werden. Da mehr und mehr Mensch-Mensch- oder Mensch-Rechner-Kommunikation öffentliche Netze benutzt, wird die Möglichkeit, den Teilnehmer zu beobachten, immer unakzeptabler. Deshalb wird ein Vermittlungs-/Verteilnetz (SBNS = switching/broadcast network structure) hergeleitet, das die Beobachtbarkeit der Teilnehmer wesentlich vermindert. Das SBNS basiert

1. physikalisch auf billiger und leistungsfähiger Mikroelektronik (z. B. Personal Computer) und auf der hohen Übertragungsgeschwindigkeit und inhärenten Broadcast-Fähigkeit lokaler Netze und
2. logisch auf der Erzeugung von Zufallszahlen und Schlüsseln für Kryptosysteme mit öffentlichen Schlüsseln.

Das Fernnetz des SBNS ist ein übliches dienstintegriertes digitales Leitungs- oder Paket-Vermittlungsnetz, dessen Endknoten Protokollumsetzer sind. Jeder Protokollumsetzer ist der Master eines lokalen Zweiweg-Broadcast-Netzes, das die Teilnehmerstationen einer Teilnehmergemeinschaft verbindet. Realisierungen lokaler Zweiweg-Broadcast-Netze werden diskutiert und Protokolle hergeleitet, die zusammen die Identifizierung des Senders oder Empfängers einer Nachricht verhindern können, aber die Bildung von anonymisierten Absendern, digitalen Unterschriften und Abrechnung ermöglichen. Fehlertoleranz und Schutz gegen Betrug werden diskutiert. Ein Kostenmodell zeigt, daß Teilnehmergemeinschaften von 10 bis 700 Teilnehmern günstig sind. Nachdem durch Broadcast räumliche Muster des Nachrichtenverkehrs wesentlich reduziert wurden, wird gezeigt, wie durch lokale Speicherung zeitliche Muster reduziert werden können. Andernfalls könnten zeitliche Muster benutzt werden, um Teilnehmer zu beobachten. Das SBNS wird mit der einzigen bekannten anderen Lösung des Verkehrsanalyseproblems verglichen. Die andere Lösung erfordert zu viel Bandbreite bei der Anwendung in einem dienstintegrierten digitalen Netz. Schließlich werden Verbindungsmöglichkeiten des SBNS mit anderen Netzen diskutiert.

Schlagwörter

Neue Medien, Datenschutz, Bildschirmtext, dienstintegriertes digitales Netz, ISDN, Vermittlungsnetz, Verteilnetz, Offenes System, traffic analysis, Verkehrsanalyseproblem, Kryptosysteme mit öffentlichen Schlüsseln, BIGFON, Datenschutz-Ergonomie

CR Categories

C.2.0 COMPUTER-COMMUNICATION NETWORKS; GENERAL;
Security and protection

E.3 DATA ENCRYPTION; Public key cryptosystems

H.4.3 INFORMATION SYSTEMS APPLICATIONS;
Communications Applications,
Electronic mail, Videotex

K.4.1 COMPUTING MILLIEUX; COMPUTERS AND SOCIETY;
Public Policy Issues; Privacy

Dieser Bericht umfaßt [Pfit_83] in verbesserter und stark detaillierter Form und den Inhalt von [Pfit_84].

Inhaltsverzeichnis

Bilderverzeichnis

1 Motivation

> With the development of television,
> and the technical advance which
> made it possible to receive and transmit
> simultaneously on the same instrument,
> private life came to an end.
>
> George Orwell

Über die Datenschutzproblematik der sogenannten Neuen Medien und unter ihnen insbesondere Bildschirmtext ist in den letzten Jahren viel diskutiert und geschrieben worden u. a. [Alke_82, Bull_82, Date_81, Gars_82, Leuz_82 Seite 113ff, Rein_81, Riha_81]. Z. B. könnte bei Bildschirmtext die Bildschirmtextzentrale nicht nur registrieren, wer welche Zeitung liest, sondern auch wer welche Artikel der Zeitung in welcher Reihenfolge wie gründlich (lange) liest. Die Länge der Beschäftigung mit der letzten übertragenen Seite einer Sitzung sowie das zeitweilige 'aus dem Fenster schauen' des Teilnehmers sind nicht erfaßbar. Dies dürfte bei einer längeren Registrierung aber kaum stören.
Allen mir bekannten Beiträgen zur Datenschutzproblematik der Neuen Medien ist gemeinsam, daß die z. B. in [KaHa_81, Kunz_83] beschriebenen Netz-Strukturen als gegeben und unveränderlich hingenommen werden. Insbesondere wird hingenommen, daß durch die Netz-Struktur bedingt die Teilnehmer auf der untersten Ebene (Physical Layer) eines Offenen Systems [DaZi_83, Jard_83, OSI_83] identifiziert werden können. Es ist dann nur noch über Gesetzgebung und Vorschriften sowie entsprechende Programmierung der Vermittlungszentralen möglich, die personenbezogenen Daten der Teilnehmer zu schützen. Gesetzgebung und Vermittlungszentralen sind aber

- für den Teilnehmer schwer verständlich bzw. undurchschaubar und
- ohne ausdrückliche Information und Zustimmung des Teilnehmers änderbar.

Folglich ist das Vertrauen vieler Teilnehmer in diese Form des Datenschutzes sehr gering und auch durch die Arbeit von Datenschutzbeauftragten, deren Kompetenzen ebenfalls nicht der Teilnehmer, sondern der Gesetzgeber festlegt, nicht wesentlich zu erhöhen.
Als Beispiel seien die Bestrebungen der baden-württembergischen

Landesregierung genannt, die Kompetenzen des Landesbeauftragten für den Datenschutz einzuschränken. Die Landesbeauftragte für den Datenschutz, Frau Dr. Ruth Leuze, schreibt in der Schlußbemerkung ihres 3. Tätigkeitsberichtes [Leuz_82]:

> "Das Jahr 1982 war ein schwieriges Jahr für den Datenschutz in Baden-Württemberg. Es stand ganz im Zeichen der Bestrebungen, den Datenschutz zurückzudrängen und so zurechtzubiegen, daß die Verwaltung altgewohnte Vorgehensweisen fortsetzen und sogar ausbauen kann."

Es ist also wünschenswert, zumindest einen Teil des Datenschutzes in dem Bereich des Systems zu realisieren, über den ausschließlich der Teilnehmer bzw. eine Teilnehmergemeinschaft verfügt. Dieser Teil des Datenschutzes ist dann nicht einfach per Gesetz aufhebbar.

Die in [Pete_81 Seite 83] getroffene Feststellung:

> "Ein Mißbrauch" (von personenbezogenen Daten) "kann strikt nur dann verhindert werden, wenn bereits die Speicherung unterbunden bzw. auf das für den Betrieb unerläßliche Maß reduziert wird."

muß also verschärft werden:

> Ein Mißbrauch von personenbezogenen Daten kann strikt nur dann verhindert werden, wenn bereits die Datenerfassungsmöglichkeit unterbunden bzw. auf das für den Betrieb unerläßliche Maß reduziert wird.

2 Vor- und Nachteile von Vermittlungs- und Verteilnetzen

> Es läßt sich erwarten,
> daß in Zukunft kein Instrument der Macht
> von Menschen über Menschen stärker sein wird
> als das der Informationstechnik.
>
> H. Sachsse

Die auf Vermittlungsnetzen (Bild 1) basierenden Neuen Medien Bildschirmtext, Kabeltextabruf [KaHa_81] und alle Dienste über das geplante BIGFON (breitbandiges integriertes Glasfaser-Fernmeldeortsnetz) [Brau_83] haben aus der Sicht des Teilnehmers folgende Vorteile (+) bzw. Nachteile (-):

+ Informationen können schnell aus beliebig großen Informationsangeboten (z. B. auch aus Euronet/Diane-Datenbanken [Bosc_82])

ausgewählt und vermittelt werden.

+ Dialoge zwischen Teilnehmer und System sowie zwischen Teilnehmer und Teilnehmer sind möglich.
- Da Teilnehmer auf den unteren Ebenen (Physical-, Data Link-, Network Layer) des Vermittlungsnetzes identifiziert werden können, werden Datenschutzmaßnahmen hauptsächlich in den Vermittlungszentralen realisiert. Diese Vermittlungszentralen könnten durch Erfassung, Speicherung und Auswertung der Betriebsdaten, die das Kommunikationsverhalten widerspiegeln, Teilnehmerprofile erstellen. Werden keine (oder unzureichende) kryptographische Verfahren angewandt, könnten die Vermittlungszentralen auch den Kommunikationsinhalt verwerten.
- Der Datenschutz ist per Gesetzes- und Softwareänderung in den Vermittlungszentralen schnell einschränkbar.

Komplementäre Vor- und Nachteile besitzen die auf Verteilnetzen ohne Rückkanal (Bild 2) basierenden Neuen Medien Videotext und Kabeltext [KaHa_81]:

- Bei gegebener Auswahlzeit ist die Informationsmenge, aus der ausgewählt werden kann, durch die Bandbreite des Verteilnetzes und die lokal verfügbare Speicherkapazität [PoPo_83] begrenzt.
- Dialoge sind nicht möglich.
+ Da es zu keiner Kommunikation zwischen Teilnehmer und Verteilzentrale kommt, entstehen auch auf diese Weise keine personenbezogenen Daten, also sind auch keine zu schützen.

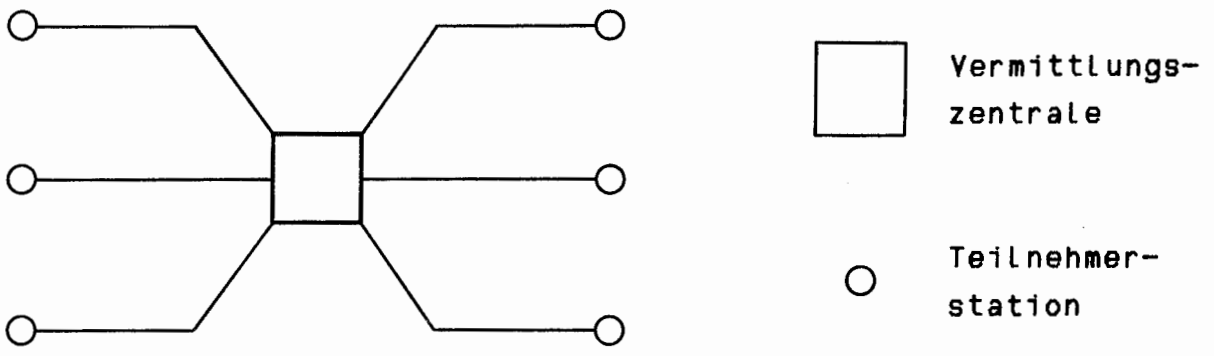
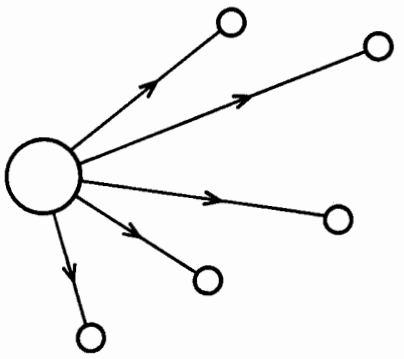
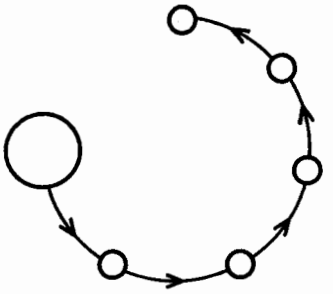


Bild_1: Vermittlungsnetz



Realisierung durch eine Leitung pro Teilnehmerstation



Realisierung durch eine Sammelleitung. Die Sammelleitung ist im Allgemeinen wesentlich kürzer als die Leitungen links, erfordert aber, daß jede Teilnehmerstation die verteilte Information unverfälscht weitergibt.

Verteilnetzzentrale

Teilnehmerstation

Bild 2: Verteilnetz ohne Rückkanal

3 Ein den Datenschutz-Bedürfnissen des Teilnehmers angepaßtes Vermittlungs-/Verteilnetz

Der Umgang mit ganzen Rechnersystemen, die sich über Kontinente erstrecken, kann nicht mehr wertfrei sein.

Wolfgang Händler

Der Teilnehmer wird sich natürlich ein System wünschen, das möglichst viele Vorteile von Vermittlungs- und Verteilnetzen unter Vermeidung möglichst vieler Nachteile zu vertretbaren Kosten realisiert.

Da Vor- und Nachteile von Vermittlungs- und Verteilnetzen sich komplementär zueinander verhalten, liegt es nahe zu versuchen, ein obige Teilnehmerwünsche befriedigendes System durch eine

Synthese von Vermittlungs- und Verteilnetz zu erhalten.

3.1 Voraussetzungen und Randbedingungen

> Rückblickend kann man immer wieder feststellen,
> wie stark hier das Denkbare -
> und damit auch das zur theoretischen
> Auseinandersetzung Herausfordernde -
> abhängig gewesen ist vom
> jeweils technisch Machbaren.
>
> K. H. Beckurts

Hierbei müssen einige durch den Stand der Technik und bereits vorhandene Einrichtungen gegebene Randbedingungen und Voraussetzungen beachtet werden:

R1 Die heute und in den nächsten Jahren vorhandenen, weit verbreiteten Vermittlungsnetze sind schmalbandig und ihre Benutzung relativ teuer [Dorr_83, KaHa_81, RosK_82, Bild_83].

R2 Die Koaxialkabeltechnik [Czaa_82, KOHT_83] und die Glasfasertechnik [BEGW_83] ermöglichen (abgesehen von in etwa konstant gebliebenen und bleibenden Kosten der Kabelverlegung) sehr preiswerte, breitbandige Verteil- und Vermittlungsnetze. Glasfasernetze sind zudem schwierig abhörbar [Norm_83 Seite 265]. Diese neuen Netze können sich im privaten, lokalen Bereich sehr schnell durchsetzen, während die Verkabelung der gesamten Bundesrepublik erheblich länger dauern wird.

R3 Vorhandene Koaxial-Gemeinschaftsantennenanlagen [Verk_83] zeigen, daß Teilnehmergemeinschaften in der Lage sind, eigene, lokale Verteilnetze installieren zu lassen und sich um deren Instandhaltung zu kümmern.

R4 Es gibt preiswerte Heim-Computer Systeme mit Schnittstellen zu einem Akustikkoppler, zu Bildschirmtext [Tiet_82 Seite 446] und zu lokalen Netzen [Farb_83] oder -andersherum betrachtet- intelligente Bildschirmtextdecoder [BMPS_83, Jabu_83, JaMM_83, MaPo_82, MauP_82, Mau1_83, Mau2_83].

R5 Kryptosysteme mit öffentlichen Schlüsseln (public key cryptosystems) sind verfügbar [Baue_82, Beth_82, comp_83, Denn_82, Laks_83, Leis_82, tuto_81]. In ihnen gehört zu jedem öffentlichen Schlüssel ö ein privater Schlüssel p. Aus ö kann

p nicht mit vernünftigem Aufwand hergeleitet werden. Mit ö verschlüsselte Nachrichten können nur mit Hilfe von p entschlüsselt werden (und in manchen Kryptosystemen mit öffentlichen Schlüsseln auch umgekehrt, z. B. in [RSA_78]). Für Nachrichten N geeigneter Länge gilt:

p(ö(N)) = N, d. h. die mit dem öffentlichen Schlüssel ö verschlüsselten Nachrichten können mit dem privaten Schlüssel p entschlüsselt werden. Diese Eigenschaft wird in diesem Papier benutzt.

ö(p(N)) = N, d. h. die mit dem privaten Schlüssel p verschlüsselten (unterschriebenen) Nachrichten können in manchen Kryptosystemen mit öffentlichen Schlüsseln mit dem öffentlichen Schlüssel entschlüsselt werden (die Unterschrift kann auf Echtheit geprüft werden). Diese Eigenschaft wird für elektronische Unterschriften benutzt [Riha_83].

Gilt ö(p(N)) = N in einem Kryptosystem nicht, so läßt sich diese Eigenschaft durch Verwendung zweier Schlüsselpaare simulieren [Giff_82 Seite 279], wenn nicht nur, wie oben gefordert, p aus ö nicht mit vernünftigem Aufwand hergeleitet werden kann, sondern auch ö nicht aus p.

Es wird angenommen, daß es mindestens ein sicheres (d. h. durch kein kryptanalytisches Verfahren in vernünftiger Zeit entschlüsselbares) und zugleich preiswert einsetzbares Kryptosystem mit öffentlichen Schlüsseln gibt. Dies wird für einige bekannte Kryptosysteme mit öffentlichen Schlüsseln allgemein vermutet. Ein Beweis dieser Vermutung ist mir nicht bekannt. In dieser Arbeit wird unterstellt, daß das verwendete Kryptosystem mit öffentlichen Schlüsseln sicher ist. Ein Großteil der Anonymität der Teilnehmer in Verteilsystemen mit Rückkanal (Abschnitt 3.2.2 und 3.2.3) beruht jedoch nicht auf der Sicherheit des Kryptosystems mit öffentlichen Schüsseln sondern darauf, daß Schlüssel dauernd gewechselt werden und ein Beobachter nicht weiß, welche Nachrichten für ihn überhaupt interessant sind.

Im folgenden wird stets angenommen, daß alle Nachrichten, Adressen etc. vor ihrer Verschlüsselung an eine genügend lange Zufallszahl gehängt werden, damit nicht die Nachricht,

Adresse etc. erraten und diese Vermutung durch Verschlüsselung mit dem öffentlichen Schlüssel verifiziert werden kann. Um die Notation kompakt zu halten, sind diese Zufallszahlen in ihr nicht aufgeführt.
öffentliche Schlüssel eines Kryptosystems mit öffentlichen Schlüsseln sind etwas prinzipiell anderes als "öffentliche" Schlüssel eines Kryptosystems mit privaten Schlüsseln. Z. B. erlaubt <<verwende die FAZ von vorgestern oder vorvorgestern ab Seite 3 Spalte 2 als "öffentlichen" Schlüssel und bitweise modulo 2 Addition als Kryptosystem mit privaten Schlüsseln>> keine geheime Kommunikation zwischen zwei Partnern, die sich nicht kennen, also insbesondere keine Vereinbarung über einen "öffentlichen" Schlüssel treffen konnten.

R6 Es gibt physikalische Zufallsgeneratoren (man verstärke etwa das Rauschen in einem Widerstand und digitalisiere das verstärkte Rauschen) und (sofern dies zu teuer oder zu langsam ist) die Möglichkeit, aus kurzen Zufallsfolgen lange Pseudozufallsfolgen algorithmisch so herzuleiten, daß die Kenntnis einiger Elemente der langen Pseudozufallsfolge die Bestimmung anderer Elemente der langen Pseudozufallsfolge nicht erlaubt [Sham_83].

3.2 Fünf Lösungsalternativen

Quidquid agis,
prudenter agas
et respice finem.
lat. Sprichwort

In den folgenden Unterabschnitten werden 5 Lösungsalternativen beschrieben und bewertet.
Die erste Lösungsalternative simuliert den heute üblichen Weg der Informationsbeschaffung durch Kauf von Zeitungen, Zeitschriften oder Büchern. Abrechnungsprobleme und Verschwendung von Bandbreite verhindern die Anwendung dieser ersten Lösungsalternative.
Die zweite Lösungsalternative ist eine neue Kombination aus lokalen Verteilnetzen mit Rückkanal (sogenannten LANs = Local Area Networks) und Kryptosystemen mit öffentlichen Schlüsseln.
Die dritte Lösungsalternative entwickelt die zweite so weiter,

daß sie mit wirtschaftlichem Aufwand realisierbar wird: das Vermittlungs-/Verteilnetz ist der Kernpunkt dieser Arbeit.
Die vierte Lösungsalternative ist eine nur der Systematik halber aufgeführte Kombination aus einem von der Post betriebenen Vermittlungsnetz als Fernnetz und privat betriebenen lokalen Vermittlungsnetzen.
Bei der fünften Lösungsalternative sind sowohl das Fernnetz als auch die lokalen Netze als Verteilnetz mit Rückkanal realisiert. Dies kann bei Satelliten-Netzen als Fernnetz interessant sein.

3.2.1 Vermittlung sehr großer Informationsmengen

> Using the new medium
> to simulate an old one
> seemed like the most
> natural thing in the world.
> Andrew S. Tanenbaum

Eine Lösungsalternative besteht darin, die Datenerfassungsmöglichkeit in einem Vermittlungssystem dadurch zu erniedrigen, daß nur sehr große Informationsmengen zum Teilnehmer übertragen werden, aus denen er lokal die Information auswählt, die ihn wirklich interessiert. Zum Beispiel fordert der Teilnehmer eine komplette Tageszeitung oder gar alle aktuellen Tageszeitungen an und wählt lokal und von der Vermittlungszentrale nicht kontrollierbar die Artikel bzw. die Zeitung aus, die ihn interessieren. R1 verbietet ein solches Vorgehen zumindest in den nächsten Jahren, da hohe Übertragungskosten, vor allem aber hohe Übertragungszeiten entstünden.
Ein in der Benutzung sehr billiges und sehr breitbandiges Glasfasernetz (z. B. ein dienstintegriertes breitbandiges digitales Netz = Breitband-ISDN) ist Voraussetzung für diese Lösungsalternative. In jedem Fall entstehen Probleme bei der Abrechnung gebührenpflichtiger Informationsangebote, da der Teilnehmer z. B. nicht alle angeforderten Tageszeitungen wird bezahlen wollen. Vom Teilnehmer überprüfbarer Datenschutz (im obigen Beispiel das Anfordern aller Tageszeitungen) sollte aber keine Geldfrage bei jeder einzelnen Benutzung eines Systems sein.

3.2.2 Verteilnetz mit Rückkanal

Die Informationsverarbeitung
ist Chance und Einladung,
in neuen Kategorien
zu denken und zu arbeiten
IBM

Die zweite Lösungsalternative besteht darin, daß die Post ein Verteilnetz mit Rückkanal (Bild 3) betreibt.

Bild 3: Verteilnetz mit Rückkanal

Zunächst werden einige Hinweise zur Realisierung eines Verteilnetzes mit Rückkanal gegeben.
Danach wird das Kommunikationsprotokoll zur anonymen Kommunikation innerhalb eines Verteilnetzes mit Rückkanal erklärt.

3.2.2.1 Hinweise zur Realisierung

Erfindungen und Innovationen sind zwar
an die technischen Mittel gebunden,
aber es gilt nicht umgekehrt,
daß ihre Entwicklung sofort einsetzt,
sobald die technischen Voraussetzungen
gegeben sind.
Konrad Zuse

Die Realisierung eines Verteilnetzes mit Rückkanal sollte so erfolgen, daß der Sender einer Nachricht auch durch Anschluß physikalischer Meßgeräte an einer beliebigen Stelle des Verteil-

netzes nicht oder zumindest nur sehr, sehr schwierig festgestellt werden kann. Diese Forderung ist die maximale Forderung, die man durch geeignete Vergabe der Sendeberechtigung und geeignete Leitungstopologie erfüllen kann: durch Anschluß physikalischer Meßgeräte an zwei beliebigen Stellen, nämlich direkt vor und nach einer Teilnehmerstation, kann die Teilnehmerstation beobachtet werden, egal wie die Sendeberechtigung vergeben und die Leitungstopologie gewählt wird.

1) Die Vergabe der Sendeberechtigung muß anonym und verteilt erfolgen, damit durch sie der Sender nicht identifiziert werden kann. Geeignete Verfahren sind ALOHA, Reservation-ALOHA, Tree Algorithms, Empty-slot-Technik (Pierce Loop), sofern Absenderstationen einen benutzten slot sofort wieder benutzen dürfen ~~oder schon die adressierte Station den empfangenen slot freigibt,~~ und Register-insertion-Technik (delay insertion loop, DLCN = Distributed Loop Computer Network) [FroI_82, Gerk_82, Liu_78, Moll_83, ReLi_76, Span_82, TanA_81 Seite 253ff, 272, 288ff, 312ff, Tane_81 Seite 460, 467, 468, Toba_80, Weit_80 Seite 61ff].

Dürfen bei Empty-slot-Technik Stationen benutzte slots nicht sofort wieder benutzen (was aus Gründen des fairen Ringzugangs sinnvoll ist) und werden slots vom Sender nach einem Ringumlauf freigegeben, ist Empty-slot-Technik kein geeignetes Verfahren, wenn die Anzahl der slots auf dem Ring, die Anzahl n der Stationen im Ring und die Reihenfolge der Stationen im Ring bekannt ist. Jede Station S im Ring kann die Absender der Nachrichten(teile) in einem bestimmten slot s identifizieren, wenn alle anderen n-1 Stationen s nacheinander benutzen. S erkennt dies daran, daß s n-1 mal hintereinander gefüllt bei ihr vorbeikommt.

Das bei Bussen häufig verwendete CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ist kein geeignetes Verfahren, da eine kurze Pause P zwischen zwei Nachrichten mit hoher Wahrscheinlichkeit die Bestimmung der Länge L des Mediums zwischen den zwei sendenden Stationen erlaubt, d. h. aus der Sicht der zuerst sendenden Station die zweite sendende Station identifiziert. Ist die Pause P kurz genug, so hörte die zweite Station mit hoher Wahrscheinlichkeit mit (carrier sense), um nach dem Ende der Nachricht sofort ihre Nachricht zu senden. Es gilt dann

P = Reaktionszeit_von_Station_2 +
2 * L / Signalgeschwindigkeit_im_Medium

also

L = (P - Reaktionszeit_von_Station_2) *
Signalgeschwindigkeit_im_Medium / 2

Analoges gilt bezüglich der Zeit, die vergeht, bis eine Kollision erkannt wird (collision detection).

Weitergabe der Sendeberechtigung für maximal eine Nachricht in einem Ring (token ring, Newhall Loop) [Gerk_82 Seite 205, TanA_81 Seite 307ff, Tane_81 Seite 468, Weit_80 Seite 61ff] ist kein geeignetes Verfahren: ist einer Station S die Reihenfolge der Stationen im Ring bekannt, dann kann S, wenn alle Stationen senden, während die Sendeberechtigung einmal von S bis S umläuft, den Absender jeder dieser Nachrichten identifizieren. Dabei wurde angenommen, daß alle Nachrichten von S empfangen werden oder S passieren. Dies ist immer der Fall, wenn der Sender einer Nachricht sie vom Ring nimmt. Falls bereits der Empfänger einer Nachricht sie vom Ring nimmt, ist es auch möglich. Wahrscheinlich ist es in diesem Fall bei einem großen Ring allerdings nur, wenn es in diesem Ring eine zentrale Station (z. B. Verteilnetzzentrale im Vermittlungs-/Verteilnetz, vgl. Abschnitt 3.2.3) gibt, die fast alle Nachrichten der anderen Stationen empfängt und S diese zentrale Station selbst oder die Station davor ist.

Gleiches gilt für den contention ring [TanA_81 Seite 311].

Weitergabe der Sendeberechtigung für alle absendebereiten Nachrichten in einem Ring erlaubt zwar nicht die Identifizierung von Sendern mit Sicherheit, erleichtert aber statistische "Angriffe", da Sendereihenfolge und Reihenfolge im Ring übereinstimmen. Also ist auch dieses Verfahren ungeeignet.

2) Neben der Vergabe der Sendeberechtigung kann auch die Leitungstopologie (Bus, Ring) Sender identifizieren, falls an die Leitung an einer Stelle geeignete Meßgeräte angeschlossen werden.

Beispielsweise kann eine ganz am Ende eines Busses angeschlossene Teilnehmerstation als Sender einer Nachricht identifiziert werden, indem zwischen ihrem Bus-Anschluß und den Bus-Anschlüssen der anderen Teilnehmerstationen an den Bus Meßgeräte angeschlossen werden, die die Ausbreitungsrichtung der Signale bestimmen.

Unter der Annahme ungleicher Sender läßt sich anhand der senderspezifischen Signalform zuordnen, welche Nachricht von welchem Sender kommt. Die Zuordnung Sender-Teilnehmerstation-Teilnehmer läßt sich dann feststellen, indem man in Zeiten minimalen Verkehrs (vgl. Abschnitt 3.3) von außerhalb fingierte Anfragen an alle Teilnehmerstationen sendet und die Signalform der Antworten beobachtet.

Unter der Annahme gleicher Sender läßt sich anhand der Signalform (verschiedene Frequenzkomponenten breiten sich verschieden schnell aus = Dispersion) möglicherweise sogar die Leitungslänge zwischen Sender und Meßgerät bestimmen, so daß die Sender von Nachrichten identifizierbar sind, wenn entweder der genaue Verlauf des Busses bekannt ist oder fingierte Anfragen in Zeiten minimalen Verkehrs (vgl. Abschnitt 3.3) an alle Teilnehmerstationen gesendet werden und die Signalform der Antworten beobachtet wird.

Hieraus folgt, daß als Leitungstopologie ein Ring (Serie von Punkt-zu-Punkt Kabeln zwischen aufeinanderfolgenden Teilnehmerstationen [TanA_81 Seite 307]) mit Vergabe der Sendeberechtigung durch Empty-slot-Technik (Pierce Loop), sofern Absenderstationen einen benutzten slot sofort wieder benutzen dürfen oder schon die adressierte Station den empfangenen slot freigibt, oder Buffer-insertion- (Register-insertion-)Technik (Delay Insertion Loop) von allen bekannten lokalen Rechnernetzkonzepten den größten Datenschutz bietet:

+ Es gibt keine am Ende angeschlossene Teilnehmerstation, da der Sender einer Nachricht sie nach genau einem Umlauf wieder vom Ring entfernt.
+ Alle Signale auf einem Kabel breiten sich in dieselbe Richtung aus.
+ Die Analyse der genauen Signalformen ergibt keinen Aufschluß über den (logischen) Absender der Nachricht, da für jedes Punkt-zu-Punkt Kabel genau ein (physikalischer) Sender existiert.

Um eine Teilnehmerstation in einer Pierce Loop, in der Absenderstationen einen benutzten slot sofort wieder benutzen dürfen oder schon die adressierte Staion den empfangenen slot freigibt, oder Delay Insertion Loop als Sender zu identifizieren, muß der Ring direkt vor und hinter ihr abgehört sowie das Abgehörte verglichen

werden. Dieses Abhören direkt vor und hinter einer Teilnehmerstation wird unmöglich gemacht oder zumindest sehr erschwert, indem der Ring an möglichst wenig Stellen durch öffentlich zugängliches Gebiet geführt wird. Z. B. werden die Wohnungen eines Mehrfamilienhauses direkt und ohne Umweg über Treppenhaus oder gar zentrale Kabelverteilkästen im Haus miteinander verbunden. Dies erhöht nicht nur den Datenschutz, sondern spart auch Kabellänge und damit Geld, vgl. Abschnitt 3.2.3.6. Diese Form der Verkabelung hat sich bei Gemeinschaftsantennenanlagen seit langem bewährt.

Wie alle Ringe haben Pierce Loop und Delay Insertion Loop folgende Vor- und Nachteile [SaPC_83]:

+ Sender und Empfänger der Punkt-zu-Punkt Kabel können gut aufeinander eingestellt werden.
+ Punkt-zu-Punkt Kabel lassen sich in Glasfasertechnik wesentlich günstiger realisieren als verteilte Bus-Systeme. Es gibt zwar zentralisierte optische Bus-Systeme, sogenannte Sternbusse (z. B. SIELOCnet [Baue_83]), doch sind diese aus Gründen des Datenschutzes ungeeignet, da es eine Stelle gibt, den Sternkoppler, an der das Verhalten aller Teilnehmerstationen beobachtet werden kann.
- Die vielen aktiven Sender im Ring bilden ein Serien-System bezüglich ihrer Verfügbarkeit. Dies muß und kann innerhalb gewisser Grenzen (vgl. [PfHä_82] oder [Pfit_82]) durch eine sich bei Ausfall der Teilnehmerstation automatisch schließenden By-Pass-Einrichtung und geeignete Dimensionierung von Sender und Empfänger kompensiert werden.

  Aus Datenschutzgründen muß die By-Pass-Einrichtung bei der Teilnehmerstation installiert sein und sie darf nur durch Ausfall der Teilnehmerstation oder Handschalter innerhalb der Wohnung des Teilnehmers geschlossen werden. Sonst könnte man die By-Pass-Einrichtung zur Identifizierung von Sendern benutzen, etwa indem man die By-Pass-Einrichtung schließt, wenn man vermutet, daß die Teilnehmerstation sendet oder empfängt. Bricht die Nachricht ab oder bleibt eine Empfangsquittung aus, war die Vermutung richtig.

  Statt By-Pass-Einrichtungen kann auch ein die Übertragungsleistung und die Verfügbarkeit steigernder doppelter Ring verwendet werden. Allerdings sollte die dann zu treffende Routing-Entscheidung nicht wie bei DDLCN [WLWT_79, Wolf_79, WoWL_79, LTCL_81, Flin_83] den kürzesten Weg zum Empfänger

wählen, sondern einen möglichen Weg zufällig. Andernfalls gibt es ganz am "Ende" angeschlossene Teilnehmerstationen, die von ihren Nachbarn leicht beobachtet werden könnten. Ab dem Ausfall von beiden Leitungen eines Leitungsabschnitts oder dem Ausfall einer Teilnehmerstation geht ein Teil des Datenschutzes verloren, da die angrenzenden Stationen durch ihre dann einzige "Verbindungsstation" zum Rest des doppelten Rings beobachtet werden können. Solange nur einzelne Leitungen eines Leitungsabschnitts und keine Teilnehmerstation ausgefallen sind, sollte ein Ring gegebenenfalls rekonfiguriert werden und, um den Datenschutz zu erhalten, nur er zum Informationsaustausch genutzt werden.

3.2.2.2 Das Kommunikationsprotokoll

> ... once we are resigned to
> having a central authority
> that knows everything,
> say Big Brother (BB),
> both secrecy and digital signatures
> can be obtained using
> conventional cryptography.
>
> Andrew S. Tanenbaum

Um eine Zuordnungsmöglichkeit der Nachrichten zu anonymen Teilnehmern zu vermeiden, erzeugt jede Teilnehmerstation für jede Informationsabfrage F bei der Verteilnetzzentrale neu eine Zufallszahl F_z, einen öffentlichen Schlüssel F_ö und einen zu F_ö gehörigen privaten Schlüssel F_p. F_z und F_ö bilden zusammen einen anonymisierten Absender.
Über den Rückkanal überträgt die Teilnehmerstation (mit dem öffentlichen Schlüssel ö der Verteilnetzzentrale verschlüsselt) F_z, F_ö und ihre Frage F_f (Bild 4). F_z und die mit F_ö verschlüsselte Antwort F_a auf F_f wird von der Verteilnetzzentrale an alle Teilnehmerstationen verteilt. Die Teilnehmerstation erkennt ihre Zufallszahl F_z und entschlüsselt mit dem zugehörigen privaten Schlüssel F_p die gewünschte Information.

ö öffentlicher Schlüssel der Verteilnetzzentrale

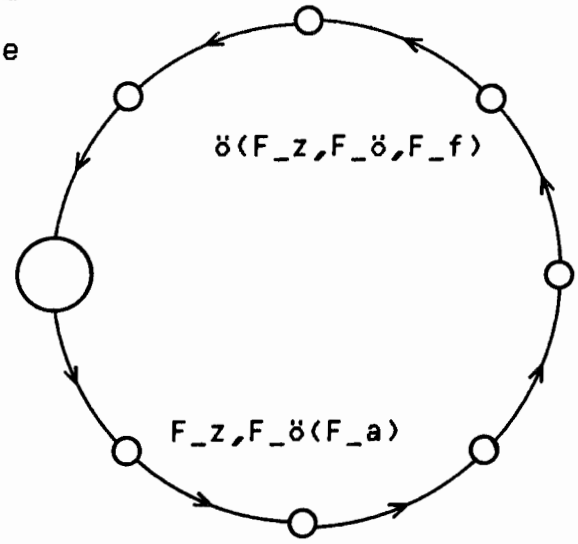
p privater Schlüssel der Verteilnetzzentrale

F_z

F_ö

F_f

F_a Antwort



ö

F_z Zufallszahl für F

F_ö öffentlicher Schlüssel für F

F_p privater Schlüssel für F

F_f Frage

F_a

Bild_4: Kommunikation im Verteilnetz mit Rückkanal

Über die Verteilnetzzentrale ist auch Kommunikation zwischen Teilnehmerstationen möglich.
Die Abrechnung gebührenpflichtiger Informationsabfragen kann wie in Abschnitt 3.2.3.3 geschildert erfolgen.
Diese zweite Lösungsalternative erfordert ein sehr, sehr breitbandiges weitverbreitetes Verteilsystem mit Rückkanal, das es zur Zeit nicht gibt und dessen Realisierbarkeit trotz Glasfasertechnik zweifelhaft erscheint. Zumindest wäre eine Realisierung sehr teuer, störanfällig und nur innerhalb eines längeren Zeitraums möglich, vgl. R2.
Die leistungsfähigsten heute im Laborbetrieb realisierten Glasfasernetze haben eine Datenrate von 2 Gbit/s [BEGW_83]. Würde

man solch ein Netz ausschließlich für Bildschirmtext von heute vorgesehener Qualität (1200 bit/s Vorwärtskanal, 75 bit/s Rückwärtskanal [Kunz_83]) verwenden und nimmt man an, daß Vorwärts-, Rückwärtskanal und alle zusätzlich zu transportierende Information etwa 2000 bit/s ergeben, so wären mit einem solchen Glasfasernetz 1 Million Bildschirmtext-Teilnehmer gleichzeitig zu versorgen. Da nicht alle gleichzeitig an Bildschirmtext teilnehmen [Kais_82 Seite 46] und, wenn sie teilnehmen, nicht dauernd Daten übertragen, kann man etwa 10 bis 100 mal so viele Teilnehmer versorgen, also 10 bis 100 Millionen.
Obwohl solch ein Verteilnetz mit Rückkanal also technisch möglich wäre, wird es aus folgenden Gründen nicht realisiert werden:

- Es wäre ein Spezialnetz für Bildschirmtext, da sonst seine Kapazität zu gering wäre. Erstrebenswert ist aber ein dienstintegriertes Netz.
- Es ist anzunehmen, daß die Anforderungen an Bildschirmtext und damit die erforderliche Übertragungskapazität pro Teilnehmer erheblich steigen werden. Dem wäre ein einziges Verteilnetz kaum gewachsen.

Die Idee einer hierarchischen Gliederung des Systems zur Senkung der erforderlichen Übertragungskapazität führt zur dritten Lösungsalternative.

3.2.3 Vermittlungs-/Verteilnetz

> Delegieren von Zuständigkeiten ist ein
> Zeichen souveräner Geisteshaltung.
> Hüten wir uns vor Menschen,
> die alles allein machen wollen.
>
> Edward Heath

Die dritte Lösungsalternative besteht darin, daß die Post ein Vermittlungsnetz betreibt, dessen Endknoten private, lokale Verteilnetze mit Rückkanal sind (Bild 5). Verteilnetzzentralen verbinden Vermittlungs- und Verteilnetz, d. h. sie sind Protokollumsetzer (gateways) [GrHS_83, BeEs_83, Schd_83].
Die in Abschnitt 3.2.2.1 gegebenen Hinweise zur Realisierung eines Verteilnetzes mit Rückkanal gelten auch für die Verteilnetze mit Rückkanal im Vermittlungs-/Verteilnetz. Auch das Kommunika-

tionsprotokoll zur anonymen Kommunikation im Verteilnetz mit Rückkanal von Abschnitt 3.2.2.2 wird im wesentlichen unverändert übernommen.

In allen Erklärungen dieses und der folgenden Unterabschnitte wird aus didaktischen Gründen von einer Unterteilung des Vermittlungs-/Verteilnetzes in genau zwei Netzebenen ausgegangen. Beide Ebenen lassen sich weiter unterteilen. Dies ist besonders beim Fernnetz aus technischen Gründen sinnvoll. Die Abschnitte 3.2.3.6 und 3.2.3.7 zeigen, daß eine Unterteilung des lokalen Verteilnetzes mit Rückkanal nicht nötig ist. Abschnitt 3.2.5 untersucht hierarchisch, d. h. in verschiedenen Netzebenen, angeordnete Verteilnetze mit Rückkanal.

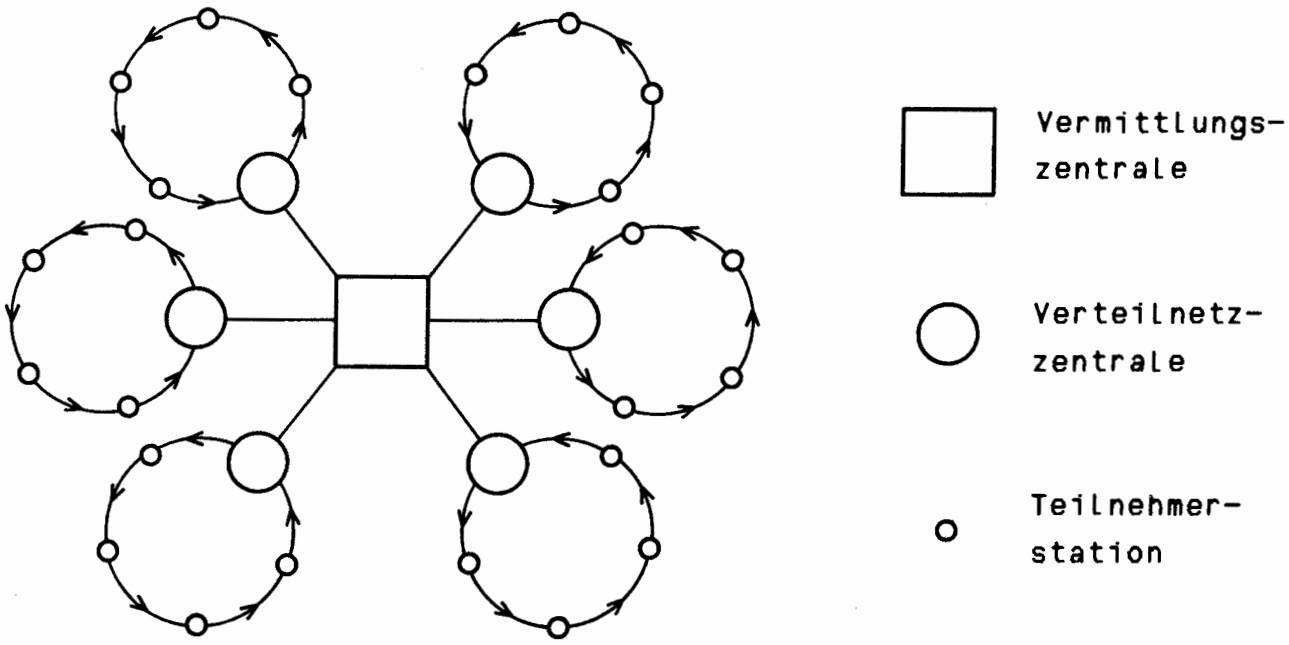


Bild 5: Vermittlungs-/Verteilnetz

3.2.3.1 Adreßverwaltung

It is important to change
one's hiding place frequently.
George Orwell

Die Adressen im Vermittlungs-/Verteilnetz sind aus 2 Komponenten zusammengesetzt:

1) Die erste Komponente ist eine logische Adresse einer Verteilnetzzentrale. Eine Verteilnetzzentrale kann durchaus mehrere logische Adressen haben. Die logischen Adressen einer Verteilnetzzentrale sind nur der Vermittlungszentrale und den Teilnehmerstationen dieser Verteilnetzzentrale bekannt und fest.
2) Die zweite Komponente ist ein Pseudonym einer Teilnehmerstation innerhalb eines lokalen Verteilnetzes mit Rückkanal. Jede Teilnehmerstation kann und sollte mehrere Pseudonyme haben. Pseudonyme können während des Betriebes vernichtet und geschaffen werden. Pseudonyme sind nur der betreffenden Teilnehmerstation bekannt.

Alle Adressen im Vermittlungs-/Verteilnetz werden mit dem öffentlichen Schlüssel ö der Vermittlungszentrale verschlüsselt, bevor sie weitergegeben und von Teilnehmerstationen benutzt werden. Die Vermittlungszentrale entschlüsselt mit ihrem privaten Schlüssel p die Adressen, bevor sie mit deren erster Komponente adressiert, ändert die verschlüsselten Adressen jedoch nicht. Das Verschlüsseln der gesamten Adresse geschieht, damit nicht aus der Übereinstimmung der ersten Komponente von Adressen Schlüsse gezogen werden können.
Zu jeder Adresse im Vermittlungs-/Verteilnetz gibt es einen zugehörigen öffentlichen Schlüssel, mit dem alle Mitteilungen an diese Adresse verschlüsselt werden. Der Empfänger entschlüsselt die Mitteilungen mit dem zugehörigen privaten Schlüssel (vgl. R5 in Abschnitt 3.1).

Alle Teilnehmer, die von allen anderen Teilnehmern erreichbar sein wollen, stehen mit einer ihrer verschlüsselten Adressen, öffentliche Adresse genannt, und dem zugehörigen öffentlichen Schlüssel in einem Teilnehmerverzeichnis. Das Teilnehmerverzeich-

nis kann nach verschiedenen Kriterien (z. B. alphabetisches Namen, -Branchenverzeichnis) sortiert sein. Es muß gegen Manipulation geschützt sein [Inge_83]. Andernfalls könnte ein Teilnehmer abgehört werden: Der Abhörer A kopiert die öffentliche Adresse t und den öffentlichen Schlüssel T_ö des Teilnehmers T und ersetzt beides im Teilnehmerverzeichnis durch eine seiner Adressen a und einen seiner öffentlichen Schlüssel A_ö. A erhält danach die für T bestimmten Nachrichten, kann sie mit A_p entschlüsseln und kopieren. Danach verschlüsselt A die für T bestimmten Nachrichten mit T_ö und sendet sie an die Adresse t.
Neben oder statt einer öffentlichen Adresse kann ein Teilnehmer private verschlüsselte Adressen mit zugehörigen öffentlichen Schlüsseln haben, die er an Freunde, Geschäftspartner etc. weitergibt. Ebenso kann er private Adressen mit zugehörigen öffentlichen Schlüsseln als anonymisierte_Absender benutzen, indem er die private Adresse und das zugehörige Schlüsselpaar nur einmal benutzt. Ein Fremder und insbesondere auch die Vermittlungszentrale kann diesen privaten Adressen keine Teilnehmerstation zuordnen.

3.2.3.2 Das Kommunikationsprotokoll im fehlerfrei arbeitenden Netz

> For the first time he perceived
> that if you want to keep a secret
> you must also hide it from yourself.
> George Orwell

Eine beidseitig strukturbedingt-anonyme Informationsabfrage F einer Teilnehmerstation A bei einer anderen Teilnehmerstation B (d. h. durch den Ablauf von F soll sowohl A möglichst wenig Informationen über B, als auch B möglichst wenig Informationen über A, als auch die Vermittlungszentrale möglichst wenig Informationen über A und/oder B gewinnen können) könnte dann folgendermaßen ablaufen (Bild 6):

Teilnehmerstation A kennt den öffentlichen Schlüssel ö der Vermittlungszentrale, die logische Adresse za ihrer Verteilnetzzentrale ZA und eine Adresse b von Teilnehmerstation B samt dem zugehörigen öffentlichen Schlüssel b_ö.

A hat in Zeiten, in denen es für sie nichts zu tun gab, auf

Vorrat aus einer Zufallszahl F_z eine private Adresse F_pa = ö(za,F_z) errechnet sowie einen öffentlichen Schlüssel F_ö und einen zu F_ö gehörigen privaten Schlüssel F_p erzeugt. Die Erzeugung der privaten Adresse F_pa und des Schlüsselpaares F_ö, F_p für diese eine Informationsabfrage F erfolgt, damit nicht über eine feste private (oder gar öffentliche) Adresse oder fest gewählte öffentliche Schlüssel eine Zuordnungsmöglichkeit der Nachrichten zu anonymen Teilnehmern besteht. F_pa und F_ö bilden zusammen einen anonymisierten Absender.

A sendet die Adresse b von B sowie F_pa, F_ö und ihre Frage F_f mit dem öffentlichen Schlüssel b_ö von B verschlüsselt an ihre Verteilnetzzentrale ZA.

ZA vermittelt die Nachricht an die Vermittlungszentrale.

Die Vermittlungszentrale entschlüsselt b mit ihrem privaten Schlüssel p und vermittelt die Abfrage gemäß der ersten Komponente der Adresse an die Verteilnetzzentrale ZB von B.

ZB verteilt die Nachricht.

B erkennt ihre Adresse b und entschlüsselt mit dem zugehörigen privaten Schlüssel b_p die Nachricht:

b_p(b_ö(F_pa,F_ö,F_f)) = F_pa,F_ö,F_f.

B sendet F_pa und ihre mit F_ö verschlüsselte Antwort F_a an ihre Verteilnetzzentrale ZB.

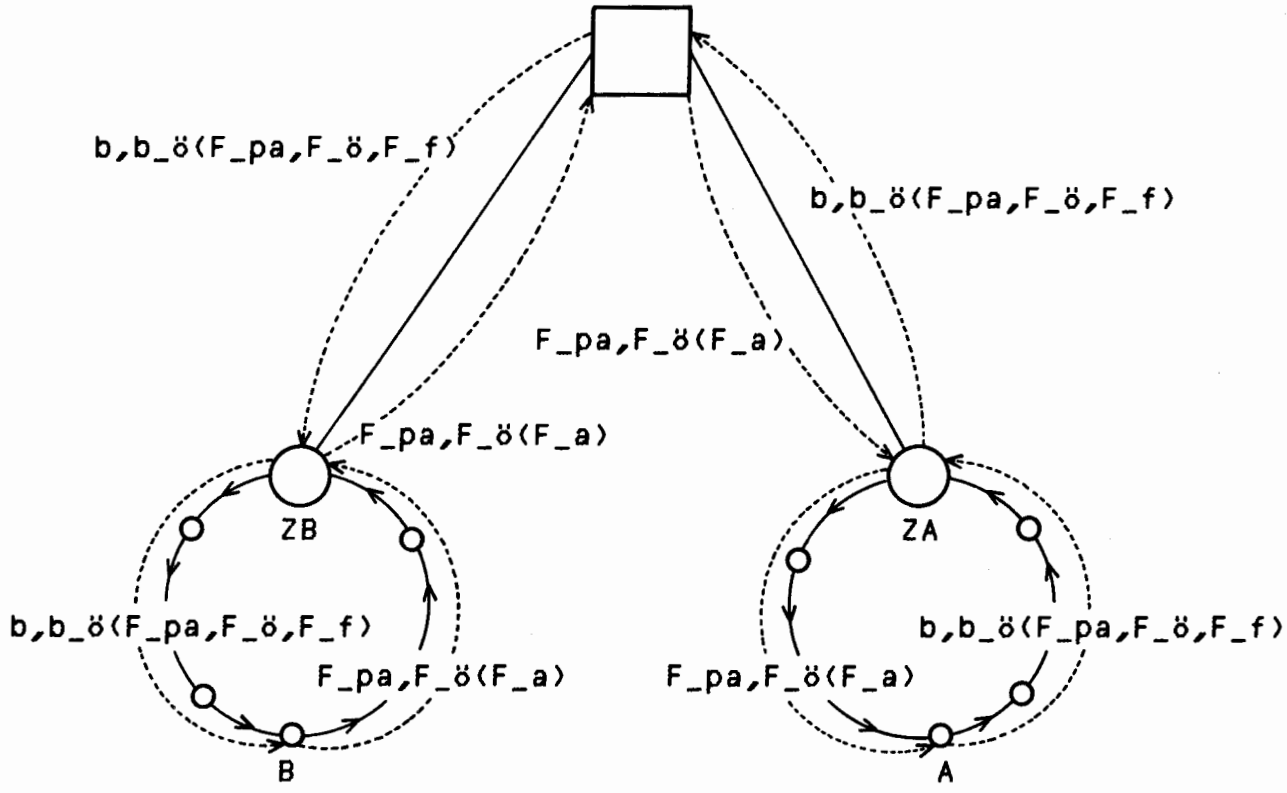
ZB vermittelt die Nachricht an die Vermittlungszentrale.

Die Vermittlungszentrale entschlüsselt F_pa mit ihrem privaten Schlüssel p und vermittelt die Nachricht gemäß der ersten Komponente der Adresse an die Verteilnetzzentrale ZA von A.

ZA verteilt die Nachricht.

A erkennt ihre private Adresse F_pa und entschlüsselt die Antwort mit ihrem für F gewählten privaten Schlüssel F_p.

ö öffentlicher Schlüssel der Vermittlungszentrale
p privater Schlüssel der Vermittlungszentrale
pr1 Projektion auf erste Adreß-Komponente
pr1(p(b)) = zb Adresse von ZB
pr1(p(F_pa)) = za Adresse von ZA



		ö	
		za	logische Adresse der Verteilnetzzentrale ZA von A
b	Adresse von B	b	
b_ö	öffentlicher Schlüssel zu b	b_ö	
b_p	privater Schlüssel zu b	F_z	Zufallszahl für F
		F_pa	= ö(za,F_z) für F gebildete private Adresse von A (anonymisierter Absender)
F_pa		F_ö	öffentlicher Schlüssel für F
F_ö		F_p	privater Schlüssel für F
F_f		F_f	Frage
F_a	Antwort	F_a	

Bild_6: Kommunikation im Vermittlungs-/Verteilnetz

Wenn es angebracht erscheint, überträgt B mit der Antwort ebenfalls einen anonymisierten Absender. Dazu hat B in Zeiten, in denen es für sie nichts zu tun gab, auf Vorrat aus einer Zufallszahl G_z eine private Adresse G_pa = ö(zb,G_z) errechnet sowie einen öffentlichen Schlüssel G_ö und einen zu G_ö gehörigen privaten Schlüssel G_p erzeugt. Statt F_pa,F_ö(F_a) sendet B F_pa,F_ö(G_pa,G_ö,F_a) an A. Dies bietet zwei Vorteile:

1) Ein einheitliches Nachrichtenformat wird möglich.
2) A kann den anonymisierten Absender G_pa,G_ö für die nächste Kommunikation mit B benutzen.

Möchte man wegen neugieriger und gutinformierter Nachbarn die Übertragung einer öffentlichen Adresse b von B im Klartext vermeiden, so kann man obiges Protokoll leicht erweitern:

Die Teilnehmerstation A verschlüsselt b mit ö und überträgt als Adresse statt b ö(b).

Die Vermittlungszentrale entschlüsselt ö(b) einmal zusätzlich mit p und ersetzt ö(b) innerhalb der Nachricht durch b.

Ohne diese zusätzliche Verschlüsselung könnten gutinformierte Nachbarn das Teilnehmerverzeichnis (Verzeichnis der öffentlichen Adressen, vgl. Abschnitt 3.2.3.1) nach b durchsuchen und Vermutungen anstellen, wer ihrer Nachbarn wohl mit B kommuniziert. Zwar läßt sich durch b der Ort von B nicht feststellen (b ist die Verschlüsselung von einer Adresse einer Verteilnetzzentrale und einem Pseudonym, vgl. Abschnitt 3.2.3.1), jedoch kann B durch von ihm explizit gegebene Information im Verzeichnis der öffentlichen Adressen (Werbung, Dienstangebot etc. oder sogar sein Name) so genau charakterisiert werden, daß Neugierde von Nachbarn geweckt wird.

Im nicht dargestellten Fall der Vermittlung einer Nachricht durch mehrere Vermittlungszentralen ist noch zu entscheiden,

1) ob b (und auf dem Rückweg F_pa) in jeder Vermittlungszentrale mit p entschlüsselt wird, dann kann man die Nachricht unverändert durch das gesamte Vermittlungs-/Verteilnetz übertragen, hat aber in jeder durchlaufenen Vermittlungszentrale den Aufwand der Entschlüsselung oder
2) ob b (und auf dem Rückweg F_pa) in der ersten durchlaufenen Vermittlungszentrale mit p entschlüsselt, dann in entschlüs-

selter Form zwischen den Vermittlungszentralen übertragen und in der letzten durchlaufenen Vermittlungszentrale wieder mit ö verschlüsselt wird oder

3) ob b (und auf dem Rückweg F_pa) in der ersten durchlaufenen Vermittlungszentrale mit p entschlüsselt und dann in entschlüsselter Form bis zur Teilnehmerstation übertragen wird, die sich in diesem Fall die "Adressen" vor der Verschlüsselung mit ö (logische Adressen ihrer Verteilnetzzentrale und alle zugehörigen von ihr gewählten Pseudonyme) merken müßte.

Die Möglichkeiten 2) und 3) können zwar Entschlüsselungsaufwand sparen, erfordern aber die Übertragung von unverschlüsselten Adressen im Vermittlungs-/Verteilnetz. Ohne die Übertragung von unverschlüsselten Adressen im Vermittlungs-/Verteilnetz ist es unter der Annahme vertrauenswürdiger Vermittlungszentralen möglich, sich als Inhaber eines anonymisierten Absenders einfach dadurch zu identifizieren, daß man den Absender vor seiner Verschlüsselung mit ö vorweist. Jeder kann durch Verschlüsselung mit ö dies leicht nachprüfen.

3.2.3.3 Abrechnung und Zulassung von Teilnehmerstationen

> If computer insecurity becomes an urgent problem,
> it may be too late to solve it.
> If it does not seem urgent today,
> then there will never be a better chance to start
> doing something about it.
>
> Adrian R. D. Norman

Da manche über ein dienstintegriertes Netz angebotenen Dienstleistungen nicht gebührenfrei sind, muß eine Möglichkeit zur Abrechnung mit Teilnehmern geschaffen werden.
In üblichen Vermittlungsnetzen erfolgt die Abrechnung folgendermaßen:

1) Die Vermittlungszentrale registriert als Repräsentant des Netzbetreibers die Benutzung von Netzbetriebsmitteln durch Teilnehmer. In bestimmten Zeitintervallen erhalten die Teilnehmer von der Vermittlungszentrale Rechnungen.
   Dieser Teil der Abrechnung könnte vermieden werden: wenn die

Datenübertragung immer billiger wird, ist eine "gerechte" Verteilung der Kosten entsprechend der Benutzung der Netzbetriebsmittel unnötig. Eine monatliche Pauschalgebühr ist ausreichend. Die monatliche Pauschalgebühr kann von der maximalen Datenrate abhängen, mit der eine Teilnehmerstation in das Netz Daten übertragen kann und darf.

2) Anbieter von speziellen Dienstleistungen über das Netz kennen ihre Kunden und rechnen direkt mit ihnen ab oder die Vermittlungszentrale ist autorisiert, für die Anbieter mit deren Kunden abzurechnen.
Im zweiten Fall kann die Vermittlungszentrale die Identität des Kunden vor dem Anbieter von speziellen Dienstleistungen verbergen, aber die Vermittlungszentrale kann und muß in diesem Fall die empfangenen speziellen Dienstleistungen registrieren. Diese Lösung hindert also die Anbieter von speziellen Dienstleistungen über das Netz "kleine Brüder" zu werden, indem sie die Vermittlungszentrale in die Lage versetzen, der "große Bruder" zu werden. Mehr über diese Problematik ist in [Orwe_49, Gute_83 Seite 116, Bull_82, Date_81, Gars_82, Pete_81, Rein_81] zu finden.

Die üblichen Formen der Abrechnung sind also in einem Vermittlungs-/Verteilnetz nicht angemessen.
Zwei Lösungen des Abrechnungsproblems mit komplementären Vor- und Nachteilen werden in den folgenden zwei Unterabschnitten beschrieben.

3.2.3.3.1 Anonyme Nummernkonten

> Bei den roten Männern gilt das Wort.
> Die weißen Männer aber verlangen
> ein Papier mit schwarzen Buchstaben.
> Karl May

Die erste Lösung ist eine Weiterentwicklung der Nummernkonten. (Genauere Informationen über Nummernkonten sind bei jeder Schweizer Bank erhältlich.)
Um ein anonymes Nummernkonto zu eröffnen, besucht man selbst (oder eine Person, der man vertraut) eine Geschäftsstelle C einer Bank oder des Netzbetreibers. Man wählt dazu eine Geschäftsstelle,

in der man nicht persönlich bekannt ist. Die Geschäftsstelle gibt einem eine Kontonummer n, man nennt der Geschäftsstelle einen von der eigenen Teilnehmerstation generierten öffentlichen Schlüssel n_ö. Der entsprechende private Schlüssel n_p wird als Passwort für das anonyme Nummernkonto verwendet.
Hat das verwendete Kryptosystem mit öffentlichen Schlüsseln nicht die Eigenschaft ö(p(N)) = N, so nennt man der Geschäftsstelle einen privaten Schlüssel und verwendet den entsprechenden öffentlichen Schlüssel, der nun natürlich geheimgehalten werden muß, als Passwort. In diesem Fall muß das Kryptosystem mit öffentlichen Schlüsseln die Eigenschaft besitzen, daß aus dem privaten Schlüssel der öffentliche Schlüssel nicht mit vernünftigem Aufwand hergeleitet werden kann. (Normalerweise wird nur gefordert, daß man aus dem öffentlichen Schlüssel den privaten nicht mit vernünftigem Aufwand herleiten kann.)
Man zahlt einen Betrag auf das anonyme Nummernkonto ein und erhält dafür eine Quittung.

Will man eine gebührenpflichtige Dienstleistung über das Vermittlungs-/Verteilnetz erhalten, benutzt man das Kommunikationsprotokoll von Kapitel 3.2.3.2 mit den folgenden Erweiterungen (Bild 7). Diese Erweiterungen sind bezüglich der zu übertragenden Information nicht optimiert, da bei Unterschriften hin und wieder Information verschlüsselt und im Klartext übertragen wird.

...

Die Teilnehmerstation A erzeugt zwei Schlüsselpaare P_ö, P_p und Q_ö, Q_p und einen elektronischen Scheck
F_e = n,n_p(Datum,Zeit,Nummer,Betrag,P_ö). Mit dem elektronischen Scheck erlaubt A C eine Bezahlung von mit P_p oder p unterschriebenen Rechnungen bis zum Gesamtbetrag Betrag. Das Schlüsselpaar P_ö, P_p dient dazu, daß B und nur B von C Geld erhält, ohne daß C B kennt. Das Schlüsselpaar Q_ö, Q_p dient dazu, daß B und nur B unterschreiben kann, welchem anonymen Nummernkonto die Gebühren für F_f gutgeschrieben werden. Nebenbei wird Q_ö, Q_p auch dazu benutzt, daß die Vermittlungszentrale, ohne A zu kennen, A für andere Teilnehmerstationen unlesbar mitteilen kann, wie hoch die Gebühren für F_f sind.
A überträgt b,b_ö(F_pa,F_ö,F_f,P_p,Q_p),ö(c,c_ö(F_e),Q_ö). c ist eine Adresse von C, c_ö der entsprechende öffentliche Schlüssel, die anderen Abkürzungen sind in Abschnitt 3.2.3.2

definiert.
Die Vermittlungszentrale VZ entschlüsselt ö(c,c_ö(F_e),Q_ö) mit ihrem privaten Schlüssel p, berechnet die Übertragungskosten ük und eine Übertragungsgebührenrechnung Datum,Zeit,Nummer,ük und sendet c,c_ö(F_e),p(Datum,Zeit,Nummer,ük) an C.
C entschlüsselt c_ö(F_e) mit c_p, sucht den zu n gehörigen öffentlichen Schlüssel n_ö in seinem Verzeichnis und entschlüsselt n_p(Datum,Zeit,Nummer,Betrag,P_ö) mit n_ö. C entschlüsselt p(Datum,Zeit,Nummer,ük) mit ö.
C prüft Datum, Zeit und die (laufende) Nummer des elektronischen Schecks und der Übertragungsgebührenrechnung. C bestimmt das Kostenlimit kl aus dem Minimum von Betrag und dem Wert w, der noch auf dem anonymen Nummernkonto ist: kl = min(Betrag,w) - ük. C subtrahiert kl und ük vom anonymen Nummernkonto:
w := w - kl - ük. C sendet ö(kl,c_ö(F_e),c_p(kl,c_ö(F_e))) an die Vermittlungszentrale.
Die Vermittlungszentrale erkennt an c_ö(F_e), um welche Abfrage es sich handelt. Ist kl negativ, bricht die Vermittlungszentrale die Abfrage an dieser Stelle ab. Andernfalls berechnet sie eine Deckungszusage F_d = p(kl,b_ö(F_pa,F_ö,F_f,P_p,Q_p)) und sendet b,b_ö(F_pa,F_ö,F_f,P_p,Q_p),F_d an B.
B erkennt ihre Adresse b und entschlüsselt mit dem zugehörigen privaten Schlüssel b_p die Nachricht und mit dem öffentlichen Schlüssel ö der Vermittlungszentrale die Deckungszusage F_d. B prüft, ob die Kosten k für F_f inklusive der Übertragungsgebühren für die Antwort durch das Kostenlimit kl der Deckungszusage F_d gedeckt sind. Gegebenenfalls berechnet B ihre Antwort F_a und eine Rechnung k,F_d,P_p(k,F_d). An die Rechnung fügt B die Adresse d einer Geschäftsstelle D an, bei der der Teilnehmer an B ein anonymes Nummernkonto besitzt, den zugehörigen öffentlichen Schlüssel d_ö sowie seine Kontonummer d_n und eine Unterschrift F_u = Q_p(k,F_d,P_p(k,F_d),d,d_ö,d_n). B sendet F_pa,F_ö(F_a),ö(k,F_d,P_p(k,F_d),d,d_ö,d_n,F_u) an die Vermittlungszentrale.
Die Vermittlungszentrale entschlüsselt
ö(k,F_d,P_p(k,F_d),d,d_ö,d_n,F_u) mit p und erkennt an F_d, um welche Abfrage es sich handelt. Danach entschlüsselt die Vermittlungszentrale F_u mit Q_ö, um die Unterschrift zu prüfen. Ist die Unterschrift nicht in Ordnung oder k > kl, bricht die Vermittlungszentrale die Abfrage ab. Die Vermitt-

lungszentrale sendet c,c_ö(k,F_d,P_p(k,F_d),c_p(kl,c_ö(F_e))) an C.
C entschlüsselt c_ö(k,F_d,P_p(k,F_d),c_p(kl,c_ö(F_e))) mit c_p und erkennt an c_p(kl,c_ö(F_e)), um welche Abfrage es sich handelt. C prüft die Unterschrift P_p(k,F_d) mit P_ö. C addiert kl - k zum Betrag des anonymen Nummernkontos n: w := w + kl - k.
Die Vermittlungszentrale berechnet den B gutzuschreibenden Betrag gb = k - Übertragungskosten der Antwort und eine elektronische Gutschrift gb,d_n,p(Datum,Zeit,Nummer,gb,d_n).
Die Vermittlungszentrale sendet
d,d_ö(gb,d_n,p(Datum,Zeit,Nummer,gb,d_n)) an D.
D prüft die Unterschrift p(Datum,Zeit,Nummer,gb,d_n) mit ö und schreibt gegebenenfalls gb dem anonymen Nummernkonto d_n gut.
Die Vermittlungszentrale berechnet die Kosten der Abfrage F_k = k + ük, unterschreibt F_k,c,c_ö(F_e) und verschlüsselt Kosten und Unterschrift mit Q_ö. Die Vermittlungszentrale sendet F_pa,F_ö(F_a),Q_ö(F_k,p(F_k,c,c_ö(F_e))) an A.
A erkennt F_pa und entschlüsselt F_ö(F_a) mit F_p und Q_ö(F_k,p(F_k,c,c_ö(F_e))) mit Q_p. A prüft die Unterschrift p(F_k,c,c_ö(F_e)) mit ö.

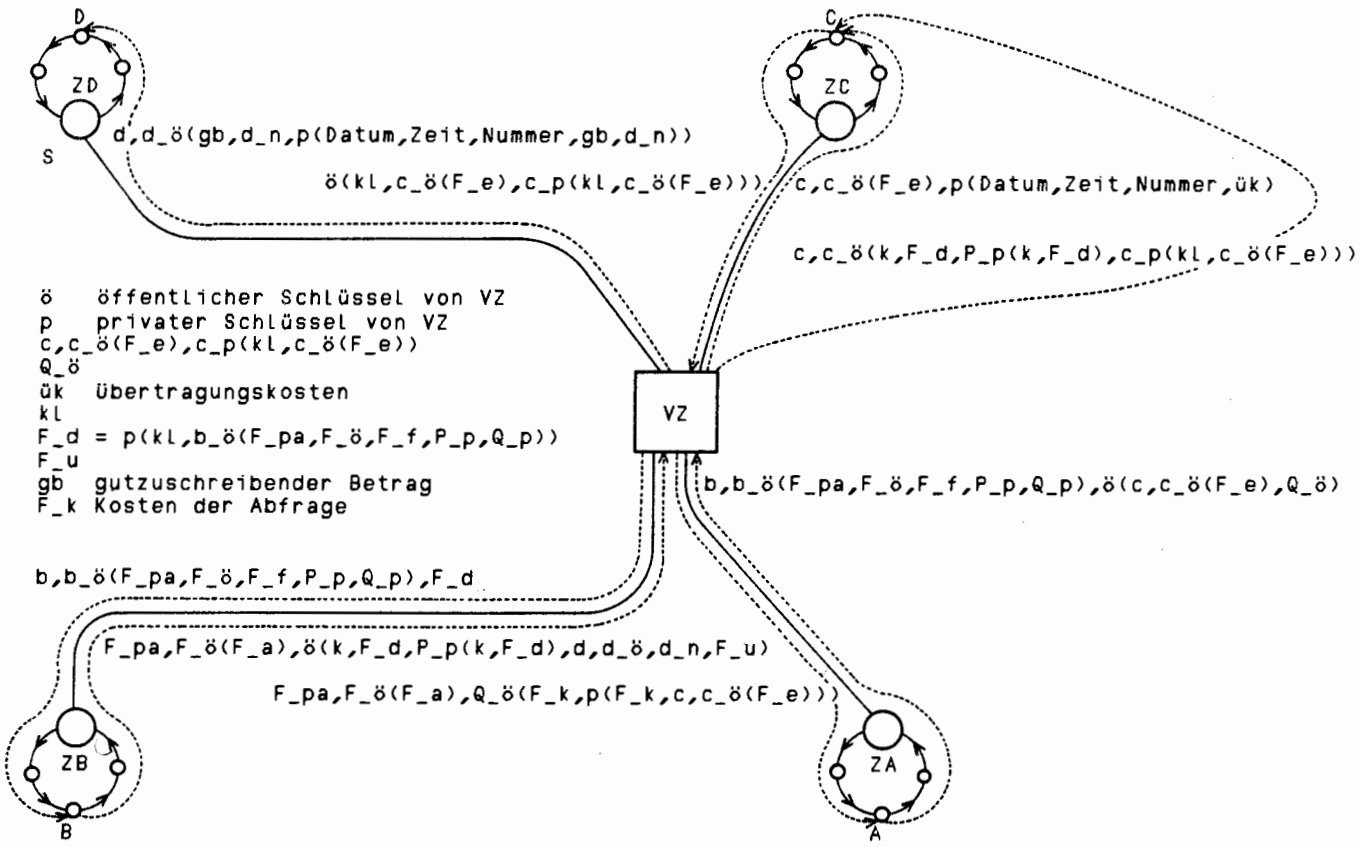
Das Protokoll stellt sicher, daß VZ, C und D gemeinsame Betrugsversuche von A und B erkennen und vereiteln können sowie A und B gemeinsame Betrugsversuche von VZ, C und D erkennen und vereiteln können.
Wählt A Schlüsselpaare P_ö, P_p bzw. Q_ö, Q_p, die nicht zueinander passen, schadet er nur sich selbst, da er keine Antwort erhält aber die Übertragungsgebühren bezahlen muß.
Ist der Teilnehmer an der Teilnehmerstation A mit der von B gelieferten Antwort F_a unzufrieden, kann er sich bei einer Schiedsstelle über B beschweren. Dazu legt A der Schiedsstelle allen Klartext und die zugehörigen öffentlichen Schlüssel vor. Die Schiedsstelle kann daraus die Nachrichten berechnen, die die Vermittlungszentrale passiert haben müssen, und sich bei der Vermittlungszentrale erkundigen, ob dies tatsächlich so war. Um dies beantworten zu können, muß sich die Vermittlungszentrale alle Nachrichten (oder Signaturen der Nachrichten, um Speicherplatz zu sparen) eine Zeitlang (Beschwerdefrist) merken. Falls gewünscht, kann die Vermittlungszentrale gb erst dann an B auf ein Konto bei D überweisen, wenn die Beschwerdefrist ohne

Beschwerde abgelaufen ist. Auf diese Weise wird das Geld für den Fall einer Beschwerde sichergestellt und dadurch der eventuell anonyme Teilnehmer an B gezwungen, auf eine berechtigte Beschwerde einzugehen. Betragssicherheit trotz absoluter Anonymität -> Waid.85 Wa Pf.85

Hat das verwendete Kryptosystem mit öffentlichen Schlüsseln nicht die Eigenschaft ö(p(N)) = N (vgl. R5 in Abschnitt 3.1), so sind die obigen Erweiterungen des Kommunikationsprotokolls durch Vertauschung der öffentlichen und privaten Schlüssel zu ändern. (Außerdem werden zwei zusätzliche Schlüsselpaare zur geheimen Kommunikation zwischen der Vermittlungszentrale und A benötigt, sowie zur Leistung von Unterschriften der Zentrale.)

d Adresse von D
d_ö öffentlicher Schlüssel zu d
d_p privater Schlüssel zu d
d_n Kontonummer

c Adresse von C
c_ö öffentlicher Schlüssel zu c
c_p privater Schlüssel zu c
n Kontonummer
n_ö öffentlicher Schlüssel zu n
w Wert auf n
c_ö(F_e)
P_ö
p(Datum,Zeit,Nummer,ük)
kl Kostenlimit
k



ö
b Adresse von B
b_ö öffentlicher Schlüssel zu b
b_p privater Schlüssel zu b
d Adresse von D
d_n Kontonummer von B bei D
F_pa
F_ö
F_f
P_p
Q_p

F_d
kl
k Kosten für F_f inklusive Übertragungsgebühren für die Antwort
F_a Antwort
F_u = Q_p(k,F_d,P_p(k,F_d),d,d_n)

ö
za logische Adresse von ZA
b
b_ö
c Adresse von C
c_ö öffentlicher Schlüssel zu c
n Kontonummer von A bei C
n_ö öffentlicher Schlüssel zu n
k_p privater Schlüssel zu n (Passwort)
F_z Zufallszahl für F
F_pa = ö(za,F_z) für F gebildete private Adresse von A
F_ö öffentlicher Schlüssel für F
F_p privater Schlüssel für F
F_f Frage
P_ö Schlüsselpaar zur Legitimation
P_p von B gegenüber C
Q_ö Schlüsselpaar zur Legitimation
Q_p von B gegenüber VZ
F_e = n,n_p(Datum,Zeit,Nummer,Betrag,P_ö) elektronischer Scheck
F_a
F_k

Bild_7: Kommunikation im Vermittlungs-/Verteilnetz mit anonymen Nummernkonten

Jeder kann so viele anonyme Nummernkonten eröffnen, wie er will. Damit man nicht im Laufe der Zeit bei der das anonyme Nummernkonto führenden Geschäftsstelle persönlich bekannt wird, sollte das anonyme Nummernkonten-System so organisiert sein, daß man an jeder Geschäftsstelle jeder Bank Geld auf jedes Nummernkonto einzahlen kann.

Die Vor- und Nachteile der anonymen Nummernkonten sind offensichtlich:

+ Anonyme Nummernkonten und folglich Gebühren können Teilnehmerstationen nicht zugeordnet werden.
+ Keine Partei kann betrügen:
  Der Teilnehmer erhält beim Einzahlen Quittungen über eingezahlte Beträge.
  Die Geschäftsstelle erhält elektronische Schecks, die nur der Teilnehmer unter Benutzung seines privaten Schlüssels ausgestellt haben kann.
  Eine ausführliche Darstellung von elektronischem Scheck-Verkehr in Rechnernetzen ist in [Riha_83] zu finden.
- Das Einzahlen auf anonyme Nummernkonten ist beschwerlich, insbesondere für Persönlichkeiten des öffentlichen Lebens, da sie (fast) überall persönlich bekannt sind.
  Dieser Nachteil kann vermieden werden, wenn einige oder besser alle Geldausgabeautomaten auch als Geldeingabeautomaten realisiert werden, an denen man anonyme Nummernkonten eröffnen und auf anonyme Nummernkonten einzahlen kann.
- Diese Abrechnungsmethode verursacht neben zusätzlichem Aufwand bei der Erzeugung von zusätzlichen Schlüsselpaaren und zusätzlichen Verschlüsselungen viel zusätzlichen Nachrichtenverkehr, wenn die das anonyme Nummernkonto führende Organisation nicht mit dem Netzbetreiber identisch ist. Diese Identität ist aber aus Gründen des Datenschutzes nicht wünschenswert.

3.2.3.3.2 Nicht manipulierbare Zähler

> Ciphers, of whatever kind, do not produce security out of nothing.
> In each case they require a secret key.
> Therefore, security always depends on the physical integrity of a device as well as on correct system design and software.
> Donald W. Davies

Die zweite Lösung des Abrechnungsproblems ist eine Weiterentwicklung der Elektrizitätszähler.

In jeder Teilnehmerstation wird ein vom Teilnehmer nicht manipulierbarer (Realisierungsmöglichkeiten werden in [Kunt_83, Pill_83] beschrieben) Zähler geführt, der die Gebühren der in Anspruch genommenen/erbrachten Dienstleistungen auf-/absummiert. Ebenso führt die Vermittlungszentrale einen Zähler für von ihr erbrachte Dienstleistungen. Der Zähler der Teilnehmerstation kann z. B. frühestens 2 Wochen nach dem letzten Lesen durch die Vermittlungszentrale abermals gelesen werden. Die Vermittlungszentrale liest etwa monatlich die Zähler der Teilnehmerstationen und verschickt Rechnungen/Gutschriften. Die Summe über alle Zähler ist null, wodurch eine Kontrolle und die Möglichkeit zur 1 Zähler-Fehlerkorrektur (wenn der defekte Zähler bekannt ist) gegeben ist.

Die beschriebene Dezentralisierung der Abrechnung und die damit verbundene Einrichtung eines nicht manipulierbaren Zählers in jeder Teilnehmerstation erfordert, daß

1) nur vom Netzbetreiber (z. B. der Post) und einer Interessenvertretung der Teilnehmer (z. B. Stiftung Warentest, TÜV) geprüfte Teilnehmerstationen verwendet werden dürfen und
2) alle Teilnehmerstationen vom Netzbetreiber registriert werden, damit die Vermittlungszentrale alle Zähler lesen und Rechnungen/Gutschriften an alle Teilnehmer verschicken kann.

Diese Forderung kann man durch Aufteilung der Teilnehmerstation in zwei unabhängige Teile abschwächen (Bild 8):
eine geprüfte und registrierte Zählinstanz, die zugleich

Ringinterface ist, erledigt die Abrechnung und bietet dem Teilnehmer eine oder mehrere Schnittstellen zum Anschluß ungeprüfter und unregistrierter Endgeräte.

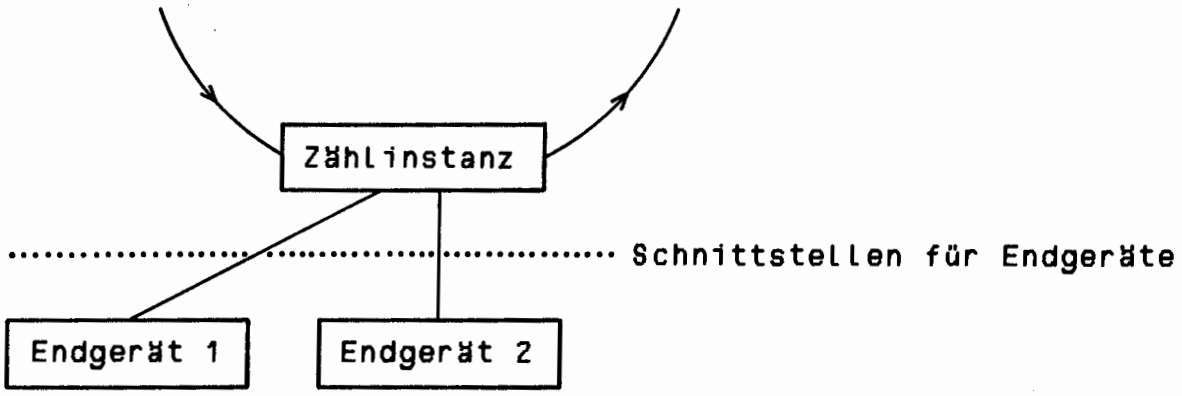


Bild_8: Aufteilung der Teilnehmerstation

Diese Aufteilung in sichere (Zählinstanzen) und unsichere (Endgeräte) Geräte entspricht dem Vorschlag, ein sicheres System durch Verbindung unsicherer Rechnersysteme ausschließlich über sichere Geräte (TNIU = Trustworthy Network Interface Unit) zu realisieren [RuRa_83]. Die Zählinstanz stellt in der Begriffswelt von Karl Rihaczek einen M-Teilnehmer dar [Riha_81 Seite 33].

Will man eine Übertragungsgebühren- (und Dienstleistungsgebühren-) pflichtige Dienstleistung über das Vermittlungs-/Verteilnetz erhalten, benutzt man das Kommunikationsprotokoll von Kapitel 3.2.3.2 mit den folgenden Erweiterungen (Bild 9). Diese Erweiterungen sind bezüglich der zu übertragenden Information nicht optimiert, da bei Unterschriften hin und wieder Information verschlüsselt und im Klartext übertragen wird.

...

(Die Teilnehmerstation A bzw. der Teilnehmer an A legt ein Kostenlimit (incl. Zeitschranke) F_kl fest. A berechnet eine Unterschrift unter F_f: F_fu = F_p(F_pa,F_ö,F_f,F_kl)). A sendet die Adresse b von Teilnehmerstation B sowie F_pa, F_ö und ihre Frage F_f (und eine zeitlich und betragsmäßig begrenzte Abbuchungsermächtigung F_kl,F_fu) mit dem öffentlichen Schlüssel b_ö von B verschlüsselt an ihre Verteilnetzzentrale

ZA. Der Zähler von A erhöht sich dabei um die Übertragungsgebühren der Nachricht.
ZA vermittelt die Nachricht an die Vermittlungszentrale.
Der Zähler der Vermittlungszentrale erniedrigt sich dabei um die Übertragungsgebühren. Die Vermittlungszentrale entschlüsselt b mit ihrem privaten Schlüssel p und vermittelt die Abfrage gemäß der ersten Komponente der Adresse an die Verteilnetzzentrale ZB von B.
ZB verteilt die Nachricht.
B erkennt ihre Adresse b und entschlüsselt mit dem zugehörigen privaten Schlüssel b_p die Nachricht. {Der Teilnehmer an B prüft, ob die Gebühren F_k für F_f durch die Abbuchungsermächtigung abgedeckt sind.} B berechnet {gegebenenfalls} ihre Antwort F_a {und die Unterschrift unter F_a: F_au = b_p(F_a,F_k). F_k,F_au ist eine Abbuchungsanweisung}. B sendet F_pa,F_ö(F_a{,F_k,F_au}) an ihre Verteilnetzzentrale ZB. Der Zähler von B prüft die Abbuchungsermächtigung und {erniedrigt sich gegebenenfalls um die Gebühren der Abfrage und} erhöht sich dabei um die Übertragungsgebühren der Nachricht.
ZB vermittelt die Nachricht an die Vermittlungszentrale.
Die Vermittlungszentrale entschlüsselt F_pa mit ihrem privaten Schlüssel p und vermittelt die Nachricht gemäß der ersten Komponente der Adresse an die Verteilnetzzentrale ZA von A. Der Zähler der Vermittlungszentrale erniedrigt sich dabei um die Übertragungsgebühren.
ZA verteilt die Nachricht.
A erkennt ihre private Adresse F_pa und entschlüsselt die Antwort F_a {inklusive Abbuchungsanweisung F_k,F_au} mit ihrem für F gewählten privaten Schlüssel F_p. {Der Zähler von A erhöht sich dabei gemäß der Abbuchungsanweisung. Diese Erhöhung des Zählers von A darf von Bedienern von A nicht verhinderbar oder manipulierbar sein. Dazu ist es sinnvoll, daß sich die Zähl-Instanz die als anonymisierten Absender verwendeten privaten Adressen, die zugehörigen privaten Schlüssel und die zeitlich und betragsmäßig begrenzten Abbuchungsermächtigungen merkt, bis die zeitliche Befristung der Abbuchungsermächtigung abläuft oder eine Antwort erfolgt. Damit kann die Zähl-Instanz sichern, daß

1) diese Antworten angenommen und entschlüsselt und die Gebühren gegebenenfalls verbucht werden und

2) nur Abbuchungsanweisungen verbucht werden, die auf einer entsprechenden Abbuchungsermächtigung beruhen.
Ist der Teilnehmer an A mit der Höhe der Gebühren nicht einverstanden, muß er mit B über die Ausstellung einer Differenz-Rechnung/-Gutschrift verhandeln.
Da alle Nachrichten unterschrieben wurden, ist dieser Disput entscheidbar. Können sich die Teilnehmer nicht einigen, so können sie sich anonym an eine Schiedsstelle wenden und ihr die ausgetauschten, unterschriebenen Nachrichten vorlegen. Die Schiedsstelle versendet dann Differenz-Rechnungen/-Gutschriften.)

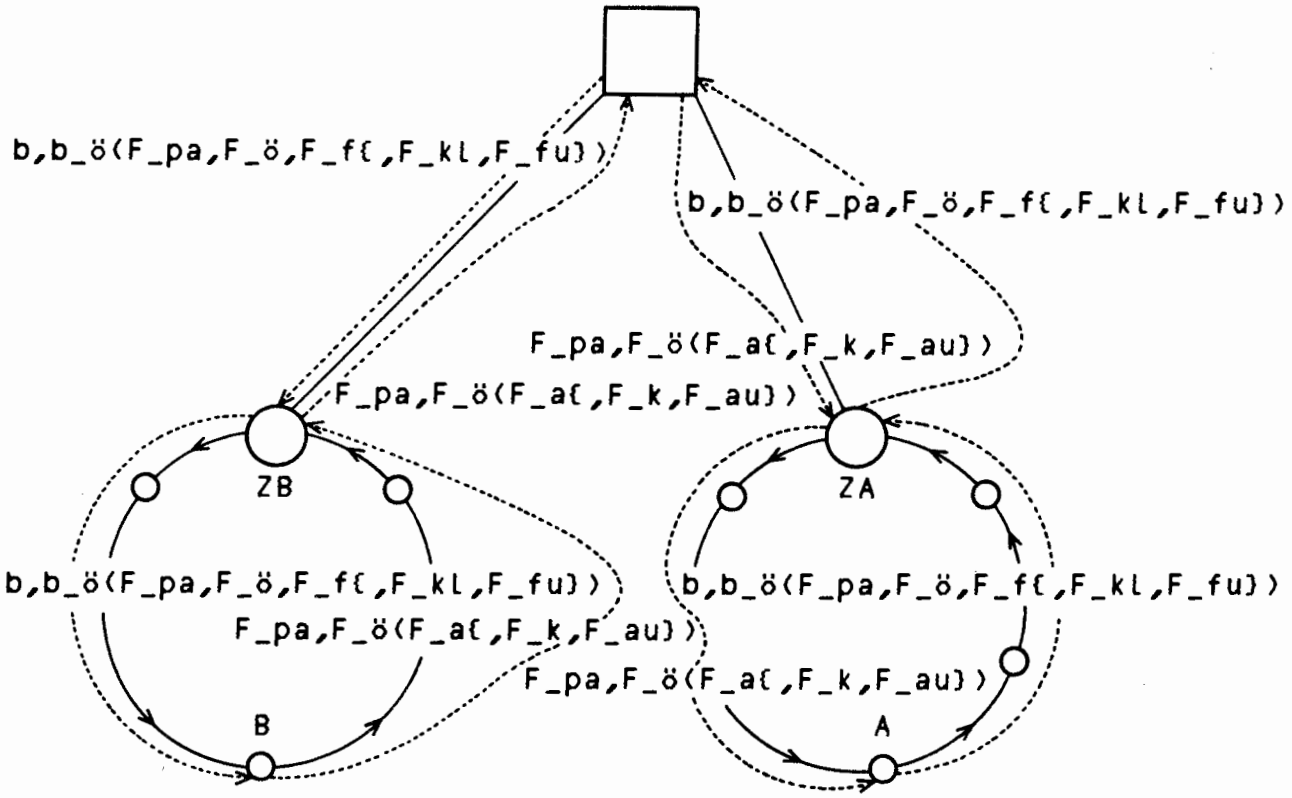
Um nicht manipulierbare Zähler in einem realen System einsetzen zu können, muß jedem Teilnehmer ein Kreditrahmen vorgegeben und dessen Einhaltung vom nicht manipulierbaren Zähler überprüft werden. Sonst könnte ein Teilnehmer durch Eingehen hoher Kredite und anschließendes Untertauchen beliebig großen Schaden anrichten.

Die Vor- und Nachteile der nicht manipulierbaren Zähler sind offensichtlich:

- Die regelmäßig gelesenen Werte der Zähler sind Teilnehmerstationen zugeordnet. Dies ist akzeptabel, wenn genug gebührenpflichtige Transaktionen zwischen dem Lesen der Zähler stattfinden.
- Wenn der Teilnehmer den nicht manipulierbaren Zähler seiner Teilnehmerstation betrügen kann, kann er alle anderen Teilnehmer (inkl. Netzbetreiber und Dienstleistungsanbieter) betrügen.
+ Das Einzahlen von Geld auf spezielle anonyme Konten ist nicht nötig.
+ Es gibt kaum extra Nachrichtenverkehr zu Abrechnungszwecken. Lediglich die Nachrichtenlänge wird etwas größer.

Da ich den Entwurf eines Vermittlungs-/Verteilnetzes unter Benutzung von nicht manipulierbaren Zählern für technisch interessanter (schwieriger) halte, wird den folgenden Kapiteln diese Abrechnungsmethode zugrunde gelegt.

ö öffentlicher Schlüssel der Vermittlungszentrale
p privater Schlüssel der Vermittlungszentrale
pr1 Projektion auf erste Adreß-Komponente
pr1(p(b)) = zb Adresse von ZB
pr1(p(F_pa)) = za Adresse von ZA



b	Adresse von B	ö	
b_ö	öffentlicher Schlüssel zu b	za	logische Adresse von ZA
b_p	privater Schlüssel zu b	b	
F_pa		b_ö	
F_ö		F_z	Zufallszahl für F
F_f		F_pa	= ö(za,F_z) für F gebildete private Adresse von A (anonymisierter Absender)
F_kl		F_ö	öffentlicher Schlüssel für F
F_fu		F_p	privater Schlüssel für F
F_a	Antwort	F_f	Frage
F_k	Kosten von F_a	F_kl	Kostenlimit und Zeitschranke
F_au	= b_p(F_a,F_k) Unterschrift unter F_a	F_fu	= F_p(F_pa,F_ö,F_f,F_kl) Unterschrift unter F_f
		F_a	

Bild_9: Kommunikation im Vermittlungs-/Verteilnetz mit nicht manipulierbaren Zählern

3.2.3.4 Erweiterungen des Kommunikationsprotokolls zur Tolerierung von Fehlern

If something can go wrong,
it will go wrong
in the worst possible manner
at the worst possible time.
Murphy

Um das Kommunikationsprotokoll in einem realen System anwenden zu können, muß es die in einem realen System unvermeidlich auftretenden Fehler tolerieren. Insbesondere muß die Konsistenz der Zähler mit sehr hoher Wahrscheinlichkeit gewahrt oder eine nicht vermeidbare Inkonsistenz diagnostiziert und begrenzt werden.
Die folgenden Erweiterungen des Kommunikationsprotokolls bieten sich an, um Leitungs- und Stationsfehler zu tolerieren:

1) Der Empfang von Nachrichten wird quittiert. Nicht auslieferbare Nachrichten werden an den Absender zurückübertragen. Dazu müssen alle Nachrichten mit einem verschlüsselten Absender (private Adresse des Senders, vgl. Abschnitt 3.2.3.1) versehen werden, da der in Abschnitt 3.2.3.2 benutzte anonymisierte Absender nur vom Empfänger entschlüsselbar ist.
2) Jede Verteilnetzzentrale unterhält Zähler, deren Stände aus Datenschutz- und Aufwandsgründen nur in etwa die Zählerstände der angeschlossenen Teilnehmerstationen sind:
   Hat sich der Zählerstand einer Teilnehmerstation seit der letzten Mitteilung an die Verteilnetzzentrale um mehr als d Einheiten geändert, teilt die Teilnehmerstation der Verteilnetzzentrale einen aktuellen In-Etwa-Zählerstand, der sich vom genauen Zählerstand um weniger als d Einheiten unterscheidet, mit, so daß die Verteilnetzzentrale den betreffenden Zähler nachführt.
   d sollte so klein gewählt werden, daß eine um d fehlerhafte Abrechnung nach seltenen Ausfällen der Teilnehmerstation den Teilnehmer und den Betreiber der Vermittlungszentrale nicht zu sehr stört. Andererseits sollte d so groß gewählt werden, daß im Mittel wesentlich mehr als eine Transaktion (z. B. gebührenpflichtige Informationsabfrage) nötig ist, um den Zählerstand um mehr als d Einheiten zu ändern. 100 DM könnte ein passender Wert für d sein.

3.2.3.5 Erweiterungen des Kommunikationsprotokolls zur Tolerierung von manchen Manipulationen am Netz

> By a routine that was not even secret,
> all letters were opened in transit.
> George Orwell

Durch Anschluß nicht geprüfter (vgl. Abschnitt 3.2.3.3.2) Geräte, die eine Teilnehmerstation, Verteilnetzzentrale oder Vermittlungszentrale teilweise simulieren, können folgende Bedrohungen entstehen (vgl. [Beth_82]):

- B1 Im Vermittlungs-/Verteilnetz wird an beliebiger Stelle eine Leitung abgehört.
- B2 Im Vermittlungs-/Verteilnetz werden an beliebiger Stelle Nachrichten teilweise geändert.
- B3 Im Vermittlungs-/Verteilnetz werden an beliebiger Stelle Nachrichten erzeugt.
- B4 Im Vermittlungs-/Verteilnetz werden an beliebiger Stelle Nachrichten empfangen, d. h. von der Leitung genommen und quittiert.

Andere Bedrohungen äußern sich wie Fehler (z. B. Sabotage) und werden durch die Maßnahmen in Abschnitt 3.2.3.4 toleriert.

B1 Abhören an einer Stelle im Vermittlungsnetz erfordert keine Erweiterung des Kommunikationsprotokolls, da alle Information nur in verschlüsselter Form übertragen und das verwendete Kryptosystem mit öffentlichen Schlüsseln als sicher angenommen wird (vgl. R5 in Abschnitt 3.1). Also kann durch Abhören keine Information über die Nachrichteninhalte gewonnen werden. Bei Verwendung einer privaten Adresse (vgl. Abschnitt 3.2.3.1) kann ebenfalls keine Information über das Nachrichtenziel gewonnen werden. Die Verwendung öffentlicher Adressen erlaubt das Gewinnen aller im Teilnehmerverzeichnis enthaltenen Information (vgl. Abschnitte 3.2.3.1 und 3.2.3.2). Diese Möglichkeit zum Gewinnen von Information über Nachrichtenziele kann durch zusätzliche Verschlüsselung öffentlicher Adressen (wie in Abschnitt 3.2.3.2 als Erweiterung vorgeschlagen) und Beibehaltung dieser zusätzlichen Verschlüsselung so lange wie möglich (bis zur letzten zu durchlaufenden Vermittlungszentrale und nicht nur bis zur ersten wie in Abschnitt 3.2.3.2

vorgeschlagen) verkleinert werden.

Auch durch Abhören eines busförmigen Verteilnetzes an einer Stelle bzw. eines ringförmigen Verteilnetzes vor und nach einer Teilnehmerstation und Vergleich kann keine Information über die Nachrichteninhalte gewonnen werden, sondern lediglich das Kommunikationsverhalten der Teilnehmerstation beobachtet werden:

1) Wann Nachrichten abgesandt oder empfangen (Quittieren (Abschnitt 3.2.3.4 1)) bedeutet Senden bei Empfang) werden.
2) Welche Adressen verwandt werden. Private Adressen (Abschnitt 3.2.3.1) erlauben keine Rückschlüsse auf den Empfänger bzw. Absender (beim Quittieren).

   Die aus öffentlichen Adressen und dem Teilnehmerverzeichnis (Abschnitt 3.2.3.1) möglichen Rückschlüsse lassen sich durch die in Abschnitt 3.2.3.2 vorgeschlagene Erweiterung des Kommunikationsprotokolls verhindern:

   Die Teilnehmerstation A verschlüsselt b mit dem öffentlichen Schlüssel der Vermittlungszentrale ö und überträgt als Adresse statt b ö(b).

   Die Vermittlungszentrale entschlüsselt ö(b) einmal zusätzlich mit ihrem privaten Schlüssel p und ersetzt ö(b) innerhalb der Nachricht durch b.

B2 Wenn zu übertragende Information redundant ist, was, wenn es nicht sowieso der Fall ist, man gegebenenfalls durch fehlererkennende Kodierung sicherstellen kann [VoKe_83 Seite 159], ist eine Veränderung der verschlüsselten Information nach der Entschlüsselung mit hoher Wahrscheinlichkeit erkennbar und kann als Fehler behandelt werden. Also braucht verschlüsselte Information nicht gesondert gegen Veränderung gesichert zu werden.

Eine Veränderung der Adreßinformation (b, F_pa) führt dazu, daß private Schlüssel nicht passen, nach der Entschlüsselung also mit hoher Wahrscheinlichkeit erkennbar falsche Information entsteht, was als Fehler behandelt werden kann. Also braucht auch Adreßinformation nicht gesondert gegen Veränderung gesichert zu werden.

B3 Die Verhinderung liegt speziell im Interesse der die Abrechnung durchführenden Vermittlungszentrale, da eine Kombination von B3 und B4 es ermöglichen würde, Zähler von z.

B. Informationsanbietern durch gebührenpflichtige Informationsabfragen zu erniedrigen, ohne daß ein anderer Zähler entsprechend erhöht würde.
Deshalb kann B3 durch Verwendung eines sicheren (Bemerkungen in R5 in Abschnitt 3.1 zu sicher gelten sinngemäß) Kryptosystems mit privaten Schlüsseln (private key cryptosystem) verhindert werden. Vor alle Nachrichten werden zusätzlich Datum und Zeit gehängt und alles zusammen mit dem netzweit gültigen privaten Schlüssel s der Vermittlungszentrale verschlüsselt. s kann nur von der Vermittlungszentrale weitergegeben werden, die s in ihrem eigenen Interesse nur weitergibt wie folgt:
s wird bei der Registrierung (Abschnitt 3.2.3.3.2) in die Teilnehmerstation überspielt. Die Teilnehmerstation ist so gebaut, daß sie s nicht preisgibt und bei mechanischer Manipulation vernichtet. Dies Verfahren wird für OSIS - Open Shops for Information Services [Riha_83], einem System zur Sicherung der Rechtsverbindlichkeit von Kommunikation mittels eines öffentlichen Kryptosystems, vorgeschlagen. Realisierungsmöglichkeiten werden in [Kunt_83, SBit_83] beschrieben. Ein ähnliches Verfahren wird in [RuRa_83] vorgeschlagen und dürfte bei der smart card bereits angewandt werden [Pill_83, smar_82]. Entsprechend wird bei der Installation der Verteilnetzzentralen verfahren, die den gleichen Mechanismus wie die Teilnehmerstationen realisieren müssen.

B4 Nimmt man in die Nachrichten ein (z. B. eine Zufallszahl enthaltendes) Feld auf, das bei Quittierung der Nachricht zurückübertragen wird, so macht die unter B3 beschriebene Verschlüsselung mit s auch das erfolgreiche Quittieren von Nachrichten durch nicht registrierte Stationen sehr unwahrscheinlich. Eventuell kann statt eines extra Feldes auch ein bestimmter Teil der Nachricht zurückübertragen werden, wenn gewährleistet ist, daß dieser Teil genügend viele verschiedene Werte annimmt.

[VoKe_83] enthält eine ausführlichere Darstellung von Bedrohungen und Gegenmaßnahmen. Alles dort gesagte kann sinngemäß auf das Vermittlungs-/Verteilnetz übertragen werden.

3.2.3.6 Realisierungsaufwand

In sum, therefore,
our object must always be:
"To design up to a standard
rather than down to a price."
Sir Herbert Durkin

Da das Vermittlungs-/Verteilnetz das Vermittlungsnetz übernimmt, wird im folgenden nur der Realisierungsaufwand eines ringförmigen Verteilnetzes mit Rückkanal mit dem üblichen Ortsnetz mit Sternstruktur verglichen. Ein busförmiges Verteilnetz mit Rückkanal wird nicht gesondert behandelt, da es ähnliche Kosten wie ein ringförmiges verursacht und in ihm Sender leichter identifiziert werden können (vgl. Abschnitt 3.2.2.1).
Der Realisierungsaufwand eines Verteilnetzes mit Rückkanal hängt von einer Unzahl Parameter ab: örtliche Verteilung der Teilnehmerstationen und Schwierigkeitsgrad der Leitungsverlegung, zu erwartendes/zu bewältigendes Nachrichten-Verkehrsaufkommen und seine zeitliche Verteilung, Antwortzeit- und Zuverlässigkeitserwartungen der Benutzer, Stand der Technik etc..
Um die Netzstruktur zu bewerten, sind jedoch keine absoluten Werte nötig: relative Werte bezüglich der alternativen Netzstrukturen genügen. Als Bezugspunkt wird der Aufwand zur Realisierung eines Sternnetzes genommen, da das Telefonnetz und seine Weiterentwicklung zum ISDN (BIGFON) in der untersten Ebene des Ortsnetzes Sternnetze sind [Brau_83, Gerk_82, Kais_82]. Andere Netzstrukturen auf der untersten Ebene des Ortsnetzes werden für Netze mit Rückkanal meines Wissens nicht diskutiert. Stern-, Bus- und Ringstruktur werden zwar verglichen, aber nur im Bereich des Anschlusses verschiedener Endgeräte eines Teilnehmers [RosK_82].
Die Kosten der untersten Ebene eines Ortsnetzes bestehen aus 2 Teilen:

1) Die eigentlichen Kosten des technischen Systems: Kabel, Sender, Empfänger etc..
   Diese Kosten steigen mit zusätzlicher Übertragungsrate an: zunächst kaum, da die technischen Möglichkeiten nicht annähernd ausgeschöpft sind; nähert man sich den technischen Möglichkeiten, steigen die Kosten stärker. Der Kostenanstieg ist jedoch höchstens linear, da man andernfalls kostengünsti-

ger mehrere leistungsschwächere Systeme parallel installieren könnte.

2) Die Installations- und Instandhaltungskosten des technischen Systems, insbesondere die Kosten der Kabelverlegung.
Die Kosten der Kabelverlegung sind fast vollständig unabhängig von der Übertragungsrate, aber proportional zur Gesamtlänge der Verkabelung. Unter Gesamtlänge der Verkabelung wird nicht die Gesamtlänge aller Kabel verstanden, sondern die Gesamtlänge aller Kabelstränge, da nicht das Hineinlegen von Kabeln, sondern das Aufreißen und Schließen von Straßen, Wänden etc. die wesentlichen Kosten verursacht.

Um die Länge der Verkabelung in der untersten Ebene eines Ortsnetzes berechnen zu können, muß man die örtliche Verteilung der Teilnehmerstationen festlegen. Ich untersuche im folgenden den Fall, daß die Teilnehmerstationen gleichmäßig in einem Quadrat der Kantenlänge 1 verteilt sind. Da sich quadratische Anzahlen von Teilnehmerstationen besonders einfach gleichmäßig verteilen und regelmäßig verbinden lassen (Bild 10) berechnet das folgende PASCAL-Programm QUADRAT die folgenden Vergleichsgrößen für quadratische Anzahlen von Teilnehmerstationen:

TEILUNG gibt die Anzahl der Teilnehmerstationen in einer Zeile, Spalte an.

ANZAHL gibt die Anzahl der Teilnehmerstationen im Quadrat der Kantenlänge 1 an.

STERNL (Sternlänge) gibt die Gesamtlänge der sternförmigen Verbindungen der Teilnehmerstationen mit dem Mittelpunkt des Quadrates an.

RINGL (Ringlänge) gibt die Gesamtlänge der ringförmigen Verbindung aller Teilnehmerstationen an.

STERNL/RINGL gibt das Verhältnis von Sternlänge zu Ringlänge an.

USTERN/MAXURING gibt das Verhältnis zwischen den Übertragungskosten auf dem Stern und den maximalen Übertragungskosten auf dem Ring an.
Die maximale Übertragungsgeschwindigkeit zu/von einer Teilnehmerstation sei 1. Die Übertragungskosten ergeben sich als Produkt von Übertragungslänge (im Sinne einer räumlichen Entfernung) und Übertragungsgeschwindigkeit.
Also sind die Übertragungskosten auf dem Stern STERNL*1;
Die maximalen Übertragungskosten auf dem Ring ergeben

sich als Produkt von RINGL und der benötigten Übertragungsgeschwindigkeit. Nach [Kais_82 Seite 46] kann man davon ausgehen, daß maximal 10% aller angeschlossenen Teilnehmerstationen gleichzeitig benutzt werden. Da nicht alle benutzten Teilnehmerstationen gleichzeitig übertragen wollen, genügt es also, die Übertragungsgeschwindigkeit des Ringes auf 0.1*ANZAHL, mindestens aber 1, zu dimensionieren. Die maximalen Übertragungskosten auf dem Ring ergeben sich durch Multiplikation mit RINGL. Diese Dimensionierung der Übertragungsgeschwindigkeit des Rings ist überreichlich, da

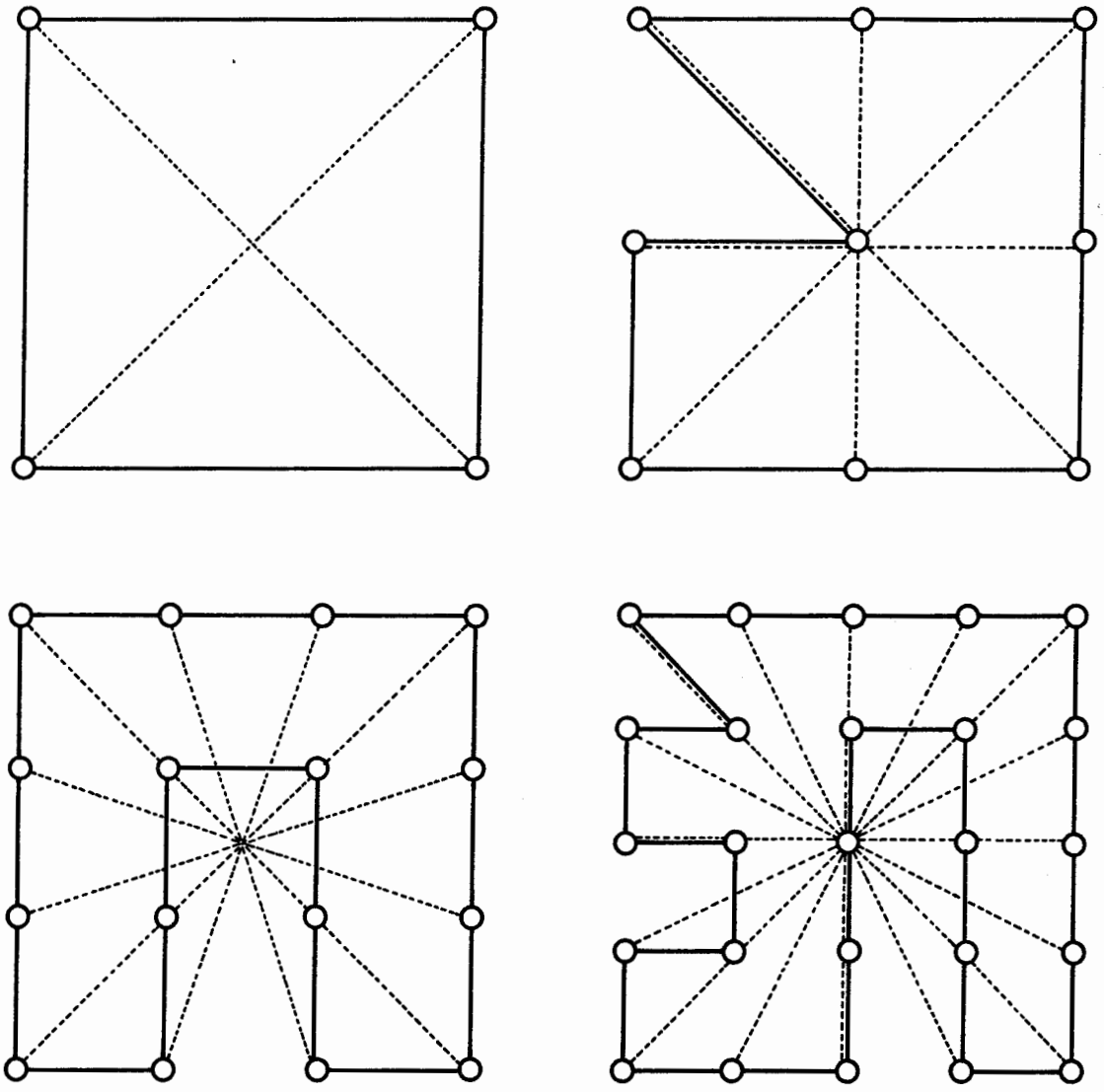
* über ihn mit einem erheblichen Anteil auch Verteilprogramme (Fernsehen, Radio etc.) übertragen werden, die unabhängig von der Anzahl der sie anfordernden Teilnehmerstationen nur höchstens einmal auf dem Ring übertragen werden müssen und
* der Durchsatz eines Rings 1 bis 2 mal so groß sein kann wie die Kapazität seiner Leitungen [BuSc_83 Seite 54].

USTERN/MINURING gibt das Verhältnis zwischen den Übertragungskosten auf dem Stern und den minimalen Übertragungskosten auf dem Ring an.
Die minimalen Übertragungskosten auf dem Ring ergeben sich, wenn man die Übertragungsgeschwindigkeit des Ringes auf 0.01*ANZAHL, mindestens aber 1, dimensioniert. Bei dieser Dimensionierung müssen die Teilnehmer bereit sein, in Stoßzeiten etwas zu warten, was sie bei der Benutzung des Telefons ja schon geübt haben.

KVBSTERN/KVBMAXURING gibt das Verhältnis zwischen den Gesamtkosten des Sterns und den Gesamtkosten des Rings unter den Annahmen an, daß die Verlegung der Kabel relativ billig im Vergleich zu den eigentlichen Kosten des technischen Systems ist und die Übertragungsgeschwindigkeit des Rings wie bei MAXURING dimensioniert ist.

KVTSTERN/KVTMINURING gibt das Verhältnis zwischen den Gesamtkosten des Sterns und den Gesamtkosten des Rings unter den Annahmen an, daß die Verlegung der Kabel relativ teuer im Vergleich zu den eigentlichen Kosten des technischen Systems ist und die Übertragungsgeschwindigkeit des Rings wie bei MINURING dimensioniert ist.

Die Bilder 11, 12, 13 stellen die vom Programm QUADRAT errechneten Zahlenkolonnen graphisch dar.



----- sternförmige Verbindung

—— ringförmige Verbindung

Bild 10: Verteilung der Teilnehmerstationen und deren stern- und ringförmige Verbindung

```
PROGRAM QUADRAT (INPUT,OUTPUT);

CONST MAXLAST = 0.1;
      MINLAST = 0.01;
      (* VGL. Kais_82 SEITE 46ff *)

      VB =    7.2; (* VERLEGENBILLIG *)
      VT = 9562.5; (* VERLEGENTEUER *)
      HOEHE = 65;
      BREITE = 70;
      BILDER = 3;

VAR I, J, ANZAHL, TEILUNG, MAXTEILUNG : INTEGER;
    MAXKAPAZITAETRING,
    MINKAPAZITAETRING,
    MAXURING,
    MINURING,
    X, Y, INKREMENT, STERNL, RINGL : REAL;
    MATRIX  : ARRAY [0..HOEHE,0..BREITE,1..BILDER] OF CHAR;

  PROCEDURE INITIALISIERE;
    VAR I, J, K : INTEGER;
    BEGIN
      FOR K := 1 TO BILDER DO
        FOR I := 0 TO HOEHE DO
          FOR J := 0 TO BREITE DO
            MATRIX[I,J,K] := ' ';
      FOR K := 1 TO BILDER DO
        FOR I := 1 TO HOEHE DO
          MATRIX[I,0,K] := '|';
      FOR K := 1 TO BILDER DO
        FOR J := 0 TO BREITE DO
          MATRIX[0,J,K] := '-';
    END; (* INITIALISIERE *)

  PROCEDURE EINTRAG(H:REAL;B:REAL;Z:CHAR;BILD:INTEGER);
    BEGIN
      MATRIX[ROUND( H                    * HOEHE),
             ROUND( B                    * BREITE),
             BILD] := Z;
```

```
    END; (* EINTRAG *)

  PROCEDURE DRUCKE;
    VAR I, J, K : INTEGER;
    BEGIN
    FOR K := 1 TO BILDER DO
      BEGIN
        WRITELN;
        WRITELN;
        FOR I := HOEHE DOWNTO 0 DO
          BEGIN
            WRITELN;
            FOR J := 0 TO BREITE DO
              WRITE( MATRIX[I,J,K] );
          END;
      END;
      WRITELN;
    END; (* DRUCKE *)

  FUNCTION LOG(B:REAL;ARGUMENT:REAL):REAL;
    BEGIN
      LOG := LN(ARGUMENT) / LN(B);
    END; (* LOG *)



BEGIN (* HAUPTPROGRAMM *)
  INITIALISIERE;

  READ(MAXTEILUNG);
  FOR TEILUNG := 2 TO MAXTEILUNG DO
    BEGIN
      ANZAHL := TEILUNG * TEILUNG;
      STERNL := 0;
      X := -0.5;
      INKREMENT := 1/(TEILUNG-1);

      FOR I := 1 TO TEILUNG DO
        BEGIN
          Y := -0.5;
```

```
      FOR J := 1 TO TEILUNG DO
        BEGIN
          STERNL := STERNL + SQRT(X*X+Y*Y);
          Y := Y + INKREMENT;
        END;
      X := X + INKREMENT
    END;

  IF TEILUNG MOD 2 = 0
    THEN RINGL := ANZAHL / (TEILUNG-1)
                  (* ANZAHL*INKREMENT *)
    ELSE RINGL := (ANZAHL-1+SQRT(2)) / (TEILUNG-1);
                  (* (ANZAHL-1+SQRT(2))*INKREMENT *)

  IF ANZAHL*MAXLAST > 1
    THEN MAXKAPAZITAETRING := ANZAHL * MAXLAST
    ELSE MAXKAPAZITAETRING := 1;

  IF ANZAHL*MINLAST > 1
    THEN MINKAPAZITAETRING := ANZAHL * MINLAST
    ELSE MINKAPAZITAETRING := 1;

  MAXURING := MAXKAPAZITAETRING*RINGL;
  MINURING := MINKAPAZITAETRING*RINGL;

  WRITE(TEILUNG:4,ANZAHL:6,' ',STERNL:7:2);
  WRITE(' ',RINGL:7:2);
  WRITE(' ',STERNL/RINGL:7:4);
  WRITE(' ',STERNL/MAXURING:7:4);
  WRITE(' ',STERNL/MINURING:7:4);
  WRITE(' ',STERNL*(VB+1)/(RINGL*VB+MAXURING):7:4);
  WRITELN(' ',STERNL*(VT+1)/(RINGL*VT+MINURING):7:4);

  EINTRAG( STERNL/3864,TEILUNG/MAXTEILUNG,'S',1 );
  EINTRAG( RINGL/ 3864,TEILUNG/MAXTEILUNG,'R',1 );

  EINTRAG( ( LOG(2, STERNL/MAXURING ) +5)/7,
                                TEILUNG/MAXTEILUNG,'A',2 );
  EINTRAG( ( LOG(2, STERNL/MINURING ) +5)/7,
                                TEILUNG/MAXTEILUNG,'I',2 );
```

```
      EINTRAG( ( LOG(2, STERNL*(VB+1)/(RINGL*VB+MAXURING) ) +2)/8,
                                    TEILUNG/MAXTEILUNG,'B',3 );
      EINTRAG( ( LOG(2, STERNL*(VT+1)/(RINGL*VT+MINURING) ) +2)/8,
                                    TEILUNG/MAXTEILUNG,'T',3 );

    END;
    DRUCKE;
END.
```

TEI-LUNG	AN-ZAHL	STERNL	RINGL	STERNL/ RINGL	USTERN/ MAXU_ RING	USTERN/ MINU_ RING	KVB_ STERN/ KVBMAX_ URING	KVT_ STERN/ KVTMIN_ URING
2	4	2.83	4.00	0.7071	0.7071	0.7071	0.7071	0.7071
3	9	4.83	4.71	1.0258	1.0258	1.0258	1.0258	1.0258
4	16	7.99	5.33	1.4977	0.9360	1.4977	1.3956	1.4977
5	25	11.71	6.35	1.8438	0.7375	1.8438	1.5587	1.8438
6	36	16.36	7.20	2.2729	0.6314	2.2729	1.7257	2.2729
7	49	21.66	8.24	2.6303	0.5368	2.6303	1.7825	2.6303
8	64	27.83	9.14	3.0434	0.4755	3.0434	1.8350	3.0434
9	81	34.67	10.18	3.4068	0.4206	3.4068	1.8259	3.4068
10	100	42.35	11.11	3.8119	0.3812	3.8119	1.8173	3.8119
11	121	50.74	12.14	4.1790	0.3454	3.4537	1.7755	4.1789
12	144	59.95	13.09	4.5794	0.3180	3.1801	1.7385	4.5792
13	169	69.87	14.12	4.9490	0.2928	2.9284	1.6839	4.9486
14	196	80.60	15.08	5.3462	0.2728	2.7277	1.6358	5.3457
15	225	92.06	16.10	5.7176	0.2541	2.5412	1.5786	5.7169
16	256	104.32	17.07	6.1126	0.2388	2.3878	1.5282	6.1116
17	289	117.31	18.09	6.4854	0.2244	2.2441	1.4731	6.4842
18	324	131.10	19.06	6.8788	0.2123	2.1231	1.4244	6.8772
19	361	145.62	20.08	7.2527	0.2009	2.0091	1.3735	7.2507
20	400	160.94	21.05	7.6448	0.1911	1.9112	1.3281	7.6424
21	441	177.00	22.07	8.0195	0.1818	1.8185	1.2819	8.0166
22	484	193.84	23.05	8.4106	0.1738	1.7377	1.2404	8.4072
23	529	211.43	24.06	8.7861	0.1661	1.6609	1.1988	8.7821
24	576	229.81	25.04	9.1763	0.1593	1.5931	1.1612	9.1718
25	625	248.92	26.06	9.5524	0.1528	1.5284	1.1238	9.5471
26	676	268.83	27.04	9.9420	0.1471	1.4707	1.0899	9.9360

27	729	289.48	28.05	10.3185	0.1415	1.4154	1.0563	10.3117
28	784	310.92	29.04	10.7076	0.1366	1.3658	1.0257	10.6999
29	841	333.10	30.05	11.0845	0.1318	1.3180	0.9955	11.0760
30	900	356.06	31.03	11.4731	0.1275	1.2748	0.9679	11.4635
31	961	379.77	32.05	11.8504	0.1233	1.2331	0.9407	11.8398
32	1024	404.27	33.03	12.2386	0.1195	1.1952	0.9157	12.2268
33	1089	429.51	34.04	12.6163	0.1159	1.1585	0.8911	12.6032
34	1156	455.54	35.03	13.0041	0.1125	1.1249	0.8683	12.9897
35	1225	482.31	36.04	13.3820	0.1092	1.0924	0.8460	13.3663
36	1296	509.86	37.03	13.7695	0.1062	1.0625	0.8254	13.7523
37	1369	538.17	38.04	14.1477	0.1033	1.0334	0.8051	14.1290
38	1444	567.25	39.03	14.5349	0.1007	1.0066	0.7862	14.5145
39	1521	597.09	40.04	14.9133	0.0980	0.9805	0.7677	14.8912
40	1600	627.70	41.03	15.3003	0.0956	0.9563	0.7504	15.2763
41	1681	659.07	42.04	15.6789	0.0933	0.9327	0.7334	15.6531
42	1764	691.21	43.02	16.0657	0.0911	0.9108	0.7175	16.0377
43	1849	724.11	44.03	16.4445	0.0889	0.8894	0.7020	16.4145
44	1936	757.79	45.02	16.8310	0.0869	0.8694	0.6873	16.7988
45	2025	792.21	46.03	17.2100	0.0850	0.8499	0.6730	17.1754
46	2116	827.42	47.02	17.5963	0.0832	0.8316	0.6595	17.5593
47	2209	863.38	48.03	17.9755	0.0814	0.8137	0.6462	17.9359
48	2304	900.11	49.02	18.3617	0.0797	0.7969	0.6337	18.3194
49	2401	937.60	50.03	18.7410	0.0781	0.7805	0.6214	18.6960
50	2500	975.87	51.02	19.1270	0.0765	0.7651	0.6098	19.0791
51	2601	1014.89	52.03	19.5064	0.0750	0.7500	0.5984	19.4555
52	2704	1054.68	53.02	19.8923	0.0736	0.7357	0.5876	19.8383
53	2809	1095.23	54.03	20.2718	0.0722	0.7217	0.5770	20.2146
54	2916	1136.56	55.02	20.6576	0.0708	0.7084	0.5669	20.5969
55	3025	1178.64	56.03	21.0373	0.0695	0.6954	0.5570	20.9731
56	3136	1221.49	57.02	21.4229	0.0683	0.6831	0.5476	21.3551
57	3249	1265.10	58.03	21.8027	0.0671	0.6711	0.5383	21.7311
58	3364	1309.49	59.02	22.1882	0.0660	0.6596	0.5295	22.1127
59	3481	1354.63	60.02	22.5680	0.0648	0.6483	0.5208	22.4885
60	3600	1400.55	61.02	22.9534	0.0638	0.6376	0.5126	22.8697
61	3721	1447.22	62.02	23.3334	0.0627	0.6271	0.5044	23.2454
62	3844	1494.67	63.02	23.7187	0.0617	0.6170	0.4967	23.6262
63	3969	1542.87	64.02	24.0988	0.0607	0.6072	0.4890	24.0017
64	4096	1591.85	65.02	24.4840	0.0598	0.5978	0.4817	24.3821
65	4225	1641.58	66.02	24.8641	0.0588	0.5885	0.4745	24.7573
66	4356	1692.09	67.02	25.2492	0.0580	0.5796	0.4676	25.1374

67	4489	1743.35	68.02	25.6294	0.0571	0.5709	0.4608	25.5124
68	4624	1795.39	69.01	26.0145	0.0563	0.5626	0.4543	25.8920
69	4761	1848.18	70.02	26.3948	0.0554	0.5544	0.4478	26.2668
70	4900	1901.75	71.01	26.7798	0.0547	0.5465	0.4417	26.6460
71	5041	1956.08	72.02	27.1601	0.0539	0.5388	0.4356	27.0205
72	5184	2011.17	73.01	27.5450	0.0531	0.5313	0.4297	27.3994
73	5329	2067.03	74.02	27.9254	0.0524	0.5240	0.4240	27.7736
74	5476	2123.66	75.01	28.3103	0.0517	0.5170	0.4184	28.1520
75	5625	2181.04	76.02	28.6907	0.0510	0.5101	0.4130	28.5259
76	5776	2239.20	77.01	29.0755	0.0503	0.5034	0.4077	28.9040
77	5929	2298.12	78.02	29.4560	0.0497	0.4968	0.4025	29.2776
78	6084	2357.81	79.01	29.8408	0.0490	0.4905	0.3975	29.6552
79	6241	2418.25	80.02	30.2213	0.0484	0.4842	0.3925	30.0285
80	6400	2479.47	81.01	30.6060	0.0478	0.4782	0.3878	30.4057
81	6561	2541.45	82.02	30.9866	0.0472	0.4723	0.3831	30.7787
82	6724	2604.20	83.01	31.3712	0.0467	0.4666	0.3785	31.1554
83	6889	2667.71	84.02	31.7519	0.0461	0.4609	0.3740	31.5281
84	7056	2731.99	85.01	32.1365	0.0455	0.4554	0.3697	31.9044
85	7225	2797.03	86.02	32.5172	0.0450	0.4501	0.3654	32.2767
86	7396	2862.84	87.01	32.9017	0.0445	0.4449	0.3613	32.6526
87	7569	2929.40	88.02	33.2825	0.0440	0.4397	0.3572	33.0246
88	7744	2996.75	89.01	33.6670	0.0435	0.4347	0.3532	33.4000
89	7921	3064.84	90.02	34.0477	0.0430	0.4298	0.3493	33.7716
90	8100	3133.72	91.01	34.4322	0.0425	0.4251	0.3455	34.1465
91	8281	3203.35	92.02	34.8130	0.0420	0.4204	0.3418	34.5177
92	8464	3273.75	93.01	35.1974	0.0416	0.4158	0.3381	34.8923
93	8649	3344.91	94.02	35.5783	0.0411	0.4114	0.3345	35.2631
94	8836	3416.84	95.01	35.9626	0.0407	0.4070	0.3310	35.6371
95	9025	3489.53	96.02	36.3436	0.0403	0.4027	0.3276	36.0075
96	9216	3562.99	97.01	36.7279	0.0399	0.3985	0.3243	36.3811
97	9409	3637.21	98.01	37.1088	0.0394	0.3944	0.3209	36.7511
98	9604	3712.20	99.01	37.4931	0.0390	0.3904	0.3177	37.1242
99	9801	3787.95	100.01	37.8741	0.0386	0.3864	0.3146	37.4938
100	10000	3864.48	101.01	38.2583	0.0383	0.3826	0.3115	37.8663

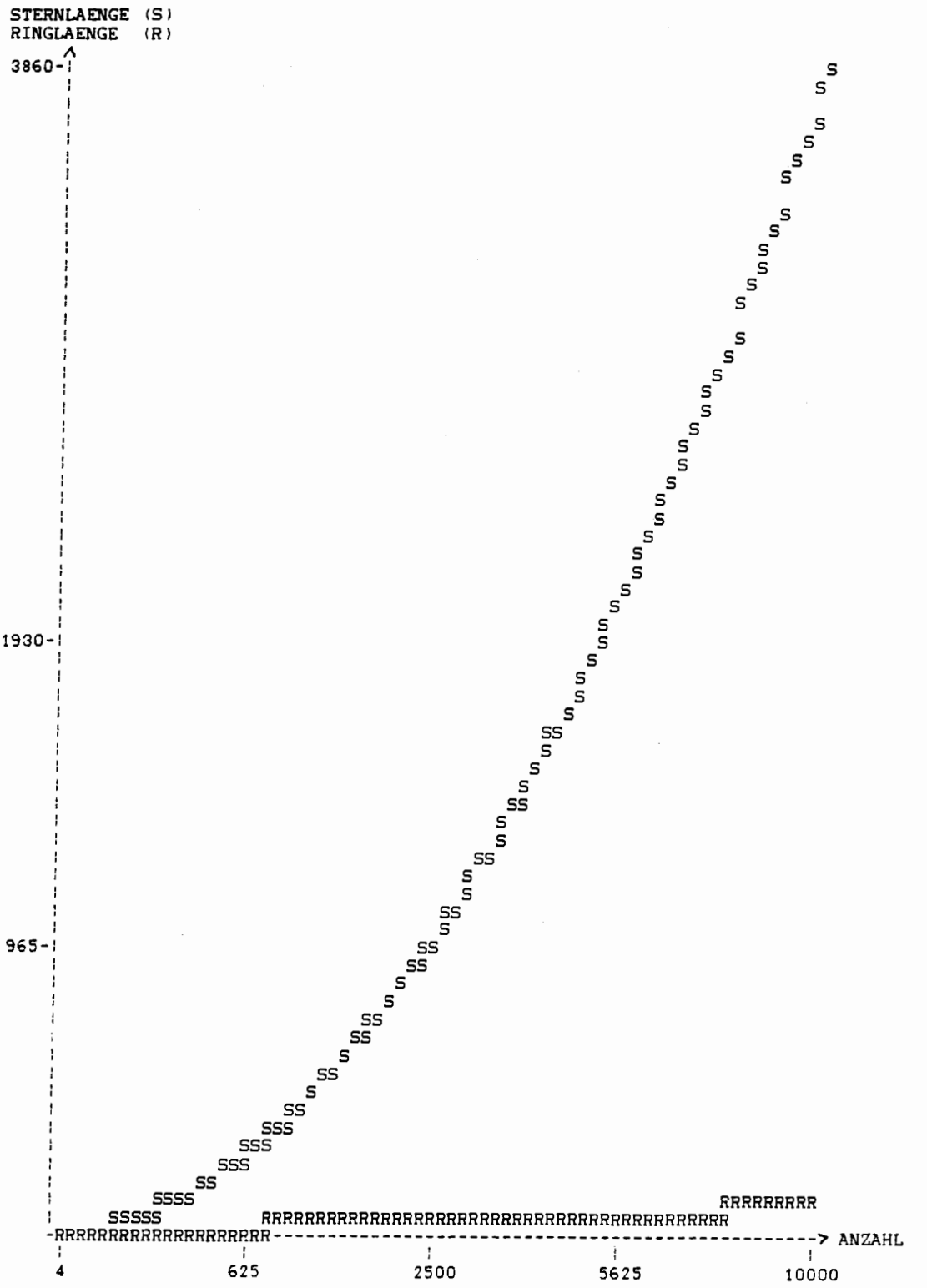


Bild 11: RINGL (R) und STERNL (S) bei quadratisch wachsender ANZAHL

Man sieht, daß STERNL wesentlich schneller wächst als RINGL. Man kann leicht beweisen, daß STERNL proportional mit der Teilnehmeranzahl wächst, RINGL aber nur mit der Quadratwurzel der Teilnehmeranzahl. Sind die Kosten der untersten Ebene des Ortsnetzes im wesentlichen durch die Länge der Kabel (Verlegekosten) bestimmt, ist der Ring ab 9 Teilnehmerstationen billiger.

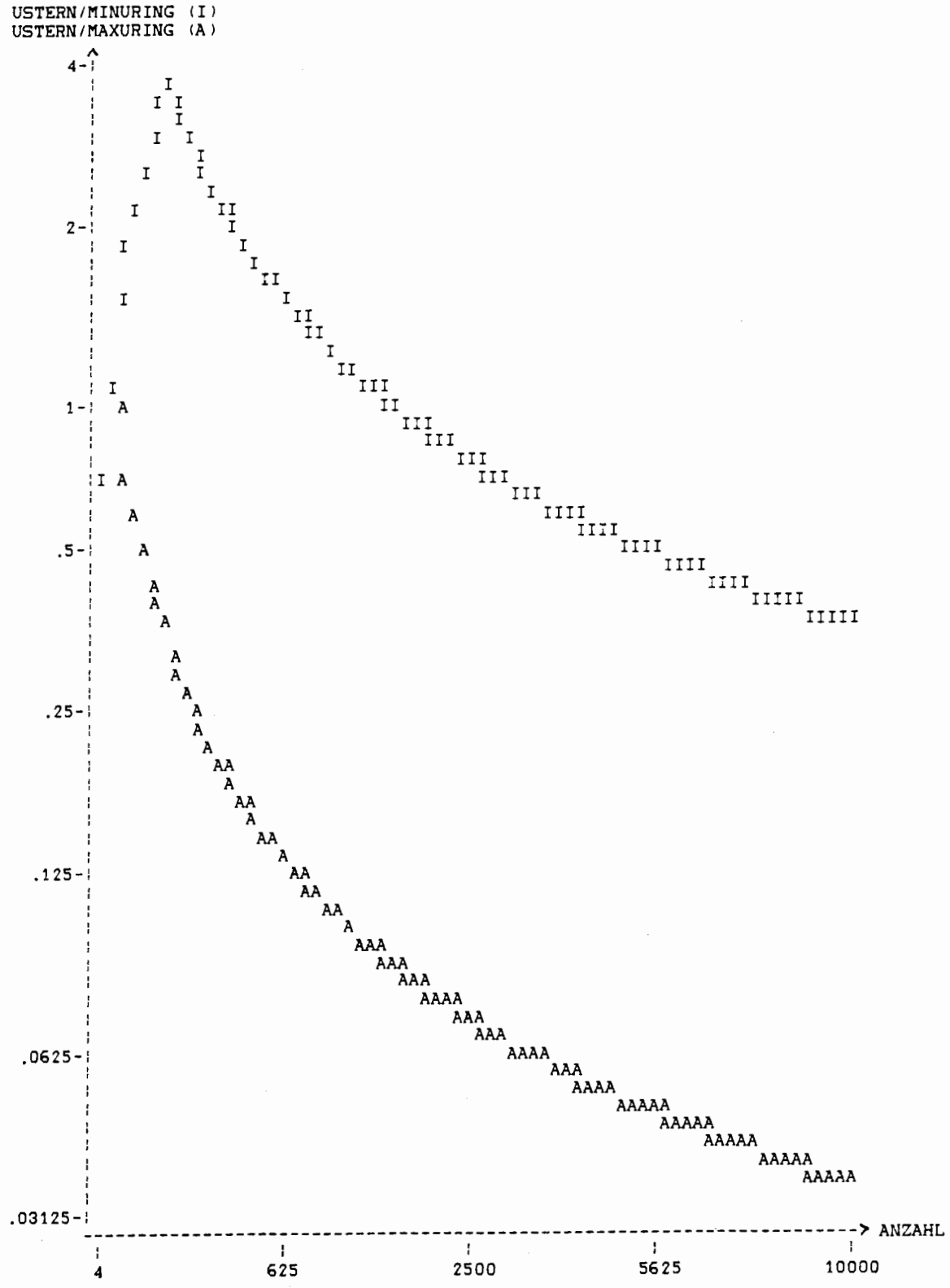


Bild 12: USTERN/MAXURING (A) und USTERN/MINURING (I) bei quadratisch wachsender ANZAHL

Sind die Kosten der untersten Ebene des Ortsnetzes im wesentlichen durch die Übertragungskosten (maximale Übertragungsgeschwindigkeit *Übertragungslänge, für den Ring ungünstige Annahme) bestimmt, sind Ring und Stern bis etwa 100 Teilnehmerstationen gleich teuer. Für mehr Teilnehmerstationen wird der Stern zunehmend

günstiger als der Ring, da die Übertragungskosten des Sterns proportional mit der Teilnehmeranzahl wachsen, die des Rings aber überproportional (Teilnehmeranzahl mal Quadratwurzel aus der Teilnehmeranzahl).

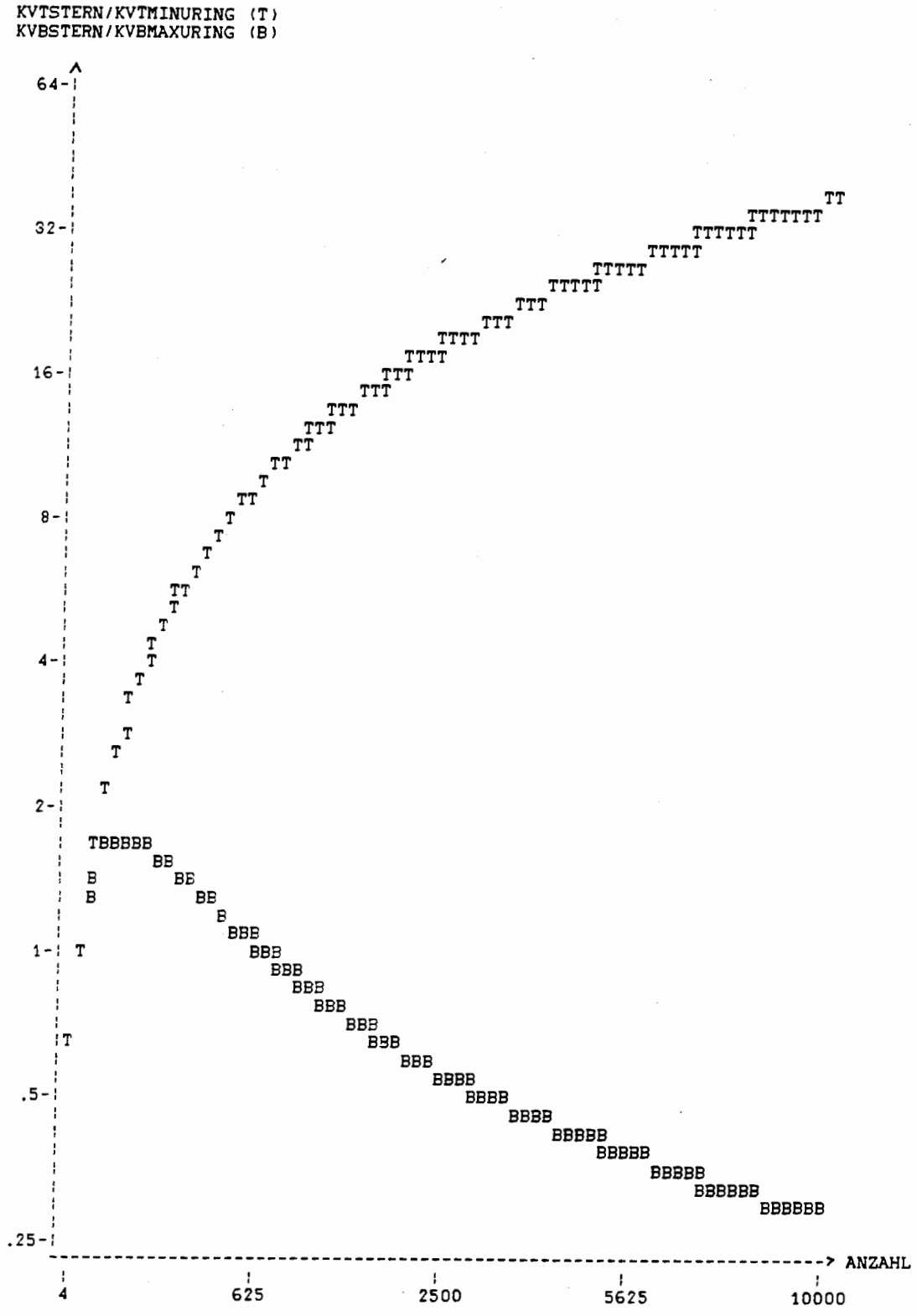


Bild 13: KVBSTERN/KVBMAXURING (B) und KVTSTERN/KVTMINURING (T) bei quadratisch wachsender ANZAHL

Mit KVBSTERN/KVBMAXURING und KVTSTERN/KVTMINURING wurde versucht, die eigentlichen Kosten des technischen Systems und die Kosten der Kabelverlegung gewichtet darzustellen. Diese Wichtung hat eine noch größere Unschärfe als die Vorhersage über die Nutzung des Systems. Insbesondere verschiebt die technische Entwicklung das Gewicht ständig so, daß das Gewicht der Kosten der Kabelverlegung größer wird.

Das Verhältnis zwischen Kosten der Kabelverlegung zu Kosten des technischen Systems unter der Annahme relativ billiger (teurer) Kosten der Kabelverlegung VB (VT) wurde errechnet wie folgt:

[Kais_82 Seite 152] nennt Verlegekosten von 30 DM/m und technische Systemkosten von 10 DM/m für Koaxialkabelstrecken in Standardtechnik. Über ein Koaxialkabel in Standardtechnik werden 12 Fernsehsignale und 24 Stereotonsignale übertragen [Kais_82 Seite 59, 62]. BIGFON bietet jedem Teilnehmer Übertragungskapazität für 5 Fernsehsignale und 4 Stereotonsignale [Brau_82], was heute als der Höchstbedarf einer Großfamilie angesehen wird. Nimmt man diese Übertragungskapazität als Einheit, so kostet das Zurverfügungstellen einer Einheit Übertragungskapazität unter Vernachlässigung der Stereotonsignale also höchstens

5/12 * 10 DM/m = 4.167 DM/m.

Das Verhältnis zwischen Kosten der Kabelverlegung und Kosten des technischen Systems unter der Annahme relativ billiger Kosten der Kabelverlegung ergibt sich also zu:

30 DM/m / 4.167 DM/m = 7.2 = VB.

Nimmt man als Einheit der Übertragungskapazität nicht das Maximalangebot von BIGFON sondern als Minimalangebot zwei digitale Telefonkanäle von je 64 kbit/s und setzt man die Übertragungskapazität eines Fernsehsignals mit 34 Mbit/s an, so kostet das Zurverfügungstellen einer Einheit Übertragungskapazität unter Vernachlässigung der Hörfunksignale

2 * 64 kbit/s / (12 * 34 Mbit/s) * 10 DM/m = 0.003137 DM/m.

Das Verhältnis zwischen Kosten der Kabelverlegung und Kosten des technischen Systems unter der Annahme relativ teurer Kosten der Kabelverlegung ergibt sich also zu:

30 DM/m / 0.003137 DM/m = 9562.5 = VT.

Bild 13 zeigt also, daß ein ein Verteilnetz mit Rückkanal realisierender Ring in jedem Fall zumindest bis etwa 784

Teilnehmerstationen zu vergleichbaren Kosten wie ein Stern realisierbar zu sein scheint.

3.2.3.7 Dimensionierung und spezielle Protokolle zur Vergabe von Sendeberechtigungen bei kontinuierlichen Sendewünschen

Wie schwer ist es,
daß der Mensch recht abwäge,
was man aufopfern muß,
gegen das, was zu gewinnen ist.
Johann Wolfgang von Goethe

Im Zuge der Digitalisierung des Ortsnetzes sollen jedem Fernsprechteilnehmer über das vorhandene Kupfer-Doppeladernetz zwei 64 kbit/s und ein 16 kbit/s Duplex-Kanäle zur Verfügung gestellt werden [RosK_82]. Zum Telefonieren wird lediglich einer der beiden 64 kbit/s Kanäle benötigt. Benutzt ein Mitglied einer Teilnehmergemeinschaft einen seiner 64 kbit/s Kanäle ausschließlich für Bildschirmtext und nimmt man an, daß, um 1200 Nutzbits/s zu übertragen, 1600 bit/s zu übertragen sind, so können über diesen einen Duplex-Kanal 40 Teilnehmer gleichzeitig mit Bildschirmtext versorgt werden. Da nicht alle gleichzeitig an Bildschirmtext teilnehmen [Kais_82 Seite 46] und, wenn sie teilnehmen, nicht dauernd Daten übertragen, können etwa 10 bis 100 mal so viele Teilnehmer versorgt werden (gleiche Annahme wie in Abschnitt 3.2.3.6). Private, lokale Verteilnetze mit etwa 400 bis 4000 Teilnehmern sind dann also ohne wesentliche zusätzliche Investitionen der Post und sogar (sofern innerhalb eines Grundstücks) ohne Genehmigung der Post realisierbar. Der Preis hierfür ist das Einrichten und Unterhalten eines privaten Spezialnetzes für Bildschirmtext.
Ein integriertes Netz mit der oben beschriebenen Struktur ist dieser Spezial-Lösung jedoch vorzuziehen. Dazu müßte die Post die reine Vermittlungs-Struktur des geplanten BIGFON in eine Vermittlungs-/Verteilstruktur ändern. Dadurch würde auch die in [Brau_83] völlig vernachlässigte Datenschutzproblematik einer "im verteilvermittelten Netz sehr einfachen Nutzungserfassung" aller Programme, also auch der bisher verteilten, entschärft.

Sofern man als Leitungstopologie für das Verteilnetz einen Bus akzeptiert (vgl. Abschnitt 3.2.2.1), kann man bei der Realisierung eines dienstintegrierten digitalen Vermittlungs-/Verteilnetzes auf der Basis eines Koaxialkabels das Verteilnetz WANGNET als Vorbild nehmen:

im Frequenzbereich bis 350 MHz werden in einem Drittel der Kapazität

* WANG Band (12 Mbit/s vergeben über CSMA/CD),
* Interconnect Band (256 Kanäle bis 9600 bit/s, 32 Kanäle 9600 bit/s, 16 Kanäle 64000 bit/s) und Utility Band (7 Fernsehkanäle)

untergebracht [Czaa_82, Elek_82].

Zur Nutzung eines derartigen lokalen Netzes als Verteilnetz mit Rückkanal bietet sich folgendes Protokoll an:

Schmalbandige Dienste mit stoßweisem Verkehrsaufkommen (bursty traffic) werden über CSMA/CD im WANG Band abgewickelt. Breitbandige Dienste mit gleichmäßigem Verkehrsaufkommen werden zunächst über das WANG Band angefordert. Die Verteilnetzzentrale teilt einen freien Kanal zu bzw. nennt im Falle von Rundfunk- oder Fernsehverteilprogrammen, die schon von anderen gehört oder gesehen werden, den Kanal (und bei Pay-TV auch einen passenden Schlüssel zur Entschlüsselung) oder lehnt die Anforderung ab, wenn die benötigten Betriebsmittel nicht verfügbar sind.

Dies für Frequenzmultiplex geeignete Protokoll der Klasse centrally controlled demand assignement [Toba_80] erspart an 4 Stellen Aufwand, ohne den Datenschutz wesentlich zu verringern:

1) Der bei gleichmäßigem breitbandigem Verkehrsaufkommen hohe Overhead und der die Einhaltung von Zeitbedingungen störende Indeterminismus bei der Vergabe der Sendeberechtigung wird auf den Overhead zweier Nachrichten (Anforderung, Ende) reduziert.
2) Der Nachrichtenaustausch zur Vereinbarung eines Kanals bei gleichmäßigem Verkehrsaufkommen kann genutzt werden, zwischen den Teilnehmern einen geheimen Schlüssel eines Kryptosystems mit geheimen Schlüsseln (z. B. DES) auszutauschen. Durch die Verschlüsselung mit einem geheimen Schlüsssel können auch hohe Datenraten preiswert verschlüsselt werden, da die Algorithmen einfacher und passende Chips bereits vorhanden sind.
3) Von mehreren Benutzern gewünschte Verteildienste belegen je

nur einmal einen Kanal, d. h. Mehrfachübertragung derselben Information wird durch Ausnutzen der Broadcast-Fähigkeit des lokalen Netzes vermieden.

4) Da die Teilnehmerstation nicht dauernd die gesamte Information auf dem Verteilnetz sondern nur die Information im WANG Band und eventuellen anderen zugeteilten Kanälen verfolgen müssen, dürften sie dadurch kostengünstiger realisierbar sein.

Nutzt man die unbelegten 2 Drittel der Kapazität von WANGNET für weitere Fernsehkanäle, so dürfte WANGNET breitbandige Verteilnetze mit Rückkanal für etwa 40 Teilnehmer ermöglichen.

Mit einer Abwandlung des obigen Protokolls für Zeitmultiplex läßt sich die Übertragungskapazität von 2 Gbit/s auf einer Glasfaser [BEGW_83] folgendermaßen nutzen:
20 Fernsehkanäle zu je 34 Mbit/s [Kais_82 Seite 102] und 100 Stereotonkanäle zu je 1 Mbit/s [Bauc_83] werden für Verteilprogramme vorgesehen,

2 Gbit/s - 780 Mbit/s = 1220 Mbit/s

bleiben für Zweiwegdienste übrig. Um abzuschätzen, wie viele Teilnehmer an einem derartigen Ring angeschlossen werden können, wird jedem Teilnehmer der Übertragungsbedarf von 2 Fernsehkanälen zugeordnet. Unter der Annahme, daß höchstens 5% der Teilnehmer gleichzeitig Bildfernsprechen, können

1220 Mbit/s / (0.05 * 2 * 34 Mbit/s) = 358

Teilnehmer an den Ring angeschlossen werden. Dabei bleibt das Dienstangebot von BIGFON erhalten. In diesem Beispiel wurde zu übertragende Verwaltungsinformation (z. B. Adressen) vernachlässigt, da hauptsächlich gleichmäßiges breitbandiges Verkehrsaufkommen angenommen wurde. Ebenfalls wurde nicht berücksichtigt, daß der Durchsatz eines Rings 1 bis 2 mal so groß wie die Kapazität seiner Leitungen sein kann [BuSc_83 Seite 54].

3.2.3.8 Mögliche Betreiber des Verteilnetzes mit Rückkanal

Alles läuft nach Programm.
Aber nicht immer programmgemäß.

Bisher wurde davon ausgegangen, daß der Betreiber des Vermittlungsnetzes (die Post) das Verteilnetz mit Rückkanal nicht betreibt, um dem Benutzer die Kontrolle seiner Datenschutzbelange zumindest teilweise zu ermöglichen.
In diesem Abschnitt wird untersucht, welche Teile des Verteilnetzes mit Rückkanal der Betreiber des Vermittlungsnetzes betreiben kann, ohne daß dadurch die Kontrolle des Benutzers über seine Datenschutzbelange abgeschwächt wird.

Wählt man als Leitungstopologie des Verteilnetzes mit Rückkanal einen Bus, so muß dem Betreiber des Vermittlungsnetzes der Zugang zum Bus aus den in Abschnitt 3.2.2.1 genannten Gründen und seiner Fähigkeit, auch private Adressen in ihre zwei Teile zu zerlegen, vollständig verwehrt werden. Der Betreiber des Vermittlungsnetzes kommt dann als Betreiber eines Teils des Verteilnetzes mit Rückkanal nicht in Betracht.

Wählt man als Leitungstopologie einen Ring, so kann der Betreiber des Vermittlungsnetzes die Verteilnetzzentrale betreiben, da er dadurch nur an einer Stelle Zugang zum Ring erhält. Ring und Teilnehmerstationen müssen aber für den Betreiber des Vermittlungsnetzes unzugänglich bleiben.
Betreibt der Betreiber des Vermittlungsnetzes die Verteilnetzzentrale, ist eine Anwendung der Maßnahme M2 in Abschnitt 3.3 zur Vermeidung zeitlicher Muster nicht sinnvoll, die Anwendung von M1 oder M3 bleibt jedoch wirksam.

3.2.3.9 Abschließende Bewertung

Im Leben ist es oft besser,
zu wollen, was man nicht hat,
als zu haben, was man nicht will.

Das Vermittlungs-/Verteilnetz erhöht den Kommunikationsaufwand im öffentlichen Vermittlungsnetz kaum, genügt also Randbedingung R1 aus Abschnitt 3.1.
R2, R3 und R4 ermöglichen die Realisierung genügend großer lokaler, privater Verteilnetze, R5 die Zustellung vertraulicher Nachrichten in einem Verteilnetz.
Wenn die Teilnehmer es wünschen, können über das vorgeschlagene Vermittlungs-/Verteilnetz auch einseitig anonyme Kommunikation sowie Kommunikation zwischen sich voll identifizierenden Teilnehmern erfolgen.
Entsprechend Abschnitt 2 bietet dieses Vermittlungs-/Verteilnetz dem Teilnehmer folgende Vor- und Nachteile:

+ Informationen können schnell aus beliebig großen Informationsangeboten ausgewählt und vermittelt/verteilt werden.
+ Dialoge sind möglich.
+ Datenschutzmaßnahmen sind in der (den) öffentlichen Vermittlungszentrale(n) des Vermittlungsnetzes und in den privaten, lokalen Verteilnetzen realisierbar.
+ Die oben beschriebene strukturbedingt-anonyme Abfrage ist nur bei Eingriffen in die privaten, lokalen Verteilnetze änderbar bzw. ist nur generell abschaffbar. Änderungen müssen also den Teilnehmern auffallen.
+ Auch bei direktem Kontakt zwischen Teilnehmern [Alke_82 Seite 90] kann die Anonymität gewahrt bleiben.
+ Bei geeigneter Dimensionierung ist es als dienstintegriertes Netz (ISDN) nutzbar.
+ Sofern das private, lokale Verteilnetz Grundstücksgrenzen nicht überschreitet, kann es zur postgebührenfreien lokalen Kommunikation genutzt werden, vgl. [MaSe_83].
- Wieviel Datenschutz die Anonymität innerhalb der Teilnehmergemeinschaft eines privaten, lokalen Verteilnetzes genau bietet, hängt vom Verhalten der Teilnehmer dieser Gemeinschaft ab. Das bekannte Problem der Anfrage an statistische Datenbanken [Denn_82 Seite 331ff, DeSc_83, Leis_82 Seite 7ff, Schl_82,

WeSc_83] ist hierauf übertragbar. Die Persönlichkeiten der Teilnehmer entsprechen den Datensätzen von Einzelpersonen in statistischen Datenbanken, die Kommunikationsabläufe entsprechen speziellen Anfragen an eine statistische Datenbank.

- Je größer die Teilnehmergemeinschaft eines privaten, lokalen Verteilnetzes ist und damit auch der durch die System-Struktur gegebene Datenschutz für den einzelnen Teilnehmer, desto weniger fällt es auf, wenn sich Unbefugte am Verteilnetz zu schaffen machen. Damit hierdurch nicht der Datenschutz eventuell erheblich gemindert wird, muß die Teilnehmergemeinschaft organisatorische Gegenmaßnahmen, z. B. Zugangskontrollen, treffen.

3.2.4 Vermittlungs-/Vermittlungsnetz

Prüfet alles und
das Gute behaltet.
Paulus

Die vierte Lösungsalternative besteht darin, daß die Post ein Vermittlungsnetz als Fernnetz betreibt, dessen Endknoten private, lokale Vermittlungsnetze sind (Bild 14).

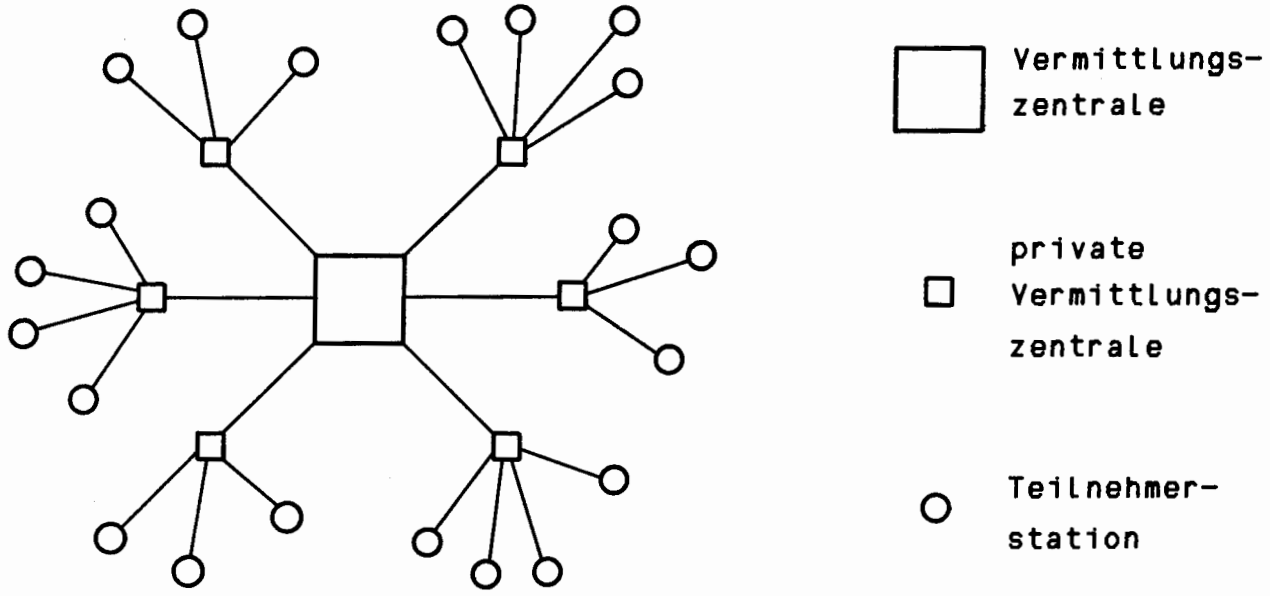


Bild_14: Vermittlungs-/Vermittlungsnetz

Die privaten, lokalen Vermittlungsnetze können als Weiterentwicklung privater Nebenstellenanlagen (PABX = Private Automatic Branch Exchange) betrachtet werden.
Da die privaten, lokalen Vermittlungsnetze geringere Anonymität als private, lokale Verteilnetze mit Rückkanal bieten (vgl. Abschnitt 3.2.2.1) und zudem teurer zu sein scheinen (vgl. Abschnitt 3.2.3.6), wird diese Lösungsalternative nicht weiter betrachtet. Sie wurde der Vollständigkeit halber erwähnt, da sie eine für europäische Verhältnisse entworfene Netzstruktur für das Protokoll von David L. Chaum ist [Chau_81]. Sein Protokoll wird mit dem Vermittlungs-/Verteilnetz in Abschnitt 3.4 verglichen.

3.2.5 Verteil-/Verteilnetz

Denn viele sind Empfänger,
aber wenige sind Adressat.
frei nach Matthäus 22,14

In diesem Abschnitt wird untersucht, inwieweit man Verteilnetze hierarchisch anordnen kann bzw. sollte (vgl. Abschnitt 3.2.3). Anders ausgedrückt: soll man verschiedene Ebenen eines Kommunikationsnetzes als Verteilnetz mit Rückkanal realisieren?
Bild 15 zeigt eine Verteil-/Verteilnetz genannte Struktur für das in Bild 5 als Vermittlungs-/Verteilnetz dargestellte System.

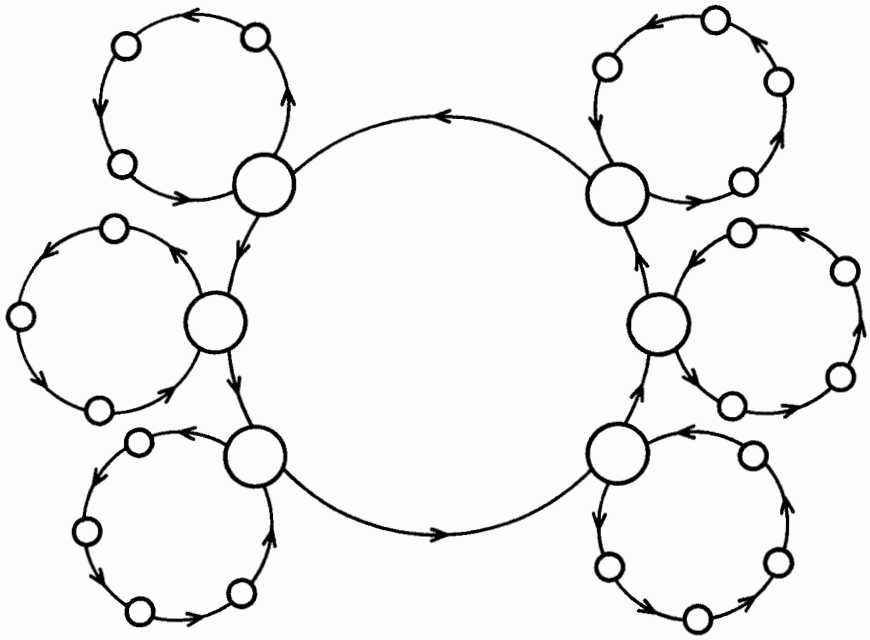


Bild 15: Verteil-/Verteilnetz

Ein Verteil-/Verteilnetz hat folgende wesentliche Vor- und Nachteile:

+ Eine Verkehrsanalyse im Fernnetz wird für einen Eindringling wesentlich schwieriger (nicht jedoch für den Fernnetzbetreiber).
- Die Datenrate im Fernnetz dürfte exzessiv hoch werden.
- Die ein lokales Verteilnetz begünstigenden anteilig hohen Verlegekosten der Kabel dürften beim Fernnetz anteilig geringer sein. Dies begünstigt ein Vermittlungsnetz.

Zusammenfassend scheint mir ein Verteil-/Verteilnetz beim

jetzigen Stand der Technik keine kostengünstige Lösung zu sein, außer die Technologie des Fernnetzes bietet Broadcast-Fähigkeit. Dies ist z. B. bei Satelliten-Netzen [Gerk_82 Seite 220] der Fall.

3.3 Vermeidung zeitlicher Muster

> The date of an incident has much the same significance as its location as an aid to confirming facts and to determining trends.
>
> Adrian R. D. Norman

Bis hierher wurden Netz-Strukturen entwickelt, die die Identifikation des Absenders/Empfängers einer Nachricht durch die räumliche Topologie des Netzes unmöglich oder zumindest sehr schwierig machen:

* Im Vermittlungs-/Verteilnetz ist keine Leitung nur einer Teilnehmerstation zugeordnet.
* Es gibt im Vermittlungs-/Verteilnetz keine eineindeutige Zuordnung Adresse-Teilnehmerstation mehr.

Möglicherweise können aber Nachrichten dem Absender/Empfänger auch durch die zeitliche Topologie der Benutzung des Netzes (zeitliche Muster) zugeordnet werden:

Der einzige (Nacht-)Schichtarbeiter in einem Verteilnetz mit Rückkanal fordert regelmäßig um 3 Uhr morgens nach seiner Rückkehr von der Arbeit eine Abendzeitung an. Diese Anforderung und auch die Länge der Abendzeitung kann ihm zugeordnet werden, da um diese Zeit normalerweise kein anderer Teilnehmer der Teilnehmergemeinschaft Nachrichten sendet oder empfängt.

Folgende Maßnahmen verhindern bzw. erschweren die Identifikation des Absenders/Empfängers durch die zeitliche Topologie der Benutzung des Netzes:

M1 Wenn immer möglich wählt die Teilnehmerstation den Absendezeitpunkt von Nachrichten innerhalb von durch Benutzererwartungen oder günstige (Nacht-)Tarife vorgegebenen Zeitintervallen zufällig.

Neben der Erhöhung des Datenschutzes wird durch M1 auch das Netz gleichmäßiger ausgelastet und durch Nutzung von (Nacht-)Tarifen Gebühren gespart.

In der Welt des obigen Beispiels bedeutet das, daß der (Nacht-)Schichtarbeiter vor der Abfahrt zur Arbeit seine Teilnehmerstation beauftragt, die gewünschte Abendzeitung zufällig zwischen z. B. 21 Uhr und 3 Uhr anzufordern.

M2 Falls zu verkehrsschwacher Zeit eine Nachricht von einer ihrer Teilnehmerstationen kommt, erzeugt die Verteilnetzzentrale sowohl im Vermittlungs- als auch im Verteilnetz weitere bedeutungslose Nachrichten (dummy traffic).

M2 ist nur sinnvoll, wenn der Teilnehmer der Verteilnetzzentrale vertraut (vgl. Abschnitt 3.2.3.8). Andernfalls könnte ja gerade sie ihn beobachten, wogegen die von ihr erzeugten bedeutungslosen Nachrichten natürlich nicht helfen.

M2 erhöht, wenn auch nur zu verkehrsschwachen Zeiten, bei Bedarf den Nachrichtenverkehr im Netz und erfordert Konventionen, wer die dadurch entstehenden Übertragungsgebühren für die bedeutungslosen Nachrichten trägt.

M3 Die Teilnehmerstationen sorgen dafür, daß der Nachrichtenverkehr nicht unter einen vorgegebenen Minimalwert sinkt, indem sie gegebenenfalls bedeutungslose Nachrichten erzeugen.

M3 erhöht, wenn auch nur zu verkehrsschwachen Zeiten, den Nachrichtenverkehr im Netz und erfordert Konventionen, wer die dadurch entstehenden Übertragungsgebühren für die bedeutungslosen Nachrichten trägt.

3.4 Vergleich mit der Lösungsalternative von David L. Chaum

Spieglein, Spieglein an der Wand,
wer ist die Schönste im ganzen Land?
Gebrüder Grimm

David L. Chaum beschreibt in [Chau_81] ein Verfahren, das innerhalb eines Vermittlungsnetzes anonyme elektronische Post ermöglicht, sofern man wenigstens einer der Vermittlungszentralen, die das elektronische Poststück passiert, vertraut.

Sein Verfahren basiert wie das Kommunikationsprotokoll von Abschnitt 3.2.2.2 auf der Benutzung eines Kryptosystems mit

MIXe müssen sich Nachrichten merken um Wiederholungen zu ignorieren

öffentlichen Schlüsseln.

Der Gewinn an Datenschutz durch die beiden Verfahren ist schwer zu vergleichen, da sie jeweils verschiedenen Funktionen im Netz vertrauen. Ebenso ist ihr Aufwand schwer zu vergleichen, da sie verschiedene Netzstrukturen benutzen.

Beschränkt man den Vergleich auf das wirklich Vergleichbare, nämlich den

Aufwand zur Verschlüsselung (V) und Entschlüsselung (E) von Nachrichten (N), Adressen (A) oder Schlüsseln (S) sowie den

Aufwand zur Erzeugung von Zufallszahlen (Z) und Schlüsselpaaren (P),

so ergibt sich folgende Vergleichstabelle (Bild 16), in der x die Anzahl der von einer Nachricht zu passierenden Vermittlungszentralen ist.

Für mein Empfinden unnötiger Aufwand beim Senden einer Nachricht im Verfahren von David L. Chaum durch x-maliges Anfügen von Zufallszahlen an die Nachricht ist in Bild 16 nicht enthalten.

Verfahren von / Dienst	Chaum	Pfitzmann
Senden einer Nachricht	(x+1) (V+E) (N+A)	(V+E) N + x E A
Bildung und Benutzung eines anonymisierten Absenders	(x+1) P + x (V+E) (A + 0.5 (x-1) S)	Z + V A + P + x E A

Bild 16: Aufwandsvergleich

Da das Wählen von Schlüsselpaaren aufwendiger als die Erzeugung von Zufallszahlen ist, ist das Verfahren von David L. Chaum also immer und für große x deutlich aufwendiger als das Kommunikationsprotokoll von Abschnitt 3.2.3.2. Das Verfahren von David L. Chaum muß zudem im Gegensatz zu M1, M2 und M3 aus Abschnitt 3.3 immer bedeutungslose Nachrichten (dummy traffic) erzeugen, da es auf einem reinen Vermittlungsnetz operiert.

Zusammenfassend kann man sagen, daß das Verfahren von David L. Chaum für elektronische Post in Rechnernetzen geeignet ist, wenn die Rechner des Netzes von verschiedenen Organisationen betrieben werden und die Benutzer wenigstens einigen Organisationen und Rechnern vertrauen (vgl. Abschnitt 3.2.4). Für kontinuierlichen Nachrichtenverkehr (Telefon, Bildfernsprechen etc.) ist das Verfahren von David L. Chaum nicht konzipiert, nicht geeignet und auch nicht adaptierbar, da zum Verbergen der eigentlichen Nachrichtenströme exzessive Mengen an bedeutungslosen Nachrichten durch das Netz geschickt und sehr häufig ver-/entschlüsselt werden müßten.
Das Verfahren von David L. Chaum kann für elektronische Post im Vermittlungsnetz eines Vermittlungs-/Verteilnetzes zusätzlich angewandt werden, um den Datenschutz noch zu erhöhen. Gibt es einen Betreiber aller Vermittlungszentralen (in Deutschland die Post) wird der Datenschutz bezüglich des Betreibers der Vermittlungszentralen dadurch jedoch nicht erhöht.

4 Anschluß des Vermittlungs-/Verteilnetzes an andere Netze

Das Wort ist schnell gesprochen,
die Tat braucht länger.
Russisches Sprichwort

Da ein Vermittlungs-/Verteilnetz nicht von heute auf morgen und eventuell auch auf Dauer aus politischen Gründen nur innerhalb einzelner Länder realisierbar ist, müssen Kommunikationsmöglichkeiten zwischen Vermittlungs-/Verteilnetzen und anderen Netzen geschaffen werden.
Da die allgemeinen Schwierigkeiten und Lösungen beim Schaffen von Kommunikationsmöglichkeiten zwischen verschiedenen Netzen bekannt sind [BeEs_83, GrHS_83, Schd_83], brauchen hier nur die durch die Vermittlungs-/Verteilstruktur bedingten Eigenschaften betrachtet zu werden:

1) Adressierung,
2) anonymisierte Absender,
3) verschlüsselte Nachrichten und
4) Gebührenabrechnung.

Folgende Lösung ist immer möglich, wenn im anderen Netz beliebige Bitfolgen übertragen werden können und dürfen:

L1 Nachrichten werden, wenn eine im eigenen Netz nicht definierte Adresse vorkommt, automatisch an einen den Netzübergang realisierenden Rechner G (gateway) geleitet, der natürlich auch explizit adressiert werden kann.
Beim Übergang Vermittlungs-/Verteilnetz anderes Netz ist die Nachricht den ersten Teil des Weges mit G's öffentlichem Schlüssel G_ö verschlüsselt. Die Nachricht besteht neben F_pa und F_ö (anonymisierter Absender) aus einer Adresse 1 (A1) und einem Inhalt 1 (I1).
G entschlüsselt sie mit seinem privaten Schlüssel G_p und überträgt die Nachricht und seinen Absender g' im anderen Netz weiter (Bild 17). g', F_pa und F_ö bilden im anderen Netz einen anonymisierten Absender.
Inhalt 2 (I2) zusammen mit F_pa und F_ö kann mit g' als Adresse im anderen Netz an G geschickt werden, der I2 mit F_ö verschlüsselt und mit der privaten Adresse F_pa weitersendet.

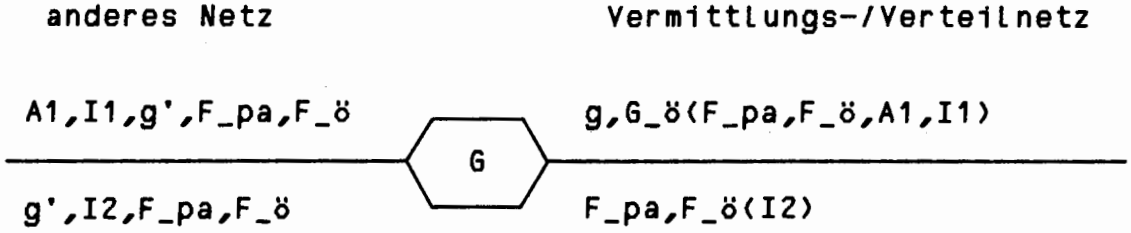


Bild 17: Netzübergang bei beliebigen Bitfolgen

G führt einen Zähler und erhält für alle aus dem Vermittlungs-/Verteilnetz angeforderten Dienste eine Abbuchungsermächtigung, mit der verfahren wird wie in Abschnitt 3.2.3.3.2 geschildert.
Für die Abrechnung der aus dem anderen Netz angeforderten Dienste muß das andere Netz (eventuell mit Hilfe von G) sorgen.

Der umgekehrte Fall, daß zuerst aus dem anderen Netz kommuniziert werden will, verläuft analog.
In beiden Fällen wird vorausgesetzt, daß der die Kommunikation wünschende Teilnehmer eine Adresse im anderen Netz in Erfahrung gebracht hat. Dies kann unkomfortabel oder gar unmöglich sein. Dies ist jedoch ein allgemeines Problem, dessen mögliche Lösungen

bekannt sind oder noch gesucht werden [Su_83].

L2 Ist auch der Teilnehmer im anderen Netz in der Lage, Nachrichten zu ver-/entschlüsseln, so können zwischen G und ihm I1,g',F_pa,F_ö bzw. zwischen ihm und G I2,F_pa,F_ö verschlüsselt übertragen werden.

L3 Können sich der Teilnehmer im andern Netz und der im Vermittlungs-/Verteilnetz auf ein gemeinsames Kryptosystem mit öffentlichen Schlüsseln einigen, so können sie öffentliche Schlüssel austauschen und ihre Inhalte damit verschlüsseln (I1, I2 in Bild 17), damit G die Inhalte nicht erfährt.
Die Teilnehmer müssen überprüfen, ob G die öffentlichen Schlüssel wirklich unverändert weitergegeben hat. Andernfalls könnte G von ihm erzeugte öffentliche Schlüssel statt die der Teilnehmer weitergeben, die eintreffenden Nachrichten mit den zugehörigen privaten Schlüsseln entschlüsseln, kopieren, mit dem nicht weitergegeben öffentlichen Schlüssel des Empfängers verschlüsseln und dann weiterübertragen.

Wenn alle den Netzübergang realisierenden Rechner in abgesprochener Weise Schlüssel substituieren, scheint die Überprüfung, daß die öffentlichen Schlüssel unverändert weitergegeben wurden, innerhalb des Netzes nicht möglich zu sein [Inge_83 Seite 231, Konh_81 Seite 346].

In [LeMa_83] ist ein Handshake-Algorithmus angegeben, der es zwei nicht bekannten Teilnehmern erlaubt zu überprüfen, ob aus einem (z. B. gedruckten) öffentlichen Verzeichnis entnommene öffentliche Schlüssel zu den verwendeten privaten Schlüsseln passen. Nach dieser Überprüfung können dann die Teilnehmer andere öffentliche Schlüssel austauschen und verfahren wie in Abschnitt 3.2.3.2.

Können oder dürfen im anderen Netz keine beliebigen Bitfolgen übertragen werden (vgl. [Abra_83]), so wird L1 leicht abgewandelt:

L4 G vergibt beim Netzübergang eine Nachrichtennummer (NN), die im anderen Netz eine zulässige Bitkombination darstellt, und merkt sich Nachrichtennummern und korrespondierende Adressen und öffentliche Schlüssel für eine gewisse Mindestzeit (Bild

18).

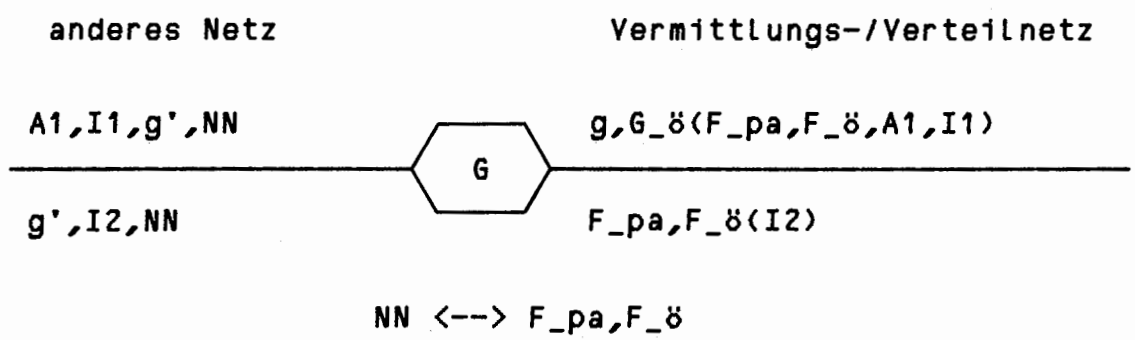


Bild_18: Netzübergang bei eingeschränkten Bitfolgen

5 Ausblick

In software,
virtually anything is possible;
however,
few things are feasible.
Cheatham

Ein angepaßtes Neues Medium muß dem Teilnehmer die Kontrolle seiner Datenschutzbelange zumindest teilweise ermöglichen (Datenschutz-Ergonomie), damit er sich nicht selber vollständig kontrolliert fühlt.
Ich hoffe, hiermit deutlich gemacht zu haben, daß

1. jedes System höchstens soviel Kontrolle seiner Teilnehmer bietet, wie es die Datenerfassung des Teilnehmerverhaltens ermöglicht und
2. System-Strukturen für Neue Medien denkbar und kostengünstig realisierbar sind, die die Datenerfassungsmöglichkeiten wesentlich verkleinern.

   Das Prinzip der entwickelten System-Strukturen besteht darin, daß nicht

   jede Teilnehmerstation nur die für sie bestimmten Nachrichten erhält,

   und auch nicht, wie in [Chau_81] vorgeschlagen und in Abschnitt 3.2.2 diskutiert,

   jede Teilnehmerstation jede Nachricht erhält,

sondern, wie in Abschnitt 3.2.3 erläutert,

jede Teilnehmerstation alle Nachrichten an eine Teilnehmerstation innerhalb ihrer Gruppe erhält.

Es ist nötig darauf hinzuarbeiten, daß unsere Gesellschaft die Strukturen ihrer Informations- und Kommunikationssysteme so wählt, daß die folgende Äußerung von Prof. Dr. Fritz-Rudolf Güntsch nicht oder zumindest nur teilweise zutrifft [Günt_82 Seite 56]:

"Dieses Eindringen von Kommunikations- und Computernetzen in alle Bereiche unseres Lebens erhöht die Kontrollierbarkeit des Individuums bei Arbeit und Freizeit, weil sich letztlich immmer mehr menschliche Tätigkeiten und Bedürfnisse in diesen Netzen und Speichern abbilden werden, wo sie gerade aufgrund der Entwicklung in der Informationsverarbeitung zunehmend intelligent und automatisch ausgewertet werden könnten. Ich spreche von >>können<< und >>Kontrollierbarkeit<<, weil wir - so wir weise sind - davon keinen Gebrauch machen.
Aber muß man wirklich Pessimist sein, um zu der Vermutung zu kommen, manch einer - und vielleicht auch der Staat - könnte irgendwann der Versuchung erliegen, diese Kontrollmöglichkeiten gegenüber Arbeits- und Konsumverhalten anderer für seine Interessen zu nutzen? Die Erhöhung dieses Kontrollpotentials und die Absenkung von bisher kostenbedingten Kontrollbarrieren sind Eigenschaften dieser technischen Entwicklung, die auch bei extremem technischen und organisatorischen Aufwand und trotz aller Datenschutznormen und anderer Regelungen nicht aus der Welt geschaffen werden können."

Danksagung

Habent sua fata libelli.
Terentianus Maurus

Für das Schaffen eines Freiraums zur selbständigen Arbeit und seine ständige Gesprächsbereitschaft danke ich Prof. Winfried Görke. Für Diskussion und Hinweise danke ich ebenso Prof. Hans Peter Bull, Dr. Klaus Dittrich, Klaus Echtle, Prof. Herbert Fiedler, Hermann Härtig, Jürgen Hülsemann, Prof. Walter Kuntz,

Dr. Axel Lehmann, einem/einer mir namentlich nicht bekannten Mitarbeiter/in von Dr. Ruth Leuze, Michael Marhöfer, Prof. H. A. Maurer, Fritz Müller, Birgit Pfitzmann, Dr. Johannes Röhrich, Dr. Jan Schlörer und Prof. Detlef Schmid.

Literatur

Abra_83 Marshall D. Abrams: End-to-end Encryption Implementation Problems in an Asynchronous Network; Proceedings IEEE INFOCOM 83, San Diego, California, April 18-21, 1983, Seite 257 bis 264

Alke_82 Horst H. Alke: Datenschutz - Schutz vor Neuen Medien? Datenschutz und Datensicherung, 2/1982, Seite 86 bis 93

Bauc_83 Helmut Bauch: BIGFON - die Übertragungstechnik; telcom report Siemens Aktiengesellschaft, Band 6, Heft 2, April 1983, Seite 57 bis 62

Baue_82 Friedrich L. Bauer: Kryptologie - Verfahren und Maximen; Informatik-Spektrum Band 5, Heft 2, Juli 1982, Seite 74 bis 81

Baue_83 Peter Baues: Kommunikation im optischen lokalen Netz SIELOCnet; GI '83 Proceedings zum Industrieprogramm, Bernd Wolfinger (ed.), 13. Jahrestagung der Gesellschaft für Informatik 3. bis 7. Oktober 1983, Universität Hamburg, Seite 52 bis 64

BeEs_83 Eric Benhamou, Judy Estrin: Multilevel Internetworking Gateways: Architecture and Applications; IEEE Computer Vol. 16, Nu. 9, September 1983, Seite 27 bis 34

BEGW_83 Clemens Baack, Gerhard Elze, Gerd Grosskopf, Godehard Walf: Digital and Analog Optical Broad-Band Transmission; Proceedings of the IEEE, Vol. 71, Nu. 2, February 1983, Seite 198 bis 208

Beth_82 Thomas Beth: Kryptographie als Instrument des Datenschutzes; Informatik-Spektrum Band 5, Heft 2, Juli 1982, Seite 82 bis 96 ergänzte Version in Thomas Beth, Peter Heß, Klaus Wirl: Kryptographie; B. G. Teubner Stuttgart 1983, Seite 10 bis 43

Bild_83 Bildschirmtext: Warten auf den Tag X; computer magazin März 1983, 12. Jahrgang, Seite 58 bis 59

BMPS_83 H. Bogensberger, H. Maurer, R. Posch, W. Schinnerl: Ein neuartiges - durch spezielle Hardware unterstütztes - Terminalkonzept für Bildschirmtext; Angewandte Informatik 3/1983, Friedr. Vieweg & Sohn, Wiesbaden, Seite 108 bis 113

Bosc_82 Wolfgang Bosch: Zwei neue Anwendungen für Bildschirmtext; ntz Band 35, Heft 12, 1982, Seite 740 bis 742

Brau_82 Ewald Braun: BIGFON - der Start für die Kommunikationstechnik der Zukunft; telcom report Band 5, Heft 2, 1982, Seite 123 bis 129

Brau_83 Ewald Braun: BIGFON - Erprobung der optischen Breitbandübertragung im Ortsnetz; telcom report Siemens Aktiengesellschaft, Band 6, Heft 2, April 1983, Seite 52 bis 53

Bull_82 Hans Peter Bull: Datenschutz und neue Medien; Datenschutz und Datensicherung, 3/1982, Seite 147 bis 152

BuSc_83 Werner Bux, Marcel Schlatter: An Approximate Method for the Performance Analysis of Buffer Insertion Rings; IEEE Transactions on Communications, Vol. COM-31, No. 1, January 1983, Seite 50 bis 55

Chau_81 David L. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; CACM Vol. 24, Nr. 2, February 1981, Seite 84 bis 88

comp_83 IEEE computer, Vol. 16, Number 2, February 1983: Data Security in Computer Networks;

Czaa_82 Franz R. Czaak: Konzepte eines lokalen Netzwerks; Kommunikationstechnologien, Neue Medien in Bildungswesen, Wirtschaft und Verwaltung, Helmut Schauer, Michael J. Tauber (eds.), Schriftenreihe der österreichischen Computer Gesellschaft Band 17, R. Oldenbourg Wien München 1982, Seite 341 bis 359

Date_81 Neue Medien und Datenschutz; Grundsätze für den Datenschutz bei den Neuen Medien (insbesondere bei Bildschirmtext und Kabelfernsehen) Beschluß der 7. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Berlin am 11. Dezember 1980; Datenschutz und Datensicherung, 3/1981, Seite 200 bis 201

DaZi_83 John D. Day, Hubert Zimmermann: The OSI Reference Model; Proceedings of the IEEE Vol. 71, Nu. 12, December 1983, Seite 1334 bis 1340

Denn_82 Dorothy Elizabeth Robling Denning: Cryptography and Data

Security; Addison-Wesley Publishing Company, Reading, Mass., 1982

DeSc_83 Dorothy E. Denning, Jan Schlörer: Inference Controls for Statistical Databases; IEEE Computer Vol. 16, Nu. 7, July 1983, Seite 69 bis 82

Dorr_83 Irwin Dorros: Telephone nets go digital; IEEE spectrum Vol. 20, Nu. 4, April 1983, Seite 48 bis 53

Elek_82 Elektronik Sonderheft Nr. 50, "Daten-Kommunikation"; 8. Teil Einführung in die Datenfernverarbeitung, Lokale Netzwerke - die Basis für integrierte Informations-Systeme; Franzis-Verlag GmbH, Karlstr. 37 - 41, 8000 München 2, ISSN 0170-0898, 1982, Seite 69 bis 77

Farb_83 Farbfernseher, Farbcomputer, Btx und Videorecorder >>Contrast<<-Programm; Markt&Technik Nr. 19 vom 13. Mai 1983 Seite 61

Flin_83 David C. Flint: The Data Ring Main; An Introduction to Local Area Networks; Computing Sciences Series, John Wiley & Sons, New York, 1983

FroI_82 Ingrid Fromm: Local Area Networks - Hochgeschwindigkeitsnetze für die Bürokommunikation; telcom report Band 5, Heft 2, 1982, Seite 66 bis 71

Gars_82 Hansjürgen Garstka: Anforderungen des Datenschutzes an Gesetze auf dem Gebiet der neuen Medien; Datenschutz und Datensicherung, 3/1982, Seite 153 bis 156

Gerk_82 Peter R. Gerke: Neue Kommunikationsnetze - Prinzipien, Einrichtungen, Systeme; Springer-Verlag, Berlin Heidelberg New York, 1982

Giff_82 David K. Gifford: Cryptographic Sealing for Information Secrecy and Authentication; Paper of the Eighth Symposium on Operating Systems Principles, 14-16 December 1981, Pacific Grove, California, CACM Vol. 25, No. 4, April 1982, Seite 274 bis 286

GrHS_83 A. Grant, D. Hutchison, W. D. Shepherd: A Gateway for Linking Local Area Networks and X.25 Networks; SIGCOMM '83 Symposium Communications Architectures & Protocols, University of Texas at Austin, March 1983, Computer Communication Review, Vol. 13, Nu. 2, Seite 234 bis 239

Günt_82 Fritz-Rudolf Güntsch: Informationstechnik und Gesellschaft; IBM Nachrichten Heft 259, April 1982, Nachgedruckt in: Technik und Gesellschaft: Innovation durch Informa-

tion, IBM, Dezember 1982, Seite 51 bis 58

Gute_83 Fred Guterl: Next-Generation Impacts, Technology watchers discuss industrial and office automation, knowledge-based systems, computer privacy, and education; IEEE spectrum Vol. 20, No. 11, November 1983, Seite 111 bis 117

Inge_83 Ingemar Ingemarsson: A Comparision Between Public-key and Conventional Encryption Methods; Proceedings of the First Security Conference, Stockholm, Sweden, 16-19 May, 1983, Viiveke FAK (ed.), North-Holland Publishing Company Amsterdam, Seite 229 bis 232

Jabu_83 W. Jaburek: Bildschirmtext und Mupid - ein computergestütztes Konferenzsystem; IIG, Universität Graz, Bericht B33, April 1983

JaMM_83 W. Jaburek, H. A. Maurer, H. Mülner: MUPID-Basic: The Language; IIG, Universität Graz, Bericht B36, April 1983

Jard_83 Richard desJardins: ISO Open Systems Interconnection Standardization Status Report; SIGCOMM '83 Symposium Communications Architectures & Protocols, University of Texas at Austin, March 1983, Computer Communication Review, Vol. 13, Nu. 2, Seite 4, 5

KaHa_81 W. Kaiser, H. Th. Hagmeyer: Elektronische Textkommunikation; Informatik-Spektrum Band 4, Heft 4, Okt. 1981, Seite 201 bis 212

Kais_82 Wolfgang Kaiser: Interaktive Breitbandkommunikation; Nutzungsformen und Technik von Systemen mit Rückkanälen; Telecommunications Band 8, Springer-Verlag Heidelberg, 1982

KOHT_83 Hiroyuki Kasai, Kenji Ohue, Takashi Hoshino, Shigeru Tsuyuki: 800 Mbit/s Digital Transmission System Over Coaxial Cable; IEEE Transactions on Communications, Vol. COM-31, No. 2, February 1983, Seite 302 bis 306

Konh_81 Alan G. Konheim: Cryptography: A Primer; John Wiley & Sons, New York, 1981

Kunt_83 Walter Kuntz: Schutz der Software und Hardware von Microrechnern gegen Mißbrauch; Handbuch der modernen Datenverarbeitung (HMD), Forkel-Verlag, Heft 109, Januar 1983, 20. Jahrgang, ISSN 0723-5208, Seite 129 bis 133

Kunz_83 H. Kunze: Neue Text- und Datenkommunikationsdienste der DBP auf der Basis neuer Technologien; Mikroelektronik Information Gesellschaft, H. Niemann, D. Seitzer, H. W.

Schüßler (Hrsg.), Springer-Verlag Heidelberg, April 1983, Seite 73 bis 96

Laks_83 S. Lakshmivarahan: Algorithms for Public Key Cryptosystems: Theory and Application; Advances in Computers Vol. 22, Marshall C. Yovits (ed.), Academic Press, New York, 1983, Seite 45 bis 108

Leis_82 Ernst L. Leiss: Principles of Data Security; Plenum Press, New York, London, 1982

LeMa_83 R. E. Lennon, S. M. Matyas: Cryptographic Key Verification; Proceedings IEEE INFOCOM 83, San Diego, California, April 18-21, 1983, Seite 265 bis 269

Leuz_82 Ruth Leuze: Datenschutz für unsere Bürger; 3. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz 1982; Herausgegeben von der Landesbeauftragten für den Datenschutz Dr. Ruth Leuze, Marienstraße 12, 7000 Stuttgart

Liu_78 Ming T. Liu: Distributed Loop Computer Networks; Advances in Computers Vol. 17, Marshall C. Yovits (ed.), Academic Press, New York, 1978, Seite 163 bis 221

LTCL_81 Ming T. Liu, Duen-Ping Tsay, Chuen-Pu Chou, Chung-Ming Li: Design of the Distributed Double-Loop Computer Network (DDLCN); Journal of Digital Systems, Vol. V, Nu. 1/2, Spring/Summer, 1981, Seite 3 bis 37

MaPo_82 H. A. Maurer, R. Posch: Der MUPID: Ein Beitrag österreichs zur Entwicklung von Bildschirmtext; IIG, Universität Graz, Bericht B17, Juni 1982

MaSe_83 H. A. Maurer, I. Sebestyen: Inhouse Versus Public Videotex Systems; Computer Networks, The International Journal of Distributed Informatique, North-Holland, Vol. 7, Nu. 5, October 1983, Seite 329 bis 342

MauP_82 H. A. Maurer, R. Posch: How to further improve interactive videotex; IIG, Universität Graz, Bericht F88, May 1982

Mau1_83 H. Maurer: Bildschirmtext - Netzwerk der Zukunft; Überblicke Informationsverarbeitung 1983, Seite 143 bis 177

Mau2_83 H. Maurer: Lokale Intelligenz zur Unterstützung von Bildschirmtext; Nachrichten für Dokumentation, herausgegeben von der Deutschen Gesellschaft für Dokumentation e. V., K. G. Saur München, Band 34, Nr. 1, Seite 8 bis 13

Moll_83 Mart L. Molle: Asynchronous Multiple Access Tree Algorithms; SIGCOMM '83 Symposium Communication Architectures & Protocols, University of Texas at Austin, March 1983, Computer Communication Review Vol. 13, Nu. 2, Seite 214 bis 218

Norm_83 Adrian R. D. Norman: Computer Insecurity; Chapman and Hall Ltd, 11 New Fetter Lane, London EC4P 4EE, 1983

OSI_83 ISO: Basic reference model for Open Systems Interconnection; ISO 7498, 1983

Pete_81 Ulrich v. Petersdorff: Das Kompetenzproblem und die datenschutzrechtliche Verantwortlichkeit bei Bildschirmtext; Datenschutz und Datensicherung, 2/1981, Seite 83 bis 86

PfHä_82 Andreas Pfitzmann, Hermann Härtig: Grenzwerte der Zuverlässigkeit von Parallel-Serien-Systemen; Fehlertolerierende Rechnersysteme, GI-Fachtagung München, März 1982, Informatik-Fachberichte Band 54, Springer Verlag, Berlin, Heidelberg, New York, 1982, Seite 1 bis 16

Pfit_82 Andreas Pfitzmann: Konfigurierung und Modellierung von Mehrmikrorechnern aus um Zuverlässigkeitsanforderungen erweiterten ADA-Programmen; Interner Bericht Nr. 8/82, Institut für Informatik IV, Fakultät für Informatik, Universität Karlsruhe, Februar 1982

Pfit_83 Andreas Pfitzmann: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien; GI '83 13. Jahrestagung der Gesellschaft für Informatik 3. bis 7. Oktober 1983, Universität Hamburg, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, Seite 411 bis 418

Pfit_84 Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability;
1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6-8, 1984, Zurich, Switzerland, Swiss Federal Institut of Technology

Pill_83 Ernst Piller: Mikroprozessorgesteuerte Speicherkarte im Scheckkarten-Format; German Chapter of the ACM Berichte 17, Microcomputing II, W. Remmele, H. Schecher (Hrsg.), Tagung III/1983 des German Chapter of the ACM vom 25. bis 27.10.83 in München, B. G. Teubner Stuttgart 1983, Seite

81 bis 95

PoPo_83 K. C. Posch, R. Posch: Two extensions of an intelligent videotex-decoder; IIG, Universität Graz, Bericht F108, January 1983

Rein_81 Günter Reiner: Datenschutz und Bildschirmtext; Datenschutz und Datensicherung, 2/1981, Seite 87 bis 90

ReLi_76 Cecil C. Reames, Ming T. Liu: Design and Simulation of the Distributed Loop Computer Network (DLCN); The 3rd Annual Symposium on Computer Architecture, January 19-21, 1976, Computer Architecture News Vol. 4, Nu. 4, Seite 124 bis 129

Riha_81 Karl Rihaczek: Datenschutz und Kommunikationssysteme; DuD-Fachbeiträge 1, Friedr. Vieweg & Sohn, Braunschweig, Wiesbaden, 1981

Riha_83 Karl Rihaczek: OSIS - Open Shops for Information Services; DuD Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Friedr. Vieweg & Sohn, Braunschweig, Heft 2, April 1983, Seite 116 bis 125

RosK_82 Karl Heinz Rosenbrock: Mögliche Integration von Fernmeldediensten im digitalen Fernsprechnetz der Deutschen Bundespost - ISDN; Zeitschrift für das Post- und Fernmeldewesen Heft 9 vom 27. September 1982

RSA_78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; CACM Vol. 21, No. 2, February 1978, Seite 120 bis 126

RuRa_83 John Rushby, Brian Randell: A Distributed Secure System; IEEE computer Vol. 16, Nu. 7, July 1983, Seite 55 bis 67

SaPC_83 J. H. Saltzer, K. T. Pogran, D. D. Clark: Why a Ring? Computer Networks, The International Journal of Distributed Informatique, North-Holland, Vol. 7, Nu. 4, August 1983, Seite 223 bis 231

SBit_83 Softwareschutz in Einchip-Mikrocomputern; Sicherungs-Bit im EPROM; Markt&Technik Nr. 42 vom 21. Oktober 1983, Seite 60 und 62

Schd_83 Norman F. Schneidewind: Interconnecting Local Networks to Long-Distance Networks; IEEE Computer Vol. 16, Nu. 9, September 1983, Seite 15 bis 24

Schl_82 Jan Schlörer: Outputkontrollen zur Sicherung statistischer Datenbanken; Informatik-Spektrum Band 5, Heft 4, Dezember 1982, Seite 224 bis 236

Sham_83 Adi Shamir: On the Generation of Cryptographically Strong Pseudorandom Sequences; acm Transactions on Computer Systems, Vol. 1, Nu. 1, February 1983, Seite 38 bis 44

smar_82 Testing a highly secure and portable data bank; Scientific American November 1982, Seite F26

Span_82 Otto Spaniol: Konzepte und Bewertungsmethoden für lokale Rechnernetze; Informatik-Spektrum Band 5, Heft 3, September 1982, Seite 152 bis 170

Su_83 Zaw-Sing Su: Identification in Computer Networks; acm SIGCOMM, Computer Communication Review Vol. 13, No. 4, October 1983, Proceedings Eigth Data Communications Symposium, Seite 51 bis 55

TanA_81 Andrew S. Tanenbaum: Computer Networks; Prentice-Hall, Englewood Cliffs, N. J., 1981

Tane_81 Andrew S. Tanenbaum: Network Protocols; acm computing surveys Vol. 13, Nu. 4, December 1981, Seite 453 bis 489

Tiet_82 Walter Tietz: Bürokommunikation - Neue Dienste; ntz Band 35, Heft 7, 1982, Seite 443 bis 447

Toba_80 Fouada A. Tobagi: Multiaccess Protocols in Packet Communication Systems; IEEE Transactions on Communications, Vol. COM-28, No. 4, April 1980, Seite 468 bis 488

tuto_81 Donald W. Davies: tutorial: The Security of Data in Networks; IEEE Catalog No. EH0183-4, 1981

Verk_83 Verkabelung schreitet voran - Einzelnetze zu einem bundesweiten Netz verbinden; Markt&Technik Nr.17 vom 29. April 1983, Seite 8

VoKe_83 Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; acm computing surveys Vol. 15, No. 2, June 1983, Seite 135 bis 171

Weit_80 Cay Weitzman: Distributed Micro/Minicomputer Systems; Prentice Hall, Englewood Cliffs, N. J., 1980;

WeSc_83 Elisabeth Wehrle, Jan Schlörer: The Partner Algorithm for Protecting Statistical Databases, extended abstract; GI '83 13. Jahrestagung der Gesellschaft für Informatik 3. bis 7. Oktober 1983, Universität Hamburg, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, Seite 134 bis 145

WLWT_79 Jacob J. Wolf, Ming T. Liu, Bruce W. Weide, D. P. Tsay: Design of a Distributed Fault-Tolerant Loop Network; FTCS-9, The Ninth Annual International Symposium on

Fault-Tolerant Computing, Madison, Wisconsin, June 20-22, 1979, Seite 17 bis 24

Wolf_79 Jacob John Wolf: Design and Analysis of the Distributed Double-Loop Computer Network (DDLCN); The Ohio State University PhD-Thesis, 1979

WoWL_79 Jacob J. Wolf, Bruce W. Weide, Ming T. Liu: Analysis and Simulation of the Distributed Double-Loop Computer Network (DDLCN); Proc. 1979 Computer Networking 3rd Symposium, Gaithersburg, Md., December 1979, Seite 82 bis 89

Stichwortverzeichnis