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


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.

Schlagwörter
Neue Medien, Datenschutz, Bildschirtext, 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
1 Motivation 6
2 Vor- und Nachteile von Vermittlungs- und Verteilnetzen 7
3 Ein den Datenschutz-Bedürfnissen des Teilnehmers angepasstes Vermittlungs-/Verteilnetz 9
  3.1 Voraussetzungen und Randbedingungen 10
  3.2 Fünf Lösungsalternativen 12
    3.2.1 Vermittlung sehr großer Informationsmengen 13
    3.2.2 Verteilnetz mit Rückkanal 14
      3.2.2.1 Hinweise zur Realisierung 14
      3.2.2.2 Das Kommunikationsprotokoll 19
    3.2.3 Vermittlungs-/Verteilnetz 21
      3.2.3.1 Adressverwaltung 23
      3.2.3.2 Das Kommunikationsprotokoll im fehlerfreien arbeitenden Netz 24
    3.2.3.3 Abrechnung und Zulassung von Teilnehmerstationen 28
      3.2.3.3.1 Anonyme Nummernkonten 29
      3.2.3.3.2 Nicht manipulierbare Zähler 36
    3.2.3.4 Erweiterungen des Kommunikationspro-
tokolls zur Tolerierung von Fehlern 41
    3.2.3.5 Erweiterungen des Kommunikationspro-
tokolls zur Tolerierung von manchen Manipulationen am Netz 42
    3.2.3.6 Realisierungsaufwand 45
    3.2.3.7 Dimensionierung und spezielle Protokolle zur Vergabe der Sendeberechtigung bei kontinuierlichen Sendewünschen 59
    3.2.3.8 Mögliche Betreiber des Verteilnetzes mit Rückkanal 62
      3.2.3.9 Abschließende Bewertung 63
    3.2.4 Vermittlungs-/Vermittlungsnetz 64
    3.2.5 Verteil-/Verteilnetz 66
3.3 Vermeidung zeitlicher Muster 67
3.4 Vergleich mit der Lösungsalternative von David L. Chaum 68
4 Anschluß des Vermittlungs-/Verteilnetzes an andere Netze 70
5 Ausblick 73
Danksagung 74
Literatur 75
Stichwortverzeichnis 83
<table>
<thead>
<tr>
<th>Bild</th>
<th>Beschreibung</th>
<th>Seitenzahl</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bild 1</td>
<td>Vermittlungsnetz</td>
<td>8</td>
</tr>
<tr>
<td>Bild 2</td>
<td>Verteilnetz ohne Rückkanal</td>
<td>9</td>
</tr>
<tr>
<td>Bild 3</td>
<td>Verteilnetz mit Rückkanal</td>
<td>14</td>
</tr>
<tr>
<td>Bild 4</td>
<td>Kommunikation im Verteilnetz mit Rückkanal</td>
<td>20</td>
</tr>
<tr>
<td>Bild 5</td>
<td>Vermittlungs-/Verteilnetz</td>
<td>22</td>
</tr>
<tr>
<td>Bild 6</td>
<td>Kommunikation im Vermittlungs-/Verteilnetz</td>
<td>26</td>
</tr>
<tr>
<td>Bild 7</td>
<td>Kommunikation im Vermittlungs-/Verteilnetz mit anony-</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>men Nummernkonten</td>
<td></td>
</tr>
<tr>
<td>Bild 8</td>
<td>Aufteilung der Teilnehmerstation</td>
<td>37</td>
</tr>
<tr>
<td>Bild 9</td>
<td>Kommunikation im Vermittlungs-/Verteilnetz mit nicht</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>manipulierbaren Zähleln</td>
<td></td>
</tr>
<tr>
<td>Bild 10</td>
<td>Verteilung der Teilnehmerstationen und deren stern-</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>und ringförmige Verbindung</td>
<td></td>
</tr>
<tr>
<td>Bild 11</td>
<td>RINGL und STENL bei quadratisch wachsender ANZAHL</td>
<td>55</td>
</tr>
<tr>
<td>Bild 12</td>
<td>USTERN/MAXURING und USTERN/MINURING bei quadratisch</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>wachsender ANZAHL</td>
<td></td>
</tr>
<tr>
<td>Bild 13</td>
<td>KVBSTERN/KVBMAXURING und KVTSTERN/KVTMINURING bei quadratisch wachsender ANZAHL</td>
<td>57</td>
</tr>
<tr>
<td>Bild 14</td>
<td>Vermittlungs-/Verteilungsnetz</td>
<td>65</td>
</tr>
<tr>
<td>Bild 15</td>
<td>Verteil-/Verteilnetz</td>
<td>67</td>
</tr>
<tr>
<td>Bild 16</td>
<td>Aufwandsvergleich</td>
<td>69</td>
</tr>
<tr>
<td>Bild 17</td>
<td>Netzübergang bei beliebigen Bitfolgen</td>
<td>71</td>
</tr>
<tr>
<td>Bild 18</td>
<td>Netzübergang bei eingeschränkten Bitfolgen</td>
<td>73</td>
</tr>
</tbody>
</table>
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


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

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 zurechtzulegen, daß die Verwaltung angewohnte Vorgehensweisen fortführen 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 [Pets_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 Speicherung 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, Kabeltextabfruf [KaHa_81] und alle Dienste über das geplante BGFON (breitbandiges integriertes Glasfaser-Endmel-degertechnetz) [Brau_83] haben aus der Sicht des Teilnehmers folgende Vorteile (+) bzw. Nachteile (-):

+ Informationen können schnell aus beliebig großen Informations- angeboten (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.


- 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 (KoHa_81):

- Bei gegebener Auswahlzeit ist die Informationsmenge, aus der ausgewählt werden kann, durch die Bandbreite des Verteilnetzes und die lokalen verfügbare Speicherkapazität [PoPo_83] begrenzt.

- Das Verhalten der Systeme ist 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 von 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].


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.


R5 Kryptosysteme mit öffentlichen Schlüsseln (public key cryptosystems) sind verfügbar [Bauh.82, Beth.82, comp.83, Denn.82, Laks.83, Leis.82, tuto.81]. In ihnen gehört zu jedem öffentlichen Schlüssel ü ein privater Schlüssel p. Aus ü kann
p nicht mit vernünftigem Aufwand hergeleitet werden. Mit 8
verschlüsselte Nachrichten können nur mit Hilfe vor p
entschlüsselt werden (und in manchen Kryptosystemen mit
öffentlichen Schlüsseln auch umgekehrt, z. B. in RSA_781).
Für Nachrichten N geeigneter Länge gilt:
\[ p(8(N)) = N, \text{ d. h. die mit dem öffentlichen Schlüssel 8}
verschlüsselten Nachrichten können mit dem
privaten Schlüssel p entschlüsselt werden. Diese
Eigenschaft wird in diesem Papier benutzt.}
\[ 8(p(N)) = N, \text{ 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].

Es wird angenommen, daß es mindestens ein sicheres
(d. h. durch kein kryptanalytisches Verfahren in vernünftiger Zeit
entschlüsselbares) und zugleich preiswirt 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 Verteilnetzwerken mit
Rückkanal (Abschnitt 3.2.2 und 3.2.3) beruht jedoch nicht auf
der Sicherheit des Kryptosystems mit öffentlichen Schlüsseln
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.

Rö Es gibt physisch-physikalische Zufallsgeneratoren (man verstärkt 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. 
at respicere unum. 
Lat. Sprichwort

In den folgenden Unterabschnitten werden 5 Lösungsalternativen beschrieben und bewertet.


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,

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 Vermittlungs system dadurch zu erweitern, 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 Vermittlungsstelle nicht kontrollierbar die Artikel bzw. die Zeitung aus, die ihn interessieren. Allerdings entscheidet er bei solchem Vorgehen zumindest in den nächsten Jahren, da hohe Übertragungskosten, vor allem aber hohe Übertragungszeiten entstünden.

3.2.2 Verteilnetz mit Rückkanal

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

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

![Diagramm von Verteilnetz mit Rückkanal](image_url)

**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 Verabredung der Sendeberechtigung und geeignete Leitungstoptologie 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 Leitungstoptologie gewählt wird.

1) Die Verabredung 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 benutztten Slot sofort wieder benutzen dürfen oder schon die adressierte Station dem empfangenen Slot freigibt, und Register-insertion-Technik (delay insertion loop, DLNC = Distributed Loop Computer Network) [FroI_81, Gerh_82, Liu_78, Moll_83, Reli_76, Span_82, TanA_81 Seite 253ff, 272, 288ff, 312ff, Tane_81 Seite 460, 467, 468, TogA_80, Wett_80 Seite 61ff].

Dürfen bei Empty-slot-Technik Stationen benutztte 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 der Stationen im Ring und die Reihenfolge der Stationen im Ring bekannt ist. Jede Station S im Ring kann die Absender der Nachrichtenteile) in einem bestimmten slot s identifizieren, wenn alle anderen n-1 Stationen nacheinander benutzt. 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 Wahrcheinlichkeit 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 Wahrcheinlichkeit mit (carrier sense), um nach dem Ende der Nachricht sofort ihre Nachricht zu senden. Es gilt dann
\[ P = \text{Reaktionszeit}_\text{von Station}_2 + \]
\[ 2 \times L / \text{Signalgeschwindigkeit}_\text{im Medium} \]
also
\[ L = (P - \text{Reaktionszeit}_\text{von Station}_2) \times \]
\[ \text{Signalgeschwindigkeit}_\text{im Medium} / 2 \]

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


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. Verteilernetzkrone 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 ([Tanen_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 Leitungstoptologie (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 dem Bus-Anschluss 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 Signalf orm 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 Signalf orm der Antworten beobachtet.

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

Hieraus folgt, daß als Leitungstoptologie ein Ring (Zweig von Punkt-zu-Punkt Kabeln zwischen aufeinanderfolgenden Teilnehmerstationen (TANAG.51 Seite 301)) mit Verzögerer 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 Datensicherheiten bietet:

+ Es gibt keine 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 Signalf orm 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 Station den empfangenen slot freigibt, oder Delay Insertion Loop als Sender zu identifizieren, muß der Ring direkt vor und hinter ihr abgezweigt sowie das Abgeführte 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 Trep penhaus 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.

Die vielen aktiven Sender im Ring bilden ein Serien-System bezüglich ihrer Verfügbarkeit. Dies muß und kann innerhalb gewisser Grenzen (vgl. [(PFHS_82) oder (Pfl_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 sandet 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 DDLON [(HLWT_79, Wolf_79, WML_79, LTDC_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 Ringes beobachtet werden können. Solange nur einzelne Leitungen eines Leitungsabschnittes und keine Teilnehmerstation ausgefallen sind, sollte ein Ring gegebenenfalls rekonfiguriert werden und, um den Datenschutz zu erhalten, nur er zum Informationsausstausch 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 Verteilnetzentrale neu eine Zufallszahl F_z, einen öffentlichen Schlüssel F_e und einen zu F_e gehörigen privaten Schlüssel F_p. F_z und F_e bilden zusammen einen anonymisierten Absender.

Über den Rückkanal überträgt die Teilnehmerstation (mit dem öffentlichen Schlüssel e der Verteilnetzentrale verschlüsselt) F_z, F_e und ihre Frage F_f (Bild 4). F_z und die mit F_e verschlüsselte Antwort F_a auf F_f wird von der Verteilnetzentrale an alle Teilnehmerstationen verteilt. Die Teilnehmerstation erkennt ihre Zufallszahl F_z und entschlüsselt mit dem zugehörigen privaten Schlüssel F_p die gewünschte Information.
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 Glasfaseretz 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 Steuerung.
Hüten wir uns vor Menschen, die alles allein machen wollen.

Edward Heath

Die dritte Lösungsalternative besteht darin, daß die Post ein Vermittlungsnetz betreibt, dessen Endnoten private, lokale Verteilnetze mit Rückkanal sind (Bild 5). Verteilnetzentralen 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 genügen 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 Adressevernichtung

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


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. RS 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 Teilnehmerverzeichn-

3.2.3 Das Kommunikationsprotokoll im fehlerfreien 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 einseitig 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 Vermittlungsstelle möglichst wenig Informationen über A und/oder B gewinnen können) könnte dann folgendermaßen ablaufen (Bild 6):

Teilnehmerstation A kennt den öffentlichen Schlüssel B der Vermittlungsstelle, die logische Adresse zu ihrer Verteilnetzentrale 2A und eine Adresse b von Teilnehmerstation B samt dem zugehörigen öffentlichen Schlüssel b_B.

A hat in Zeiten, in denen es für sie nichts zu tun gab, auf
Vorrat aus einer Zufallszahl $p_z$ eine private Adresse $F_{pa} = 8(Pa, F_z)$ errechnet sowie einen öffentlichen Schlüssel $F_8$ und einen zu $F_8$ gehörigen privaten Schlüssel $F_p$ erzeugt. Die Erzeugung der privaten Adresse $F_{pa}$ und des Schlüsselpaares $F_8, F_p$ 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 $F_8$ bilden zusammen einen anonymisierten Absender.

$A$ sendet die Adresse $b$ von $B$ sowie $F_{pa}, F_8$ und ihre Frage $F_f$ mit dem öffentlichen Schlüssel $b_8$ von $B$ verschlüsselt an ihre Verteilnetzentrale $ZA$.

$ZA$ 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 Verteilnetzentrale $ZB$ von $B$.

$ZB$ verteilt die Nachricht.

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

$b_p(b_8(F_{pa}, F_8, F_f)) = F_{pa}, F_8, F_f$.

$B$ sendet $F_{pa}$ und ihre mit $F_8$ verschlüsselte Antwort $F_a$ an ihre Verteilnetzentrale $ZB$.

$ZB$ 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 Verteilnetzentrale $ZA$ von $A$.

$ZA$ verteilt die Nachricht.

$A$ erkennt ihre private Adresse $F_{pa}$ und entschlüsselt die Antwort mit ihrem für $F$ gewählten privaten Schlüssel $F_p$. 
\( \hat{o} \) öffentlicher Schlüssel der Vermittlungszentrale
p privater Schlüssel der Vermittlungszentrale
\( \text{pr} \) Projektion auf erste Adreß-Komponente
\( \text{pr}(p(b)) = zb \) Adresse von ZB
\( \text{pr}(p(F_{pa})) = za \) Adresse von ZA

\( b, b_\hat{o}(F_{pa}, F_\hat{o}, F_f) \)
\( F_{pa}, F_\hat{o}(F_a) \)
\( b, b_\hat{o}(F_{pa}, F_\hat{o}, F_f) \)
\( F_{pa}, F_\hat{o}(F_a) \)

\( za \) logische Adresse der Vermittlungszentrale ZA von A

\( b \)
\( b_\hat{o} \) öffentlicher Schlüssel zu b
\( b_p \) privater Schlüssel zu b

\( F_{pa} \)
\( F_\hat{o} \) öffentlicher Schlüssel für F
\( F_f \) privater Schlüssel für F
\( F_a \) Antwort

\( F_z \) Zufallszahl für F
\( F_{pa} = \hat{o}(za, F_z) \) für F gebildete private Adresse von A
(anonymisierter Absender)

\textbf{Bild 6: Kommunikation im Vermittlungs-/Verteilnetz}
Wann 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 6,2 eine private Adresse G_p₂ = 4(zb,6,2) errechnet sowie einen öffentlichen Schlüssel G₈ und einen zu G₈ gehörigen privaten Schlüssel G_p erzeugt. Stattdessen F_p₂F₈(F_p₈) sendet B F_p₂F₈(G_p₂,G₈,F_p₈) an A. Dies bietet zwei Vorteile:
1) Ein einheitliches Nachrichtenformat wird möglich.
2) A kann den anonymisierten Absender G_p₂,G₈ für die nächste Kommunikation mit B benutzen.

Möchte man wegen neugieriger und gut informierter Nachbarn die Übertragung einer öffentlichen Adresse b von B im Klartext vermeiden, so kann man obiges Protokoll leicht erweitern:
Die Teilnehmerstation A verschliesselt b mit G₈ und überträgt als Adresse statt b G₈(b).
Die Vermittlungsstelle entschlüsselt G₈(b) einmal zusätzlich mit p und ersetzt G₈(b) innerhalb der Nachricht durch b.

Ohne diese zusätzliche Verschlüsselung könnten gut informierte Nachbarn das Teilnehmerverzeichnis (Verzeichnis der öffentlichen Adressen, vgl. Abschnitt 3.2.3.1) nach b durchsuchen und Vermutungen anstellen, was 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 Verteilernetzstelle und einem Pseudonym, vgl. Abschnitt 3.2.3.1), jedoch kann B durch von ihm explizit gegebene Information im Verzeichnis der öffentlichen Adressen (Vermittlung, 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 Vermittlungsstellen ist noch zu entscheiden,
1) ob b (und auf dem Rückweg F_p₂) in jeder Vermittlungsstelle mit p verschlüsselt wird, dann kann man die Nachricht unverändert durch das gesamte Vermittlungs-/Verteilnetz übertragen, hat aber in jeder durchlaufenen Vermittlungsstelle den Aufwand der Verschlüsselung oder
2) ob b (und auf dem Rückweg F_p₂) in der ersten durchlaufenen Vermittlungsstelle mit p verschlüsselt, dann in entschlüss-
selter Form zwischen den Vermittlungszentralen übertragen und in der letzten durchlaufenen Vermittlungszentrale wieder mit 8 verschlüsselt wird oder

3) ob b (und auf dem Rückweg F_p_a) 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 8 (logische Adressen ihrer Verteilernetz- zentrale und alle zugehörigen von ihr gewählten Pseudonymen) merken müßte.


3.2.3.3 Abrechnung und Zulässigkeit 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:


Dieser Teil der Abrechnung könnte vermieden werden, wenn die

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 Förwe 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.

7.2.3.1 Anonyme Nummernkonten

Bez 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, beobacht man selbst (oder eine Person, der man vertraut) eine Geschäftsstelle 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. Δ. Der entsprechende private Schlüssel n.p wird als Passwort
für das anonyme Nummernkonto verwendet.
Hat das verwendete Kryptosystem mit öffentlichen Schlüsseln nicht
die Eigenschaft \( \text{ord}(N) = N \), so nennt man der Geschäftsstelle
einen privaten Schlüssel und verwendet den entsprechenden
öffentlichen Schlüssel, der nun natürlich gehärtet 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 zahlte einen Betrag auf das anonyme Nummernkonto ein und
erhält dafür eine Quittung.
Will man eine gebührenpflichtige Dienstleistung über das
Vermittlungs-/Verteilernetz erhalten, benutzt man das Kommunikati-
onsprotokoll 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_0, P_p
und Q_0, Q_p und einen elektronischen Scheck
F_e = n.n_p(Datum,Zeit,Nr,Betrag,P_0). Mit dem elektronischen
Scheck erlaubt A eine Bezahlung von mit P_p oder p
unterschriebenen Rechnungen bis zum Gesamtbetrag Betrag. Das
Schlüsselpaar P_0, P_p dient dazu, daβ B und nur B von C Geld
erhält, ohne daß C B kennt. Das Schlüsselpaar Q_0, Q_p dient
dazu, daß B und nur B unterschreiben kann, welchem anonymen
Nummernkonto die Gebühren für F_e gutgeschrieben werden.
Nebenbei wird Q_0, Q_p auch dazu benutzt, daß die Vermittlungs-
zentrale, ohne A zu kennen, A für andere Teilnehmerstationen
unlesbar mittelbar kann, wie hoch die Gebühren für F_e sind.
A überträgt b,b_0(F_p,a,F_s,F_e,F_p,Q_p),Q_c,c_c(F_e),Q_0, c
ist eine Adresse von c, c_c der entsprechende öffentliche
Schlüssel, die anderen Abkürzungen sind in Abschnitt 3.2.3.2.
definiert.

Die Vermittlungscentrale VZ entschlüsselt $b(c,c_s(F_e),Q_s)$ mit ihrem privaten Schlüssel $p$, berechnet die Übertragungskosten $G_k$ und eine Übertragungsgebührenrechnung Datum, Zeit, Nummer, $G_k$ und sendet $c,c_s(F_e),p(Datum, Zeit, Nummer, G_k)$ an C.

C entschlüsselt $c_s(F_e)$ mit $c_p$, sucht den zu $n$ gehörigen öffentlichen Schlüssel $n_s$ in seinem Verzeichnis und entschlüsselt $n,p(Datum, Zeit, Nummer, Betrag, P_s)$ mit $n_s$. C entschlüsselt $p(Datum, Zeit, Nummer, G_k)$ mit $a$.

C prüft Datum, Zeit und die (laufende) Nummer des elektronischen CHECKS und der Übertragungsgebührenrechnung. C bestimmt das Kostenlimit $K_l$ aus dem Minimum von Betrag und dem Wert $w$, der noch auf dem anonymen Nummernkonto ist: $K_l = \min(\text{Betrag}, w) - G_k$.

C subtrahiert $K_l$ und $G_k$ vom anonymen Nummernkonto: $w := w - K_l - G_k$. C sendet $b(k, c_s(F_e), c_p(k, c_s(F_e)))$ an die Vermittlungscentrale.

Die Vermittlungscentrale erkennt an $c_s(F_e)$, um welche Abfrage es sich handelt. Ist $K_l$ negativ, bricht die Vermittlungscentrale die Abfrage an dieser Stelle ab. Andernfalls berechnet sie eine Deckungszusage $F_d = p(k, b_s(F_{pa}, F_s, F_{f}, P_{pa}, Q_p))$ und sendet $b_s(F_{pa}, F_s, F_{f}, P_{pa}, Q_p), F_d$ an B.

B erkennt ihre Adresse $b$ und entschlüsselt mit dem zugehörigen privaten Schlüssel $b_p$ die Nachricht und mit dem öffentlichen Schlüssel $a$ der Vermittlungscentrale die Deckungszusage $F_d$. B prüft, ob die Kosten $K_l$ für $F_f$ inklusive der Übertragungsgebühren für die Antwort durch das Kostenlimit $K_l$ der Deckungszusage $F_d$ gedeckt sind. Gegebenenfalls berechnet B ihre Antwort $F_a$ und eine Rechnung $k,F_d,P_p(t,F_d)$. 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 $d_s$, sowie seine Kontonummer $d_n$ und eine Unterschrift $F_u = Q_s(k,F_d,P_p(k,F_d),d_s,d_n,F_u)$. B sendet $F_{pa},F_s,(F_a),b(k,F_f,P_p(k,F_d),d_s,d_n,F_u)$ an die Vermittlungszentrale.

Die Vermittlungszentrale entschlüsselt $b(k,F_f,P_p(k,F_d),d_s,d_n,F_u)$ mit $p$ und erkennt an $F_d$, um welche Abfrage es sich handelt. Danach entschlüsselt die Vermittlungszentrale $F_u$ mit $Q_s$, um die Unterschrift zu prüfen. Ist die Unterschrift nicht in Ordnung oder $K_l > k_l$, bricht die Vermittlungszentrale die Abfrage ab. Die Vermitt-
lungezentrale sendet $c, c, \delta(k, F_d, p(k, F_d), c, p(k_l, c, \delta(F_e)))$

an C.

C entschlüsselt $c, \delta(k, F_d, p(k, F_d), c, p(k_l, c, \delta(F_e)))$ mit $c, p$ und erkennt an $c, p(k_l, c, \delta(F_e))$, um welche Abfrage es sich handelt. C prüft die Unterschrift $p_k, p(d, F_d)$ mit P, B. C addiert $k_1$ zum Betrag des anonymen Nummernkontos n: $w := w + k_1 - k$.

Die Vermittlungszentrale berechnet den B gutzuschreibenden Betrag $g_b = k - Übertragungskosten der Antwort und eine
elektronische Gutschrift $g_b, d, p(Datum, Zeit, Nummer, gb, d, n)$. Die Vermittlungszentrale sendet

d, d, b(gb, d, n, p(Datum, Zeit, Nummer, gb, d, n)) an D.

D prüft die Unterschrift $p(Datum, Zeit, Nummer, gb, d, n)$ mit P und

schreibt gegebenenfalls gb dem anonymen Nummernkonto d, n gut.

Die Vermittlungszentrale berechnet die Kosten der Abfrage $F_k = k + \delta_k$, unterschreibt $F, k, c, \delta(F_e)$ und verschlüsselt Kosten und Unterschrift mit Q, B. Die Vermittlungszentrale sendet $F, p, a, F, b(F_a), b(F_e), p_k, p(F_k, c, \delta(F_e))$ an A.

A erkennt $F, p, a$ und entschlüsselt $F, \delta(F_a)$ mit $F, p$ und

$Q_b(F_k, p(F_k, c, \delta(F_e)))$ mit $Q, p$. A prüft die Unterschrift

$p(F_k, c, \delta(F_e))$ mit B.

Das Protokoll stellt sicher, daß YZ, C und D gemeinsame Betrags-
versuche von A und B erkennen und vereiteln können sowie A und B
gemeinsame Betragsversuche von YZ, C und D erkennen und vereiteln
können.

Wählt A Schlüsselpaare P, B, P, B, B, P, B, B, das 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 Spächer-
plaz zu sparen) eine Zeitlang (Beschwerdefrist) merken. Falls
gevünscht, kann die Vermittlungszentrale gb erst dann an B auf

ein Konto bei D überweisen, wenn die Beschwerdefrist ohne

Hat das verwendete Kryptosystem mit öffentlichen Schlüsseln nicht die Eigenschaft \( q(p(N)) = N \) (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 geheime Kommunikation zwischen der Vermittlungszentrale und A benötigt, so wie zur Leistung von Unterschriften der Zentrale.)
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 an 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 Geldautomaten auch als Geldgabeanlagen realisiert werden, an denen man anonyme Nummernkonten eröffnen und auf anonyme Nummernkonten einzahlen kann.

3.2.3.3.2 Nicht manipulierbare Zähler

Die zweite Lösung des Abrechnungsproblems ist eine Weiterentwicklung der Elektrizitätszähler.


Die beschriebene Zentralisierung 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 CENSICHRIT werden, damit die Vermittlungs zentrale 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 den Teilnehmer eine oder mehrere Schnittstellen zum Anschluß ungeprüfter und unregulierter 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 (TNUI = Trustworthy Network Interface Unit) zu realisieren [RuRa_83]. Die Zählinstanz stellt in der Begriffswelt von Karl Ribacek einen M-Teilnehmer dar [Ribac 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 $F_f$: $F_{fu} = F_p(F_{pa}, F_{u}, F_f, F_{kl})$. A sendet die Adresse $b$ von Teilnehmerstation B sowie $F_{pa}$, $F_{u}$ und ihre Frage $F_f$ (und eine zeitlich und betragsmäßig begrenzte Abbuchungsmächtigung $F_{kl}, F_{fu}$) mit dem öffentlichen Schlüssel $b^8$ von B verschlüsselt an ihre Verteilnetzentrale
ZA. Der Zähler von A erhöht sich dabei um die Übertragungsgebühren der Nachricht.

ZA vermittelt die Nachricht an die Vermitt lungszentrale.

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 Verteilnetzentrale ZB von B.

ZB vertäuf 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_k(F_{au},F_{f},F_{au}) an ihre Verteilnetzentrale ZB. Der Zähler von B prüft die Abbuchungsermächtigungen 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 Verteilnetzentrale ZA von A. Der Zähler der Vermittlungszentrale erniedrigt sich dabei um die Übertragungsgebühren.

ZA vermittelt die Nachricht.

A erkennt ihre private Adresse F_{pa} und entschlüsselt die Antwort F_a (inclusiv 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 Bedienen von A nicht verhindert oder manipulierbar sein. Dazu ist es sinnvoll, daß sich die Zahl-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 Zahl-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 einzusetzen zu können, muß jedem Teilnehmer ein Kreditrahmen vorgegeben und dessen Einhaltung vom nicht manipulierbaren Zähler überprüft werden. Sonst könnte ein Teilnehmer durch Eingabe hoher Kredite und anschließendes Umtauchen 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 den Lesen der Zähler stattfinden.
- Wenn der Teilnehmer den nicht manipulierbaren Zähler seiner Teilnehmerstation beträgt, kann er alle anderen Teilnehmer (inkl. Netzbetreiber und Dienstleistungsanbieter) beträgen.
- 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.
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 in einem realen System unvermeidlich auftreten den Fehler tolerieren. Insbesondere muß die Konsistenz der Zähler mit sehr hoher Wahrscheinlichkeit gewahrt oder eine nicht vermeidbare Inkonstanz 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 anonymierte Absender nur vom Empfänger entschlüsselbar ist.

2) Jede Verteilnetzentrale 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 Verteilnetzentrale um mehr als d Einheiten geändert, teilt die Teilnehmerstation der Verteilnetzentrale einen aktuellen In-Etwa-Zählerstand, der sich von genauen Zählerstand um weniger als d Einheiten unterscheidet, mit, so daß die Verteilnetzentrale den betreffenden Zähler nachführt.

a 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 in 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, Verteilernetzzentrale oder Vermittlungs-zentrale teilweise simulieren, können folgende Bedrohungen entstehen (vgl. Beth 823):

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 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. 85 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 verwendet 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 [VöK_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 Adresseinformation (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 Ablehnung durchführenden Vermittlungszentrale, da eine Kombination von B3 und B4 es ermöglichen würde, Zähler von z.
B. Informationsanbietern durch geschnittenpflichtige Informationen abfragen zu erübrigen, ohne daß ein anderer Zähler entsprechend erhöht würde.

Deshalb kann B3 durch Verwendung eines sicheren (Bemerkungen in Abschnitt 3.1 zu sicher gelten sinnvoller) 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 3.2.3.3.1) in die Teilnehmerstation überspielt. Die Teilnehmerstation ist so gebaut, daß sie s nicht proligiert und bei mechanischer Manipulation vernichtet. Dies Verfahren wird für OISIS - Open Shops for Information Services [Riga_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 [KuRa_83] vorgeschlagen und dürfte bei der smart card bereits angewandt werden [Pill_83, smar_82]. Entsprechend wird bei der Installation der Verteilnetzentralen 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.

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 überschneidet, 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 ihmender leichter identifiziert werden können (vgl. Abschnitt 3.2.2.1).

Der Realisierungsaufwand eines Verteilnetzes mit Rückkanal hängt von einer Unzahl Parameter ab: ortliche Verteilung der Teilnehmerstationen und Schwierigkeitsgrad der Leitungsverlegung, zu erwartendes/zu bewältigendes Nachrichten-Verkehrs aufkommen und seine zeitliche Verteilung, Antwortzeit- und Zuverlässigkeitserwartungen der Benutzer, Stand der Technik etc.


Die Kosten der untersten Ebene eines Ortsnetzes bestehen aus 2 Teilen:

1) Die eigenen 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 kostenoptimi-
ger mehrere leistungsschwächere Systeme parallel installieren könnte.


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 dem 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 [Kais82 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 übrigens, da

1. Über ihn mit einem erheblichen Anteil auch Verreführungsprogramme (Fernsehen, Radio etc.) übertragen werden, die unabhängig von der Anzahl der sie anfordernden Teilnehmerstationen nur höchstens einmal auf dem Ring übertragen werden müssen und

2. der Durchsatz eines Rings 1 bis 2 mal so groß sein kann wie die Kapazität seiner Leitungen [BuSc83 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.


Die Bilder 11, 12, 13 stellen die vom Programm QUASRAT errechneten Zahlenelementen 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;
(* YGL. Kn ab SEITE 4df f *)

VB = 7.2; (* VERLEGEBIL LIG *)
VT = 9362.5; (* VERLEGENSTEMER *)
HOEHE = 65;
BREITE = 70;
BILDER = 3;

VAR I, J, ANZAHL, TEILUNG, MAXTEILUNG : INTEGER;
MAXKAPAZITAETSTRING,
MINKAPAZITAETSTRING,
MAXURUNG,
MINURUNG,
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] := '1';
    FOR K := 1 TO BILDER DO
      FOR J := 0 TO BREITE DO
        MATRIX[0,J,K] := '-';
  END; (* INITIALISIERE *)

PROCEDURE EINTRAG(H:REAL;S:REAL;Z:CHAR;BILD:INTEGER);
BEGIN
  MATRIX[ROUNDS( H ) ,
         ROUND(  S ) ,
         BILD] := Z;
end;
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;
END; (* DRUCKE *)

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

BEGIN (* HAUPTPROGRAMM *)
  INITIALISIERE;
  READ(MAXTEILUNG);
  FOR TEILUNG := Z 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 MAXKAPAZITATRING := ANZAHL * MAXLAST
ELSE MAXKAPAZITATRING := 1;

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

MAXURING := MAXKAPAZITATRING*RINGL;
MINURING := MINKAPAZITATRING*RINGL;

WRITE(TEILUNG:4,ANZAHL:6,' ',STERNL:7:2);
WRITE(' ',RINGL:7:2);
WRITE(' ',STERNL/RINGL:7:4);
WRITE(' ',STERNL/MAXRING:7:4);
WRITE(' ',STERNL/MINRING:7:4);
WRITE(' ',STERNL*(YB+1)/(RINGL*YB+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 );
### TEILUNG ZAHL

<table>
<thead>
<tr>
<th>TEILUNG</th>
<th>STERNL.</th>
<th>RINGL.</th>
<th>STERNL.</th>
<th>RINGL.</th>
<th>USTERN.</th>
<th>USTEM.</th>
<th>KYB.</th>
<th>KYT.</th>
<th>KVBM.</th>
<th>KVMIN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>2.83</td>
<td>4.00</td>
<td>0.7071</td>
<td>0.7071</td>
<td>0.7071</td>
<td>0.7071</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>4.83</td>
<td>4.71</td>
<td>1.0258</td>
<td>1.0258</td>
<td>1.0258</td>
<td>1.0258</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>7.99</td>
<td>5.33</td>
<td>1.4977</td>
<td>0.9360</td>
<td>1.4977</td>
<td>1.3956</td>
<td>1.4977</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>11.71</td>
<td>6.35</td>
<td>1.8438</td>
<td>0.7375</td>
<td>1.8438</td>
<td>1.5587</td>
<td>1.8438</td>
<td>1.5587</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>36</td>
<td>16.36</td>
<td>7.20</td>
<td>2.2729</td>
<td>0.6314</td>
<td>2.2729</td>
<td>1.7257</td>
<td>2.2729</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>49</td>
<td>21.66</td>
<td>8.24</td>
<td>2.6303</td>
<td>0.5368</td>
<td>2.6303</td>
<td>1.7825</td>
<td>2.6303</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>64</td>
<td>27.83</td>
<td>9.14</td>
<td>3.0434</td>
<td>0.4755</td>
<td>3.0434</td>
<td>1.8350</td>
<td>3.0434</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>81</td>
<td>34.67</td>
<td>10.18</td>
<td>3.4068</td>
<td>0.4266</td>
<td>3.4068</td>
<td>1.8259</td>
<td>3.4068</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>100</td>
<td>42.35</td>
<td>11.11</td>
<td>3.8119</td>
<td>0.3812</td>
<td>3.8119</td>
<td>1.8173</td>
<td>3.8119</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>121</td>
<td>50.74</td>
<td>12.14</td>
<td>4.1799</td>
<td>0.3454</td>
<td>4.1799</td>
<td>1.7755</td>
<td>4.1799</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>144</td>
<td>59.95</td>
<td>13.09</td>
<td>4.5794</td>
<td>0.3180</td>
<td>4.5794</td>
<td>1.7385</td>
<td>4.5794</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>169</td>
<td>69.87</td>
<td>14.12</td>
<td>4.9490</td>
<td>0.2928</td>
<td>4.9490</td>
<td>1.6639</td>
<td>4.9486</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>196</td>
<td>80.60</td>
<td>15.08</td>
<td>5.3462</td>
<td>0.2728</td>
<td>5.3462</td>
<td>1.6358</td>
<td>5.3457</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>225</td>
<td>92.06</td>
<td>16.10</td>
<td>5.7176</td>
<td>0.2541</td>
<td>5.7141</td>
<td>1.5786</td>
<td>5.7169</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>256</td>
<td>104.32</td>
<td>17.07</td>
<td>6.1126</td>
<td>0.2388</td>
<td>6.1387</td>
<td>1.5323</td>
<td>6.1116</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>289</td>
<td>117.31</td>
<td>18.09</td>
<td>6.4854</td>
<td>0.2244</td>
<td>6.4854</td>
<td>1.4731</td>
<td>6.4842</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>324</td>
<td>131.10</td>
<td>19.06</td>
<td>6.8788</td>
<td>0.2123</td>
<td>6.8788</td>
<td>1.4244</td>
<td>6.8772</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>361</td>
<td>145.42</td>
<td>20.08</td>
<td>7.2527</td>
<td>0.2009</td>
<td>7.2691</td>
<td>1.3735</td>
<td>7.2507</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>400</td>
<td>160.94</td>
<td>21.05</td>
<td>7.6448</td>
<td>0.1911</td>
<td>7.6448</td>
<td>1.3281</td>
<td>7.6424</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>441</td>
<td>177.00</td>
<td>22.07</td>
<td>8.0195</td>
<td>0.1818</td>
<td>8.0195</td>
<td>1.2891</td>
<td>8.0166</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>484</td>
<td>193.84</td>
<td>23.05</td>
<td>8.4106</td>
<td>0.1738</td>
<td>8.4106</td>
<td>1.2404</td>
<td>8.4072</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>529</td>
<td>211.43</td>
<td>24.06</td>
<td>8.8761</td>
<td>0.1661</td>
<td>8.8761</td>
<td>1.1984</td>
<td>8.8782</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>576</td>
<td>229.81</td>
<td>25.04</td>
<td>9.1763</td>
<td>0.1593</td>
<td>9.1763</td>
<td>1.1612</td>
<td>9.1718</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>676</td>
<td>268.83</td>
<td>27.04</td>
<td>9.9420</td>
<td>0.1471</td>
<td>9.9420</td>
<td>1.0899</td>
<td>9.9360</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>729</td>
<td>289.48</td>
<td>28.05</td>
<td>10.3185</td>
<td>0.1413</td>
<td>1.4154</td>
<td>1.0563</td>
<td>10.3117</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>784</td>
<td>310.92</td>
<td>29.04</td>
<td>10.7072</td>
<td>0.1366</td>
<td>1.3658</td>
<td>1.0257</td>
<td>10.6999</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>841</td>
<td>333.10</td>
<td>30.05</td>
<td>11.0645</td>
<td>0.1318</td>
<td>1.3180</td>
<td>0.9955</td>
<td>11.0760</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>900</td>
<td>356.06</td>
<td>31.03</td>
<td>11.4731</td>
<td>0.1275</td>
<td>1.2748</td>
<td>0.9479</td>
<td>11.4435</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>941</td>
<td>379.77</td>
<td>32.05</td>
<td>11.8504</td>
<td>0.1233</td>
<td>1.2331</td>
<td>0.9047</td>
<td>11.3938</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>1024</td>
<td>404.27</td>
<td>33.03</td>
<td>12.2386</td>
<td>0.1195</td>
<td>1.1952</td>
<td>0.8917</td>
<td>12.2248</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>1089</td>
<td>429.51</td>
<td>34.04</td>
<td>12.6163</td>
<td>0.1159</td>
<td>1.1585</td>
<td>0.8811</td>
<td>12.6032</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>1156</td>
<td>455.54</td>
<td>35.03</td>
<td>13.0041</td>
<td>0.1123</td>
<td>1.1249</td>
<td>0.8683</td>
<td>12.9897</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>1225</td>
<td>482.31</td>
<td>36.04</td>
<td>13.3820</td>
<td>0.1092</td>
<td>1.0924</td>
<td>0.8480</td>
<td>13.3643</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>1296</td>
<td>509.86</td>
<td>37.03</td>
<td>13.7695</td>
<td>0.1062</td>
<td>1.0625</td>
<td>0.8254</td>
<td>13.7523</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>1369</td>
<td>538.17</td>
<td>38.04</td>
<td>14.1477</td>
<td>0.1033</td>
<td>1.0334</td>
<td>0.8051</td>
<td>14.1290</td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>1444</td>
<td>567.25</td>
<td>39.03</td>
<td>14.5349</td>
<td>0.1007</td>
<td>1.0066</td>
<td>0.7862</td>
<td>14.5145</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>1521</td>
<td>597.09</td>
<td>40.04</td>
<td>14.9131</td>
<td>0.0980</td>
<td>0.9805</td>
<td>0.7677</td>
<td>14.8912</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>1600</td>
<td>627.70</td>
<td>41.03</td>
<td>15.2903</td>
<td>0.0956</td>
<td>0.9563</td>
<td>0.7504</td>
<td>15.2763</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>1681</td>
<td>659.07</td>
<td>42.04</td>
<td>15.6679</td>
<td>0.0933</td>
<td>0.9372</td>
<td>0.7334</td>
<td>15.6531</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>1764</td>
<td>691.21</td>
<td>43.02</td>
<td>16.0467</td>
<td>0.0911</td>
<td>0.9108</td>
<td>0.7175</td>
<td>16.0377</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>1849</td>
<td>724.11</td>
<td>44.03</td>
<td>16.4445</td>
<td>0.0889</td>
<td>0.8894</td>
<td>0.7020</td>
<td>16.4145</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>1936</td>
<td>757.79</td>
<td>45.02</td>
<td>16.8310</td>
<td>0.0869</td>
<td>0.8694</td>
<td>0.6873</td>
<td>16.7988</td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>2025</td>
<td>792.21</td>
<td>46.03</td>
<td>17.2100</td>
<td>0.0850</td>
<td>0.8549</td>
<td>0.6730</td>
<td>17.1754</td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>2116</td>
<td>827.42</td>
<td>47.02</td>
<td>17.5963</td>
<td>0.0832</td>
<td>0.8316</td>
<td>0.6595</td>
<td>17.5535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>2209</td>
<td>863.38</td>
<td>48.03</td>
<td>17.9875</td>
<td>0.0814</td>
<td>0.8137</td>
<td>0.6462</td>
<td>17.9359</td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>2304</td>
<td>900.11</td>
<td>49.02</td>
<td>18.3817</td>
<td>0.0797</td>
<td>0.7969</td>
<td>0.6337</td>
<td>18.3194</td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>2401</td>
<td>937.60</td>
<td>50.03</td>
<td>18.7840</td>
<td>0.0781</td>
<td>0.7805</td>
<td>0.6214</td>
<td>18.6960</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>2500</td>
<td>975.87</td>
<td>51.02</td>
<td>19.1927</td>
<td>0.0765</td>
<td>0.7651</td>
<td>0.6098</td>
<td>19.0791</td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>2601</td>
<td>1014.89</td>
<td>52.03</td>
<td>19.6046</td>
<td>0.0750</td>
<td>0.7500</td>
<td>0.5984</td>
<td>19.4555</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>2704</td>
<td>1054.68</td>
<td>53.02</td>
<td>20.0173</td>
<td>0.0736</td>
<td>0.7357</td>
<td>0.5876</td>
<td>19.8383</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>2809</td>
<td>1095.23</td>
<td>54.03</td>
<td>20.4217</td>
<td>0.0722</td>
<td>0.7217</td>
<td>0.5770</td>
<td>20.2146</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>2914</td>
<td>1136.56</td>
<td>55.02</td>
<td>20.8271</td>
<td>0.0708</td>
<td>0.7084</td>
<td>0.5669</td>
<td>20.5969</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>3025</td>
<td>1178.66</td>
<td>56.03</td>
<td>21.2334</td>
<td>0.0695</td>
<td>0.6954</td>
<td>0.5570</td>
<td>20.9731</td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>3136</td>
<td>1221.47</td>
<td>57.02</td>
<td>21.6429</td>
<td>0.0683</td>
<td>0.6831</td>
<td>0.5476</td>
<td>21.3551</td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>3249</td>
<td>1265.10</td>
<td>58.03</td>
<td>22.0547</td>
<td>0.0671</td>
<td>0.6711</td>
<td>0.5383</td>
<td>21.7371</td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>3364</td>
<td>1309.69</td>
<td>59.02</td>
<td>22.4682</td>
<td>0.0660</td>
<td>0.6596</td>
<td>0.5295</td>
<td>22.1217</td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>3481</td>
<td>1334.63</td>
<td>60.02</td>
<td>22.8838</td>
<td>0.0648</td>
<td>0.6483</td>
<td>0.5208</td>
<td>22.4885</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>3600</td>
<td>1400.55</td>
<td>61.02</td>
<td>23.2954</td>
<td>0.0638</td>
<td>0.6376</td>
<td>0.5126</td>
<td>22.8697</td>
<td></td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>3721</td>
<td>1447.22</td>
<td>62.02</td>
<td>23.7133</td>
<td>0.0627</td>
<td>0.6271</td>
<td>0.5044</td>
<td>23.2454</td>
<td></td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>3844</td>
<td>1494.67</td>
<td>63.02</td>
<td>24.1318</td>
<td>0.0617</td>
<td>0.6170</td>
<td>0.4967</td>
<td>23.6262</td>
<td></td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>3969</td>
<td>1542.87</td>
<td>64.02</td>
<td>24.5508</td>
<td>0.0607</td>
<td>0.6072</td>
<td>0.4890</td>
<td>24.0071</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>4096</td>
<td>1591.85</td>
<td>65.02</td>
<td>24.9804</td>
<td>0.0598</td>
<td>0.5978</td>
<td>0.4817</td>
<td>24.3821</td>
<td></td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>4225</td>
<td>1641.58</td>
<td>66.02</td>
<td>25.4104</td>
<td>0.0588</td>
<td>0.5885</td>
<td>0.4745</td>
<td>24.7573</td>
<td></td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>4356</td>
<td>1692.09</td>
<td>67.02</td>
<td>25.8429</td>
<td>0.0578</td>
<td>0.5796</td>
<td>0.4676</td>
<td>25.1374</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4489 1743.35</td>
<td>68.02 25.6294 0.0571 0.5709 0.4608 25.5124</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-------------</td>
<td>-----------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>4624 1795.39</td>
<td>69.01 26.0145 0.0563 0.5626 0.4543 25.8920</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>4751 1848.18</td>
<td>70.02 26.3948 0.0554 0.5544 0.4478 26.2668</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>4900 1901.75</td>
<td>71.01 26.7798 0.0547 0.5465 0.4417 26.6460</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>5041 1956.08</td>
<td>72.02 27.1601 0.0539 0.5388 0.4356 27.0205</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>5184 2011.17</td>
<td>73.01 27.5450 0.0531 0.5313 0.4297 27.3994</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>5329 2067.03</td>
<td>74.02 27.9254 0.0524 0.5240 0.4240 27.7736</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>5476 2123.46</td>
<td>75.01 28.3103 0.0517 0.5170 0.4184 28.1520</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>5625 2181.04</td>
<td>76.02 28.6907 0.0510 0.5101 0.4130 28.5259</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td>5776 2239.20</td>
<td>77.01 29.0755 0.0503 0.5034 0.4077 28.9040</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td>5927 2298.12</td>
<td>78.02 29.4560 0.0497 0.4968 0.4025 29.2776</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>6084 2357.81</td>
<td>79.01 29.8408 0.0490 0.4905 0.3975 29.6552</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>6241 2418.25</td>
<td>80.02 30.2223 0.0484 0.4842 0.3923 30.0285</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>6400 2479.47</td>
<td>81.01 30.6060 0.0478 0.4782 0.3878 30.4057</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>6561 2541.45</td>
<td>82.02 30.9866 0.0472 0.4723 0.3831 30.7787</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>6724 2604.20</td>
<td>83.01 31.3712 0.0467 0.4666 0.3785 31.1554</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>6889 2667.71</td>
<td>84.02 31.7519 0.0461 0.4609 0.3740 31.5281</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>7056 2731.99</td>
<td>85.01 32.1365 0.0455 0.4554 0.3697 31.9044</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>7225 2797.03</td>
<td>86.02 32.5172 0.0450 0.4501 0.3654 32.2767</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>7396 2862.54</td>
<td>87.01 32.9017 0.0445 0.4449 0.3613 32.6526</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>7569 2929.40</td>
<td>88.02 33.2825 0.0440 0.4397 0.3572 33.0246</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>7744 2996.75</td>
<td>89.01 33.6670 0.0435 0.4347 0.3532 33.4000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>89</td>
<td>7921 3064.84</td>
<td>90.02 34.0477 0.0430 0.4298 0.3493 33.7716</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>8100 3133.72</td>
<td>91.01 34.4322 0.0425 0.4251 0.3455 34.1465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>8281 3203.35</td>
<td>92.02 34.8130 0.0420 0.4204 0.3418 34.5177</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>8464 3273.75</td>
<td>93.01 35.1974 0.0416 0.4158 0.3381 34.8923</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>8649 3344.91</td>
<td>94.02 35.5783 0.0411 0.4114 0.3345 35.2631</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>8836 3416.84</td>
<td>95.01 35.9624 0.0407 0.4070 0.3310 35.6371</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>9025 3489.53</td>
<td>96.02 36.3436 0.0403 0.4027 0.3276 36.0075</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>9216 3562.99</td>
<td>97.01 36.7279 0.0399 0.3985 0.3243 36.3811</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>9409 3637.21</td>
<td>98.01 37.1088 0.0394 0.3944 0.3209 36.7511</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>9604 3712.20</td>
<td>99.01 37.4931 0.0390 0.3904 0.3177 37.1242</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>9801 3787.95</td>
<td>100.01 37.8741 0.0386 0.3864 0.3146 37.4938</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>10000 3864.48</td>
<td>101.01 38.2583 0.0383 0.3826 0.3115 37.8663</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.
Sind die Kosten der untersten Ebene des Ortsnetzes in 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: KVSTERN/KVBMAXURING (B) und KVSTERN/KVTMINURING (T) bei quadratisch wachsender ANZAHL.

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

\[
\frac{5}{12} \times 10 \text{ DM/m} = 4,167 \text{ DM/m}.
\]

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

\[
30 \text{ DM/m} / 4,167 \text{ DM/m} = 7,2 \times \text{ VB}.
\]

Nimmt man als Einheit der Übertragungskapazität nicht das Maximalangebot von BIGFON sondern als Minimallangebot 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

\[
2 \times 44 \text{ kbit/s} / (12 \times 34 \text{ Mbit/s}) \times 10 \text{ DM/m} = 0.003137 \text{ DM/m}.
\]

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

\[
30 \text{ DM/m} / 0.003137 \text{ DM/m} = 9562,5 = \text{ VT}.
\]

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 Sendevölkern

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

Im Zuge der **Digitalisierung des Ortes** sollen jeden Fernsprechtteilnehmer über das vorhandene Kupfer-Doppeladernetz zwei 64 kbit/s und ein 16 kbit/s Duplex-Kanal 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 Nutzzbits/s zu übertragen, 1400 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). Privates, lokale Verteilnetze mit etwa 400 bis 4000 Teilnehmern sind dann also ohne wesentliche zusätzliche Investitionen der Post und sogar (sofern innerhalb 500m Grundstücks) ohne Genehmigung der Post realisierbar. Der Preis hierfür ist das Einrichten und Unterhalten eines privaten Spezialnetzes für Bildschirmtext.

Sofort 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 4800 bit/s) und Utility Band (7 Fernsehkanäle) untergebracht [Czaa_82, Elek_82].


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 Schlüssel 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 Verteilernetz sondern nur die Information im WANG Band und eventuellen anderen zugeteilten Kanälen verfolgen müssen, dürften sie dadurch kostengünstiger realisierbar sein.

Nutz 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:


1220 Mbit/s / (0.05 x 2 x 34 Mbit/s) = 35

Teilnehmer an den Ring angeschlossen werden. Dabei bleibt das Dienstangebot von BIGFON erhalten. In diesem Beispiel wurde zu übertragende Verwaltungsinformation (z. B. Adressen) vernachlässigigt, da hauptsächlich gleichermaßen breitbandiges Verkehrsaufkommen angenommen wurde. Ebenfalls wurde nicht berücksichtigt, daß der Durchsatz eines Ringes 1 bis 2 mal so groß wie die Kapazität seiner Leitungen sein kann [Busc_83 Seite 34].
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 dadurch die Kontrolle des Benutzers über seine Datenschutzbelange abgeschwächt wird.

Wählt man als Leitungstypologie des Verteilnetzes mit Rückkanal einen Bus, so muß der 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 Leitungstypologie einen Ring, so kann der Betreiber des Vermittlungsnetzes die Verteilnetzcentrale 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 Verteilnetzcentrale, 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-/Verteilernetz 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-/Verteilernetz auch einseitig anonyme Kommunikation sowie Kommunikation zwischen sich voll identifizierenden Teilnehmern erfolgen. Entsprechend Abschnitt 2 bietet dieses Vermittlungs-/Verteilernetz dem Teilnehmer folgende Vor- und Nachteile:

+ Informationen können schnell aus beliebig großer Information angeboten 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. [Maß_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, Desh_83, Leis_82 Seite 7ff, Schli_82]...
WeSc_83J 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 Eckknoten 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


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 (Kerk 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:

x Im Vermittlungs-/Verteilnetz ist keine Leitung nur einer Teilnehmerstation zugeordnet.

x Es gibt im Vermittlungs-/Verteilnetz keine eindeutige 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 einzelge (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 Absendezzeitpunt von Nachrichten innerhalb von durch Benutzererwarten- tungen oder günstige (Nacht-)Tarife vorgegebenen Zeitintervallen zufällig.
Neben der Erhöhung des Datenschutzes wird durch M1 auch das Netz gleichmäßig 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. 27 Uhr und 3 Uhr anzufordern.

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

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

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

3.4 Vergleich mit der Lösungsalternative von David L. Chaum

Spiegelin, Spiegelin 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

H Ike müssen sich Nachrichten wegen ihrer Wiederaufnahme zu

ignorieren
öffentlichen Schlüsseln.

Der Gewinn an Datenschutz durch die beiden Verfahren ist schwer zu vergleichen, da sie jeweils verschiedensten 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 Vermittlungscentra-


<table>
<thead>
<tr>
<th>Dienst</th>
<th>Chaum</th>
<th>Pfützmann</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senden einer Nachricht</td>
<td>((x+1) (Y+E) (N+A))</td>
<td>((Y+E) N+x E A)</td>
</tr>
<tr>
<td>Bildung und Benutzung eines anonymisierten Absenders</td>
<td>((x+1) P + ) (x (Y+E) (A + 0.5 (x-1) S))</td>
<td>(Z + Y A + P + ) (X E A)</td>
</tr>
</tbody>
</table>

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.

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 ans Weges mit G's öffentlichen Schlüssel G@ verschlüsselt. Die Nachricht besteht neben F_pa und F@ (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_8 bilden im anderen Netz einen anonymisierten Absender.
Inhalt 2 (I2) zusammen mit F_pa und F_8 kann mit g' als Adresse im anderen Netz an G geschickt werden, der I2 mit F_3 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 I2,F_pa,F_6 bzw. zwischen ihm und G I2,F_pa,F_8 verschlüsselt übertragen werden.

L3 Können sich der Teilnehmer im anderen 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 344].

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 entnommenen öffentliche Schlüssel zu den verwendeten privaten Schlüsseln passen, nach der 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 6 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
Bild 18: Netzübergang bei eingeschränkten Bitfolgen

5 Ausblick

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

Cheatham

Ein angemähtes 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 bestimnten 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 Teilnehmer-
station innerhalb ihrer Gruppe erhält.

Es ist nötig darauf hinzuwirken, 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
dele Bereiche unseres Lebens erhöht die Kontrollierbarkeit des
Individuums bei Arbeit und Freizeit, weil sich letztlich immer
mehr menschliche Tätigkeiten und Bedürfnisse in diesen Netzen
und Sprechern abbilden werden, wo sie gerade aufgrund der
Entwicklung in der Informationsverarbeitung zunehmend intelli-
gent und automatisch ausgeführt 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 Versuch verlieren, 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
extremen 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 Buhl, Dr. Klaus Dittrich, Klaus Echtli, Prof. Herbert
Fiedler, Hermann Hürting, Jürgen Hülsemann, Prof. Walter Kunz,
Dr. Axel Lehmann, einem/einer mir namentlich nicht bekannten Mitarbeiter/in von Dr. Ruth Leuze, Michael Marholfer, Prof. H. A. Maurer, Fritz Müller, Birgit Pfitzmann, Dr. Johannes Rührich, Dr. Jan Schütz und Prof. Detlef Schmid.

Literatur
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 Ubertragungstechnik; telecom 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
BeEs_83 Eric Benhamou, Judy Estrin: Multilevel Internetworking Gateways: Architecture and Applications; IEEE Computer Vol. 16, Nr. 9, September 1983, Seite 27 bis 34
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 Wirt: Kryptographie; B. G. Teubner Stuttgart 1983, Seite 10 bis 43
Bild_33 Bildschirmtext: Warten auf den Tag X; computer magazin März 1983, 12. Jahrgang, Seite 58 bis 59

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; telecom report Band 5, Heft 2, 1982, Seite 123 bis 129.

Brau_83 Ewald Braun: BIGFON - Erprobung der optischen Breitbandübertragung im Ortsnetz; telecom 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.


Denn_82 Dorothy Elizabeth Robling Denning: Cryptography and Data
Schoöler (Hrsg.), Springer-Verlag Heidelberg, April 1983, Seite 73 bis 96


LeMa_83 R. E. Lennon, S. M. Matyaes: 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


MaPo_82 H. A. Maurer, R. Posch: Der MUPID: Ein Beitrag Österreichs zur Entwicklung von Bildschirmtext; IIG, Universität Graz, Bericht F87, Juni 1982


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

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

Mau2_83 H. Maurer: Lokale Intelligenz zur Unterstützun 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 17


Pete_81 Ulrich v. Patersdorff: Das Kompetenzzproblem und die datenschutzrechtliche Verantwortlichkeit bei Bildschirmtext; Datenschutz und Datensicherung, 7/1981, Seite 83 bis 86


Pff_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


Pfitt_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

Pili_83 Ernst Piller: Mikroprozessorgesteuerte Speicherkarte im Scheckkarten-Format; German Chapter of the ACM Berichte 17, Microcomputing II, W. Remmele, H. Schechel (Hrsg.), Tagung III/1983 des German Chapter of the ACM vom 25. bis 27.10.83 in München, B. G. Teubner Stuttgart 1983, Seite
PoPo_83 K. C. Posch, R. Posch: Two extensions of an intelligent videodetox-decoder; IIG, Universität Graz, Bericht F101, January 1983
Rein_81 Günter Reiner: Datenschutz und Bildschirmtext; Datenschutz und Datensicherung, 2/1981, Seite 87 bis 90
ReLi_76 Cecil C. Reamee, 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, Nr. 1, Seite 124 bis 129
Riha_83 Karl Rihaček: OSI - Open Shops for Information Services; OvD Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Friedr. Vieweg & Sohn, Braunschweig, Heft 5, April 1983, Seite 116 bis 125
RosK_82 Karl Heinz Rosenbrock: Mögliche Integration von Fernmelde- diensten im digitalen Fernsprechnetz der Deutschen Bundespost - ISDN; Zeitschrift für das Post- und Fernmeldewesen Heft 9 vom 27. September 1982
RuRa_83 John Ruchby, Brian Randell: A Distributed Secure System; IEEE computer Vol. 14, Nr. 7, July 1983, Seite 55 bis 67
SBits_83 Software-Schutz 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, Nr. 9, September 1983, Seite 15 bis 24
Schl_82 Jan Schlöwer: Outputkontrollen zur Sicherung statistischer Datenbanken; Informatik-Spektrum Band 5, Heft 4, Dezember 1982, Seite 224 bis 236

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


Tane_81 Andrew S. Tanenbaum: Network Protocols; acm computing surveys Vol. 13, No. 4, December 1981, Seite 453 bis 489

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


Verk_83 Verlagerung schreitert voran - Einzelnetze zu einem Bundesweiten Netz verbinden; Mitit&Technik Nr. 17 vom 29. April 1983, Seite 8


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

Abbuchungsermäßigung 37
Abrechnung 23
ALOHA 15
anonyme Nummernkonten 29
Beschwerdefrist 32
BISFON 7, 45, 58, 59
Bildschirmtext 6, 59
Bus 16, 62
Chaum 68
CSMA/CD 15
Datenschutz 6, 7, 8, 9, 13, 17, 18, 19, 35, 41, 59, 60, 62, 63, 69, 73
Datenschutz-Ergonomie 73
DDLCN 18
dienstintegriertes digitales Netz 13, 45, 63
Distributed Double-Loop Computer Network 18
Distributed Loop Computer Network 15
DLCN 15
ISDN 13, 45, 63
Kreditrahmen 39
Kryptosystem mit öffentlichen Schlüsseln 10, 11
Loop 15, 16
 Neue Medien 6
Newhall Loop 16
nicht manipulierbare Zähler 36
offenes System 6
öffentlicher Schlüssel 10, 11
Pierce Loop 15
privater Schlüssel 10, 11
räumliche Topologie 67
register 'Insertion Loop' 15
Ring 16
SBNs 2, 3
Scheck 30
Schiedsstelle 32, 39
Smart card 44
traffic analysis 1
Verkehrsanalyseproblem 2
Vermittlungsnetz 7, 8
Vermittlungs-/Vermittlungsnetz 64, 65
Vermittlungs-/Verteilnetz 21
Verteilnetz 9, 14
Verteilnetz mit Rückkanal 14
Verteilnetzzentrale 9, 14
Verteil-/Verteilnetz 66
zeitliche Muster 67
zeitliche Topologie 67