4 Effizienter Einsatz der Grundverfahren

In Kapitel 2 wurden Grundverfahren beschrieben, die es den Teilnehmern eines digitalen Kommunikationsnetzes ermöglichen, anonym voreinander wie auch vor dem Kommunikationsnetz Informationseinheiten auszutauschen. In Kapitel 3 wurde die effiziente Realisierung dieser Grundverfahren behandelt, wobei ersichtlich wurde, daß sie in reiner Form für einige der geplanten Dienste eines breitbandigen diensteintegrierenden Digitalnetzes heutzutage und in der näheren Zukunft nicht oder nur mit unvertretbarem Aufwand einsetzbar sind.

Um auch solche Dienste mit (teilnehmer-)überprüfbarem Datenschutz realisieren zu können, müssen die Grundverfahren effizienter eingesetzt werden. Gegebenenfalls ist ein (hoffentlich guter) Kompromiß zwischen Nutzleistung und Datenschutz, insbesondere Anonymität zu suchen.

Deshalb werden in Abschnitt 4.1 die Grundverfahren verglichen und ihre Einsatzprobleme diskutiert. Danach wird in den Abschnitten 4.2 und 4.3 behandelt, wie die Grundverfahren durch Einführung verschieden geschützter Verkehrsklassen und/oder hierarchische Gliederung des Kommunikationsnetzes und dadurch induzierte Klasseneinteilung der Teilnehmer bezüglich Anonymität (vgl. Abschnitt 2.1.1) genügend effizient eingesetzt werden können.

4.1 Vergleich der bzw. Probleme mit den Grundverfahren

Zuerst wird der Einsatz umcodierender MIXe zum **Schutz der Kommunikationsbeziehung** betrachtet. Um die Summe der Kosten des Kommunikationsnetzes unter Einschluß aller MIXe und die durch ihr gleichzeitiges Ausgeben von Nachrichten oder Paketen bzw. Schalten von Kanälen bedingten Verzögerungszeiten erträglich zu halten, kann es, wie in Abschnitt 3.2.2.4 unter der Annahme der Vermeidung bedeutungsloser Nachrichten hergeleitet wurde, nur relativ wenige MIXe geben, die dann sehr leistungsfähig, aber auch sehr komplex sind. Die große Mehrzahl der Teilnehmer ist damit gezwungen, ihren Datenschutz in wenige „fremde Hände“ zu legen und genießt daneben keinen oder nur sehr ineffizienten Schutz ihres Sendens und bei fehlender Verteilung auch nur sehr, sehr ineffizienten Schutz ihres Empfangens. (Mittels bedeutungsloser Nachrichten und MIXen kann zwar sowohl das Senden als auch das Empfangen der Teilnehmerstationen geschützt werden. Jedoch ist diese Kombination nur unter speziellen Randbedingungen sinnvoll, siehe Abschnitte 6.2 und 6.3.) Gerade die Effizienz von letzterem ist sehr wichtig, da die Übertragung von Fernsehprogrammen auf absehbare Zukunft einen erheblichen Teil des Nachrichtenaufkommens ausmachen wird. Außerdem dürfte es schwierig sein, die Existenz von Trojanischen Pferden in den komplexen MIXen auszuschließen oder, sofern dies nicht hinreichend sicher möglich ist, zumindest sehr viele verschiedene unabhängige Hersteller dieser sehr leistungsfähigen MIXe zu haben.

Will man ein Netz für die Bundesrepublik Deutschland, also einen Staat mit Fernmeldemonopol, konstruieren, so hat der Lösungsansatz der umcodierenden MIXe einen zusätzlichen (durch eine kleine Modifikation des Fernmeldemonopols jedoch vermeidbaren, siehe Abschnitt 6.2) Nachteil: Da erforderlich ist, daß die MIXe nicht zusammen gegen die Benutzer arbeiten, sollten sie verschiedene Betreiber haben. Dies bedeutet, daß jede Nachricht das öffentliche Netz mehrmals durchläuft, da nicht einfach dessen Vermittlungsstellen allein als MIXe eingesetzt werden können. Dadurch wird auch dieses Verfahren für ein breitbandiges Netz sehr übertragungsaufwendig. In jedem Fall muß auch noch die Verantwortung für die Dienstqualität zwischen dem Betreiber des öffentlichen Netzes und den Betreibern der MIXe geregelt werden, was in Abschnitt 7.1.2 ausführlich diskutiert wird.

<table>
<tr><td colspan="3"></td><td colspan="4">Schutz des Verkehrs</td></tr>
<tr><td colspan="3"></td><td colspan="2">homogen
(Verkehr einheitlich geschützt)</td><td colspan="2">heterogen
(verschieden geschützte Verkehrsklassen)</td></tr>
<tr><td colspan="3"></td><td>ein Grundverfahren</td><td>mehrere Grundverfahren</td><td>alternative Grundverfahren oder verschieden sichere Realisierungen</td><td>Grundverfahren teilweise kombiniert</td></tr>
<tr><td rowspan="3">Schutz der Teilnehmer</td><td>einheitlich</td><td></td><td>eine Anonymitätsklasse durch ein Grundverfahren (Abschnitte 2.5, 2.6 und Kap. 3)</td><td>eine Anonymitätsklasse durch gleichzeitige Anwendung mehrerer Grundverfahren (MIXe und Verteilung in Abschnitt 2.5.2; Überlagerndes Senden auf RING- oder BAUM-Netz in Abschnitt 2.5.3.2 und 2.6)</td><td>Asymmetrische Netze für Massenkommunikation (Abschnitt 4.2.1)

Aufwandsreduktion bei nicht sensitivem Verkehr (Abschnitt 4.2.2)

Verschieden sichere Realisierungen (Abschnitt 4.2.3)</td><td>Kombination von Grundverfahren für besonders sensitiven Verkehr (Abschnitt 4.2.4)</td></tr>
<tr><td rowspan="2">hierarchisch

(Teilnehmerklassen bezüglich Schutz)</td><td>statisch feste Hierarchiegrenze</td><td colspan="2">Eine Anonymitätsklasse bezüglich Hierarchiegrenze (Abschnitt 4.3.1.1)</td><td colspan="2">Mehrere Anonymitätsklassen bezüglich Hierarchiegrenze (Abschnitt 4.3.1.2)</td></tr>
<tr><td>dynamisch adaptierbare Hierarchiegrenze</td><td colspan="2">Eine Anonymitätsklasse bezüglich Hierarchiegrenze (Abschnitt 4.3.2.1)</td><td colspan="2">Mehrere Anonymitätsklassen bezüglich Hierarchiegrenze (Abschnitt 4.3.2.2)</td></tr>
</table>

Bild 48: Klassifizierung der Möglichkeiten des effizienten Einsatzes der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten

Aus all diesen Gründen ist es zweckmäßiger, primär die Verfahren aus Abschnitt 2.5.3 zum **Schutz des Senders** und Verteilung (Abschnitt 2.5.1) zum **Schutz des Empfängers** zu verwenden.

Wie in Abschnitt 4.2 beschrieben wird, ist es aus Gründen der Effizienz des Kommunikationsnetzes und der Verschiedenartigkeit der Dienste unsinnig, allen Verkehr (etwa in einem *homogenen* Kommunikationsnetz) einheitlich zu schützen. Insbesondere beim Aufwand für den Schutz des Senders kann bei vielen Diensten gespart werden, indem er etwa bei Massenkommunikation [Kais_82], z. B. Fernsehen, ganz eingespart und bei Diensten geringer Sensitivität ggf. eingeschränkt wird.

Aus Leistungsgründen ist ein breitbandige Individualkommunikation ermöglichendes offenes Kommunikationsnetz, in dem alle Informationseinheiten an alle Teilnehmerstationen verteilt werden, in den nächsten zwei Jahrzehnten nur mit unvertretbarem Aufwand realisierbar. Ein Kommunikationsnetz, das dieses Verfahren einsetzt, muß folglich ab einer gewissen Größe *hierarchisch* gegliedert werden. Die Nachrichten werden dabei nicht an alle, sondern nur an hinreichend viele Teilnehmerstationen verteilt (multicast), so daß die hierarchische Gliederung eine Klasseneinteilung der Teilnehmer bezüglich (Empfänger-)Anonymität induziert. Zweckmäßigerweise wird eine damit verträgliche hierarchische Gliederung auch für das Verfahren zum Schutz des Senders verwendet. All dies wird in Abschnitt 4.3 ausführlich diskutiert.

Wie Bild 48 zeigt, können beide Klassen von effizienzsteigernden Maßnahmen zu – bezüglich Schutz – hierarchischen heterogenen Kommunikationsnetzen kombiniert werden.

4.2 Heterogene Kommunikationsnetze: verschieden geschützte Verkehrsklassen in einem Netz

Um die hohen Leistungsanforderungen (nach großem Durchsatz und kurzen Verzögerungszeiten) mancher Dienste des geplanten breitbandigen diensteintegrierenden Digitalnetzes erfüllen zu können, wird in diesem Abschnitt nach einem effizienten Einsatz der Grundverfahren aus Abschnitt 2.5 mittels der Bildung von **Verkehrsklassen** (bezüglich der Kriterien Leistungsanforderungen und nötigem Schutz) und deren Ungleichbehandlung bezüglich Schutz gesucht.

Die genauen Forderungen bezüglich Durchsatz, Verzögerungszeit und Schutz sind zwar bei verschiedenen Diensten teilweise gravierend unterschiedlich, da es aber mit dem (hochauflösenden) Bildfernsprechen mindestens einen Dienst gibt, der alle Forderungen zusammen stellt, muß man, um eine technische Alternative zu den Plänen der DBP zu haben, ein Netz entwerfen, das alle diese Forderungen gleichzeitig hinreichend gut erfüllt.

Zumindest im Teilnehmeranschlußbereich sollten aus Kostengründen auch alle anderen Dienste auf derselben physischen Netzstruktur abgewickelt werden, da dann (und nur dann) die Übertragungsbandbreite ohne Mehraufwand dynamisch zwischen den Diensten aufgeteilt und damit effizienter genutzt werden kann. Ein zusätzlicher Vorteil ist, daß dann nur *ein Übertragungsnetz* zu unterhalten ist, was – wie die Erfahrung lehrt – weniger aufwendig als der Unterhalt mehrerer Netze ist. Wie in Kapitel 5 beschrieben wird, kann und muß dieses eine Übertragungsnetz fehlertolerant ausgelegt werden, da in einer „Informationsgesellschaft“ von seiner kontinuierlichen Verfügbarkeit größere materielle und immaterielle Werte abhängen werden. Die

Erfahrung lehrt, daß auch der Unterhalt eines fehlertoleranten Übertragungsnetzes weniger aufwendig als der Unterhalt mehrer unabhängiger Netze vergleichbarer Nutzleistung und Gesamtverfügbarkeit ist. Zur notdürftigen Tolerierung von innerhalb des leitungsgebundenen (fehlertoleranten) *diensteintegrierenden Kommunikationsnetzes* nicht tolerierbaren Mehrfachfehlern dienen dann, wie am Ende von Abschnitt 1.1 bemerkt wurde und in Abschnitt 9.1 aufgegriffen wird, Funknetze.

In den Unterabschnitten dieses Abschnitts werden folgende, die Effizienz steigernde Maßnahmen behandelt:

In Abschnitt 4.2.1 wird gezeigt, wie durch die Berücksichtigung spezieller Eigenschaften der Massenkommunikationsdienste [Kais_82] effizientere, sogenannte *asymmetrische* Kommunikationsnetze entstehen.

In Abschnitt 4.2.2 werden Möglichkeiten zur Reduktion des Aufwands bei nicht sensitivem Verkehr im MIX-, DC-, RING- und BAUM-Netz aufgezeigt.

In Abschnitt 4.2.3 werden verschieden sichere Realisierungen der Grundverfahren aufgegriffen.

In Abschnitt 4.2.4 wird behandelt, wie auch bei Verwendung eines einheitlichen Übertragungsnetzes Dienste, die weniger hohe Leistungsanforderungen stellen, mit anderen Protokollen behandelt werden können, um noch stärkeren Datenschutz zu garantieren.

4.2.1 Asymmetrische Kommunikationsnetze für Massenkommunikation

Alle Massenkommunikationsdienste [Kais_82] besitzen zwei Eigenschaften, die für einen effizienten Einsatz der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten wichtig sind:

1. Bei ihnen ist lediglich der Schutz der Interessens- und dazu der Verkehrsdaten (genauer: Schutz des Empfängers) notwendig, vgl. Abschnitt 1.2. Inhaltsdaten müssen nicht um ihrer selbst willen geschützt werden.
   Allenfalls aus Abrechnungsgründen ist dies nötig, z. B. bei Fernsehen mit Bezahlung gesehener Sendungen – Pay-per-View-TV. Dies kann sehr einfach erfolgen, indem die Inhaltsdaten Ende-zu-Ende-verschlüsselt werden und den Käufern der Massenkommunikationssendung mit den in Kapitel 8 beschriebenen Transaktionsprotokollen für anonyme Partner der oder die passenden Schlüssel verkauft werden. Bezüglich der Sicherheit der Verschlüsselung brauchen nicht dieselben hohen Kriterien wie bei personenbezogenen Daten, militärischen oder Geschäftsgeheimnissen angelegt zu werden. Es genügt völlig, wenn das Brechen aufwendiger oder langwieriger als das Besorgen des Massenkommunikationsdienstinhaltes über einen anderen Käufer ist.
2. Für die Erbringung des Dienstes braucht Information nur vom Dienstanbieter zum Teilnehmer, nicht aber (oder zumindest: so gut wie nicht) vom Teilnehmer zum Dienstanbieter übertragen zu werden.

Für die Gestaltung eines Kommunikationsnetzes eröffnet dies folgende, die Effizienz ohne Abschwächung des Datenschutzes steigernde Möglichkeiten:

1. Bei Massenkommunikationsdiensten kann in der Regel auf Ende-zu-Ende-Verschlüsselung und implizite Adressierung verzichtet werden.
2. Da in der überschaubaren Zukunft nur ein relativ kleiner Anteil aller Teilnehmer auch Anbieter von Massenkommunikationsdiensten, die nennenswerte Bandbreite beanspruchen, sein wird, ist es möglich, das Kommunikationsnetz *asymmetrisch* zu gestalten: In Richtung zum Teilnehmer kann dann im Teilnehmeranschlußbereich (erheblich) mehr Information fließen als in Richtung vom Teilnehmer.

Letzteres kann durch den in Abschnitt 3.2.1 skizzierten optischen Überlagerungsempfang zusammen mit der in Abschnitt 3.3.1 erwähnten (analogen) optischen Verstärkung sehr effizient realisiert werden. Allerdings bedingt diese Effizienzsteigerung auch zwei Einschränkungen.

Einerseits ist der Nutzungsspielraum eingeschränkt: Nur in Richtung zum Teilnehmer vorhandene Bandbreite, die vor allem abends für hochauflösendes Fernsehen benötigt wird, kann nicht morgens zur Abwicklung der Verkehrsspitze des Bürokommunikationsverkehrs, insbesondere für (hochauflösendes) Bildfernsprechen, verwendet werden.

Andererseits sind nicht alle Grundverfahren für Senderanonymität mit einer asymmetrischen Gestaltung des Kommunikationsnetzes geschickt kombinierbar: Da nicht sehr viele (analoge) optische Verstärker hintereinander geschaltet werden können, ohne daß auch (ursprünglich) digitale Signale nicht mehr eindeutig erkennbar sind, harmoniert eine asymmetrische Gestaltung nicht gut mit dem Konzept der „Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung“, insbesondere dem RING-Netz.

4.2.2 Aufwandsreduktion bei nicht sensitivem Verkehr im MIX-, DC-, RING- und BAUM-Netz

Nicht aller Kommunikationsverkehr ist sensitiv: Wenn beispielsweise jeder Haushalt von den Versorgungsbetrieben für Elektrizität und Wasser monatlich seine Rechnung bzw. Abbuchungsmitteilung erhält, ist nicht die Tatsache an sich, sondern nur die Zusammensetzung und Höhe sensitiv.

Während in diesem Beispiel *Sensitivität in einem objektiven Sinne* verwendet wird, wurde mir in zahllosen Diskussionen (beispielsweise mit David Chaum) immer wieder nahegelegt, die Teilnehmer doch selbst entscheiden zu lassen, welchen Kommunikationsverkehr sie für sensitiv halten und – um Aufwand zu sparen – nur diesen zu schützen. Gegen diesen Vorschlag, *Sensitivität im jeweils subjektiven Sinne* zum Maßstab des Schutzes des Kommunikationsverkehrs zu machen, gibt es folgende wichtige Gegenargumente:

1. Zwar dürfte die durch Verkehrsanalyse gewinnbare Information in vielen Fällen für sich allein (zumindest in einem subjektiven Sinn) nicht sensitiv sein, sie kann aber möglicherweise mit anderen Informationen kombiniert das Erschließen (auch im subjektiven Sinne) sensitiver Information ermöglichen.
2. Die Tatsache, ob, wann und welche Dienste ein Teilnehmer subjektiv als sensitiv einstuft, ist personenbezogene Information, die meines Erachtens zu schützen ist.
   Dies kann allerdings vermieden werden, indem Diensten global eine bestimmte Sensitivität zugeordnet wird. Letzteres hat wiederum den Nachteil, daß dadurch möglicherweise

Dienste für einen Angreifer unterscheidbar werden, die dies vorher nicht waren. Dies führt dazu, daß Dienste mit ähnlicher Verkehrscharakteristik jeweils derselben Sensitivitätsklasse zugeordnet werden sollten.

3. Wenn Maßnahmen zum Schutz der Verkehrs- und Interessensdaten nur wenig ergriffen werden, kann bereits ihre Ergreifung einen Verdacht hervorrufen. Die Angst vor diesem Verdacht und seinen möglichen Folgen kann wiederum die Teilnehmer von der Ergreifung der Maßnahmen abhalten.
4. Obiges Argument für subjektive Sensitivität wird meist mit der Forderung kombiniert, daß nur die Teilnehmer, die Schutz ihrer Verkehrs- und Interessensdaten wünschen, die dabei entstehenden Kosten tragen sollen. Diese Kosten wären bei geringer Nachfrage in der Tat hoch. Das Gegenargument hierfür ist, daß überprüfbarer Datenschutz keine Frage der persönlichen Kaufkraft sein sollte, da sonst manche, obwohl sie den Schutz ihrer Verkehrs- und Interessensdaten für nötig halten, die eigentlich notwendigen Maßnahmen aus Kostengründen nicht in Anspruch nehmen. Etwas allgemeiner gesagt: Meines Erachtens ist es rechtlich nicht zulässig, die (überprüfbare) Wahrung von Grundrechten an die Zahlung von (extra) Gebühren zu koppeln.

Nach diesen Bemerkungen dazu, was sinnvollerweise unter nicht sensitivem Verkehr zu verstehen ist, werden nun Möglichkeiten zur Reduktion des Aufwands von nicht sensitivem Verkehr in für Anonymität entworfenen Kommunikationsnetzen aufgezeigt. Der Reihe nach werden das MIX-, DC-, RING- und BAUM-Netz behandelt.

Wenn MIXe zum Schutz der Kommunikationsbeziehung verwendet werden, braucht nicht sensitiver Verkehr natürlich keine MIXe zu durchlaufen. Dies verringert sowohl die Zahl der nötigen MIXe (bzw. ihre nötige Leistungsfähigkeit, wobei damit evtl. auch der Schutz der Kommunikationsbeziehung abgeschwächt wird) als auch die Übertragungskapazität, die das von den MIXen verwendete Übertragungs- und Vermittlungsnetz bereitstellen muß. Bei der letzten Aussage ist unterstellt, daß die Vermittlungszentralen des Kommunikationsnetzes nicht mit den MIXen identisch sind, vgl. Abschnitt 4.1, und MIXe nicht, wie in [Pfit_86] und Abschnitt 6.2 vorgeschlagen, in der unmittelbaren Nähe von Vermittlungszentralen errichtet sind.

Bei allen Kommunikationsnetzen mit Verteilung (DC-, RING- und BAUM-Netz) können für nicht sensitiven Verkehr konstante öffentliche offene implizite Adressen verwendet werden. Die Verwendung konstanter öffentlicher Adressen spart Aufwand bei der Adreßerzeugung und Verteilung, die Verwendung offener impliziter Adressen spart Aufwand bei der Adreßerkennung.

Beim DC-Netz kann Senderanonymität für einen Teil der Bandbreite eingespart werden, indem in diesem Teil keine Schlüssel überlagert werden. Dies spart Aufwand beim Schlüsselaustausch und bei der Schlüsselgenerierung sowie möglicherweise bei der Überlagerung. Ebenso braucht dieser Teil der Bandbreite dann nicht unbedingt mit anonymen Mehrfachzugriffsverfahren verwaltet zu werden. Beispielsweise können Fernsehstationen jeweils feste Kanäle zugewiesen werden.

Entsprechendes gilt für das RING- und BAUM-Netz, so daß bei ersterem in dem etwa für Fernsehen verwendeten Teil der Bandbreite selbstverständlich keine leer/belegt Bits in Übertragungsrahmen oder umlaufende Senderechtszeichen nötig sind.

4.2.3 Verschieden sichere Realisierung der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten

In diesem Abschnitt werden verschieden sichere Realisierungen der Grundverfahren diskutiert. Dies erscheint vor allem beim MIX- und DC-Netz lohnend.

4.2.3.1 Fest vorgegebene MIX-Kaskaden beim MIX-Netz

In Abschnitt 2.5.2.1 habe ich hergeleitet, daß zur Erreichung eines bei gegebenen MIXen maximalen Schutzes der Kommunikationsbeziehung „alle Nachrichten des betrachteten Zeitintervalls jeweils gleichlang sein und die MIXe jeweils gleichzeitig (und deshalb auch in gleicher Reihenfolge) durchlaufen müssen“.

Dies legt nahe, evtl. dienstspezifisch feste Reihenfolgen von MIXen (sogenannte MIX-Kaskaden) vorzugeben, wodurch eine wesentlich effizientere Implementierung der MIXe und des von den MIXen benutzten Vermittlungs- und Übertragungsnetzes möglich ist: Der Adressier- und Wegwahlaufwand wird drastisch reduziert, die Reihenfolge der MIXe kann auf die Topologie des Übertragungsnetzes abgestimmt werden, die Synchronisation der MIXe auf die Übertragungsrate und Verzögerungszeit des Übertragungsnetzes und die zu behandelnden Informationseinheiten (Pakete, Nachrichten, Kanäle, vgl. Abschnitt 3.2.2.1) und all dies zusammen auf die Anforderungen des bzw. der abzuwickelnden Dienste, vgl. Abschnitt 3.2.2.4.

Der Effizienzgewinn ist offensichtlich, was aber ist der „Preis“ dafür? Er besteht darin, daß sich der einzelne Teilnehmer nicht mehr MIXe seines Vertrauens beliebig aussuchen und zu einer MIX-Folge kombinieren kann. Insbesondere kann er nicht jeweils selbst einer der MIXe sein, denen er vertraut und die er folglich benutzt. Beide Nachteile sind meiner Meinung nach nicht schwerwiegend:

Für viele Dienste können, wie in Abschnitt 3.2.2.4 hergeleitet wurde, ohne genaue Abstimmung der MIXe aufeinander und das von ihnen benutzte Vermittlungs- und Übertragungsnetz nur sehr wenige MIXe benutzt werden. Bei ihnen verbessert die oben beschriebene Vorgabe die Zahl der benutzbaren MIXe und steigert auch dadurch den Schutz der Kommunikationsbeziehung. Bei der Festlegung der Vorgabe sollte darauf geachtet werden, daß an den MIX-Kaskaden jeweils sehr unterschiedliche Betreiber beteiligt sind: wird jeweils ein MIX von beispielsweise der CDU, dem DGB, den Grünen, der katholischen Kirche und einer schweizer Bank betrieben, so wird einer solchen MIX-Kaskade fast jeder vertrauen können, da es genügt, wenn er einem Betreiber vertraut. Entsprechendes wie für die Betreiber gilt natürlich auch für die Entwerfer und Produzenten der verwendeten MIXe.

Daß viele Teilnehmer jeweils auch als MIX-Betreiber fungieren, ist nach dem in Abschnitt 3.2.2.4 Gesagten sowieso unmöglich.

4.2.3.2 Verschieden sichere Schlüsselerzeugung beim DC-Netz

Wie schon in Abschnitt 3.2.3 unter dem Stichpunkt „Implementierung der Pseudozufallszahlengeneratoren“ erwähnt wurde, kann die Bandbreite eines DC-Netzes in verschiedene Bereiche eingeteilt werden, in denen jeweils verschieden sicher erzeugte Schlüssel verwendet werden.

Beispielsweise könnten in allernächster Zukunft für elektronische Post echte Zufallszahlen oder kryptographisch starke Pseudozufallszahlenfolgen, für andere schmalbandige Dienste wie Telefon auf (verallgemeinertem, vgl. Anhang) DES basierende Pseudozufallszahlenfolgen und für breitbandige Dienste auf nichtlinear rückgekoppelten Schieberegistern basierende verwendet werden (vgl. Abschnitte 2.2.2.1, 2.2.2.2 und 2.2.2.3). Mit der Weiterentwicklung der Kryptosysteme, ihrer Implementierungen und der verfügbaren Implementierungs-„Technologie“ können (und sollten) dann jeweils sicherer erzeugte Schlüssel „nachgerüstet“ werden.

4.2.4 Kombination von Grundverfahren für besonders sensitiven Verkehr

In diesem Abschnitt wird behandelt, wie auch bei Verwendung eines einheitlichen Übertragungsnetzes Dienste, die weniger hohe Leistungsanforderungen stellen, mit anderen Protokollen behandelt werden können, um noch stärkeren Datenschutz zu garantieren.

Es bietet sich insbesondere an, zusätzlich zum Schutz der Kommunikationsbeziehung durch MIXe auch den Empfänger durch Verteilung zu schützen bzw. RING- oder BAUM-Netz durch überlagerndes Senden zu ergänzen.

4.2.4.1 MIX-Netz und Verteilung

Wird das MIX-Netz für besonders sensitiven Verkehr mit Verteilung kombiniert, so wird nicht nur der erzielbare Schutz größer (Schutz des Empfängers zusätzlich zum Schutz der Kommunikationsbeziehung), sondern es kann auch beim MIX-Netz erheblicher Aufwand eingespart werden.

Wie in Abschnitt 2.5.2.3 hergeleitet wurde, muß beim MIX-Netz (ohne Verteilung) – um gegenseitige Anonymität zwischen Sender und Empfänger zu garantieren – die Verschlüsselung aus einem äußeren Senderanonymitätsteil und einem inneren Empfängeranonymitätsteil bestehen. Werden nun „letzte Informationseinheiten“ an alle verteilt, so kann der Empfängeranonymitätsteil eingespart werden. Dies kann entweder genutzt werden, um den Verschlüsselungsaufwand und die Zahl der durchlaufenen MIXe, kurz den Aufwand des MIX-Netzes, zu halbieren. Oder es kann genutzt werden, im Senderanonymitätsteil mehr Verschlüsselungen und zu durchlaufende MIXe vorzusehen und dadurch den Schutz des Senders zu steigern.

In jedem Fall fallen alle wesentlichen Probleme beim Ausfall eines MIXes (vgl. Abschnitt 2.5.2) weg: Rückadressen sind bei Verwendung von Verteilung „letzter Informationseinheiten“ ganz normale implizite Adressen. Einerseits werden diese durch den Ausfall von MIXen nicht unbrauchbar, andererseits können sie beliebig oft verwendet werden, sollten erste Versuche am Ausfall von MIXen oder des Verteilnetzes scheitern. Entsprechendes gilt, wenn statt Verteilung

partielle Verteilung (multicast) und damit eine Kombination aus expliziter und impliziter Adressierung, etwa in einem Vermittlungs-/Verteilnetz (vgl. Abschnitt 4.3), verwendet wird.

4.2.4.2 Überlagerndes Senden auf RING- und BAUM-Netz

Wie in den Abschnitt 2.5.3.2 erwähnt wurde, kann RING- und BAUM-Netz um überlagerndes Senden erweitert werden. Dies kann natürlich nicht nur bezüglich der ganzen Bandbreite, sondern auch bezüglich eines Teiles und damit früher oder mit sicherer erzeugten Schlüsseln geschehen, vgl. Abschnitte 2.2.2.3, 2.5.3.1, 3.2.3 und 4.2.3.2.

Wie schon in Abschnitt 2.5.3.2 erwähnt und in den Abschnitten 3.2.3 und 3.3.3 ausführlich diskutiert wurde, ist die Topologie des BAUM-Netzes für überlagerndes Senden geeigneter als die des RING-Netzes. Dafür ist bei der Erweiterung des BAUM-Netzes um überlagerndes Senden zusätzlicher Aufwand für eine Synchronisation des Überlagerns von Informationseinheiten und Schlüsseln nötig, vgl. Abschnitt 3.2.3. Beim RING-Netz kann das Übertragungsnetz in trivialer Weise zur Synchronisation verwendet werden.

4.3 Hierarchische Kommunikationsnetze

Die in Abschnit 4.2 beschriebenen Möglichkeiten zum effizienten Einsatz der Grundverfahren aus Abschnitt 2.5 erweitern zwar deren Anwendungsspektrum, erlauben aber immer noch keine mit vertretbarem Aufwand heute oder in der näheren Zukunft durchführbare Realisierung eines Kommunikationsnetzes für interaktive Dienste mit hohen Leistungsanforderungen (nach großem Durchsatz und kurzen Verzögerungszeiten) und hoher Teilnehmerzahl. Folglich muß ein Kommunikationsnetz, auf dem solche Dienste möglich sein sollen, bezüglich des Schutzes des Empfängers und Senders in zwei oder mehr Stufen hierarchisch gegliedert werden. Wie in Abschnitt 4.1 erklärt, induziert eine hierarchische Gliederung eine Klasseneinteilung der Teilnehmer bezüglich Anonymität. Dies bedeutet, daß die Teilnehmer nicht mehr unter (fast) allen, sondern nur noch innerhalb ihrer **Anonymitätsklasse** anonym sind. Damit dies den in den Abschnitten 1.3, 1.4 und 2.1 diskutierten Zielen genügt, müssen diese Anonymitätsklassen hinreichend groß sein, so daß negative Folgen nicht statt einem anonymen alle Mitglieder einer Anonymitätsklasse treffen können, vgl. bethlehemitischer Kindermord [Mt 2,16].

Welche technischen Möglichkeiten zur Erzielung möglichst großer Anonymitätsklassen es gibt, wird in den folgenden Unterabschnitten ausführlich diskutiert. Die wichtigen Entscheidungen hierbei sind,

1. ob Hierarchiegrenzen *statisch fest* sind oder an die Verkehrslast *dynamisch adaptiert* werden und
2. ob es bezüglich der Hierarchiegrenzen jeweils nur *eine* oder *mehrere* Anonymitätsklassen gibt.

Beide Entscheidungen sind orthogonal, d. h. es gibt alle vier Kombinationen. Sie werden in der bereits in Bild 48 angeführten Reihenfolge betrachtet.

Da sie für alle Varianten hierarchischer Kommunikationsnetze gültig sind, werden zuvor aber noch einige Bemerkungen über (anonyme) hierarchische Adressen gemacht.

Entsprechend der hierarchischen Struktur des Kommunikationsnetzes sind die verwendeten Adressen ebenfalls mehrstufig: Wird auf einer Stufe des hierarchischen Kommunikationsnetzes verteilt, so können auf der entsprechenden Adressierungsstufe implizite Adressen verwendet werden. Anderenfalls müssen explizite Adressen verwendet werden.

Entsprechend dem in den Abschnitten 2.5.1 und 3.1.1 Gesagtem wird *verdeckte* implizite Adressierung dabei nur bei *öffentlichen* Adressen verwendet. Diese Verwendung verdeckter impliziter Adressierung ist bei breitbandigen Diensten und Telefon höchstens beim Kanalaufbau nötig. Hierfür gibt es genügend schnelle Implementierungen von asymmetrischen Konzelationssystemen, vgl. Abschnitt 2.2.2.3. Für die Übertragung von Folgenachrichten kann dann offene Adressierung mit privaten Adressen verwendet werden.

Explizite Adressen sollten, wenn sie Verteilungsstufen (insbesondere die des Senders) durchlaufen, nicht von Unbefugten interpretiert werden können. Dies kann beispielsweise dadurch erreicht werden, daß sie von der Teilnehmerstation des Senders mit einem öffentlich bekannten Chiffrierschlüssel der ersten, die explizite Adresse verwendenden Station verschlüsselt werden. In Anlehnung an die Begriffsbildung in Abschnitt 2.5.1 wird dies mit **verdeckter expliziter Adressierung** bezeichnet.

Pakete und Nachrichten werden mittels dieser Adressen abschnittsweise übermittelt. Hierzu kann eine Zwischenspeicherung in Hierarchiegrenzen überbrückenden **Protokollumsetzern** (gateways) nötig sein.

Ebenso werden Kanäle von den Protokollumsetzern aus den Kanälen einzelner Hierarchieebenen zusammengesetzt.

Beides wird im folgenden nur noch da explizit erwähnt, wo es Optimierungen ermöglicht oder attraktiver macht.

4.3.1 Statisch feste Hierarchiegrenze

Für eine statisch feste Hierarchiegrenze spricht, daß sie

+ konzeptionell sehr einfach ist,
+ entsprechend leicht durch eine passende physische Gestaltung des Kommunikationsnetzes unterstützt werden kann und
+ mit allen Grundverfahren aus Abschnitt 2.5 gleichermaßen gut kombinierbar ist.

4.3.1.1 Eine Anonymitätsklasse bezüglich Hierarchiegrenze

Für eine Anonymitätsklasse bezüglich einer Hierarchiegrenze spricht, daß dies

+ konzeptionell sehr einfach ist und
+ entsprechend der Aufwand auf die Lösung einer Aufgabe konzentriert wird.

Letzteres ist insbesondere dann, wenn die Entwurfskosten hoch verglichen mit den Reproduktionskosten sind, ein entscheidender Vorteil.

Für eine statisch feste Hierarchiegrenze kombiniert mit einer Anonymitätsklasse bezüglich der Hierarchiegrenze spricht, daß bei der Benutzung solch eines Netzes keine Fehler bezüglich der Anonymität gemacht werden können: jeder Teilnehmer ist bezüglich des Sendens und Empfangens jeweils in ein und derselben Anonymitätsklasse anonym. Da bei interaktiven Diensten ein Angreifer schließen kann, daß der Teilnehmer in der Schnittmenge beider Anonymitätsklassen liegt, und es bezüglich der Hierarchiegrenze nur eine Anonymitätsklasse gibt, scheint es sehr sinnvoll zu sein, die Hierarchiegrenze bezüglich Senden und Empfangen gleich zu wählen, so daß dann auch die induzierten Anonymitätsklassen gleich sind.

Entsprechend ist diese der vier Kombinationsmöglichkeiten mit den gerade motivierten zusätzlichen Einschränkungen die älteste vorgeschlagene [Pfit_83].

Im folgenden wird zunächst der Fall untersucht, daß auf beiden Seiten der Hierarchiegrenze verschiedene Übermittlungskonzepte verwendet werden; danach der, daß auf beiden Seiten verteilt wird.

4.3.1.1.1 Vermittlungs-/Verteilnetz

Solange die spezielle Natur und Benutzung der Teilnehmerstationen noch unbekannt ist, scheint die vernünftigste Definition der „Datenschutz-Qualität“ eines Kommunikationsnetzes mit Schutz von Sender und Empfänger die zu sein, unter wieviel Teilnehmerstationen Sender und Empfänger von Informationseinheiten bei gegebenem Aufwand anonym bleiben können.

Die einfachste und für viele Fälle auch effizienteste Realisierung einer Hierarchie bezüglich Schutz von Sender und Empfänger ist ein **Vermittlungs-/Verteilnetz**, das folglich gemäß obiger Definition die größtmögliche „Datenschutz-Qualität“ besitzt [Pfit_83, Pfi1_83, Pfit_84, Pfi1_85]. Das Vermittlungs-/Verteilnetz besteht aus Verteilnetzen im Teilnehmeranschlußbereich und einem Vermittlungsnetz, das diese Verteilnetze verbindet (Bild 49, oben). Die Verteilnetze werden so groß realisiert, wie dies bei gegebenem Aufwand möglich ist. Das Vermittlungsnetz kann beim Vermittlungs-/Verteilnetz ohne Rücksicht auf den Datenschutz nach Leistungsgesichtspunkten gebaut werden und verwendet etwa explizite Adressen zur Vermeidung globaler Verteilung. Es sollte den Datenschutz aber soweit möglich unterstützen.

Beispielsweise können die Vermittlungszentralen einfacher und weniger flexibel sein als in den geplanten Netzen, da in einem Datenschutz garantierenden Netz ohnehin viele Funktionen in die Teilnehmerstationen ausgelagert werden, die in den geplanten Netzen für die Vermittlungszentralen vorgesehen sind. Dadurch kann die Überprüfung der Vermittlungszentralen auf Trojanische Pferde durch den Netzbetreiber oder gar Datenschutzbeauftragte lohnender sein, insbesondere falls man auf die freie Speicherprogrammierbarkeit verzichtete, so daß heimliche Systemänderungen erschwert würden (vgl. Abschnitt 2.1.2).

Ohne Einführung mehrerer Anonymitätsklassen bezüglich der Hierarchiegrenze können, sofern leistungsfähige und preiswerte MIXe verfügbar und die Teilnehmerstationen zu den nötigen Verschlüsselungen in der Lage sind, die in jedem Verteilnetz gesendeten Informationseinheiten jeweils eine zugehörige MIX-Kaskade (vgl. Abschnitt 4.2.3.1) durchlaufen.

In jedem Fall tragen jedoch die Verteilnetze die Hauptlast der Anonymisierungsmaßnahmen. Sie können entsprechend den gegebenen Anforderungen hinsichtlich Leistung und Kosten und

in Abhängigkeit von (bei der Bebauungsart des zu verkabelnden Gebietes) zu erwartenden Angreifern durch physikalische Ringe als RING-Netz bzw. physikalische Bäume als BAUM-Netz oder durch überlagerndes Senden in einer dafür geeigneten Topologie realisiert werden. Um die beispielsweise für diensteintegrierende Netze geforderte sehr hohe Netzverfügbarkeit zu erreichen, müssen allerdings insbesondere die Verteilnetze noch um Fehlertoleranz-Maßnahmen erweitert werden, ohne dadurch den Datenschutz zu untergraben. Wie dies geschehen kann, wird in Kapitel 5 beschrieben.

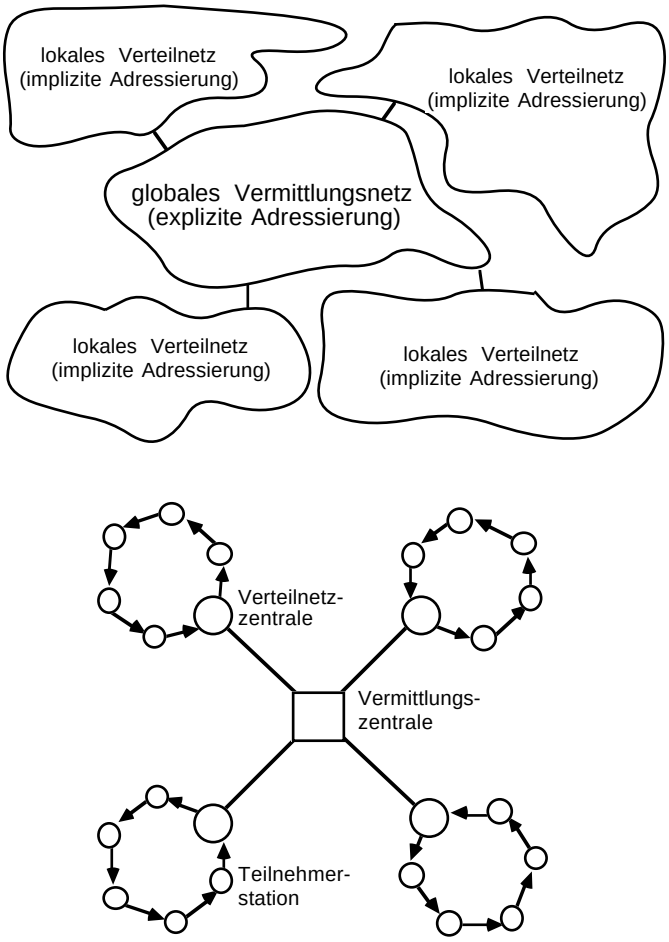

Bild 49: Allgemeine physikalische Struktur des Vermittlungs-/Verteilnetzes (oben) und eine günstige Topologie (unten)

Hält man das in Abschnitt 2.2.3.2 für das RING-Netz beschriebene Angreifermodell für realistisch, ist also die in Bild 49 unten dargestellte Topologie (Ringstruktur im Teilnehmeranschlußbereich) günstig.

Genügend schnelle Übertragungssysteme zur Implementierung von Ringstrukturen sind im Laborstadium verfügbar [BeEn_85], die Realisierung eines Vermittlungs-/Verteilnetzes mit dem Verfahren des RING-Netzes also möglich. Die Ergebnisse erster Übertragungsleistungs-, Zuverlässigkeits- und Kostenuntersuchungen [Pfi1_83, Bürl_84, Bürl_85, Mann_85, Papa_84] lassen für diese Netze ein in etwa gleichgroßes Leistung/Kosten-Verhältnis wie für die üblichen reinen Vermittlungsnetze erwarten.

Entsprechendes gilt für BAUM-Netze.

Möchte man auch bei Umzingelung einzelner Teilnehmerstationen den Sender von Nachrichten verbergen, muß man das in Abschnitt 2.2.3.1 beschriebene überlagernde Senden mit Hilfe paarweise gemeinsamer Schlüssel verwenden, für das es gemäß Abschnitt 3.3.3 günstigere Topologien als Ringstrukturen im Teilnehmeranschlußbereich gibt.

Realisiert man im Teilnehmeranschlußbereich digitale Signalregenerierung auf einer geeigneten Übertragungstopologie, so kann diese – wie in Abschnitt 2.5.3.2 erwähnt – mit überlagerndem Senden kombiniert werden.

Entsprechend der Bemerkung über (anonyme) hierarchische Adressen in Abschnitt 4.3 erhält im Vermittlungs-/Verteilnetzes jede Nachricht als Adresse eine explizite Adresse des Verteilnetzes des Empfängers und eine implizite Adresse des Empfängers innerhalb seines Verteilnetzes.

Nach dem in Abschnitt 4.3 bereits genannten Prinzip sollte beim Vermittlungs-/Verteilnetz die für das Vermittlungsnetz bestimmte explizite Adresse des Verteilnetzes des Empfängers für die übrigen Teilnehmerstationen des Verteilnetzes des Senders unkenntlich gemacht werden. Da die implizite Adresse erst nach der expliziten benötigt wird, kann dies in der Form geschehen, daß die Teilnehmerstation des Senders die vollständige Adresse mit einem öffentlich bekannten Chiffrierschlüssel des Vermittlungsnetzes verschlüsselt.

Bezüglich der Beobachtbarkeit der Kommunikation entspricht ein Vermittlungs-/Verteilnetz der „klassischen“ Situation, daß zwischen Großrechnern, die von sehr vielen Teilnehmern gleichzeitig genutzt werden, Ende-zu-Ende-verschlüsselt kommuniziert wird [VoKe_83]. Hierbei ist unterstellt, daß der Angreifer die Großrechner nicht soweit unterwandern kann, daß er von ihnen Verkehrsdaten einzelner Teilnehmer oder fremde Nutzdaten erhält.

Nach diesen allgemeinen Überlegungen ist es lohnend, einige spezielle Optimierungen zu betrachten, die bei den lokalen Verteilnetzen möglich sind. Die lokalen Verteilnetze sind über **Verteilnetzzentralen**, die als Protokollumsetzer fungieren, mit dem Vermittlungsnetz verbunden. Diese Verteilnetzzentralen empfangen und senden einen erheblichen Teil aller im lokalen Verteilnetz übertragenen Informationseinheiten, benötigen dabei aber keinen Schutz ihres Empfangens oder Sendens.

Wird ein RING-Netz mit umlaufenden Übertragungsrahmen (ÜR) als lokales Verteilnetz verwendet, so kann die Verteilnetzzentrale Übertragungsrahmen, deren Inhalt sie korrekt empfangen hat und die sie zum globalen Vermittlungsnetz weiterleitet, als leer kennzeichnen oder sofort selbst füllen. Eine Kombination hiervon und dem in Abschnitt 3.1.4.3 beschriebenen Ringzugriffsprotokoll zur Realisierung von Duplex-Kanälen durch fortlaufende Benutzung je eines ÜR erlaubt sehr effiziente Kanalvermittlung im Vermittlungs-/Verteilnetz.

Wird ein DC-, RING-2-f- oder BAUM-Netz als lokales Verteilnetz verwendet, so sollte die Verteilnetzzentrale die im Verteilnetz gesendeten Informationseinheiten als erster empfangen. Dann kann sie sie einerseits möglichst früh weiterleiten und hat andererseits die Kontrolle über den Verteilkanal. Im Verteilkanal braucht sie dann Informationseinheiten, die nicht für das lokale Verteilnetz bestimmt sind, nicht zu senden, so daß sie – je nach Mehrfachzugriffsprotokoll –

deren „Bandbreite“ zur Verteilung von aus dem Vermittlungsnetz ankommenden Informationseinheiten (inkl. Massenkommunikation) verwenden kann. Wie bereits in [Pfi1_85 Seite 62] erwähnt, muß die Verteilnetzzentrale den am Mehrfachzugriffsprotokoll beteiligten Stationen die Kontrollinformation des Mehrfachzugriffsprotokolls natürlich zukommen lassen. Da dies bei den meisten Protokollen von Abschnitt 2.5.3.2.2 bzw. 3.1.2 nur wenige Bits sind, fällt dies kaum ins Gewicht.

Allerdings sei darauf hingewiesen, daß dann beim überlagernden Senden Mehrfachzugriffsprotokolle mit viel Kontrollinformation nicht anwendbar sind: Weder ist bei einem Kanal mit kurzer Verzögerungszeit die Regel anwendbar, daß nur gesendet werden darf, wenn auf dem Kanal gerade keine Übertragung stattfindet (CSMA), noch ist bei Kollisionsauflösungsalgorithmen eine deterministische Auflösung von Kollisionen möglich. Globales Überlagerndes Empfangen ist aber weiterhin möglich: Zwar kann nur die Verteilnetzzentrale „globales“ überlagerndes Empfangen praktizieren, da sie aber den Verteilkanal kontrolliert, kann sie, nachdem sie global überlagernd empfangen hat, die Informationseinheiten entweder in ihr lokales Verteilnetz oder in das globale Vermittlungsnetz weiterleiten.

Wie in Abschnitt 2.6 erläutert wurde, können Verteilung, MIX-, DC- und sogar RING- und BAUM-Netz als *virtuelle*, d. h. in fast beliebigen Schichten implementierbare Konzepte betrachtet werden. Entsprechendes gilt für das Vermittlungs-/Verteilnetz (wie auch für alle anderen, im folgenden beschriebenen hierarchischen Kommunikationsnetze) [Pfi1_85 Seite 63].

Deshalb kann und sollte man sich zuletzt fragen, warum die Stationen von Teilnehmern, die *räumlich* nahe beieinander sind, in einem lokalen Verteilnetz zusammengefaßt werden – und nicht die von bezüglich ihres Kommunikationsverhaltens *ähnlichen* Teilnehmern. Beispielsweise arbeiten viele Studenten höherer Semester einige Stunden später am Tag als die meisten anderen Leute oder lesen andere Zeitungen als Arbeiter. Wird beispielsweise die BILD-Zeitung um 6 Uhr früh in einem lokalen Verteilnetz bestellt, das 999 Studenten und einen Arbeiter verbindet, so ist ziemlich klar, wer dies veranlaßte. Die Antwort auf obige Frage ist, daß diese lokalen Verteilnetze durch lokale Netze (LANs) weit effizienter implementiert werden können als durch Weitverkehrsnetze (WANs) mit Verteilung. So kann man hoffentlich mit einer technisch effizienten Version unseres gerade erwähnten lokalen Verteilnetzes nicht nur 999 Studenten, sondern zusätzlich noch 999 Arbeiter verbinden. Dies erscheint vielversprechender, als einander ähnliche Teilnehmer in kleinen „virtuellen“ Verteilnetzen zusammenzuschließen. Denn ich habe weder eine kanonische Definiton, was ähnliche Teilnehmer sind (einander in einer Hinsicht ähnliche Teilnehmer können in anderer Hinsicht sehr verschieden sein), noch ein kanonisches Maß für Unbeobachtbarkeit von Teilnehmern, das Ähnlichkeiten zwischen Teilnehmern berücksichtigt.

4.3.1.1.2 Verteil-/Verteilnetz

Neben der im vorherigen Abschnitt erwähnten, anzustrebenden Vergrößerung der Verteilnetze eines Vermittlungs-/Verteilnetzes kann man sich auch bemühen, die Verkehrsanalyse in der oberen Hierarchiestufe eines zweistufigen hierarchischen Netzes zu verhindern oder zumindest zu erschweren, indem auch sie durch ein Verteilnetz realisiert wird [Pfi1_83 Seite 66f]. Dadurch entsteht ein Verteil-/Verteilnetz (Bild 50).

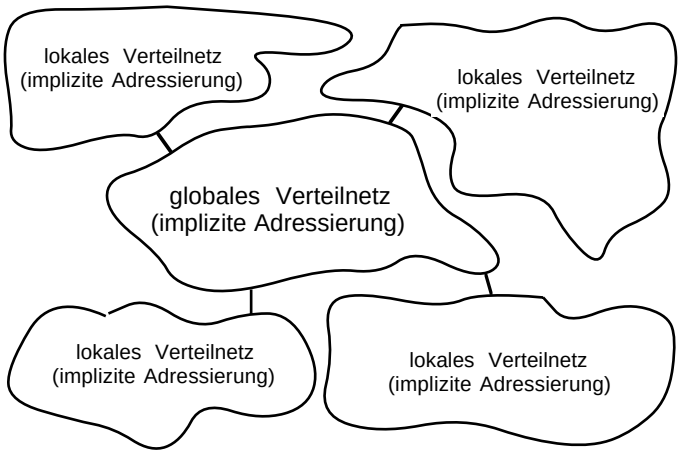

Bild 50: Allgemeine physikalische Struktur des Verteil-/Verteilnetzes

Die Realisierung des globalen Verteilnetzes ist jedoch nur dann lohnend, wenn darin überlagerndes Senden zum Schutz des Senders angewandt wird (denn Unbeobachtbarkeit der Leitungen im Fernnetz ist unrealistisch) und die Verteilnetzzentralen, die als Protokollumsetzer (gateway) zwischen dem äußerst breitbandigen globalen Verteilnetz und den weniger breitbandigen lokalen Verteilnetzen agieren, verschiedene Betreiber haben oder einem verändernden Zugriff des Betreibers durch geeignete Gehäuse entzogen werden können. Hierbei gelten die in Abschnitt 2.1.2 gemachten Bemerkungen sinngemäß: die Realisierung solcher Gehäuse ist noch sehr teuer und erschwert die Wartung der Anlage noch übermäßig. Zusätzlich muß ausgeschlossen werden, daß die Verteilnetzzentralen von Anfang an Trojanische Pferde enthalten, vgl. Abschnitt 2.1.2. Ist dies nicht erreichbar, so muß wenigstens eine verdeckte Zusammenarbeit der Trojanischen Pferde dadurch unwahrscheinlich gemacht werden, daß die Verteilnetzzentralen verschiedene Entwerfer und Produzenten haben.

Außerdem können auch die schnellsten, bei Extrapolation der bisherigen Entwicklung in den nächsten zwei Jahrzehnten realisierbaren Verteilnetze den Fernverkehr eines nationalen breitbandigen diensteintegrierenden Netzes, geschweige denn den eines internationalen, nicht bewältigen. Noch viel problematischer ist eine genügend schnelle, aber kryptographisch sichere Erzeugung der zu überlagernden Schlüssel (vgl. Abschnitt 2.2.2.3).

Für die ferne Zukunft, als Spezialnetz oder als untere Stufen eines drei- oder mehrstufigen hierarchischen Netzes können Verteil-/Verteilnetze jedoch geeignet sein, da sie – sofern obige Voraussetzungen in (teilnehmer-)überprüfbarer Weise erfüllt sind – fast die Sender- und Empfängeranonymität eines „flachen“ DC-, RING- oder BAUM-Netzes bieten. Im Gegensatz zu diesen „flachen“ Verteilnetzen müssen beim Verteil-/Verteilnetz fast alle Leitungen, nämlich alle Leitungen in den lokalen Verteilnetzen, und fast alle Stationen, nämlich alle Teilnehmerstationen, nicht mit der Bitrate des globalen Verteilnetzes arbeiten. Deshalb dürfte ein Verteil-/Verteilnetz weit weniger aufwendig als ein entsprechendes „flaches“ Verteilnetz sein [Pfi1_85 Seite 64].

Entsprechend der Bemerkung über (anonyme) hierarchische Adressen in Abschnitt 4.3 erhält im Verteil-/Verteilnetzes jede Nachricht als Adresse eine implizite Adresse des Verteilnetzes des Empfängers und eine implizite Adresse des Empfängers innerhalb seines Verteilnetzes.

4.3.1.2 Mehrere Anonymitätsklassen bezüglich Hierarchiegrenze

Mehrere Anonymitätsklassen bezüglich einer Hierarchiegrenze entstehen, wenn in der *übergeordneten* Hierarchieebene verschiedene Maßnahmen zum Schutz der Verkehrs- und Interessensdaten ergriffen werden, wenn es sich also mit anderen Worten bei der übergeordneten Hierarchieebene um ein (bezüglich Schutz) *heterogenes* Kommunikationsnetz handelt.

Bei *wählbaren Anonymitätsklassen* muß sich jeder Teilnehmer darüber im Klaren sein, daß, sofern für einen Angreifer verkettbare Verkehrsereignisse mit verschiedenen Maßnahmen zum Schutz der Verkehrs- und Interessensdaten geschützt werden, die erzielte Anonymität nur dem Durchschnitt aller jeweils gewählten Anonymitätsklassen entspricht. Identifiziert sich ein Teilnehmer nicht explizit, so entspricht die minimale Anonymität aber in jedem Fall der des untergeordneten Verteilnetzes. Insbesondere bei einer statisch festen Hierarchiegrenze kann damit ein vorgegebenes Minimum nicht unterschritten werden, das jedoch etwa bei einem heterogenen untergeordneten Verteilnetz gemäß Abschnitt 4.2.3 nicht allzu hoch liegen muß.

Insbesondere bei einer statisch festen Hierarchiegrenze bieten sich folgende Möglichkeiten für einen variablen Schutz der Verkehrs- und Interessensdaten in der übergeordneten Hierarchieebene an:

In einem Vermittlungsnetz können MIXe für manche Dienste bzw. besonders sensitiven Verkehr den Datenschutz wesentlich erhöhen, wodurch ein **Vermittlungs∨MIX-/Verteilnetz** entsteht. Die effizienzsteigernde Maßnahme fest vorgegebener MIX-Kakaden aus Abschnitt 4.2.3.1 kann selbstverständlich angewendet werden.

In einem Verteilnetz können natürlich entsprechend Abschnitt 4.2.3.2 Schlüssel verschieden sicher erzeugt oder gemäß Abschnitt 4.2.4.2 überlagerndes Senden und digitale Signalregenerierung für manche Dienste bzw. besonders sensitiven Verkehr kombiniert werden. Im Fall der Kombination ensteht beispielsweise entweder ein **RING-∨DC-/Verteilnetz** oder ein **BAUM-∨DC-/Verteilnetz**.

4.3.2 Dynamisch an Verkehrslast adaptierbare Hierarchiegrenze

Eine dynamisch an die Verkehrslast adaptierbare Hierarchiegrenze hat – wie zu erwarten – entgegengesetzte Eigenschaften wie eine statisch feste: Eine dynamisch adaptierbare Hierarchiegrenze ist

- konzeptionell komplizierter,
- entsprechend schwieriger (sprich: aufwendiger) durch eine passende physische Gestaltung des Kommunikationsnetzes zu unterstützen und
- nicht mit allen Grundverfahren aus Abschnitt 2.5 gleichermaßen gut kombinierbar.

Andererseits kann man hoffen, durch die dynamische Grenze das Kommunikationsnetz insgesamt wesentlich effizienter nutzen zu können. Sei dies, indem

+ bei geringem Verkehr größerer Schutz von Sender- und/oder Empfänger geboten wird oder
+ wesentlich mehr Verkehr, dann aber bei geringerem Schutz von Sender- und/oder Empfänger abgewickelt werden kann.

Allerdings sind beide Vorteile zu relativieren:

Werden die Anonymitätsklassen bezüglich Senden und Empfangen bei vom Angreifer verkettbaren Verkehrsereignissen verschieden groß gewählt, so liegt der Beobachtete in der Schnittmenge aller Anonymitätsklassen. Hieraus folgt, daß die *Anonymitätsklassen immer so gewählt werden sollten, daß kleinere vollständig in der nächstgrößeren enthalten sind.* Wie im folgenden deutlich wird, ist dies nicht nur für die Anonymität nützlich, sondern auch besonders unaufwendig zu realisieren.

Ein Angreifer kann zumindest in seiner Umgebung durch Erzeugen „unnötigen“ Verkehrs die Anonymitätsklassen klein halten. Dies ist allerdings von allen Betroffenen (genauer: ihren Teilnehmerstationen) wahrnehmbar und ggf. über Maßnahmen der Abrechnung (vgl. Abschnitt 7.2) zu begrenzen.

Wie bei der statisch festen Hierarchiegrenze wird auch hier zuerst der Fall untersucht, daß es bezüglich der Hierarchiegrenze nur eine Anonymitätsklasse gibt, und danach erst der allgemeine Fall.

4.3.2.1 Eine Anonymitätsklasse bezüglich Hierarchiegrenze

Wie in Abschnitt 4.3.1.1 spricht für eine Anonymitätsklasse bezüglich einer Hierarchiegrenze, daß dies

+ konzeptionell einfacher ist und
+ entsprechend der Aufwand auf die Lösung einer Aufgabe konzentriert wird.

Letzteres ist insbesondere dann, wenn die Entwurfskosten hoch verglichen mit den Reproduktionskosten sind, ein entscheidender Vorteil.

Für eine dynamisch an die Verkehrslast adaptierbare Hierarchiegrenze kombiniert mit einer Anonymitätsklasse bezüglich dieser Hierarchiegrenze spricht, daß bei der Benutzung solch eines Netzes keine Fehler bezüglich der Anonymität gemacht werden können, sofern – wie oben empfohlen – die *Anonymitätsklassen immer so gewählt werden, daß kleinere vollständig in der nächstgrößeren enthalten sind*: jeder Teilnehmer ist bezüglich des Sendens und Empfangens jeweils in der momentan größtmöglichen Anonymitätsklasse anonym. Da bei interaktiven Diensten ein Angreifer schließen kann, daß der Teilnehmer in der Schnittmenge beider Anonymitätsklassen liegt, und es bezüglich der Hierarchiegrenze nur eine Anonymitätsklasse gibt, scheint es sehr sinnvoll zu sein, die Hierarchiegrenze bezüglich Senden und Empfangen gleich zu wählen, so daß dann auch die induzierten Anonymitätsklassen gleich sind.

Im folgenden wird zunächst erläutert, wie ein DC-Netz effizient dynamisch partitioniert werden kann, so daß in jeder Partition Informationseinheiten anonym und autonom gesendet werden können. Diese Partitionierbarkeit eines Verteilnetzes mit Schutz des Senders ist eine Voraussetzung für eine dynamisch an die Verkehrslast adaptierbare Hierarchiegrenze.

Danach wird wieder zunächst der Fall untersucht, daß auf beiden Seiten der Hierarchiegrenze verschiedene Übermittlungskonzepte verwendet werden; danach der, daß auf beiden Seiten verteilt wird.

4.3.2.1.1 Dynamisch partitionierbares DC-Netz

Um ein DC-Netz effizient dynamisch partitionieren und dadurch in jedem Teil Informationseinheiten anonym und autonom senden zu können, muß eine Partitionierung bezüglich aller in Bild 30 gezeigten und in den Abschnitten 3.1.2, 3.2.3 und 3.3.3 beschriebenen Schichten erfolgen.

Im wesentlichen bedeutet dies, daß die Übertragungstopologie des DC-Netzes effizient partitionierbar gewählt werden und eine jeweils dazu passende Überlagerungstopologie definiert sein muß. Ebenso ist der Schlüsselaustausch so zu gestalten, daß bei jeder Partitionsmöglichkeit des DC-Netzes einerseits in jedem Teil genügend viele, einen Zusammenhang aller Teilnehmer garantierende Schlüssel ausgetauscht wurden und andererseits natürlich alle gerade überlagerten Schlüssel jeweils paarweise im selben Teil liegen. Denn nur dann können in jedem Teil Informationseinheiten anonym und autonom gesendet werden. Mit anderen Worten: Damit in den Teilen des DC-Netzes jeweils parallel kommuniziert werden kann, muß die *Schlüsseltopologie* zur Partitionierung passen. Da es keinen wesentlichen Aufwand verursacht, zu jeder möglichen Partitionierung des DC-Netzes jeweils separate Schlüssel auszutauschen, ist diese Forderung in trivialer Weise erfüllbar.

Wird die in Abschnitt 3.3.3 empfohlene Baumtopologie als Übertragungs- und Überlagerungstopologie gewählt, so ist diese in kanonischer Weise in Unterbäume partitionierbar. Bild 51 zeigt den für die Anwendung wichtigen Spezialfall, daß eine Partitionierung jeweils von inneren Knoten des Baumes, die von der Wurzel des Baumes gleichweit entfernt sind, durchgeführt wird: jeder dieser inneren Knoten sendet sein (globales) Überlagerungsergebnis nicht an seinen Vaterknoten weiter, sondern verteilt es (statt eines vom Vaterknoten empfangenen) an seine Söhne. In Bild 51 werden die Nachrichten N_1, N_2, N_3 und N_4 gleichzeitig verteilt.

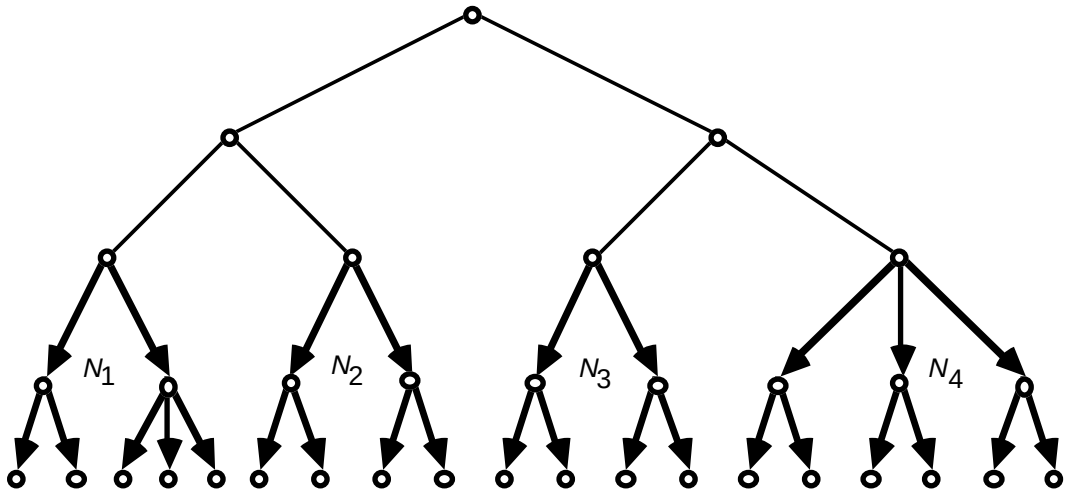

Bild 51: Dynamisch partitionierbares baumförmiges DC-Netz

In einem dynamisch partitionierbaren DC-Netz kann also wahlweise

- mit der größtmöglichen Anonymität (bis auf paarweises überlagerndes Empfangen und Konferenzschaltung, vgl. Abschnitte 3.1.2.5 und 3.1.2.6) maximal mit der Bitrate des DC-Netzes Information gesendet und empfangen werden oder

- mit entsprechend kleineren, durch die Partitionierung induzierten Anonymitätsklassen und damit geringerer Anonymität mit maximal dem Produkt aus der Zahl der Teile und der Bitrate des DC-Netzes. Hierbei kann es je nach Auslegung des dynamisch partitionierbaren DC-Netzes sehr viele verschiedene Partitionierungsmöglichkeiten geben.

Wie in [Pfi1_85 Seite 66ff] beschrieben erlaubt ein zyklisches Umschalten zwischen keiner, globaler und lokaler Partitionierung (ggf. bezüglich der Zeitdauer der jeweiligen Partitionierung mittels Beobachtung des Verkehrs in adaptiver Weise) bereits eine **hierarchische Verwendung**: ohne Partitionierung wird beispielsweise interkontinentaler Kommunikationsverkehr, mit globaler Partitionierung beispielsweise nationaler Kommunikationsverkehr und mit lokaler Partitionierung beispielsweise örtlicher Kommunikationsverkehr abgewickelt – die Wahl einer (echten) Partition entspricht dabei einer Routingfunktion und damit einer expliziten Adresse. Bei der beschriebenen hierarchischen Verwendung können besonders sensitive Nachrichten oder Kommunikationsdienste mit geringem Übertragungsvolumen natürlich in globaleren Partitionierungen als eigentlich nötig abgewickelt werden. Entsprechendes kann auch für mäßig sensitive Nachrichten oder weitere Kommunikationsdienste dann geschehen, wenn das dynamisch partitionierbare DC-Netz gerade nur wenig ausgelastet ist. Sind die globaleren Partitionen so gewählt, daß sie lokalere entweder ganz oder keine ihrer Stationen enthalten, d. h. sind globalere Partitionen *gröbere* als lokale bzw. lokalere *feinere* als globale, so ist die Empfehlung von Abschnitt 4.3.2 befolgt, daß die *Anonymitätsklassen immer so gewählt werden sollten, daß kleinere vollständig in der nächstgrößeren enthalten sind.* Entsprechend kann bei von der Verkehrssituation abhängiger Wahl einer gröberen Partitionierung auch bezüglich vom Angreifer verkettbarer Informationseinheiten keine kleinere Anonymitätsklasse resultieren als ohne.

Schon die physisch bedingte Verzögerungszeit ist in globalen Partitionen größer als in lokalen. Bei geeigneter Realisierung gemäß den Abschnitten 3.2.3 und 3.3.3 stellt dies aber kein Problem dar, sofern jeweils passende Mehrfachzugriffsprotokolle verwendet werden: CSMA/CD (vgl. Abschnitt 3.1.2.3.6) ist etwa für ein weltweites DC-Netz sicherlich ungeeignet. Wirklich problematisch dürfte für die meisten Anwendungen die durch die Überlastung der „globalen Partitionierungszeiten“ entstehenden, unbeschränkten Wartezeiten werden. Dies legt nahe, nicht nur ein bezüglich seiner Übertragungs- und Überlagerungsrate homogenes und damit im engeren Sinne nichthierarchisches DC-Netz hierarchisch zu verwenden, sondern echt hierarchische Kommunikationsnetze zu realisieren. Zwei Möglichkeiten hierzu werden in den folgenden Abschnitten beschrieben, wobei wie üblich mit einem Vermittlungsnetz als oberer Hierarchieebene begonnen und danach ein Verteilnetz als obere Hierarchiebene betrachtet wird.

Der Vollständigkeit halber sei hier noch erwähnt, daß selbstverständlich auch ein BAUM-Netz und sogar ein RING-Netz dynamisch partitioniert werden kann. Beim BAUM-Netz erfolgt dies in vollständiger Analogie zum DC-Netz, beim RING-Netz gemäß dem in Bild 52 veranschaulichten Verfahren der „**Kleeblatt-Ringe**“: Im übergeordeneten RING-Netz benachbarte Stationen sind auch im ihnen untergeordneten RING-Netz in gleicher „Richtung“ benachbart.

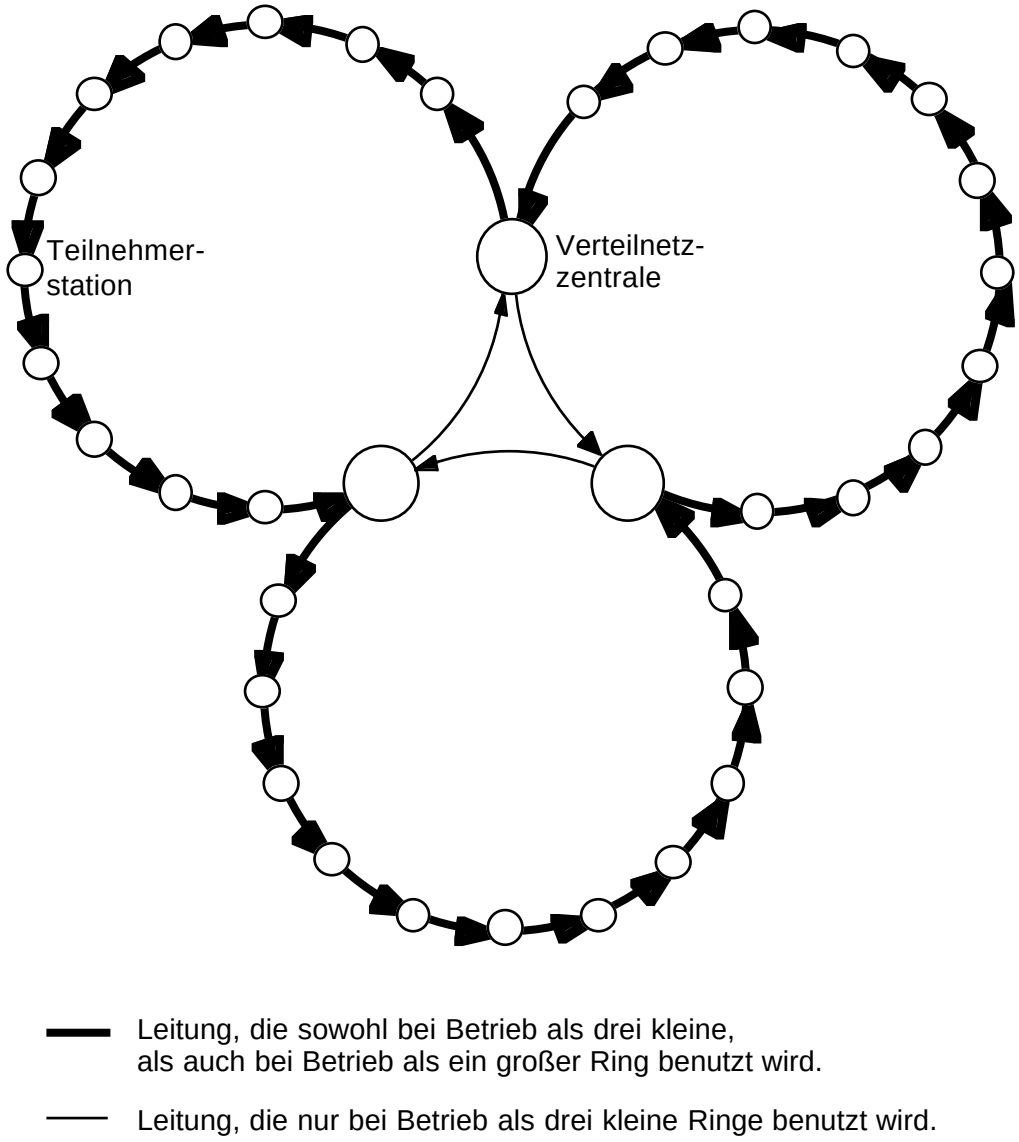

Bild 52: Dynamisch partitionierbares RING-Netz

4.3.2.1.2 Dynamisch adaptierbares Vermittlungs-/DC-Netz

Ein dynamisch adaptierbares Vermittlungs-/DC-Netz erlaubt es, die Grenze zwischen dem globalen Vermittlungsnetz und den lokalen DC-Netzen zu verschieben und damit das Netz als Ganzes an die momentane Verkehrslast zu adaptieren. Ein dynamisch adaptierbares Vermittlungs-/DC-Netz entsteht, indem in einem Vermittlungs-/Verteilnetz (vgl. Abschnitt 4.3.1.1.1) als Verteilnetze dynamisch partitionierbare DC-Netze (vgl. Abschnitt 4.3.2.1.1) verwendet werden und in diesen DC-Netzen jeweils mehrere, in verschiedenen Partitionen liegende Stationen als Protokollumsetzer (gateway) fungieren können. Letzteres verursacht natürlich einigen Aufwand.

Werden baumförmige DC-Netze verwendet, so sollten geschickterweise die der Wurzel des Baumes nahen Stationen als Protokollumsetzer fungieren können (Bild 53).

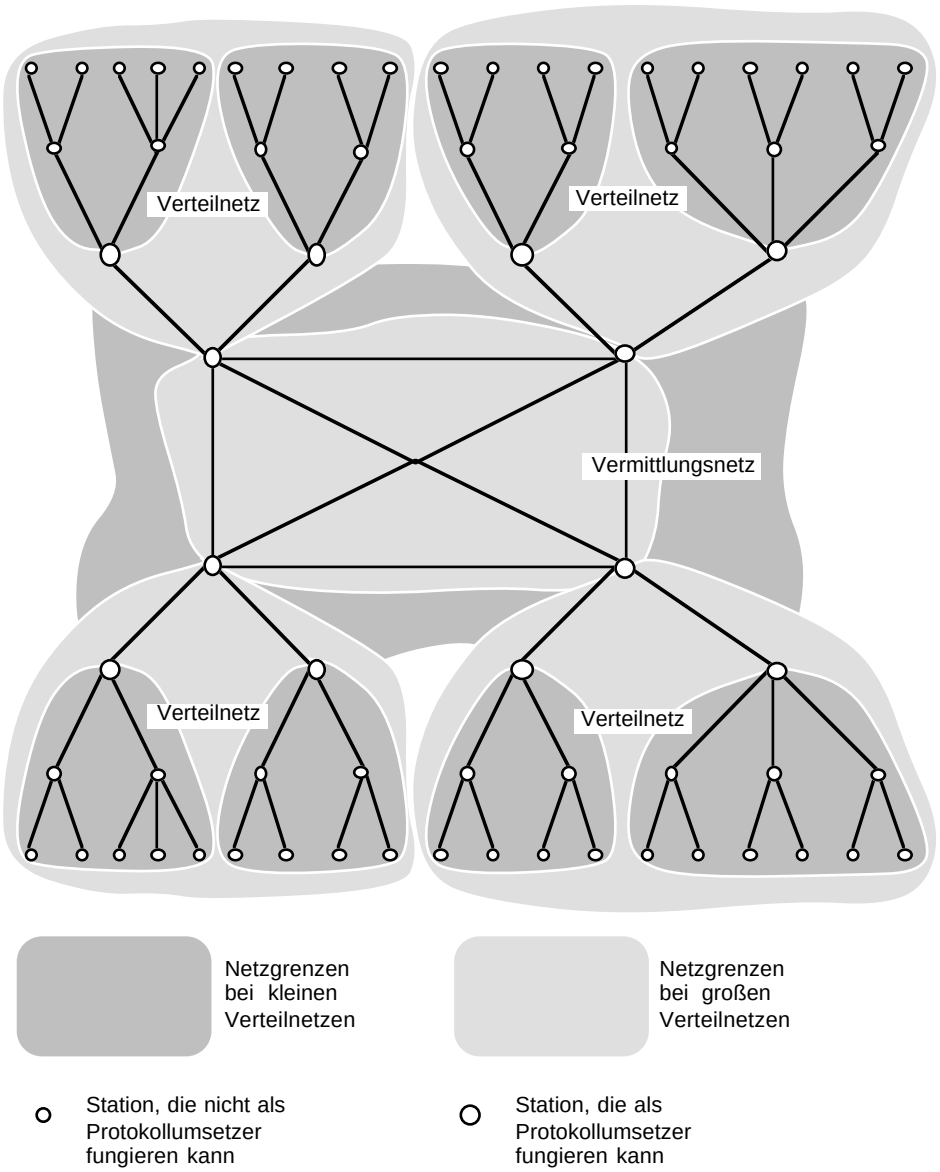

Bild 53: Dynamisch adaptierbares Vermittlungs-/DC-Netz mit dynamisch partitionierbaren baumförmigen DC-Netzen

Zusätzlich zur adaptiven Verschiebung der Grenze zwischen dem globalen Vermittlungsnetz und den lokalen DC-Netzen entsprechend der momentanen Verkehrslast als Ganzem ist es in einem dynamisch adaptierbaren Vermittlungs-/DC-Netz leicht möglich, die Grenze zwischen Vermittlungsnetz und Verteilnetzen für verschieden sensitive und/oder verschieden übertragungsaufwendige Verkehrsklassen verschieden zu wählen. Hierdurch entstehen im dynamisch adaptierbaren Vermittlungs-/DC-Netz verschiedene Verkehrsklassen, aber bezüglich jeder dieser Grenzen nur eine, so daß diese Bemerkung tatsächlich in diesen Abschnitt gehört. Mittels Zeitmultiplex können diese verschiedenen Verkehrsklassen quasi zeitgleich bedient werden.

Natürlich können alle diese verkehrsklassenspezifischen Grenzen zwischen Vermittlungs- und DC-Netz in Abhängigkeit von der Netzbelastung als Ganzem oder dem Verkehrsaufkommen in den einzelnen Verkehrsklassen wiederum dynamisch verschoben werden.

4.3.2.1.3 Dynamisch adaptierbares DC-/DC-Netz

Ein dynamisch adaptierbares DC-/DC-Netz erlaubt es, die Grenze zwischen dem globalen und den lokalen DC-Netzen zu verschieben und damit die Größe der lokalen DC-Netze an deren momentane Verkehrslast zu adaptieren. Ein dynamisch adaptierbares DC-/DC-Netz entsteht, indem in einem Verteil-/Verteilnetz (vgl. Abschnitt 4.3.1.1.2) als lokale Verteilnetze dynamisch partitionierbare DC-Netze (vgl. Abschnitt 4.3.2.1.1) verwendet werden und in diesen lokalen DC-Netzen jeweils mehrere, in verschiedenen Partitionen liegende Stationen als Protokollumsetzer (gateway) zum schnelleren globalen DC-Netz fungieren können. Letzteres verursacht natürlich einigen Aufwand.

Werden baumförmige lokale DC-Netze verwendet, so sollten geschickterweise die der Wurzel des Baumes nahen Stationen als Protokollumsetzer fungieren können (Bild 54).

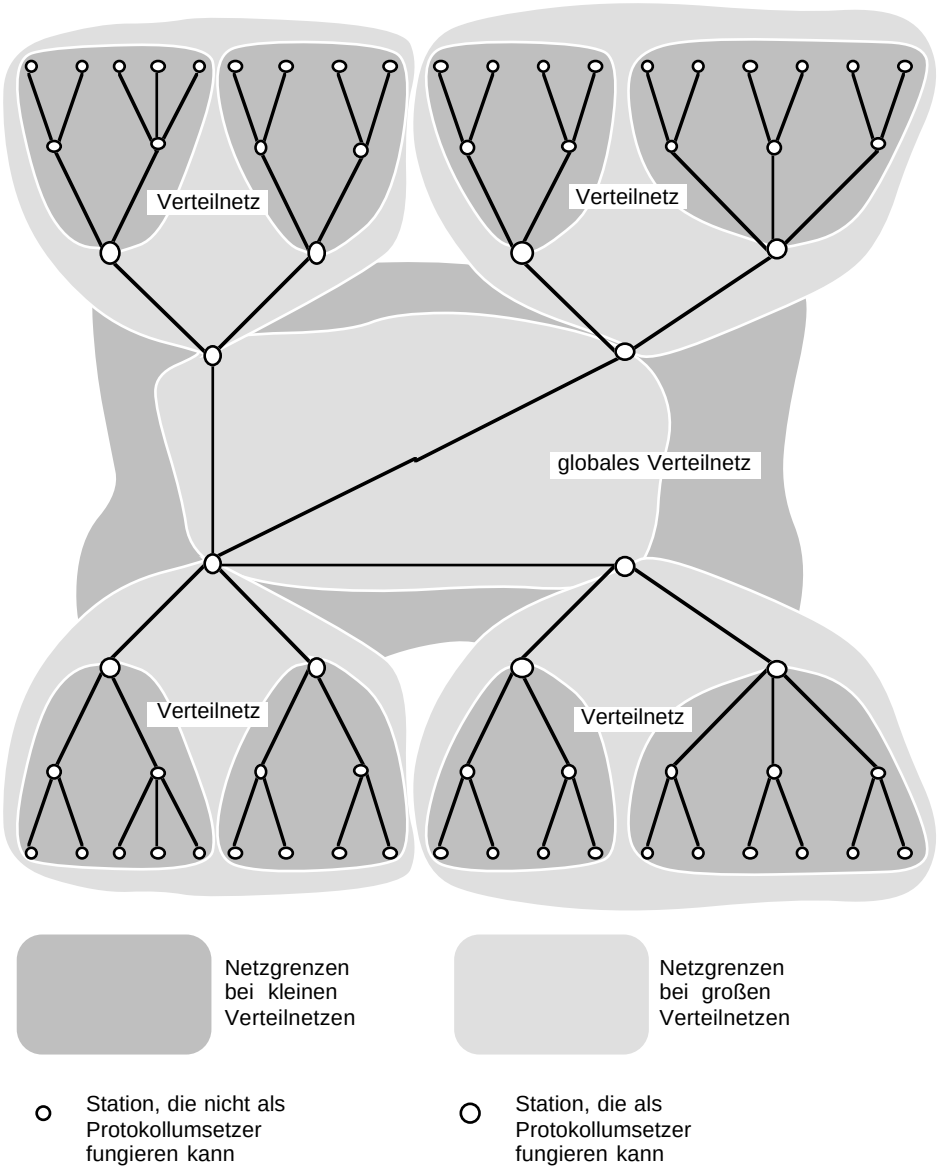

Bild 54: Dynamisch adaptierbares DC-/DC-Netz mit dynamisch partitionierbaren baumförmigen lokalen DC-Netzen

Zusätzlich zur adaptiven Verschiebung der Grenze zwischen dem globalen und den lokalen DC-Netzen entsprechend der momentanen Verkehrslast der lokalen DC-Netze ist es in einem dynamisch adaptierbaren DC-/DC-Netz leicht möglich, die Grenze zwischen globalem und lokalen Verteilnetzen für verschieden sensitive und/oder verschieden übertragungsaufwendige Verkehrsklassen verschieden zu wählen. Hierdurch entstehen im dynamisch adaptierbaren DC-/DC-Netz verschiedene Verkehrsklassen, aber bezüglich jeder dieser Grenzen nur eine, so daß diese Bemerkung tatsächlich in diesen Abschnitt gehört. Mittels Zeitmultiplex können diese verschiedenen Verkehrsklassen quasi zeitgleich bedient werden.

Natürlich können alle diese verkehrsklassenspezifischen Grenzen zwischen globalem und lokalen Verteilnetzen in Abhängigkeit von der lokalen Netzbelastung als Ganzem oder dem Verkehrsaufkommen in den einzelnen Verkehrsklassen wiederum dynamisch verschoben werden.

Die Bemerkungen in Abschnitt 4.3.1.1.2 über die Anwendbarkeit eines Verteil-/Verteilnetzes gelten sinngemäß auch für dynamisch adaptierbare DC-/DC-Netze.

4.3.2.2 Mehrere Anonymitätsklassen bezüglich Hierarchiegrenze

Mehrere Anonymitätsklassen bezüglich einer statisch festen wie auch einer dynamisch adaptierbaren Hierarchiegrenze entstehen, wenn in der *übergeordneten* Hierarchieebene verschiedene Maßnahmen zum Schutz der Verkehrs- und Interessensdaten ergriffen werden, wenn es sich also mit anderen Worten bei der übergeordneten Hierarchieebene um ein (bezüglich Schutz) *heterogenes* Kommunikationsnetz handelt.

Bei *wählbaren Anonymitätsklassen* muß sich jeder Teilnehmer darüber im Klaren sein, daß, sofern für einen Angreifer verkettbare Verkehrsereignisse mit verschiedenen Maßnahmen zum Schutz der Verkehrs- und Interessensdaten geschützt werden, Anonymität nur unter den Teilnehmern erzielt wird, die in allen für die verkettbaren Verkehrsereignisse jeweils gewählten Anonymitätsklassen enthalten sind. Hierbei ist es ohne Belang, ob verschiedene Anonymitätsklassen durch eine dynamisch an die Verkehrslast adaptierte Hierarchiegrenze oder verschiedenen Schutz im übergeordneten Kommunikationsnetz entstehen.

Identifiziert sich ein Teilnehmer nicht explizit, so entspricht die minimale Anonymität aber in jedem Fall der des untergeordneten Verteilnetzes. Insbesondere bei einer dynamisch verschiebbaren Hierarchiegrenze muß darauf geachtet werden, daß damit ein vorgegebenes Minimum nicht unterschritten werden kann.

Bei einer dynamisch verschiebbaren Hierarchiegrenze bieten sich folgende Möglichkeiten für einen variablen Schutz der Verkehrs- und Interessensdaten in der übergeordneten Hierarchieebene an:

In einem Vermittlungsnetz können MIXe für manche Dienste bzw. besonders sensitiven Verkehr den Datenschutz wesentlich erhöhen, wodurch ein **dynamisch adaptierbares Vermittlungs∨MIX-/DC-Netz** entsteht. Die effizienzsteigernde Maßnahme fest vorgegebener MIX-Kakaden aus Abschnitt 4.2.3.1 kann selbstverständlich angewendet werden.

Auch im globalen Verteilnetz eines dynamisch adaptierbaren DC-/DC-Netzes können natürlich entsprechend Abschnitt 4.2.3.2 Schlüssel verschieden sicher erzeugt werden.

5 Fehlertoleranz

Da in einem realen Kommunikationssystem Fehler auftreten, wird in diesem Kapitel untersucht, ob und wie diese unter Erhaltung der Anonymität bzw. Unbeobachtbarkeit der Netzbenutzer toleriert werden können. Es gilt, die Diskrepanz zwischen der *Fehlertoleranz*, die eine globale Sicht des Gesamtsystems und des Zusammenhangs von Verkehrsereignissen erfordern kann, und der *Anonymität*, *Unbeobachtbarkeit* und *Unverkettbarkeit*, die je nur eine lokale Sicht des Gesamtsystems durch die Stationen der Netzbenutzer und den Netzbetreiber erlauben, aufzulösen.

Beispielsweise wären explizite Sender- und Empfänger-Adressen in jeder Informationseinheit für die Fehlertoleranz vorteilhaft (Lokalisierung fehlerhafter Übertragungsstrecken oder Sender, fehlertolerante Wegsuche), würden jedoch sofort Sender und Empfänger jeder Informationseinheit identifizieren.

Fehlertoleranz ist insbesondere bei den Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten aus den Abschnitten 2.5.2 und 2.5.3 nötig, da es sich bei ihnen jeweils um *Seriensysteme im Sinne der Zuverlässigkeit* handelt [Pfi1_85 Seite 70]:

- Alle MIXe einer gewählten Folge von MIXen müssen funktionieren, damit die entsprechend verschlüsselten Informationseinheiten oder Adressen entsprechend entschlüsselt und schlußendlich dem Empfänger in ihm verständlicher Form zugestellt werden können.
- Jede Station eines DC-, RING- oder BAUM-Netzes kann durch fehlerhaftes Verhalten jede Nutzdatenübertragung in ihrem Netz unmöglich machen.

Wird auf Fehler (zumindest innerhalb des Kommunikationsnetzes) nicht reagiert, so gelten die Anonymitäts-, Unbeobachtbarkeits- und Unverkettbarkeitsaussagen samt ihrer Beweise aus Abschnitt 2.5 und Kap. 3 natürlich weiterhin. Solange fehlerhaftes Verhalten von Stationen einem Angreifer nicht mehr Information liefert, als dem beim verwendeten Verfahren „stärkstzulässigen“ Angreifer zugebilligt wird, untergräbt beliebiges fehlerhaftes Verhalten von Stationen im allgemeinen nicht die Anonymität bzw. Unbeobachtbarkeit anderer. Dies ist natürlich bezüglich der eigenen Anonymität bzw. Unbeobachtbarkeit bei beliebigem fehlerhaftem Verhalten nicht der Fall: eine Teilnehmerstation kann etwa in der Weise fehlerhaft werden, daß sie ihre Nachrichten nicht mehr (Ende-zu-Ende-)verschlüsselt und mit einem expliziten Absender versieht.

Auf Fehler nicht zu reagieren ist also für andere Stationen ein bezüglich Anonymität und Unbeobachtbarkeit durchaus akzeptables Verhalten. Die Verfügbarkeit der Kommunikationsdienste dürfte aber wegen der Serieneigenschaft so niedrig sein, daß solche Kommunikationsnetze nicht benutzt und damit ihre Anonymität bzw. Unbeobachtbarkeit auch nicht genutzt werden. Eine explizite, aktive Reaktion auf Fehler ist also unumgänglich, obwohl solch eine Erweiterung der von den Stationen auszuführenden Protokolle durchaus die Anonymität und Unbeobachtbarkeit in subtilerer Weise als im obigen Beispiel (explizite Sender- und Empfänger-Adressen) untergraben kann. (Man betrachte etwa den aktiven Verkettungsangriff über

Betriebsmittelknappheit in Abschnitt 2.6 unter dem Aspekt, daß der Ausfall von Betriebsmitteln auch eine Ursache von Betriebsmittelknappheit sein kann.) Folglich müssen die um eine explizite, aktive Reaktion auf Fehler erweiterten Protokolle bezüglich Datenschutzeigenschaften noch einmal neu untersucht werden.

Dies sei durch das folgende, [Höck_85 Seite 50ff] entnommene **Beispiel zur Auswirkung höherer Protokolle auf Senderanonymitätseigenschaften im RING-Netz** verdeutlicht:

In Abschnitt 3.1.4.1 wurden die zulässigen Aktivitäten eines Angreifers so eingeschränkt, daß sie keine der eingekreisten Stationen zu nicht spezifiziertem Verhalten zwingen dürfen. Man kann also beliebige Aktivitäten erlauben, wenn das Verhalten einer Station vollständig spezifiziert ist. Hierzu müssen die Protokolle um eine Reaktion auf Fehler bzw. Protokollverstöße erweitert werden.

Da es für eine Station sehr viele Möglichkeiten gibt, wie sie auf Fehler reagieren kann, soll hier anhand von zwei speziellen Möglichkeiten gezeigt werden, daß die Anonymität einmal erhalten bleiben und einmal verloren gehen kann.

Bei Ringen mit umlaufenden Übertragungsrahmen (ÜR) kann es vorkommen, daß Nachrichten zu übermitteln sind, die nicht in einen ÜR passen. In diesem Falle muß die Nachricht in Pakete zerlegt und in mehreren ÜR übermittelt werden.

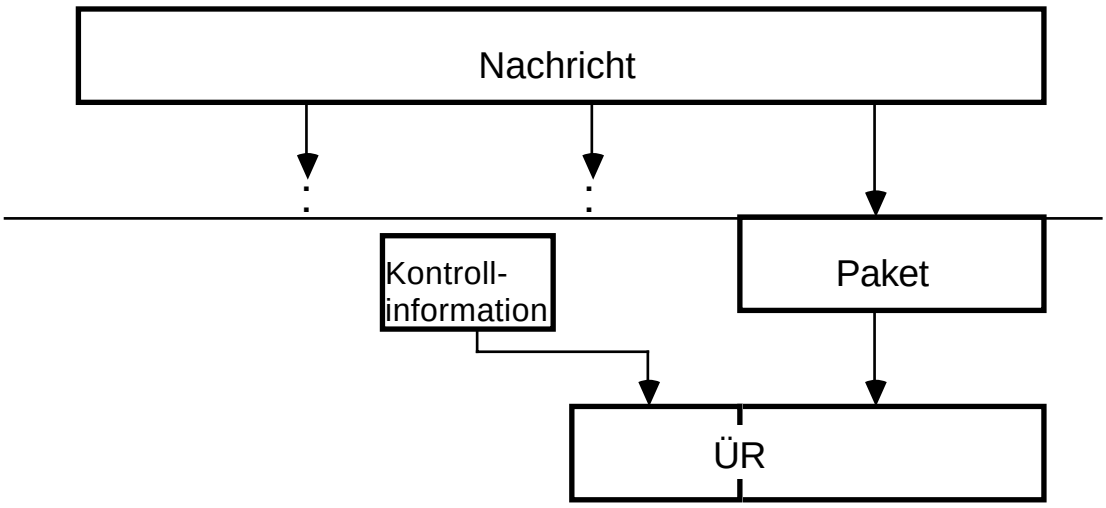

Bild 55: Zuordnung der Begriffe Nachricht, Paket, ÜR zueinander und zu Schichten

Zerstört ein Fehler oder der Angreifer nun einen ÜR, so hat dies den gleichen Effekt, als wäre die Übertragungsstrecke nicht zuverlässig. Beim anonymen Abfragen (vgl. Abschnitt 3.1.4.2) erkennt die sendende Station den Fehler und kann darauf reagieren.

1. Möglichkeit: Nur das betroffene Paket wird noch einmal übertragen, so daß die Pakete für den Angreifer unabhängig bleiben. Der Beweis von Abschnitt 3.1.4.2 ist übertragbar, da man die Informationseinheiten in Bild 41 einfach als Pakete deuten kann.

2. Möglichkeit: Die gesamte Nachricht wird als fehlerhaft übermittelt betrachtet, noch einmal in Pakete zerlegt und abgeschickt. Für dieses Vorgehen kann es verschiedene Gründe geben. Zum einen kann es Gesichtspunkte geben, die die Implementierung betreffen und es günstig erscheinen lassen, die Fehlerbehandlung auf der höheren Schicht durchzuführen. Zum anderen ist es denkbar, daß eine Nachricht auf der Empfängerseite nur dann lesbar ist, wenn die Pakete in der richtigen Reihenfolge eintreffen. Aus welchem Grund auch immer die Fehlerbehandlung so durchgeführt wird, der Angreifer kann bei gezielter Zerstörung von nur einem Paket in den Besitz von Kontextwissen kommen, das ihm in günstigen Fällen erlaubt, den Sender der gesamten Nachricht herauszufinden. Durch Bitmustervergleich kann er nämlich die wiederholt gesendeten Pakete identifizieren. Dadurch weiß er, welche Pakete zur gleichen Nachricht gehören und damit von der gleichen Station stammen. Dieses Wissen kann er etwa bei folgender Beobachtung verwerten.

Wie in Abschnitt 3.1.4 bezeichnet $e1$ den Eingang der ersten vom Angreifer umzingelten Station, $a2$ den Ausgang der zweiten. Die Inhalte verschiedener Übertragungsrahmen sind durch Kommata getrennt nebeneinandergeschrieben, dieselben Übertragungsrahmen in verschiedenen Umläufen untereinander.

	$e1$	$a2$
Umlauf i	(....., leer, leer, ….)	(....., P1, X , ….)
Umlauf i+1	(....., ℙ1, X , ….)	(....., P2, P3, ….)
Umlauf i+2	(....., P2, P3 , ….)	(....., ..., ..., ….)

Der Angreifer zerstört etwa das Paket P1 (durch Konturschrift angedeutet). Durch die Wiederholung der gesamten Nachricht und Bitmustervergleich stellt er fest, daß P1, P2 und P3 zur gleichen Nachricht gehören und damit von der gleichen Station stammen. Wird dann durch die Implementierung ausgeschlossen, daß eine Station gleichzeitig zwei Nachrichten sendet, so muß X von der anderen Station gesendet worden sein. Da in diesem ÜR jedoch später P3 gesendet wird, kann X nur von Station 1 und P3 nur von Station 2 gesendet worden sein. Also wurde auch P1 und P2 von der Station 2 gesendet. *(Ende des Beispiels)*

Im gerade beschrieben Beispiel gewinnt ein Angreifer dadurch Information, daß er

1. nochmals übertragene Informationseinheiten (wieder-)erkennen kann, d. h. die ursprüngliche und die nochmals übertragene Informationseinheit sind für ihn verkettbar, und
2. erkennt er durch die gemeinsame nochmalige Übertragung aller Nachrichtenteile einer Nachricht einen Zusammenhang zwischen Informationseinheiten, die im Beweis als unverkettbar angenommen wurden, was bei sicherer Ende-zu-Ende-Verschlüsselung ansonsten durchaus eine realistische Annahme ist.

Um möglichst weitgehende Unverkettbarkeit zu erreichen, sollten Informationseinheiten folglich anders verschlüsselt werden, wenn sie nochmals gesendet werden müssen. Außerdem sollte dies nochmalige Senden wie überhaupt jede Reaktion auf Fehler innerhalb der durch den Kommunikationsdienst vorgegebenen Grenzen zu einem zufälligen Zeitpunkt geschehen. Leider

kann auch durch diese beiden Maßnahmen meist keine perfekte Unverkettbarkeit erreicht werden, da eine andere Verschlüsselung natürlich nicht gegen Angriffe von Instanzen hilft, die diese Verschlüsselung entschlüsseln können (müssen), und für viele Dienste explizite, aktive Reaktionen auf Fehler innerhalb kurzer Zeit nötig sind, und deshalb zeitliche Korrelationen bestehen.

Kann keine perfekte Unverkettbarkeit erreicht werden, so müssen alle Anonymitäts-, Unbeobachtbarkeits- und Unverkettbarkeitsaussagen samt ihrer Beweise aus Abschnitt 2.5 und Kap. 3 neu überdacht und ggf. geführt werden.

Da (fast) jeder Kommunikationsdienst vom allerersten Sender bis zum letztendlichen Empfänger zuverlässig arbeiten muß, muß zwar (fast) immer eine Ende-zu-Ende-Kontrolle und ggf. Ende-zu-Ende-Fehlerbehebung durchgeführt werden – und sei dies nur eine Fehlerbehebung außerhalb des Kommunikationsnetzes, wodurch dann die Anonymität und Unbeobachtbarkeit ggf. auch untergraben werden kann. Fehlertoleranz-Maßnahmen sollten aber aus zwei Gründen Ende-zu-Ende-Fehlerbehebung vermeiden, wenn immer dies möglich ist:

1. Da bei Ende-zu-Ende-Fehlerbehebung die durch den Kommunikationsdienst vorgegebenen Grenzen für eine Reaktion auf den Fehler naturgegebenermaßen enger sind als bei geeignet entworfener Fehlerbehebung, die nicht wieder „ganz von vorne“ anfangen muß, ist bei Ende-zu-Ende-Fehlerbehebung die unvermeidbare Verkettung über zeitliche Zusammenhänge besonders groß. Ebenso ist sie für Anonymität und Unbeobachtbarkeit besonders gefährlich, da sie die eigentlich anonym und unbeobachtbar zu haltende Instanz zu einer expliziten, aktiven Reaktion zwingt.
2. Unabhängig von Forderungen nach Datenschutz, insbesondere Anonymität und Unbeobachtbarkeit, kann die Leistung von Ende-zu-Ende-Fehlerbehebung in Hinsicht auf die durchschnittliche Übertragungszeit, Varianz der Übertragungszeit oder des erzielbaren Durchsatzes (jeweils alles bezüglich fehlerfreier Übertragung) unbefriedigend sein. Beispielsweise ist Ende-zu-Ende-Fehlerbehebung mittels nochmaliger Übertragung nur bei transienten Fehlern (sporadisches Fehlerauftreten), bei denen zudem das Kommunikationsnetz selbst intakt bleibt, oder dann wirksam, wenn die nochmalige Übertragung die „Fehlerstellen“ umgehen kann. (Die Fehlerklasse der transienten Fehler, bei denen das Kommunikationsnetz selbst intakt bleibt, umfaßt beispielsweise verfälschte Nachrichten, einzelne verlorene oder verdoppelte Nachrichten u. ä.)

Beim Entwurf von Fehlertoleranzverfahren muß zunächst mittels eines **Fehlermodells** definiert werden, was unter einem Fehler verstanden wird, insbesondere wo Fehler entstehen, wie sie sich äußern und wie sie sich ausbreiten können.

Um effiziente Fehlertoleranzverfahren entwerfen zu können, ist danach mittels einer **Fehlervorgabe** festzulegen, wieviele von welchen Sorten Fehlern (mindestens) toleriert werden müssen. Außerdem ist mittels einer **Dienstvorgabe** zu definieren, welche Beeinträchtigungen der eigentlichen Dienstabwicklung durch Fehler bzw. Fehlerbehandlung akzeptabel sind.

Um den Aufwand von Fehlertoleranzverfahren gering zu halten, wird üblicherweise davon ausgegangen, daß **Fehler** (im Gegensatz zu *Angriffen*) „aus Versehen“ entstehen, sei es durch *falschen Entwurf*, *falsche Produktion*, *unerlaubte Umgebungsbedingungen* oder einfach *physische Alterung*.

Insbesondere bei den letzten beiden Fehlerursachen kann im Fehlermodell eines räumlich weit verteilten Systems davon ausgegangen werden, daß Fehler an verschiedenen Stellen des

Systems unabhängig voneinander auftreten. Man muß sich aber über die Konsequenzen solch einer Annahme klar sein: Weder kann dann von solch einem Fehlertoleranzverfahren die Tolerierung von (Natur-)Katastrophen entsprechend weiter räumlicher Ausdehnung, beispielsweise Überschwemmung eines Stadtviertels, noch die Tolerierung entsprechend massiver (externer) Sabotageakte erwartet werden. Beides tritt aber (hoffentlich) weitaus seltener als „ganz gewöhnliche Fehler“ auf. Deshalb ist es sinnvoll, Katastrophen und massive (externe) Sabotage mit anderen Verfahren und unter größeren Einschränkungen der Kommunikationsnetzbenutzer (schwächere Dienstvorgabe) mittels für spezielle **Katastrophenmodelle** entworfener **Katastrophentoleranzverfahren** zu behandeln:

- Sind etwa bei einer Überschwemmung Übertragungsleitungen weitgehend unbrauchbar, so sind nur noch Funknetze verwendbar. Entsprechend sollte bei der zur Zeit stürmischen Entwicklung des öffentlichen mobilen Funks in allen neuen Systemen und Geräten vorgesehen werden, daß im Katastrophenfall Notrufe höhere Priorität als Privatkommunikation haben sowie weitere, normalerweise etwa für Massenkommunikation [Kais_82], insbesondere Unterhaltung, verwendete Frequenzbänder nach Erhalt einer „Freigabenachricht“ von den Mobilfunkgeräten jeweils eine gewisse Zeitlang mitverwendet werden können. Leider wird dies bei der Einführung von Mobilfunksystemen heutzutage genausowenig beachtet wie die in Abschnitt 9.1 zu diskutierenden bei Mobilfunksystemen auftretenden Datenschutzprobleme.
- Sind etwa bei (externer) Sabotage etliche Übertragungs- und Vermittlungssysteme zerstört, so daß anonyme und unbeobachtbare Kommunikation nicht mehr möglich ist, so sollte das Kommunikationsnetz so rekonfiguriert werden können, daß die verbleibende Übertragungs- und Vermittlungskapazität für beobachtbare Kommunikation genutzt und dies den Teilnehmern selbstverständlich angezeigt wird. Dieses Umkonfigurieren ist insbesondere bei den Grundverfahren möglich und lohnend, die Anonymität und Unbeobachtbarkeit nicht durch übertragungstechnische, sondern kryptographische Techniken realisieren, nämlich beim MIX- und DC-Netz.
- Um nicht durch Ausfall oder Zerstörung eines zentralen Gerätes oder Kabelkellers (heute etwa die Ortsvermittlungsstelle bzw. deren Kabelkeller) alle leitungsgebundenen Übertragungs- und zugehörige Vermittlungseinrichtungen eines geographischen Gebietes zu „verlieren“, sollten etwa öffentliche Fernsprechstellen (z. B. Telefonzellen) über ausschließlich andere Kabelkeller an andere Vermittlungseinrichtungen angeschlossen werden. Gegebenenfalls können die Verkehrsdaten öffentlicher Fernsprechstellen weniger geschützt werden als die personen- oder firmenbezogener Anschlüsse.

Bezüglich der ersten beiden Fehlerursachen ist eine Unabhängigkeit allenfalls bezüglich von unabhängigen Parteien entworfener und produzierter Subsysteme realistisch, vgl. [Ande_84, EcPf_85, Aviz_85, AvLa_86].

Noch weniger Annahmen sind dann sinnvoll möglich, wenn Fehler nicht „aus Versehen“ oder mittels (externer) Sabotageakte entstehen, sondern etwa als raffinierte Entwurfs- oder Produktionsfehler (Trojanische Pferde) eingebaut werden, vgl. Abschnitt 2.1.2. Vorstellbar etwa wäre, daß manche Einrichtungen bei Vorliegen gewisser Betriebszustände (etwa bestimmtes Datum, Eingabebefehl des Netzbetreibers, sehr unwahrscheinliches Bitmuster bei den Nutzdaten) ihr Verhalten vollständig ändern. Nicht nur Datenschutz, sondern auch die Verfügbarkeit von Kommunikationsdiensten kann dann natürlich in keiner Weise mehr garantiert werden,

wenn diese Dienste von solchermaßen entworfenen oder produzierten Subsystemen abhängen. Öffentliche Fernsprechstellen sollten folglich nicht nur über andere Kabelkeller an andere Vermittlungseinrichtungen angeschlossen werden, sondern diese Vermittlungs- und Übertragungseinrichtungen sollten auch von anderen entworfen und produziert sein – sofern Entwurfs- und Produktionsfehler nicht ausgeschlossen werden können, vgl. Abschnitt 2.1.2.

Interne Fehler, die nicht „aus Versehen“ entstehen, werden – wie teilweise schon angedeutet – als **aktive Angriffe** bezeichnet. Bezüglich massiver aktiver Angriffe gilt ähnliches wie unter Katastrophentoleranz ausgeführt wurde: man muß froh sein, wenn überhaupt noch Kommunikation möglich ist, Schutz der Verkehrsdaten ist in solch einer Situation nicht zu gewährleisten. Wie bei „normalen“ Fehlern ist es aber auch bei begrenzten aktiven Angriffen (genauer: bei aktiven Angriffen von in ihren Fähigkeiten begrenzten Angreifern) sinnvoll, den Schutz der Verkehrsdaten nicht sofort um der Nutzleistung willen aufzugeben.

Mit diesen Bemerkungen zu Fehlertoleranz (im engeren Sinne), Katastrophentoleranz und Tolerierung aktiver Angriffe wurde ein riesiges Gebiet skizziert, dessen vollständige Behandlung einerseits den Rahmen dieser Arbeit bei weitem sprengen würde, andererseits glücklicherweise nicht nötig ist:

Fehler- und Katastrophentoleranzverfahren per se, d. h. ohne Betrachtung der Interaktionen mit den in den Abschnitten 2.3 und 2.5 beschriebenen speziellen Verfahren werden seit langem erforscht und partiell eingesetzt und sind somit (zumindest theoretisch) Standard, vgl. AnLe_81, SiSw_82, EcPf_85]. Entsprechendes gilt – wie in Abschnitt 1.2 unter dem Schlagwort Sicherheitsproblem bereits erwähnt – für die Tolerierung aktiver Angriffe per se, vgl. [VoKe_83, Denn_82, DaPr_84]. Alle diese Verfahren werden deshalb an den jeweiligen Stellen jeweils nur kurz erwähnt.

Wie oben bereits begründet wurde, erscheint es aussichtslos, in Katastrophensituationen noch die Verkehrsdaten schützen zu wollen – andererseits handelt es sich bei den meisten Kommunikationsereignissen in einer Katastrophensituation sicherlich um in einem objektiven Sinne nicht sensitiven Verkehr (vgl. Abschnitt 4.2.2), denn jeder wird z. B. bei einer Überschwemmung versuchen, mit den Notdiensten Kontakt aufzunehmen. (Wegen der Aufregung der Menschen bei Katastrophensituationen und der daraus häufig resultierenden Unvollständigkeit der Absender- und Ortsangabe kann es in ihnen sogar zweckmäßig sein, diese Angaben automatisch zu übertragen.)

Somit bleibt nur die Interaktion zwischen den in den Abschnitten 2.3 und 2.5 beschriebenen speziellen Datenschutz-Verfahren einerseits und Fehlertoleranz (im engeren Sinne) und Tolerierung aktiver Angriffe andererseits übrig. Dies kann und wird im Rest dieses Kapitels bewältigt werden:

- Zunächst werden einige weitere, für alle speziellen Datenschutz-Verfahren gültige Bemerkungen zur Ende-zu-Ende-Fehlerbehebung gemacht.
- Danach werden jeweils in eigenen Abschnitten – wo nötig – spezielle Fehlertoleranzverfahren für Verschlüsselung, Verteilung, MIX, DC-, BAUM-, RING-Netz sowie hierarchische Netze entwickelt und bewertet. Diese Gliederung erlaubt es, jeden der Abschnitte gesondert zu lesen. Dadurch soll eine bessere Verständlichkeit, insbesondere des Ineinandergreifens aller Fehlertoleranz-Maßnahmen in je einem Netz erreicht werden.

- Im letzten Abschnitt dieses Kapitels wird schließlich auf die Tolerierung aktiver Angriffe unter Erhaltung von Anonymität und Unbeobachtbarkeit eingegangen. Da hierbei die Gemeinsamkeiten der in den Abschnitten 2.3 und 2.5 beschriebenen speziellen Verfahren dominieren, erfolgt dies für alle Verfahren gemeinsam.

Zusammenfassend kann man sagen, daß die Grundverfahren aus den Abschnitten 2.3 und 2.5 so erweitert werden, daß sie begrenzt viele Fehler und aktive Angriffe tolerieren, aber weiterhin Anonymität und Unbeobachtbarkeit gewähren. Dabei stellt sich heraus, daß entweder zwischen Fehlertoleranz einerseits und Anonymität, Unbeobachtbarkeit und Unverkettbarkeit andererseits abzuwägen ist oder auf kontinuierliche Nutzleistung im Fehler- bzw. Angriffsfall verzichtet werden muß.

Um die Interaktion zwischen den in den Abschnitten 2.3 und 2.5 beschriebenen speziellen Datenschutz-Verfahren einerseits und Fehlertoleranz (im engeren Sinne) und Tolerierung aktiver Angriffe andererseits zu verstehen, wird die Auswirkungen von Fehlern im Schichtenmodell von Bild 30 betrachtet. In diesem Schichtenmodell benutzt eine Schicht die Dienste tieferliegender Schichten und stellt den höherliegenden Schichten ihre Dienste zur Verfügung. Einerseits kann ein Fehler, der in einer Schicht auftritt, in dieser Schicht selbst oder in der (oder den) nächsthöheren Schicht(en) toleriert werden. Der Fehler kann auch zu einem Fehler in der (oder den) nächsthöheren Schicht(en) führen, welcher (oder: welche) dann ebenfalls toleriert werden muß (müssen). Andererseits sollten und können Systeme so gebaut werden, daß ein Fehler, der in einer Schicht auftritt, nie zu einem Fehler in der nächsttieferen Schicht führt [AnLe_81 Seite 298, Gold_84].

Hieraus und aus dem in Abschnitt 2.6 Gesagtem folgt, daß die in Bild 30 dunkel hinterlegten, tiefen (Teil)Schichten ohne Rücksicht auf Anonymität, Unbeobachtbarkeit und Unverkettbarkeit mit beliebigen Maßnahmen zur Tolerierung von Fehlern und aktiven Angriffen versehen werden können. Mit anderen Worten: In diesen (Teil)Schichten findet keine Interaktion zwischen Datenschutzverfahren einerseits und Verfahren zur Tolerierung von Fehlern und aktiven Angriffen andererseits statt. Deshalb werden diese (Teil)Schichten im Rest dieses Kapitels kaum noch erwähnt.

Die nicht hinterlegten, mittleren (Teil)Schichten schaffen innerhalb des Kommunikationsnetzes Anonymität, Unbeobachtbarkeit und Unverkettbarkeit. Aber sie schaffen auch, wie zu Beginn dieses Kapitels erläutert, Seriensysteme im Sinne der Zuverlässigkeit. Diese (Teil)Schichten müssen, will man nicht einfach mehrere unabhängige Kommunikationsnetze „parallel“ benutzen, um Verfahren zur Tolerierung von Fehlern und aktiven Angriffen erweitert werden. Hier findet dann natürlich eine Interaktion zwischen Datenschutzverfahren einerseits und Verfahren zur Tolerierung von Fehlern und aktiven Angriffen andererseits statt.

Da die hell hinterlegten, höheren (Teil)Schichten Anonymität, Unbeobachtbarkeit und Unverkettbarkeit erhalten müssen und zumindest Ende-zu-Ende-Fehlerbehebung – wenn auch selten – durchführen müssen, findet auch auf ihnen eine Interaktion zwischen Datenschutzverfahren einerseits und Verfahren zur Tolerierung von Fehlern und aktiven Angriffen andererseits statt. Da die Protokolle der höheren Schichten 4, 5, 6, 7 üblicherweise nur die Dienste für einen Teilnehmer (und damit natürlich auch die Teilnehmer, die mit ihm kommunizieren wollen) betreffen und üblicherweise in Geräten des Teilnehmers implementiert sind und Teilnehmer bei Ausfall ihrer Geräte natürlich keine Erbringung von Kommunikationsdiensten erwarten können,

werden Teilnehmer ihre Geräte ggf. intern (und damit für andere bis auf die höhere Verfügbarkeit) unsichtbar fehlertolerant machen. Da zudem eine relativ große zeitliche Entkopplung zwischen den relativ langsamen Ereignissen dieser höheren Schichten und den viel schnelleren (und zahlreicheren) der mittleren und tieferen Schichten besteht, dürfte solch eine redundante Auslegung der Teilnehmerstationen kaum Probleme bezüglich Datenschutzverfahren aufwerfen, sieht man von den bereits erwähnten, daß fehlerhafte Stationen natürlich keine expliziten Adressen anfügen oder die Ende-zu-Ende-Verschlüsselung unterlassen dürfen, ab. Deshalb werden im Rest dieses Kapitels nur die Funktionen der hell hinterlegten, höheren (Teil)Schichten behandelt, die die schnelle Interaktion vieler Teilnehmerstationen betreffen (und deshalb in Bild 30 explizit eingezeichnet sind).

Weitere, für alle speziellen Datenschutzverfahren gültigen **Bemerkungen zur Ende-zu-Ende-Fehlerbehebung**:

In allen Datenschutzverfahren der Abschnitte 2.3 und 2.5 werden Informationseinheiten sensitiven Inhalts zwischen Sender und Empfänger verschlüsselt übertragen, d. h. *Ende-zu-Ende-Verschlüsselung* wird eingesetzt. Wie erwähnt ist es aus Gründen der Fehlertoleranz nötig, Ende-zu-Ende-Protokolle zu verwenden, um Fehler auch ganz am Anfang oder Ende der Übermittlungsstrecke entdecken und ggf. beheben zu können; außerdem dienen diese Protokolle auch der Sicherheit (Schutz vor Erfolg von Angriffen). Durch Sequenznummern, Zeitstempel, fehlererkennende Codes u. ä. lassen sich Übermittlungsfehler erkennen, um eine Wiederholung der Übermittlung zu initiieren. Gleichzeitig lassen sich auch aktive Angriffe, z. B. das Wiederholen alter, ehemals gültiger Informationseinheiten erkennen (vgl. Abschnitt 5.8 und [VoKe_83]). Damit die Protokollinformationen keine Anhaltspunkte über Sender bzw. Empfänger von Informationseinheiten liefern, sollten sie vernünftigerweise selbst unter der Ende-zu-Ende-Verschlüsselung vor Unbeteiligten verborgen werden. Dies wiederum impliziert, daß das verwendete Konzelationssystem gegen Angriffe mit bekanntem Klartext sicher sein muß (vgl. Abschnitt 2.2). Ansonsten könnte die starre Struktur der Informationseinheiten dazu verwendet werden, das Konzelationssystem zu brechen. Wie bereits angemerkt wurde, ist dies Verbergen der Protokollinformation vor Unbeteiligten das Besterreichbare.

Bei allen Datenschutzverfahren kann man, wie erwähnt, zur Leistungssteigerung *anonyme Kanäle* schalten. Fehler in diesen Kanälen lassen sich mit denselben Maßnahmen wie bei einzelnen Nachrichten oder Paketen tolerieren. Die erforderlichen Zusatzinformationen müssen dann für die Dauer eines Kanals gespeichert werden. Im folgenden werden daher Kanäle meistens nicht extra betrachtet.

5.1 Verschlüsselung

Zwischen Verschlüsselung einerseits und Tolerierung von Fehlern und aktiven Angriffen andererseits gibt es folgende relevanten Interaktionen:

Zerstört oder ändert ein Fehler oder aktiver Angriff eine Informationseinheit, in der ein Schlüssel ausgetauscht wird, so kann der Empfänger nicht richtig ver- oder entschlüsseln. Da ein Schlüsselaustausch üblicherweise in Authentifikation (zumindest aber Integrität) garantieren-

der Weise erfolgt (vgl. Abschnitt 2.2), kann dies vom Empfänger mit an Sicherheit grenzender Wahrscheinlichkeit sofort und damit vor einer Benutzung des Schlüssels bemerkt werden. Ist der Schlüsselaustausch nötig (und kann nicht etwa der bisher benutzte weiter benutzt werden), so muß der Empfänger des Schlüssels vom Sender eine erneute Übermittlung anfordern, die ggf. über einen anderen Weg erfolgen kann. Gegen einen Verlust von richtig erhaltenen Schlüsseln kann man sich durch Verwendung eines Schwellwertschemas [Sham_79] und Speicherung der „Schlüsselteile“ an verschiedenen Stellen schützen.

Zerstört oder ändert ein Fehler oder aktiver Angriff eine verschlüsselte Informationseinheit, so kann sie im allgemeinen nicht richtig entschlüsselt werden. Bei synchronen Stromchiffren ist danach im allgemeinen auch keine Entschlüsselung der folgenden Informationseinheiten möglich, vgl. Abschnitt 2.2.2.1. Da es einerseits günstig ist, wenn sowohl Ende-zu-Ende- als auch Verbindungs-Verschlüsselung mit einer Stromchiffre durchgeführt wird, damit etwa zur Fehlerbehebung nochmals übermittelte Informationseinheiten unterschiedlich verschlüsselt und ihre Wiederholung für Unbeteiligte nicht erkennbar ist, empfehlen sich für den praktischen Einsatz selbstsynchronisierende Stromchiffren, die mittels der in Abschnitt 2.2.2.1 beschriebenen Konstruktionen aus Blockchiffren erzeugt werden können. Im Gegensatz zu synchronen erlauben selbstsynchronisierende Stromchiffren eine einfachere Fehlerbehebung und bei manchen Diensten, z. B. Telefon, sogar einen vollständigen Verzicht auf Fehlerbehebung bei kurzen transienten Fehlern (oder aktiven Angriffen).

5.2 Verteilung

Zwischen Verteilung einerseits und Tolerierung von Fehlern und aktiven Angriffen andererseits gibt es folgende zwei relevanten Interaktionen:

Empfänger, die *Informationseinheiten fehlerhaft oder gar nicht erhalten*, sollten unabhängig davon, ob sie sie überhaupt benötigen, auf einen fehlerfreien Empfang – etwa mittels nochmaliger Übertragung – bestehen. Anderenfalls könnte eine Reaktion auf fehlerhafte oder gar nicht erhaltene Informationseinheiten den bzw. die Empfänger verraten. Bei der praktischen Durchführung dieser Regel stößt man möglicherweise an zwei Grenzen:

Einerseits können Teilnehmerstationen möglicherweise nicht die gesamte ihnen zufließende Information gleichzeitig empfangen (vgl. Abschnitt 3.2.1) und deshalb manche fehlerhaften Informationseinheiten gar nicht erkennen.

Andererseits könnte es keine Instanz geben, von der eine fehlerfreie Kopie angefordert werden kann. Letzteres kann durch eine kurzzeitige Speicherung aller verteilten Informationseinheiten in einem (oder mehreren) global bekannten Speicher(n) ohne irgendwelche Einschränkungen des Datenschutzes gelöst werden.

Bezüglich der Erkennung fehlerhafter Verteilung bzw. aktiver Angriffe auf die Verteilung sei an das in Abschnitt 2.5.1 Gesagte erinnert.

Ähnlich wie bei Verschlüsselung muß bei *impliziter Adressierung* darauf geachtet werden, daß implizite Adressen auch bei Verfälschung oder Verlust von vorangehenden Informationseinheiten richtig erkannt werden. Dies kann durch Verwendung einer Blockchiffre bei verdeck-

ter impliziter Adressierung perfekt erreicht werden. Bei offener impliziter Adressierung mit jeweils nur einmal verwendeten Adressen, die zum Zwecke des Adreßvergleichs in einen Assoziativspeicher geschrieben und nach Erhalt einer entsprechend adressierten Informationseinheit durch die folgende Adresse ersetzt werden (vgl. Abschnitt 2.5.1), ist dies nicht ohne weiteres möglich. Zwar können bei einer Fehlervorgabe von maximal k aufeinanderfolgenden verlorenen oder verfälschten Informationseinheiten statt der nächsten immer die k+1 nächsten Adressen jeder Adreßfolge in einen entsprechend um den Faktor k+1 größeren Assoziativspeicher geschrieben werden, was gegen kurzzeitige Störungen hilft. Bei längeren Störungen müssen Sender und Empfänger aber – etwa mittels Nachrichten mit verdeckter impliziter Adressierung – neu synchronisiert werden.

5.3 MIX-Netz

Im MIX-Netz ohne Verteilung „letzter“ (vgl. Abschnitt 2.5.2.3) Informationseinheiten sind andere Fehlerbehebungs-Verfahren als Ende-zu-Ende-Zeitschranken und nochmalige Übermittlung bei Überschreitung der Zeitschranken ganz besonders nötig, da dieses Fehlerbehebungsverfahren bei manchen Diensten nicht zufriedenstellend funktioniert: bei elektronischer Post (electronic mail) etwa gibt es keine sinnvollen Zeitschranken. Außerdem muß bei anonymen Rückadressen der ursprüngliche Generierer eine neue anonyme Rückadresse als Ersatz einer durch Ausfall eines MIXes unbrauchbar gewordenen bilden – der Verwender der Rückadresse kann dies nicht (vgl. Abschnitt 2.5.2.3). Dieses Problem kann allerdings durch das Verfahren des anonymen Abrufs statt „normaler“ anonymer Rückadressen vermieden werden, vgl. Abschnitt 2.5.2.6.

Für die hiermit motivierten und in den folgenden Unterabschnitten hergeleiteten Fehlertoleranzverfahren wird als einheitliche und angemessene graphische Notation die von Bild 20 verwendet. Dargestellt wird jeweils die Übermittlung einer Nachricht (als Beispiel einer von anderen unabhängigen Informationseinheit) vom Sender S über 5 MIXe zum Empfänger E, die dabei verwendeten Schlüssel und ihre Kenntnis, sowie die Reihenfolge von Verschlüsselungs-, Transfer- und Entschlüsselungsoperationen. Wie in den Bildern 19 und 20 wird das einfachste Verschlüsselungsschema (direktes Umcodierungsschema für Senderanonymität) abgebildet.

Da keine Informationseinheiten eingezeichnet sind, kann man Bild 20 auch als Darstellung des (abstrakten) Verschlüsselungs-, Transfer- und Entschlüsselungsschemas verstehen. Ebenso kann, da keine genauen Verschlüsselungsstrukturen gezeigt sind, Bild 20 auch als Abbildung eines indirekten Umcodierungsschemas – sei es für Sender-, sei es für Empfängeranonymität oder beides – verstanden werden, das nur die wesentlichen, nämlich nachrichtenunabhängigen Schlüssel sowie Ver- und Entschlüsselungen zeigt.

Man erkennt an Bild 20 noch deutlicher die Serieneigenschaft als an Bild 19. Fällt nur ein MIX auf dem Weg zwischen S und E aus, so kann die Nachricht nicht weiter entschlüsselt und übertragen werden.

Wie schon in Abschnitt 2.6 begründet und aus Bild 30 ersichtlich, basiert das MIX-Netz auf einem in den Schichten 0 (medium), 1 (physical) und 2 (data link) sowie der unteren Teilschicht

der Schicht 3 (network) ohne Rücksicht auf Datenschutzforderungen realisierbaren Kommunikationsnetz. Wie schon begründet, impliziert dies, daß diese Schichten des Kommunikationsnetzes konventionelle Fehlertoleranz-Maßnahmen verwenden können, ohne dadurch die Anonymität bzw. Unbeobachtbarkeit der Netzteilnehmer zu gefährden. Transiente sowie permanente Fehler in diesen Schichten können also von diesen selbst toleriert werden.

Die MIXe selbst müssen und können so gebaut oder mittels organisatorischer Maßnahmen betrieben werden, daß sich Fehler (oder aktive physische Angriffe) mit an Sicherheit grenzender Wahrscheinlichkeit nicht so auswirken, daß der MIX seinen geheimen Dechiffrierschlüssel ausgibt, Informationseinheiten mehrfach mixt oder in falscher Reihenfolge ausgibt. Hingegen ist es akzeptabel, daß er bei schwerwiegenden Fehlern (oder aktiven physischen Angriffen) seine Schlüssel „vergißt“ und seinen Dienst vollständig einstellt (fail-stop Betrieb [ScSc_83]). Um möglichst selten Fehler extern tolerieren zu müssen, ist es natürlich möglich, den MIX intern fehlertolerant aufzubauen, solange bei diesem Aufbau obige Bedingungen auch bei Fehlern oder aktiven Angriffen eingehalten werden.

Extern wahrnehmbare transiente Fehler in den MIXen werden von den Ende-zu-Ende-Protokollen zwischen Sender *S* und Empfänger *E* erkannt und durch wiederholtes Senden toleriert. (Zur Leistungssteigerung ist auch eine weitere Zwischenstufe mit MIX-zu-MIX-Protokollen möglich.) Es bleiben somit nur noch die extern wahrnehmbaren permanenten Fehler in MIXen. Diese Fehler sind mit den üblichen Techniken zu erkennen bzw. zu lokalisieren, z. B. der Ausfall eines MIXes durch Zeitschranken bzw. die Diagnose, welcher MIX ausfiel, durch das Ausbleiben eines zyklisch zu gebenden Lebenssignals (Nachricht mit Datum und Zeit sowie Unterschrift, I’m alive message). Die permanenten Ausfälle von MIXen erfordern darüber hinaus geeignete Methoden zur Fehlerbehebung. Prinzipiell gibt es drei Möglichkeiten [Pfi1_85]:

Die erste, in Abschnitt 5.3.1 beschriebene, erfordert keine Koordination von MIXen. Sie stellt aber ein Ende-zu-Ende-Protokoll dar, was – wie erwähnt – für die Unverkettbarkeit und damit auch die Anonymität bzw. Unbeobachtbarkeit ungünstig ist.

Im Gegensatz hierzu ist Koordination zwischen MIXen bei den beiden anderen nötig und eine nicht Ende-zu-Ende arbeitende Fehlerbehebung deshalb möglich, da bei ihnen MIXe in die Lage versetzt werden, andere zu ersetzen. Wie dies geschehen kann und was dabei zu beachten ist, wird in Abschnitt 5.3.2 behandelt.

Besonderheiten beim Schalten von Kanälen werden für alle drei Möglichkeiten gemeinsam in Abschnitt 5.3.3 behandelt.

In Abschnitt 5.3.4 wird dann eine quantitative Bewertung aller drei Möglichkeiten durchgeführt.

5.3.1 Verschiedene MIX-Folgen

Bei der ersten Möglichkeit versucht der Sender eine Wiederholung der Übermittlung auf einem anderen Weg (Bild 56), d. h. über eine disjunkte MIX-Folge (in der Begriffswelt der Fehlertoleranz [EcGM_83, gekürzt auch in BeEG_86]: *dynamisch aktivierte Redundanz*). Diese Lösung ist einfach, aber (wie dynamisch aktivierte Redundanz generell) langsam, da das Ende-zu-Ende-Protokoll zuerst den Fehler erkennen (i. allg. durch Ende-zu-Ende-Zeitschranken) und

dann eine zweite Übermittlung einleiten muß, möglicherweise ohne zu wissen, welcher MIX defekt ist.

Im MIX-Netz ohne Verteilung „letzter“ Informationseinheiten und ohne anonymen Abruf sind gemäß Abschnitt 2.5.2.3 anonyme Rückadressen mit langer Gültigkeit zum Schutz des Empfängers nötig. Bei anonymen Rückadressen mit langer Gültigkeit ist obiges Fehlertoleranzverfahren dann sehr aufwendig, wenn keine zeitliche Beziehung zwischen Nachrichten und Antworten besteht, wie dies z. B. bei elektronischer Post (electronic mail) der Fall ist. Der Empfänger *E* kann, falls die erhaltene Rückadresse ausfällt (wenigstens ein MIX in dieser Folge ist defekt), keine Übermittlung auf einem anderen Weg versuchen. Dies gilt auch, wenn immer zwei oder mehr anonyme Rückadressen mit langer Gültigkeit (*statisch erzeugte Redundanz*) ausgetauscht werden und in jeder Folge ein MIX defekt ist. Der ursprüngliche Sender *S* (genauer: seine Teilnehmerstation) müßte also, solange er von *E* keine Antwort erhielt, *E* (genauer: seiner Teilnehmerstation) immer wieder neue anonyme Rückadressen mitteilen, was in den meisten Fällen völlig überflüssig ist, da *E* lediglich bisher noch keine Zeit fand, eine Antwort zu formulieren. Alternativ kann sich *S* auch immer wieder informieren, welche MIXe inzwischen ausgefallen sind, und *E* nur dann neue anonyme Rückadressen mit langer Gültigkeit mitteilen, wenn alle *E* bisher mitgeteilten anonymen Rückadressen mit langer Gültigkeit ausgefallen sind oder waren, denn auch im letzteren Fall können sie – nach einem Fehlversuch von *E* – für diesen inzwischen permanent unbrauchbar sein.

Diese erste Möglichkeit der Fehlertoleranz läuft auf ein alle Stationen involvierendes **Zwei-Phasen-Konzept** hinaus. In der einen Phase werden Informationseinheiten anonym übertragen, in der anderen werden Fehler toleriert, z. B. dadurch daß nach jedem Ausfall eines MIXes alle Sender allen Empfängern neue anonyme Rückadressen zukommen lassen, in denen der ausgefallene MIX nicht benötigt wird (in der Begriffswelt der Fehlertoleranz: *dynamisch erzeugte*, dynamisch aktivierte *Redundanz*). Da im MIX-Netz ohne Verteilung „letzter“ Informationseinheiten an alle Stationen und ohne anonymen Abruf aus Gründen der gegenseitigen Anonymität von Sender und Empfänger alle Adressen anonyme Rückadressen sein müssen (Abschnitt 2.5.2.4), erfordert diese Neuverteilung in ihm zwingend eine Indirektionsstufe in Form von nichtanonymen Stellen zur Neuverteilung der Adressen (etwa die bereits in Abschitt 2.5.2.4 erwähnten Adreßverzeichnisse mit anonymen Rückadressen): nach Ausfall eines MIXes wird dies allen Stationen mitgeteilt und jede sendet den nichtanonymen Stellen zur Adreßverteilung mit einem Senderanonymitätsschema über die noch intakten MIXe eine Liste der unbrauchbar gewordenen anonymen Adressen, jeweils eine anonyme Ersatzadresse und eventuell noch weitere anonyme Adressen, da diese ja je nur einmal verwendet werden können und also von Zeit zu Zeit sowieso nachgeliefert werden müssen.

Im MIX-Netz mit Verteilung „letzter“ Informationseinheiten an alle Stationen sind anonyme Rückadressen überflüssig, da durch Verteilung und normale implizite Adressen der Empfänger vollständig geschützt ist. Also müssen in solch einem MIX-Netz auch nach Ausfall von MIXen keine neuen Adressen ausgetauscht werden. Eine Liste der ausgefallenen MIXe sollte natürlich an alle Stationen verteilt werden, damit sie diese MIXe für das Senderanonymitätsschema nicht verwenden.

Entsprechendes gilt beim Verfahren des anonymen Abrufs.

Eine im Fehlerfall Zeit sparende Variation dieser Möglichkeit der Ende-zu-Ende-Protokolle mit statisch oder dynamisch aktivierter Redundanz besteht darin, jeden anonymen Informationstransfer parallel über mehrere disjunkte MIX-Folgen auszuführen (statisch oder dynamisch erzeugte, *statisch aktivierte Redundanz*).

Nachteil jeder Ende-zu-Ende-Fehlerbehebung ist, daß statistische Angriffe über Senderaten von Informationseinheiten – wie zu Beginn dieses Kapitels bereits erwähnt – möglich sind, die ggf. eine Verkettung von Verkehrsereignissen bewirken können. Besonders ausgeprägt ist dies bei MIX-Netzen ohne Verteilung „letzter" Informationseinheiten und bei individueller Wahl der Ende-zu-Ende-Zeitschranken (genauer: der Zeitschrankenintervalle, innerhalb derer zu einem zufälligen Zeitpunkt reagiert wird) bzw. bei individueller Wahl der Anzahl der parallel auszuführenden Informationstransfers.

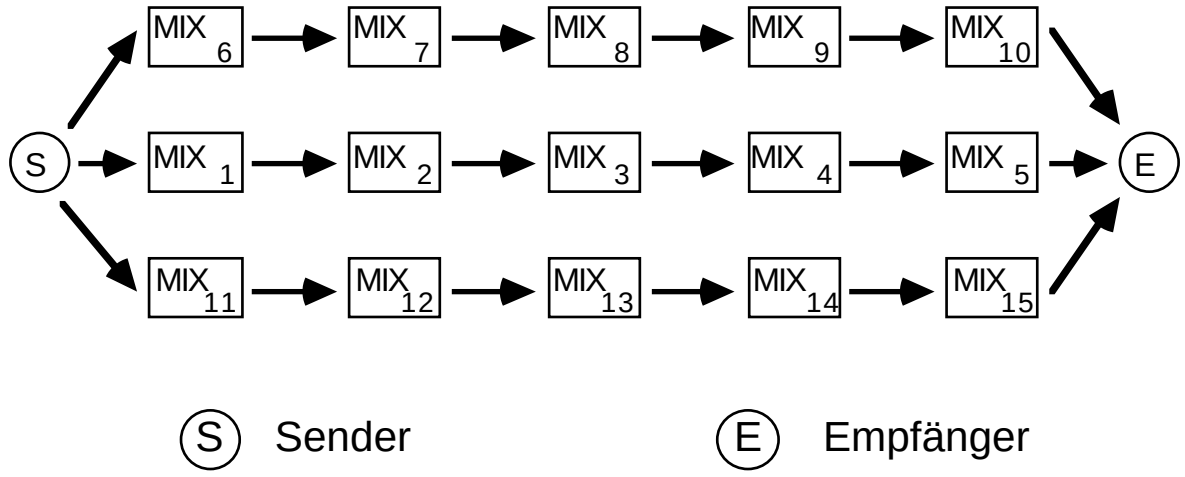

Bild 56: Zwei zusätzliche alternative Wege über disjunkte MIX-Folgen

Können statistische Angriffe über Senderaten von Informationseinheiten ignoriert werden, so gilt das folgende Datenschutz-Kriterium.

> **Datenschutz-Kriterium**:
> Verschiedene MIX-Folgen sind genauso sicher wie die ursprünglichen Schemata (vgl. Abschnitt 2.5.2), sofern bei jeder verwendeten MIX-Folge mindestens ein MIX nicht vom Angreifer kontrolliert wird.
> Hierbei ist es unerheblich, ob der nicht kontrollierte MIX korrekt mixt oder (etwa, sofern er ausgefallen ist) gar nicht.

5.3.2 Ersetzen von MIXen

Um eine nicht Ende-zu-Ende arbeitende Fehlerbehebung zu ermöglichen und damit alle Nachteile der ersten Möglichkeit zu vermeiden, werden bei der zweiten und dritten Möglichkeit MIXe in die Lage versetzt, andere zu ersetzen. Dies ist insbesondere für die Verfügbarkeit sehr vorteilhaft, verursacht aber das im folgenden Unterabschnitt behandelte *Koordinations-Problem*.

Die Möglichkeit des Ersetzens von MIXen wird statisch vorgesehen (*statisch erzeugte Redundanz*) – bei dynamisch erzeugter Redundanz bräuchten keine MIXe ersetzt zu werden. Es könnte, wie in Abschnitt 5.3.1, eine ganz andere MIX-Folge gewählt werden.

Statisch erzeugte Redundanz kann generell entweder statisch oder dynamisch aktiviert werden.

Dabei ist eine statische Aktivierung bezüglich des Ersetzens eines MIXes nichts anderes als eine verteilte, intern fehlertolerante Implementierung eines MIXes (vgl. Abschnitt 5.3), wobei die Funktion des Sendens der Eingabe an alle verteilten Teile des MIXes an den vorangehenden MIX (bzw. das unterliegende Kommunikationsnetz) und die Funktion des Sammelns der Ausgaben aller verteilten Teile und die Bildung des Gesamtergebnisses an den nachfolgenden MIX delegiert wird. Nicht delegierbar ist eine Koordinierung aller verteilten Teile des MIXes (vgl. auch Abschnitt 5.3.2.1). Die Koordinierung muß sicherstellen, daß alle nicht ausgefallenen Teile in jedem Schub (vgl. Abschnitt 2.5.2) jeweils die gleichen Eingabe-Informationseinheiten bearbeiten. Anderenfalls kann ein aktiver Angreifer Differenzen zwischen den Eingabe- und Ausgabe-Informationseinheiten einzelner Teile des MIXes herbeiführen und zur Überbrückung des verteilt implementierten MIXes bezüglich des Schutzes der Kommunikationsbeziehung nutzen. Dies gelingt genau dann, wenn Durchschnitte oder Differenzen der Schübe die Kardinalität 1 haben, vgl. Abschnitt 2.5.2.

Eine statische Aktivierung bezüglich des Ersetzens mehrerer MIXe in Folge ist bezüglich des Schutzes der Kommunikationsbeziehung problematisch, da

- das bereits mehrfach erwähnte Koordinations-Problem dann jeweils für die MIXe in Folge bezüglich jeder Stufe besteht und
- eine Informationseinheit nur unter solchen Informationseinheiten bezüglich des Schutzes der Kommunikationsbeziehung geschützt werden kann, die jeweils dieselben MIXe in Folge durchlaufen, d. h. sowohl jeweils dieselben MIXe hintereinander als auch gleichviele Folgen parallel.

Eine statische Aktivierung bezüglich des Ersetzens mehrerer MIXe in Folge ist also nur bei fest vorgegebenen MIX-Kaskaden (vgl. Abschnitt 4.2.3.1) möglich.

Da beide Möglichkeiten statisch erzeugter, statisch aktivierter Redundanz einerseits sehr aufwendig und andererseits bezüglich des Entwurfsspielraums uninteressant zu sein scheinen, wird in den folgenden Unterabschnitten 5.3.2.1 bis 5.3.2.3 ausschließlich statisch erzeugte, *dynamisch aktivierte* Redundanz behandelt.

In Abschnitt 5.3.2.4 wird dann untersucht, inwieweit statisch erzeugte, statisch oder dynamisch aktivierte Redundanz und MIX-zu-MIX-Verschlüsselung zur Verringerung der nötigen Koordinierung zwischen MIXen verwendet werden können.

5.3.2.1 Das Koordinations-Problem

Im MIX-Netz, wie es in Abschnitt 2.5.2 beschrieben wurde, war jeder MIX dafür verantwortlich, solange er sein Schlüsselpaar beibehält, Informationseinheiten mit ihm höchstens einmal zu mixen. Anderenfalls könnte ein Angreifer einen MIX bezüglich einer Informationseinheit, die er zweimal mixt, überbrücken, da sie mit hoher Wahrscheinlichkeit die einzige in den entsprechenden Ausgaben des MIXes zweimal enthaltene Informationseinheit ist.

Können MIXe in die Lage versetzt werden, andere zu ersetzen, so wird diese Verantwortung jedes *einzelnen* MIXes auf ein von ihm und denjenigen MIXen, die ihn möglicherweise ersetzen können, gebildetes *Team* übertragen. Dabei muß das Team dieser Verantwortung auch dann gerecht werden, wenn eine beliebige Teilmenge des Teams ausgefallen und die Kommunikation zwischen nicht ausgefallenen Teammitgliedern unterbrochen ist. Insbesondere dürfen Informationseinheiten, die von ausgefallenen oder gerade unerreichbaren Teammitgliedern bereits gemixt wurden, nicht nochmal von einem Teammitglied gemixt werden – obwohl ein Angreifer versuchen wird, genau das zu erreichen.

Diese Aufgabe kann von einem einfachen Protokoll zwischen den Teammitgliedern gelöst werden. Allerdings ist der Aufwand dieses Protokolls, nämlich die durch seine Ausführung verursachte zusätzliche Verzögerungszeit der eigentlichen Nachrichten sowie die zusätzliche Kommunikation zwischen sowie der zusätzliche Speicherplatz in MIXen, erheblich.

> **Ineffizientes Koordinations-Protokoll** [Pfi1_85 Seite 74]:
> Bevor ein MIX Informationseinheiten mixt, schickt er alle seine Eingabe-Informationseinheiten an alle Teammitglieder, die nicht ausgefallen sind.
> Der MIX mixt eine Informationseinheit nur, nachdem ihm von allen nicht ausgefallenen Teammitgliedern bestätigt wurde, daß sie diese Eingabe-Informationseinheit noch nicht gemixt haben und auch nicht mixen werden.
> Ein ausgefallener MIX bekommt von den anderen Teammitgliedern alle Informationseinheiten, die gemixt wurden oder gemixt werden sollen, bevor er selbst wieder zu mixen beginnt.

Um dieses Koordinations-Protokoll ausführen zu können, muß jeder MIX des Teams alle Informationseinheiten, die von anderen Teammitgliedern oder ihm selbst gemixt wurden (bzw. gemixt werden wollten), speichern. Um den dazu benötigten Speicherplatz erträglich zu halten, können die in Abschnitt 2.5.2.6 beschriebenen drei Möglichkeiten zur Verkleinerung des Speicher- und Suchaufwands (öffentlich bekannte Dechiffrierschlüssel der MIXe öfter tauschen; Zeitstempel; verkürzende Hash-Funktion) verwendet werden.

Wird die Methode der verkürzenden Hash-Funktion bereits vom Anfrager und nicht erst von den Antwortern (im obigen Koordinations-Protokoll) angewandt, so reduziert diese Möglichkeit nicht nur den Speicher- und Suchaufwand, sondern auch den Kommunikationsaufwand.

Andere Methoden zur Verringerung des Kommunikationsaufwandes und der Verzögerungszeit der eigentlichen Nachrichten sind spezifisch für die zweite und dritte Möglichkeit und werden deshalb in den folgenden Abschnitten 5.3.2.2 und 5.3.2.3 behandelt.

Das obige ineffiziente Koordinations-Protokoll setzt voraus, daß MIXe sicher wissen, welche MIXe des Teams ausgefallen bzw. nicht ausgefallen sind. Anderenfalls könnte ein Angreifer zwei Gruppen voneinander zu isolieren und zu überzeugen versuchen, daß die MIXe der anderen Gruppe ausgefallen sind. Ist ihm das gelungen, so ist ein erfolgreicher Angriff leicht. Um dies auch dann zu verhindern, wenn MIXe nicht sicher wissen, welche MIXe des Teams ausgefallen bzw. nicht ausgefallen sind, kann obiges Koordinations-Protokoll um die Regel erweitert werden, daß

nur dann gemixt wird, wenn eine absolute Mehrheit funktioniert (und miteinander kommunizieren kann).

Dies kann mit den üblichen Authentifikationstechniken garantiert werden, vgl. Abschnitt 2.2. Hier – wie auch bei den folgenden effizienten Koordinations-Protokollen – wird der anfragende MIX bei der Bestimmung der absoluten Mehrheit immer als aktiv zustimmend reagierend, d. h. positiv mitgezählt.

5.3.2.2 MIXe mit Reserve-MIXen

Die zweite Möglichkeit (der drei am Ende von Abschnitt 5.3 angekündigten) besteht darin, daß der geheime Schlüssel des ausgefallenen MIXes einem oder mehreren anderen MIXen, die z. B. von derselben Organisation betrieben werden, bekannt ist (Bild 57) oder von vielen MIXen, die z. B. von sich gegenseitig mißtrauenden Organisationen betrieben werden, durch Verwendung eines Schwellwertschemas [Sham_79] rekonstruiert werden kann [Pfi1_85].

Beides ermöglicht ohne Änderungen der Adreß- oder Verschlüsselungsschemata ein MIX-zu-MIX-Protokoll, indem der jeweilige Sender oder MIX bei Ausfall eines (oder mehrerer) MIXe die Informationseinheit zu einem nicht ausgefallenen Mitglied des entsprechenden Teams übermittelt. Dazu benötigt er Information über Ausfälle von MIXen sowie die Teamstruktur. Beides kann entweder global bekannt sein oder auf Anfrage mitgeteilt werden – der Ausfall eines MIXes etwa durch Ausbleiben einer Antwort (Empfangsquittung). Auf die ebenfalls nötige Information über die Erreichbarkeit von MIXen, die durch Ausfälle von Teilen des unterliegenden Kommunikationsnetzes eingeschränkt sein kann, wird aus den zu Beginn dieses Kapitels dargelegten Gründen nicht weiter eingegangen.

In der Begriffswelt der Fehlertoleranz ausgedrückt handelt es sich also um *statisch erzeugte, dynamisch aktivierte Parallel-Redundanz.*

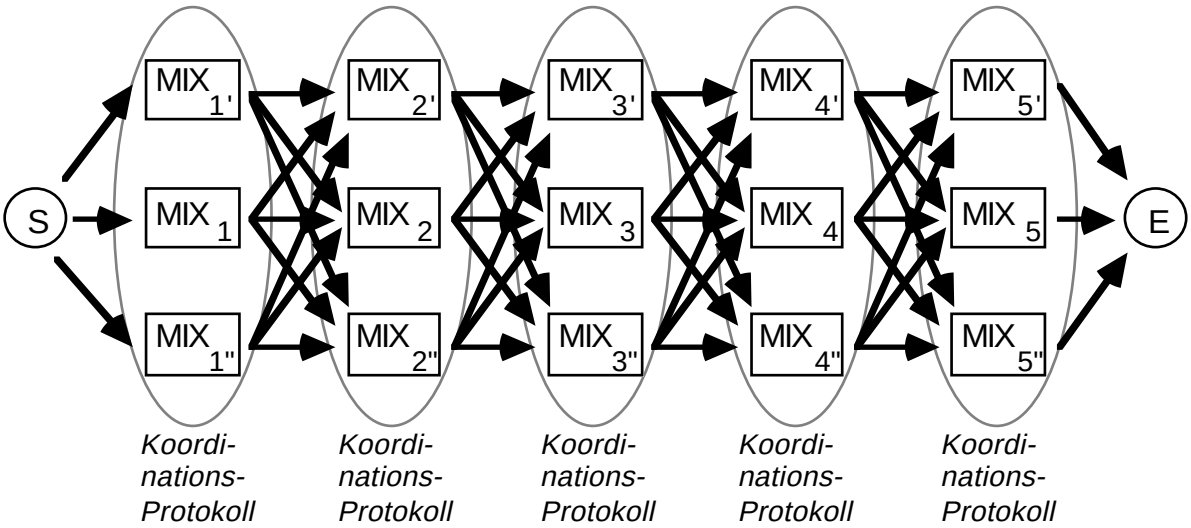

Bild 57: MIX_i kann alternativ von MIX_i' oder MIX_i'' ersetzt werden (i = 1, 2, 3, 4, 5)

Wie angekündigt, kann der Aufwand des Koordinations-Protokolls zur Verhinderung mehrfachen Mixens derselben Informationseinheit drastisch reduziert werden:

> **Effizientes Koordinations-Protokoll für MIXe mit Reserve-MIXen** [Pfi1_85 Seite 75f]:
> Jegliche zusätzliche Verzögerung des Mixens kann vermieden werden, wenn jeder MIX mit seinen Reserve-MIXen vereinbart, daß sie nur dann mit seinem Schlüssel mixen, wenn er ausgefallen ist.
> Es genügt dann, daß er seine Eingabe-Informationseinheiten an eine deutlich größere als absolute Mehrheit aller Teammitglieder spätestens dann abschickt, wenn er die zugehörigen Ausgabe-Informationseinheiten ausgibt. Hört er auf zu mixen, wenn er innerhalb eines vorgegebenen Zeitraums keine authentifizierten Empfangsbestätigungen einer absoluten Mehrheit aller anderen Teammitglieder erhält, so kann ein Angreifer ihn mittels Isolierung höchstens bezüglich der Informationseinheiten überbrücken, für die er noch keine Empfangsbestätigung erhielt.
> Reserve-MIXe, deren Ausfall ein MIX überprüfen kann (etwa mittels authentifizierter Kommunikation mit dessen Kommunikationsprozessor), brauchen bei der Ermittlung einer (absoluten) Mehrheit nicht gezählt zu werden.
> Ist ein MIX ausgefallen, so können die Reserve-MIXe einen von ihnen als seinen *Vertreter* bestimmen (und etwa zur Rekonstruktion des MIX-Schlüssels befähigen, falls ein Schwellwertschema [Sham_79] verwendet wurde). Der Vertreter verhält sich genauso wie der MIX, sofern er nicht ausgefallen wäre, bis er entweder selbst auch ausfällt (und die übrigen Reserve-MIXe einen neuen Vertreter bestimmen) oder der vertretene MIX repariert ist und synchronisiert mit dem Ende des stellvertretenden Mixens seines Vertreters mit seinem Mixen beginnt.

Meiner Meinung nach wird das Risiko, daß ein Angreifer einen MIX bezüglich der Informationseinheiten, für die er noch keine Empfangsbestätigungen erhielt, mittels Isolierung überbrücken kann, bei weitem durch die Vermeidung jeder zusätzlichen Verzögerung des Mixens aufgewogen. Denn aktive Angriffe, die diese Schwäche des Koordinations-Protokolls auszunutzen versuchen, können leicht entdeckt werden (zumindest wenn sie oft erfolgen) und müssen an sehr vielen Stellen in aufeinander abgestimmter Weise eingreifen, wenn Informationseinheiten jeweils mehrere MIXe durchlaufen: Um den Weg einer bestimmten Informationseinheit von ihrem Sender zu ihrem Empfänger zu verfolgen, muß ein Angreifer in jedem Team, von dem jeweils ein Mitglied die Informationseinheit mixen muß, den gerade aktiven MIX (kontrollieren oder) zum Ausfall bringen oder isolieren, nachdem er diese Informationseinheit mixte.

Ein MIX sollte solche MIXe als seine Reserve-MIXe wählen, die physisch zumindest einige zehn Kilometer auseinanderliegen, damit sich so wenig Fehler (oder aktive physische Angriffe) wie möglich auf mehrere auswirken [Pfi1_85 Seite 76], vgl. das zu Beginn von Kapitel 5 im Kontext des Fehlermodells Gesagte.

Betreibt eine Organisation mehrere MIXe an räumlich weit entfernten Stellen, so scheint es sehr vernünftig zu sein, daß diese MIXe füreinander als Reserve-MIXe fungieren.

Datenschutz-Kriterium:
Wenn die MIXe geeignet koordiniert sind, so sind MIXe mit Reserve-MIXen genauso sicher wie die ursprünglichen Schemata (vgl. Abschnitt 2.5.2), sofern bei einem der in der Verschlüsselungsstruktur verwendeten MIXe sein Team nicht vom Angreifer kontrolliert wird.
Ein Team wird zumindest dann nicht vom Angreifer kontrolliert, wenn er kein Teammitglied kontrolliert oder aber bei Verwendung eines Schwellwertschemas sowohl nicht den eigentlichen MIX, als auch keinen Vertreter, als auch weniger als zur Rekonstruktion des Schlüssels nötige MIXe des Teams kontrolliert (und damit nie den Schlüssel erhält) als auch keine absolute Mehrheit der MIXe des Teams kontrolliert (sonst könnte diese Mehrheit auch ohne Ausfall des gerade mixenden MIXes einen Stellvertreter etablieren lassen und beide parallel und unkoordiniert mixen lassen).

5.3.2.3 Auslassen von MIXen

Die dritte Möglichkeit besteht darin, daß jeder MIX in jeder Nachricht genügend Information erhält, um einen MIX (oder im allgemeinen Fall: bis zu *ü* MIXe mit einer beliebigen natürlichen Zahl *ü*) überbrücken und auslassen zu können [Pfi1_85 Seite 77ff].

Im Gegensatz zur zweiten benötigt die dritte Möglichkeit Änderungen der Adreß- oder Verschlüsselungsschemata, um ebenfalls ein MIX-zu-MIX-Protokoll zu ermöglichen. Diese geänderten Adreß- und Verschlüsselungsschemata werden in Abschnitt 5.3.2.3.1 hergeleitet.

Danach werden in Abschnitt 5.3.2.3.2 Datenschutz-Kriterien zur Charakterisierung der mit diesen Adreß- und Verschlüsselungsschemata bei geeigneter Koordinierung erreichbaren Anonymität der Kommunikationsbeziehung aufgestellt.

In den Abschnitten 5.3.2.3.3 und 5.3.2.3.4 werden dann passende und möglichst effiziente Koordinations-Protokolle für die zwei möglichen Betriebsarten entwickelt: entweder werden nur ausgefallene, d. h. möglichst wenig, MIXe ausgelassen, oder aber möglichst viele. Letzteres verkompliziert das Koordinations-Problem, erlaubt aber in manchen Situationen einen Effizienzgewinn.

5.3.2.3.1 Nachrichten- und Adreßformate

Um das Verständnis zu erleichtern, wird zuerst der Fall beschrieben, daß jeder MIX den nächsten MIX in einer Folge gewählter MIXe auslassen kann. In diesem Fall kann dies Fehlertoleranzverfahren den Ausfall eines oder sogar mehrerer nicht aneinandergrenzender MIXe tolerieren.

Um einen MIX auslassen zu können, muß sein Vorgänger nicht nur die für ihn bestimmte Nachricht bilden können, sondern auch die für seinen Nachfolger bestimmte (Bild 58).

Wenn jeder MIX die Nachrichten sowohl für seinen Nachfolger als auch für dessen Nachfolger separat erhält, wächst die Länge der Nachrichten exponentiell mit der Zahl der benutzten MIXe. Um dies zu vermeiden, wählt der Sender einer Nachricht (wie bei allen indirekten Umcodierungsschemata, vgl. Abschnitt 2.5.2) für jeden MIX einen unterschiedlichen Schlüssel (beispielsweise eines effizienten symmetrischen Konzelationssystems), mit dem dieser MIX die

für seinen Nachfolger bestimmte Nachricht entschlüsselt. Jeder MIX erhält diesen und den für seinen Nachfolger bestimmten Schlüssel mit seinem öffentlich bekannten Dechiffrierschlüssel verschlüsselt. Separat und mit den öffentlich nicht bekannten Schlüsseln entsprechend verschlüsselt erhält er den Rest der Nachricht. Die Adressen der nächsten beiden MIXe können jeder Nachricht unverschlüsselt vorangestellt oder mit den beiden erwähnten Schlüsseln zusammen mit dem öffentlich bekannten Dechiffrierschlüssel des MIXes verschlüsselt werden. Im folgenden wird dies formaler beschrieben.

kennt	kennt	kennt	kennt	kennt	kennt	kennt
$c_1,c_2,c_3,$ c_4,c_5,c_E	$c_1,c_2,c_3,$ $c_4,c_5,c_E,$ d_1	$c_1,c_2,c_3,$ $c_4,c_5,c_E,$ d_2	$c_1,c_2,c_3,$ $c_4,c_5,c_E,$ d_3	$c_1,c_2,c_3,$ $c_4,c_5,c_E,$ d_4	$c_1,c_2,c_3,$ $c_4,c_5,c_E,$ d_5	$c_1,c_2,c_3,$ $c_4,c_5,c_E,$ d_E
bildet zufällig $k_5,k_4,k_3,$ k_2,k_1	erfährt k_1,k_2	erfährt k_2,k_3	erfährt k_3,k_4	erfährt k_4,k_5	erfährt k_5	

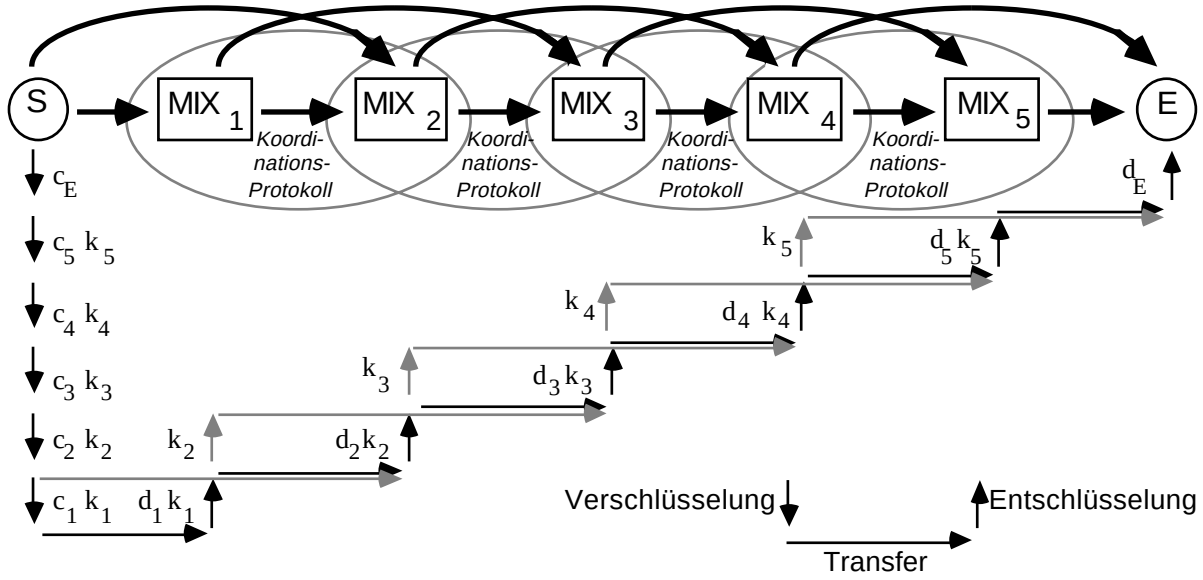

Bild 58: Jeweils ein MIX kann ausgelassen werden; Die Koordinations-Protokolle werden im Bild zwischen Gruppen minimalen Umfangs abgewickelt

Sei wie in Abschnitt 2.5.2 $A_1,...,A_n$ die Folge der Adressen und $c_1,...,c_n$ die Folge der öffentlich bekannten Chiffrierschlüssel der gewählten MIX-Folge $MIX_1,...,MIX_n$, wobei c_1 auch ein geheimer Schlüssel eines symmetrischen Kryptosystems sein kann. Sei A_{n+1} die Adresse des Empfängers, der zur Vereinfachung der Notation MIX_{n+1} genannt wird, und c_{n+1} sein Chiffrierschlüssel. Sei $k_1,...,k_n$ die gewählte Folge nichtöffentlicher Schlüssel (beispielsweise eines symmetrischen Konzelationssystems). Der Sender bildet die Nachrichten N_i, die MIX_i erhalten wird, gemäß dem folgenden rekursivem Bildungsschema ausgehend von der Nachricht N, die der Empfänger (MIX_{n+1}) erhalten soll:

$N_{n+1} = c_{n+1}(N)$ (Schema 1)
$N_n = c_n(k_n),k_n(A_{n+1},N_{n+1})$
$N_i = c_i(k_i,A_{i+1},k_{i+1}),k_i(A_{i+1},N_{i+1})$ für $i = 1,...,n\text{-}1$

Selbstverständlicherweise ist dies Schema nicht das einziggeeignete. Beispielsweise erfüllt das folgende Schema denselben Zweck:

$N_{n+1} = c_{n+1}(N)$ (Schema 2)
$N_n = c_n(k_n,A_{n+1}),k_n(N_{n+1})$
$N_i = c_i(k_i,A_{i+1},k_{i+1},A_{i+2}),k_i(N_{i+1})$ für $i = 1,...,n\text{-}1$

Der Sender sendet jeweils N_1 an MIX_1.

In beiden Schemata kann MIX_i die Nachrichten N_{i+1} und N_{i+2} sowie die Adressen A_{i+1} und A_{i+2} aus N_i berechnen.

Bei einigen im folgenden diskutierten Koordinations-Protokollen ist es auch wichtig, daß MIX_i überprüfen kann, daß sein Vorgänger $MIX_{i\text{-}1}$ kein Bit der Nachricht N_i geändert hat (und entsprechend auch sonst niemand, da $MIX_{i\text{-}1}$ am meisten über die Nachricht erfuhr und deswegen am zielgerichtetsten handeln konnte).

Solange die Kryptosysteme nicht gebrochen sind, kann ein Angreifer nur Nachrichtenteile gezielt verändern, zu denen er die verwendeten Schlüssel kennt. Anderenfalls geht die Nachricht einfach verloren oder wird von einer Station, bei der die Nachricht nach ihrer Entschlüsselung mittels fehlererkennender Codes als fehlerhaft erkannt wird, einfach ignoriert. In beiden Fällen gewinnt der Angreifer dadurch keine für ihn nützliche Information. Also hat $MIX_{i\text{-}1}$ die Möglichkeiten, den ganzen mit c_i verschlüsselten Teil zu ersetzen (ohne den Inhalt des ursprünglichen lesen zu können, da er zwar c_i, nicht aber d_i kennt) oder nur an dem mit k_i verschlüsselten Teil zu manipulieren.

Die Gefahr hierbei ist, daß er versuchen kann, die Adressen zu ändern. Dies ist für den Schutz der Kommunikationsbeziehung nicht kritisch, solange Adressen nur für die Vermittlung von Nachrichten verwendet werden, da sowieso unterstellt ist, daß der Angreifer alle Leitungen kontrolliert. Es kann aber dann kritisch werden, wenn die Nachrichten festlegen, welche MIXe sich miteinander koordinieren müssen, damit keine Nachricht zweimal gemixt wird.

In beiden Schemata müßte der Angreifer den mit c_i verschlüsselten Teil ändern, um eine Adresse zu ändern. Um dies zu tun, muß er ein neues k_i erfinden. Dann wird dies aber nach der Entschlüsselung des jeweils mit k_i verschlüsselten Teiles, nämlich $k_{i+1}(A_{i+2},N_{i+2})$ in Schema 1 oder $k_{i+1}(N_{i+2})$ in Schema 2 erkannt. Dazu müssen diese Teile jeweils genug Redundanz enthalten, damit MIX_i dies bereits feststellen kann.

Wird ein Koordinations-Protokoll verwendet, bei dem diese Überprüfung nicht nötig ist, kann in Schema 1 das erste A_{i+1} weggelassen werden.

Die Wahl zwischen Schema 1 und Schema 2, d. h. ob A_{i+2} im ersten, mit einem aufwendigen asymmetrischen Konzelationssystem verschlüsselten Teil oder im zweiten, mit einem weniger aufwendigen symmetrischen Konzelationssystem verschlüsselten Teil (unter dem Namen A_{i+1} für $i := i+1$) enthalten ist, hängt vom verwendeten asymmetrischen Konzelationssystem

ab: Muß etwa aus Gründen der Sicherheit des asymmetrischen Konzelationssystems die Länge der mit ihm verschlüsselten Informationseinheiten so groß sein (wie dies etwa für RSA, vgl. Abschnitt 2.2.1.2 der Fall ist), daß A_{i+2} auf jeden Fall mit hineinpaßt, ist es natürlich sinnvoller Schema 2 zu verwenden, anstatt in Schema 1 mit zufälligen Bitketten aufzufüllen. Denn es ist trivialerweise weniger aufwendig, A_{i+2} mit dem aufwendigeren asymmetrischen Konzelationssystem ohne zusätzlichen Aufwand mitverschlüsseln zu lassen als A_{i+2} (unter dem Namen A_{i+1} für $i := i+1$) mit dem weniger aufwendigen symmetrischen Konzelationssystem mit zusätzlichem Aufwand zu ver- und entschlüsseln. Wenn A_{i+2} irgendwelche Redundanz enthält, so ist (im Prinzip) Vorsicht geboten, daß die Entropie (d. h. der zufällige und deshalb dem Angreifer unbekannte Informationsgehalt) von k_i,A_{i+1},k_{i+1},A_{i+2} nicht zu gering wird. Aber da das symmetrische Kryptosystem eine vollständige Suche über seinen Schlüsselraum vereiteln muß (vgl. Abschnitt 2.2.1.1), die Schlüssellänge dafür also zu groß sein muß (was ab etwa 100 Bit Länge sicher der Fall ist), enthalten sowohl k_i als auch k_{i+1} genug Entropie.

Können mit dem asymmetrischen Konzelationssystem so kurze Informationseinheiten sicher verschlüsselt werden, daß in ihnen nicht einmal Platz für A_{i+1} ist, so kann eine **Einwegfunktion** *f* verwendet werden. Eine Einwegfunktion (one-way function) ist eine bekanntgegebene oder öffentlich bekannte Funktion, bei der jeder, der sie kennt, zu einem Argument leicht den Funktionswert berechnen kann, aber niemand zu einem ihm vorgegebenen Funktionswert mit vertretbarem Aufwand ein passendes Argument finden kann [DaPr_84 Seite 137, 223f]. Etwas genauer formuliert bedeutet dies, daß niemand zu einem ihm vorgegebenen Funktionswert ein passendes Argument einfacher als dadurch finden kann, daß er alle möglichen Argumente (in einer möglichst geschickten Reihenfolge) ausprobiert – die Sicherheit einer Einwegfunktion kann also nie informationstheoretisch, sondern immer nur komplexitätstheoretisch sein, vgl. Abschnitt 2.2.2.2. Mit den üblichen Bezeichnungen „Urbild“ für das Funktionsargument und „Bild“ für den Funktionswert kann dies sehr kurz formuliert werden:

Urbild $\rightarrow$ Bild ist leicht, Bild $\rightarrow$ Urbild ist schwer.

Nach dem in Abschnitt 2.2 über Kryptosysteme Gesagten kann aus jeder symmetrischen Blockchiffre eine Einwegfunktion gewonnen werden, indem zu genügend vielen vorgegebenen Klartext-Schlüsseltext-Paaren der Schlüssel gesucht wird. „Genügend viele“ deshalb, weil es zu einem Klartext-Schlüsseltext-Paar nicht nur sehr viele passende Schlüssel geben kann, sondern es auch leicht sein kann, einen zu bestimmen. Dies ist z. B. bei MDES, vgl. Anhang, der Fall. (Für den mit DES und MDES vertrauten Leser wird hier kurz skizziert, wie dies geschehen kann: Werden die Substitutionen so gewählt, daß in jeder Substitution jeder Ausgabewert vorkommt, was sehr sinnvoll ist, so kann zu einem vorgegebenen Klartext-Schlüsseltext-Paar ein passender Schlüssel sehr leicht folgendermaßen bestimmt werden. Falls sie nicht sowieso festgelegt sind, definiere zuerst die Permutationen. Wähle danach beliebige Werte für die ersten 14•48 Schlüsselbits und führe ausgehend vom Klartext die ersten 14 Runden von MDES durch. Errechne ausgehend vom Schlüsseltext den Wert vor der Ausgangspermutation. Hieraus ergeben sich die Ausgabewerte jeder Substitution. Bestimme jeweils einen hierzu passenden Eingabewert. Hieraus ergeben sich die Schlüsselbits von Runde 15 und 16.)

Ebenso kann aus jedem asymmetrischen Konzelationssystem eine Einwegfunktion gewonnen werden, indem der geheimgehaltene Schlüssel vergessen wird.

Es gibt noch andere, effizientere Implementierungen, beispielweise solche, die aus Bitketten (bit strings) variabler (und deshalb beliebig großer) Länge als Argumente Bitketten konstanter Länge (z. B. von 100 Bit Länge) als Funktionswerte erzeugen [DaPr_84 Seite 280f]. Deshalb ist das im folgenden beschriebene Verfahren tatsächlich sinnvoll.

Da dies keine Arbeit über Kryptographie, sondern nur über manche ihrer Anwendungen ist, wird die Einwegfunktion erst hier (und nicht in Abschnitt 2.2) eingeführt und der tiefere theoretische Zusammenhang zwischen Kryptosystemen und Einwegfunktionen nicht diskutiert. Generelle Bemerkungen hierzu finden sich in [Yao1_82, GoGM_84, Kran_86].

Damit die Einwegfunktion *f* nicht durch vollständige Suche über den Adreßraum invertiert werden kann, sollte sie ggf. nicht nur auf eine Adresse, sondern zusätzlich auf etwas, das viel Entropie enthält, angewendet werden. Dann kann der Funktionswert mehr Entropie enthalten als die Adresse. Um MIX_{i-1} daran zu hindern, A_{i+1} in N_i zu ändern, kann dann folgendes Verschlüsselungsschema verwendet werden:

$$\begin{aligned} N_{n+1} &= c_{n+1}(N) \\ N_n &= c_n(k_n),k_n(A_{n+1},N_{n+1}) \\ N_i &= c_i(k_i,k_{i+1}),k_i(f(k_{i+1},A_{i+1}),A_{i+1},N_{i+1}) \qquad \text{für } i = 1,...,n\text{-}1 \end{aligned} \qquad \text{(Schema 3)}$$

Jeder MIX_i prüft, ob *f* auf das angewandt, was er für k_{i+1},A_{i+1} hält, den ersten Teil des entschlüsselten Restes der Nachricht ergibt.

Um A_{i+1} unentdeckt verändern zu können, müßte MIX_{i-1} den entsprechenden Funktionswert $f(k_{i+1},X)$ für ein $X \neq A_{i+1}$ finden. Dies aber ist bei einer Einwegfunktion ohne Kenntnis von k_{i+1} unmöglich.

Als nächstes ist zu zeigen, wie die anonymen Rückadressen von Abschnitt 2.5.2.3 ebenfalls fehlertolerant gemacht werden können.

Damit der Benutzer einer anonymen Rückadresse auch bei Ausfall eines oder sogar mehrerer nicht aneinandergrenzender MIXe, die in der Rückadresse verwendet wurden, antworten kann, wird eine *fehlertolerante anonyme Rückadresse* (R_1,A_1,k_0,k_1) folgendermaßen gebildet, wobei der *Rückadreßteil* wie in Abschnitt 2.5.2.3 ausgehend von einem zufällig gewählten eindeutigen Namen *e* gebildet wird:

$$\begin{aligned} R_{m+1} &= e \\ R_m &= c_m(k_m),k_m(A_{m+1},R_{m+1}) \\ R_j &= c_j(k_j,A_{j+1},k_{j+1}),k_j(A_{j+1},R_{j+1}) \qquad \text{für } j = 1,...,m\text{-}1 \end{aligned} \qquad \text{(Schema 4a)}$$

Der Benutzer der fehlertoleranten anonymen Rückadresse benutzt (R_1,A_1,k_0,k_1) und den Inhalt seiner Antwortnachricht I, um $N_1 = R_1,k_0(I)$ zu bilden. Dies sendet er unter Verwendung von A_1 an MIX_1, sofern dieser nicht ausgefallen ist. Anderenfalls verwendet er k_1, um A_2 zu finden, $N_2 = R_2,k_1(k_0(I))$ zu bilden und unter Verwendung von A_2 an MIX_2 zu senden.

Erhält MIX_j eine Nachricht $N_j = (R_j,I_j)$, wobei I_j der *Nachrichteninhaltsteil* und R_j der oben definierte Rückadreßteil ist, benutzt er seinen geheimgehaltenen Dechiffrierschlüssel d_j dazu, k_j, A_{j+1} und k_{j+1} aus R_j zu erhalten.

Danach kann er $I_{j+1} = k_j(I_j)$ bilden, $k_j(A_{j+1},R_{j+1})$ entschlüsseln und $N_{j+1} = (R_{j+1},I_{j+1})$ unter Verwendung von A_{j+1} an MIX_{j+1} senden, sofern dieser nicht ausgefallen ist.

Anderenfalls bildet MIX_j auch $I_{j+2} = k_{j+1}(I_{j+1})$, entschlüsselt $k_{j+1}(A_{j+2},R_{j+2})$ und sendet $N_{j+2} = (R_{j+2},I_{j+2})$ an MIX_{j+2}.

Während all diesen Schritten kann MIX_j (genau wie bei Schema 1) überprüfen, daß an den Rückadreßteilen nichts verändert wurde.

Zusammenfassend wird die Nachricht N_j, die MIX_j erhalten soll, vom Inhalt der Antwortnachricht I nach dem folgenden rekursiven Schema gebildet:

$$\begin{array}{lllll} N_1 & = & R_1,I_1; & I_1 = k_0(I) & \\ N_j & = & R_j,I_j; & I_j = k_{j-1}(I_{j-1}) & \text{für } j = 2,...,m+1 \end{array} \qquad \text{(Schema 4b)}$$

Nur derjenige, der die fehlertolerante anonyme Rückadresse gebildet hat, kann $I_{m+1} = k_m(...k_1(k_0(I))...)$ entschlüsseln, denn er generierte die Schlüssel k_0 bis k_m.

Dieses fehlertolerante anonyme Rückadreßschema wurde in Schema 1 entsprechender Weise gebildet. Variationen gemäß Schema 2 und Schema 3 sind möglich und kanonisch.

Als nächstes werden alle Schemata von der Fehlervorgabe höchstens eines ausgefallenen MIXes hintereinander auf höchstens $ü$ (überbrückbare) ausgefallene MIXe hintereinander verallgemeinert. Diese Verallgemeinerung erlaubt eine weitere wesentliche Verbesserung der Verfügbarkeit. Die fehlertoleranten Verschlüsselungsschemata, die eine direkte Überbrückung von $ü$ MIXen erlauben, können die folgenden drei Grundformen haben. In allen dreien kann MIX_i (bei $i \le n\text{-}ü$) N_{i+1} bis $N_{i+ü+1}$ und A_{i+1} bis $A_{i+ü+1}$ aus N_i berechnen und überprüfen, daß seine Vorgänger nichts an der Nachricht unerlaubterweise verändert haben, da sie $k_{i+ü+1}$ nicht kennen. Ist $i > n\text{-}ü$, kann MIX_i N_{i+1} bis N_{n+1} und A_{i+1} bis A_{n+1} aus N_i berechnen und überprüfen, daß diejenigen seiner Vorgänger, die ihn nicht sowieso überbrücken können, nichts an der Nachricht unerlaubterweise verändert haben, da sie k_n nicht kennen.

Erweiterung von Schema 1:

$$\begin{array}{lll} N_{n+1} & = & c_{n+1}(N) \\ N_i & = & c_i(k_i,A_{i+1},k_{i+1},...,A_n,k_n),k_i(A_{i+1},N_{i+1}) \quad \text{für } i = n\text{-}ü+1,...,n \\ N_i & = & c_i(k_i,A_{i+1},k_{i+1},...,A_{i+ü},k_{i+ü}),k_i(A_{i+1},N_{i+1}) \quad \text{für } i = 1,...,n\text{-}ü \end{array} \qquad \text{(Schema 5)}$$

Erweiterung von Schema 2:

$$\begin{array}{lll} N_{n+1} & = & c_{n+1}(N) \\ N_i & = & c_i(k_i,A_{i+1},k_{i+1},...,A_n,k_n,A_{n+1}),k_i(N_{i+1}) \quad \text{für } i = n\text{-}ü+1,...,n \\ N_i & = & c_i(k_i,A_{i+1},k_{i+1},...,A_{i+ü},k_{i+ü},A_{i+ü+1}),k_i(N_{i+1}) \quad \text{für } i = 1,...,n\text{-}ü \end{array} \qquad \text{(Schema 6)}$$

Da – wie erwähnt – eine Einwegfunktion lange Bitketten komprimieren kann, da beispielsweise 100 Bit als Funktionswert ausreichen, ist das folgende Schema besonders für große $ü$ geeignet.

Erweiterung von Schema 3:

$N_{n+1} = c_{n+1}(N)$ (Schema 7)
$N_i = c_i(k_i,...,k_n),k_i(f(k_n,A_{i+1},...,A_n),A_{i+1},N_{i+1})$ für $i = n\text{-}ü+1,...,n$
$N_i = c_i(k_i,...,k_{i+ü}),k_i(f(k_{i+ü},A_{i+1},...,A_{i+ü}),A_{i+1},N_{i+1})$ für $i = 1,...,n\text{-}ü$

Als nächstes wird das fehlertolerante Rückadreßschema (Schema 4) zu einer *ü Ausfälle hintereinander tolerierenden anonymen Rückadresse* $(R_1,A_1,k_0,k_1,...,k_ü)$ verallgemeinert.

Auch hier ist dies nur das von Schema 1 abgeleitete Verschlüsselungsschema, in dem der Rückadreßteil wie eine Nachricht in Schema 5 gebildet wird. Von den Schemata 2 oder 3 (bzw. 6 oder 7) abgeleitete Verschlüsselungsschemata sind möglich und kanonisch.

R_j und I_j haben dieselbe Bedeutung wie in Schema 4.

Erweiterung von Schema 4:

$R_{m+1} = e$ (Schema 8a)
$R_j = c_j(k_j,A_{j+1},k_{j+1},...,A_m,k_m),k_j(A_{j+1},R_{j+1})$ für $j = m\text{-}ü+1,...,m$
$R_j = c_j(k_j,A_{j+1},k_{j+1},...,A_{j+ü},k_{j+ü}),k_j(A_{j+1},R_{j+1})$ für $j = 1,...,m\text{-}ü$

$N_1 = R_1,I_1;\quad I_1 = k_0(I)$ (Schema 8b = Schema 4b)
$N_j = R_j,I_j;\quad I_j = k_{j\text{-}1}(I_{j\text{-}1})$ für $j = 2,...,m+1$

Alle Verschlüsselungsschemata dieses Abschnitts sind [Pfi1_85 Seite 78ff] entnommen.

5.3.2.3.2 Datenschutz-Kriterien

Sofern die MIXe (beispielsweise durch das ineffiziente Koordinations-Protokoll von Abschnitt 5.3.2.1) geeignet koordiniert sind, so daß sie niemals dieselbe Transformation auf dieselbe Nachricht zweimal anwenden, ist die Sicherheit beim Auslassen von MIXen, d. h. unter Verwendung der Verschlüsselungsschemata von Abschnitt 5.3.2.3.1 wie untenstehend charakterisierbar. Wieder wird zuerst der Fall behandelt, daß jeder MIX nur den nächsten MIX auslassen kann.

Datenschutz-Kriterium [vgl. Pfi1_85 Seite 83f]:
Wenn die MIXe geeignet koordiniert sind, so sind die Schemata 1, 2 und 3 genauso sicher wie das nichtfehlertolerante indirekte Umcodierungsschema (vgl. Abschnitt 2.5.2), sofern entweder

a) der erste MIX, der die Nachricht mixt oder
b) zumindest zwei im Verschlüsselungsschema aufeinanderfolgende MIXe, die, sofern sie nicht ausgefallen sind, miteinander kommunizieren können und deren Kommunikation bei Ausfall eines MIXes vom (unterliegenden) Kommunikationsnetz zuverlässig gepuffert wird, so daß der ausgefallene MIX vom anderen an ihn Abgesendetes auch dann zum Zeitpunkt des Abschlusses seiner Reparatur erhält, wenn der andere dann gerade ausgefallen ist, oder
c) zumindest zwei im Verschlüsselungsschema aufeinanderfolgende MIXe und eine absolute Mehrheit aller MIXe

vom Angreifer nicht kontrolliert sind.

Für das fehlertolerante anonyme Rückadreßschema (Schema 4) muß im obigen Kriterium Bedingung a) lediglich durch „der Sender der Antwortnachricht und der erste MIX, der die Nachricht mixt oder“ ersetzt werden.

Für die erweiterten Schemata, bei den jeder MIX die nächsten *ü* MIXe auslassen kann, gilt fast dasselbe Kriterium. Lediglich „zwei“ muß durch „*ü*+1“ ersetzt werden.

Begründungen für diese Datenschutz-Kriterien folgen in den beiden nächsten Abschnitten zusammen mit und für verschiedene Betriebsarten und bei ihnen geeigneten effizienten Koordinations-Protokollen.

5.3.2.3.3 Auslassen von möglichst wenig MIXen

Bei der ersten Betriebsart werden möglichst wenig MIXe ausgelassen. Dies bedeutet, daß nur solche MIXe ausgelassen werden, die ausgefallen (oder etwa durch Fehler des unterliegenden Kommunikationsnetzes unerreichbar geworden) sind. Bild 59 veranschaulicht das sowohl generell als auch an einem Beispiel. Dieses Beispiel wird im nächsten Abschnitt, der die entgegengesetzte Strategie, nämlich das Auslassen so vieler MIXe wie möglich, erläutert, in Bild 60 wieder aufgegriffen.

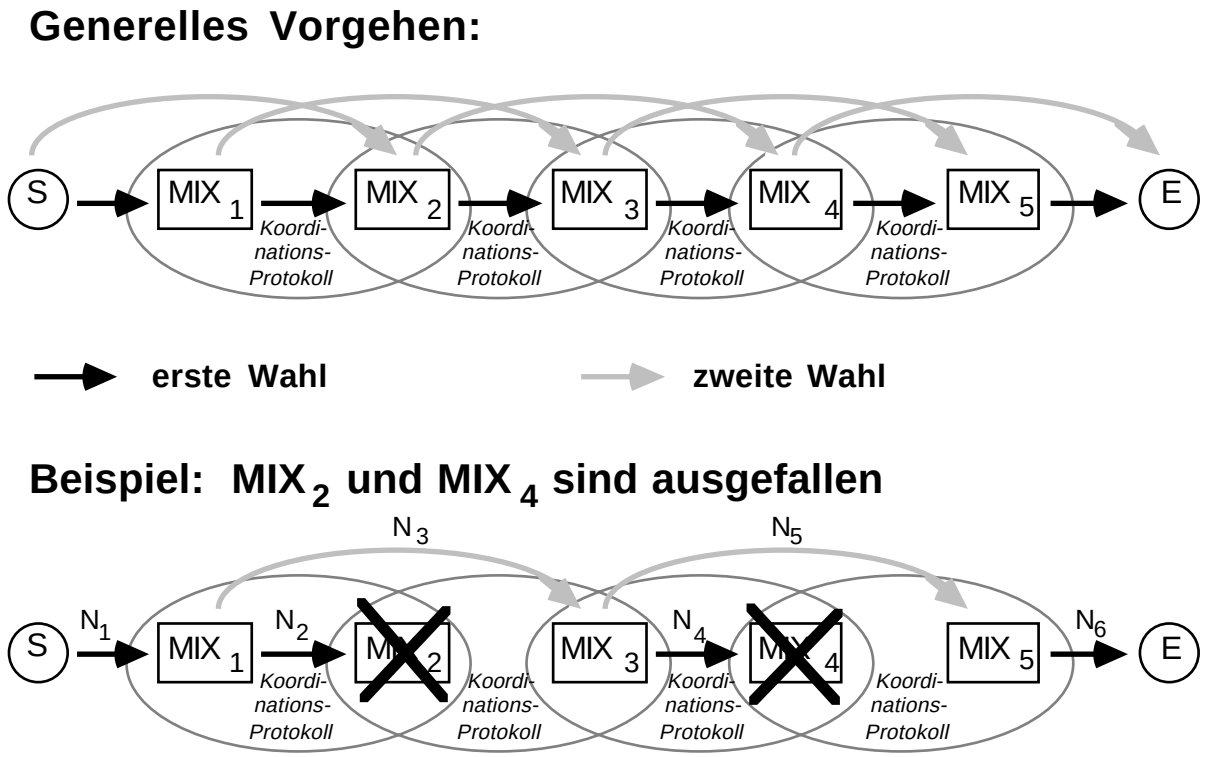

Bild 59: Auslassen von möglichst wenig MIXen bei einem Verschlüsselungsschema, bei dem jeweils ein MIX ausgelassen werden kann; Die Koordinations-Protokolle werden im Bild zwischen Gruppen minimalen Umfangs abgewickelt.

Zunächst wird an einem Beispiel erläutert, wie ein Angreifer zwei MIXe bei der Betriebsart „Auslassen von möglichst wenig MIXen“ überbrücken kann, sofern diese nicht geeignet koordiniert sind.

Beispiel:

Seien die MIXe MIX_u und MIX_{u+1} zwei bezüglich der Verschlüsselungsstruktur aufeinanderfolgende MIXe, die von einem Angreifer, der alle anderen MIXe kontrolliert, nicht kontrolliert werden. Sofern MIX_u und MIX_{u+1} unkoordiniert handeln, kann sie der Angreifer mit folgendem Trick überbrücken: Er sendet N_u an MIX_u und teilt diesem mit, daßMIX_{u+1} ausgefallen ist. MIX_u wird entsprechend N_{u+2} an MIX_{u+2} senden. Zusätzlich sendet der Angreifer N_{u+1} an MIX_{u+1} und teilt diesem mit, daß MIX_{u+2} nicht ausgefallen ist. Es ist bemerkenswert, daß der Angreifer gegenüber MIX_{u+1} nicht lügen muß, da MIX_{u+1} seinen Vorgänger nicht kennt. MIX_{u+1} wird entsprechend N_{u+2} an MIX_{u+2} senden. Die Nachricht, die MIX_{u+2} zweimal erhält, ist die zu N_u und N_{u+1} gehörige. *(Ende des Beispiels)*

Wie schon erwähnt kann das ineffiziente Koordinations-Protokoll von Abschnitt 5.3.2.1 natürlich auch bei der Betriebsart „Auslassen von möglichst wenig MIXen“ verwendet werden. In diesem Fall muß ein MIX, der einen anderen ausläßt, berücksichtigen, daß er nicht einmal, sondern zweimal mixt. Für jedes Mixen muß er das Koordinations-Protokoll separat, d. h. nacheinander, ausführen.

Eine effizientere Koordinierung kann folgendermaßen erreicht werden:

> **Effizientes Koordinations-Protokoll für „Auslassen von möglichst wenig MIXen“** [Pfi1_85 Seite 85f]:
> Jeder MIX sendet seine Eingabe-Informationseinheiten spätestens dann an alle anderen MIXe, wenn er die entsprechenden Ausgabe-Informationseinheiten ausgibt. Dies erlaubt ihnen, diese Informationseinheiten nicht noch einmal zu mixen, selbst wenn der MIX sofort nach der Ausgabe ausfällt.
> Ein MIX läßt nur dann einen MIX aus, wenn er entweder dessen Ausfall (etwa durch authentifizierte Kommunikation mit dessen Kommunikationsprozessor) überprüfen kann oder aber dieser MIX von einer absoluten Mehrheit aller MIXe für ausgefallen erklärt wird und er auf regelmäßig an ihn abgeschickte Anfragen nicht antwortet.
> Ein MIX, der entweder überprüfbar ausgefallen ist oder aber von einer absoluten Mehrheit für ausgefallen erklärt wurde, wird nur bezüglich Nachrichten ausgelassen, die er nie als gemixt bekanntgab.
> Andererseits mixt ein MIX nur, wenn er mit einer absoluten Mehrheit aller MIXe regelmäßig kommunizieren kann. MIXe, deren Ausfall der betrachtete MIX überprüfen kann (s. o.), brauchen bei der Bestimmung einer absoluten Mehrheit nicht gezählt zu werden.
> Ist ein ausgefallener MIX repariert oder ein intakter MIX nicht mehr durch Ausfall des unterliegenden Kommunikationsnetzes (sei es durch Fehler „aus Versehen“, sei es durch einen aktiven Angriff) von der Mehrheit der anderen MIXen isoliert, so kündigt er seine Bereitschaft, wieder zu mixen, an und wartet eine gewisse Weile. Dies erlaubt allen MIXen, mit denen er kommunizieren kann, zu antworten. Er beginnt nur dann wieder zu mixen, wenn er von einer absoluten Mehrheit der MIXe eine authentifizierte Bestätigung ihrer Kenntnisnahme und eine Liste aller inzwischen gemixten Nachrichten erhält.

Einigen sich alle Teilnehmer, potentiell nicht alle MIXe zum Auslassen aller anderen zu befähigen, kann die zur Koordinierung notwendige Kommunikation drastisch reduziert werden: Jeder MIX sendet seine Eingabe-Informationseinheiten nur den MIXen, die von Teilnehmern potentiell zu seinem Auslassen befähigt werden. Nur diese MIXe (und natürlich er selbst) werden bei der Bestimmung einer absoluten Mehrheit berücksichtigt.

Wie in Abschnitt 5.3.2.2 wird auch hier meiner Meinung nach das Risiko, daß ein Angreifer einen MIX bezüglich der Informationseinheiten, für die er noch keine Empfangsbestätigungen erhielt, mittels Isolierung überbrücken kann, bei weitem durch die Vermeidung jeder zusätzlichen Verzögerung des Mixens aufgewogen. Denn aktive Angriffe, die diese Schwäche des Koordinations-Protokolls auszunutzen versuchen, können leicht entdeckt werden (zumindest wenn sie oft erfolgen) und müssen an sehr vielen Stellen in aufeinander abgestimmter Weise eingreifen, wenn Informationseinheiten jeweils mehrere MIXe durchlaufen: Um den Weg einer bestimmten Informationseinheit von ihrem Sender zu ihrem Empfänger zu verfolgen, muß ein Angreifer in jedem Team, von dem jeweils ein Mitglied die Informationseinheit mixen muß, den gerade aktiven MIX (kontrollieren oder) zum Ausfall bringen oder isolieren, nachdem er diese Informationseinheit mixte.

Bei diesem Koordinations-Protokoll ist die Tatsache wichtig, daß jeder MIX überprüfen kann, ob sein Vorgänger die Nachricht unbefugt verändert hat. Anderenfalls könnte ein Angreifer zwei bezüglich der Verschlüsselungsstruktur aufeinanderfolgende MIXe überbrücken:

Seien abermals die MIXe MIX_u und MIX_{u+1} zwei bezüglich der Verschlüsselungsstruktur aufeinanderfolgende MIXe, die von einem Angreifer nicht kontrolliert werden, der die MIXe MIX_{u-1} und MIX_{u+2} kontrolliert. Sei X ein ausgefallener MIX. Der Angreifer ändert A_{u+1} in N_u in die Adresse von X. Deshalb denkt MIX_u, daß X der folgende MIX ist, überprüft, ob X ausgefallen ist, und läßt folglich einen MIX aus, indem er N_{u+2} an MIX_{u+2} sendet. Der Angreifer kann auch N_{u+1} berechnen, was er an MIX_{u+1} sendet. Entsprechend gibt auch MIX_{u+1} die Nachricht N_{u+2} aus. Der Angreifer weiß, daß die Nachricht, die MIX_{u+2} zweimal erhält, die N_u entsprechende ist.

Im folgenden wird das in Abschnitt 5.3.2.3.2 gegebene Datenschutz-Kriterium begründet. Hierzu werden die Fälle a), b) und c) des Kriteriums der Reihe nach durchgegangen.

a) Wird der erste MIX, der die Nachricht erhält, mixt und ausgibt vom Angreifer nicht kontrolliert, so bewirkt er genauso „viel“ Schutz der Kommunikationsbeziehung wie jeder MIX im in Abschnitt 2.5.2 beschriebenen nichtfehlertoleranten indirekten Umcodierungsschema.

So bleibt nur noch der Fall zu untersuchen, daß mindestens zwei im Verschlüsselungsschema aufeinanderfolgende MIXe, MIX_u und MIX_{u+1} genannt, vom Angreifer A nicht kontrolliert werden.

b) Kontrolliere A alle anderen MIXe und seien MIX_u und MIX_{u+1} in der Lage, miteinander zu kommunizieren, sofern beide nicht ausgefallen sind. Außerdem werde ihre Kommunikation vom (unterliegenden) Kommunikationsnetz zuverlässig gepuffert, so daß ein ausgefallener MIX vom anderen an ihn Abgesendetes auch dann zum Zeitpunkt des Abschlusses seiner Reparatur erhält, wenn der Absender gerade ausgefallen ist.

A hat 3 sinnvolle Handlungsmöglichkeiten: er kann N_u zu MIX_u senden oder N_{u+1} zu MIX_{u+1} und im letzteren Fall entweder behaupten, daß MIX_{u+2} ausgefallen ist oder nicht. Tut *A* irgendetwas anderes, werden sich MIX_u und MIX_{u+1} weigern, mit *A* zusammenzuarbeiten, da die Verschlüsselungsschemata so sind, daß *A* an den Nachrichten N_u und N_{u+1} nichts unentdeckt verändern kann. Im folgenden werden diese drei Handlungsmöglichkeiten H1, H2 und H3 der Reihe nach untersucht.

Sei zuerst angenommen, daß MIX_u und MIX_{u+1} nicht ausgefallen sind.

H1 MIX_u erhält N_u und gibt N_{u+1} aus. Dies gibt *A* keine Information über die betrachtete Nachricht, da der von ihm kontrollierte MIX X_{u-1} die Nachricht N_{u+1} genausogut berechnen könnte.

Möglicherweise ist dies eine Bedrohung des Schutzes der Kommunikationsbeziehung für andere Nachrichten. Wie zu Beginn von Abschnitt 2.5.2.1 erwähnt wurde, gilt folgendes: Arbeiten alle anderen Sender und Empfänger von Nachrichten, die von einem MIX zusammen gepuffert und umsortiert ausgegeben wurden, zusammen, so kann der MIX von ihnen prinzipiell bezüglich der von einem anderen gesendeten Nachrichten überbrückt werden. Praktisch ist dies besonders schlimm, wenn es einem Angreifer möglich ist, von $n+1$ zusammen gepufferten und umsortierten Nachrichten selbst n zu liefern. Diese Schwäche wird also nicht durch das Fehlertoleranzverfahren bewirkt. Ihre negativen Folgen werden vermieden, indem jedesmal viele Nachrichten von unterschiedlichen Sendern gemixt werden.

H2 MIX_{u+1} erhält N_{u+1} und gibt N_{u+2} aus. Dies untergräbt den Schutz der Kommunikationsbeziehung der betrachteten Nachricht nicht, da MIX_{u+1} auch andere Nachrichten abwartet und alle zusammen mit geänderter Codierung und in anderer Reihenfolge ausgibt.

H3 MIX_{u+1} erhält N_{u+1} und gibt N_{u+3} aus. Dies untergräbt den Schutz der Kommunikationsbeziehung der betrachteten Nachricht nicht, da MIX_{u+1} auch andere Nachrichten abwartet und alle zusammen mit geänderter Codierung und in anderer Reihenfolge ausgibt.

Der entscheidende Punkt ist, daß MIX_u in allen Fällen weiß, daß MIX_{u+1} nicht ausgefallen ist, und deshalb niemals N_{u+2} ausgibt.

Ist einer der beiden MIXe ausgefallen, so schützt der andere die Kommunikationsbeziehung durch die Umformung von N_{u+1} zu N_{u+2}. Da beide immer kommunizieren können, sofern keiner ausgefallen ist, und jeder nach einem Ausfall das vom anderen Abgesendete zuverlässig erhält, bewirkt das Koordinations-Protokoll, daß der ausgefallene MIX nach seiner Reparatur nicht noch einmal N_{u+1} in N_{u+2} umformt.

Sind beide MIXe ausgefallen, ist die Kommunikationsbeziehung auch geschützt, da keiner die Umformung von N_{u+1} in N_{u+2} vornimmt. Ist einer der beiden repariert, so stellt das Koordinations-Protokoll sicher, daß einer der obigen Fälle anwendbar ist.

c) Der andere noch zu betrachtende Fall ist, daß MIX_u und MIX_{u+1} miteinander nicht kommunizieren können, obwohl sie beide nicht ausgefallen sind, oder das

(unterliegende) Kommunikationsnetz nicht zuverlässig puffert. In diesem Fall wird eine absolute Mehrheit aller MIXe nicht von *A* kontrolliert.
In diesem Fall stellt das Koordinations-Protokoll sicher, daß höchstens einer der beiden MIXe MIX_u und MIX_{u+1} als nicht ausgefallen erklärt wird und der andere dies spätestens nach kurzer Zeit merkt, selbst wenn *A* ihn durch einen aktiven Angriff von der Mehrheit isoliert.
Für alle Nachrichten, die nicht in dieser kurzen Zeit gemixt wurden, gilt das Argument für den Fall b).
Die Zahl der in dieser kurzen Zeit gemixten Nachrichten kann bei Anewendung des effizienten Koordinations-Protokolls klein gehalten werden. Bei Verwendung des ineffizienten Koordinations-Protokolls ist die Zahl 0.

Hiermit sind alle Fälle erschöpft und die Begründung des Datenschutz-Kriteriums damit beendet.

Da die Verschlüsselungsstruktur bei den fehlertoleranten anonymen Rückadressen bis auf den irrelevanten Unterschied, daß der Nachrichteninhaltsteil ver- statt entschlüsselt wird, genau gleich ist, und dieselben Koordinations-Protokolle verwendet werden, gilt obige Begründung des Datenschutz-Kriteriums auch für sie.

Auch die Begründungen des Datenschutz-Kriteriums für die Verschlüsselungsstrukturen, bei denen jeder MIX die $\ddot{u}$ nächsten MIXe auslassen kann, können aus der Begründung für die Situation $\ddot{u}$=1 kanonischerweise hergeleitet werden und sind deshalb weggelassen.

5.3.2.3.4 Auslassen von möglichst vielen MIXen

Bei der zweiten Betriebsart werden möglichst viele MIXe ausgelassen. Dies bedeutet, daß nur dann nicht jeweils 1 bzw. bei den erweiterten Schemata $\ddot{u}$ MIXe ausgelassen werden, wenn der dann nächste ausgefallen (oder etwa durch Fehler des unterliegenden Kommunikationsnetzes unerreichbar geworden) ist.

Etwas formaler lautet dies: MIX_i sendet $N_{i+\ddot{u}+1}$ zu $MIX_{i+\ddot{u}+1}$, wenn immer $MIX_{i+\ddot{u}+1}$ nicht ausgefallen ist. Nur wenn $MIX_{i+\ddot{u}+1}$ ausgefallen ist, sendet er $N_{i+\ddot{u}}$ an $MIX_{i+\ddot{u}}$. Nur wenn auch $MIX_{i+\ddot{u}}$ ausgefallen ist, sendet er $N_{i+\ddot{u}-1}$ an $MIX_{i+\ddot{u}-1}$, und so weiter.

Bild 60 verdeutlicht dies (wie Bild 59) für den Fall $\ddot{u}$=1. Auch das verwendete Beispiel ist dasselbe.

Verglichen mit der Betriebsart „Auslassen von möglichst wenig MIXen“, bei der MIX_i die Nachricht N_{i+1} an MIX_{i+1} sendet, sofern dieser nicht ausgefallen ist, spart die Betriebsart „Auslassen von möglichst vielen MIXen“ möglicherweise Übertragungsaufwand, erhöht möglicherweise den Durchsatz und senkt möglicherweise die durchschnittliche Verzögerungszeit. Die vielen „möglicherweise“ resultieren daher, daß die Koordinierung bei der Betriebsart „Auslassen von möglichst vielen MIXen“ schwieriger ist. Insbesondere kann das in Abschnitt 5.3.2.3.3 angegebene effiziente Koordinations-Protokoll für „Auslassen von möglichst wenig MIXen“ nicht angewendet werden, da ein MIX nicht lokal bestimmen kann, ob sein Mixen das Mixen eines anderen MIXes ersetzt.

Durch eine kleine Änderung der Verschlüsselungsschemata ist dies jedoch möglich:

Der ursprüngliche Generierer jeder (Rück-)Adresse sieht in jedem Rückadreßteil R_j ein extra Bit vor, das er genau dann setzt, wenn der entsprechende MIX_j das Mixen eines anderen ersetzt. Kein anderer MIX kann den Wert dieses Bits unerkannt verändern, vgl. Abschnitt 5.3.2.3.1.

Wenn MIX_j sieht, daß er das Mixen keines anderen MIXes ersetzt, kann er das effiziente Koordinations-Protokoll von Abschnitt 5.3.2.3.3 ausführen, d. h. er kann die Eingabe-Nachrichten gleichzeitig an die anderen MIXe senden und mixen. Insbesondere kann er die Ausgabe-Nachrichten ausgeben, bevor er von den anderen MIXen eine Empfangsbestätigung erhalten hat.

Wenn MIX_j sieht, daß er das Mixen eines anderen MIXes ersetzt, muß er das ineffiziente Koordinations-Protokoll von Abschnitt 5.3.2.1 ausführen.

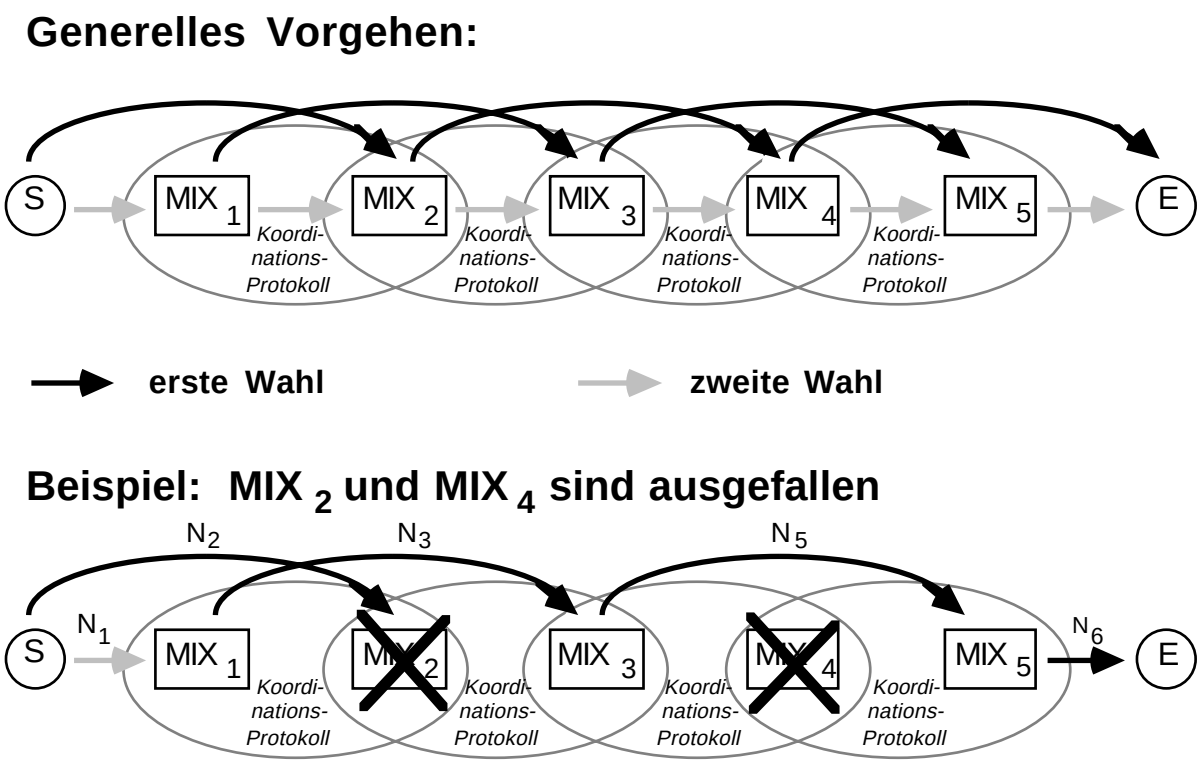

Bild 60: Auslassen von möglichst vielen MIXen bei einem Verschlüsselungsschema, bei dem jeweils ein MIX ausgelassen werden kann; Die Koordinations-Protokolle werden im Bild zwischen Gruppen minimalen Umfangs abgewickelt.

Werden, um das Risiko zu vermeiden, daß MIXe bezüglich Nachrichten, für die sie noch keine Empfangsbestätigungen erhielten, überbrückt werden, die ursprünglichen Verschlüsselungsschemata und das ineffiziente Koordinations-Protokoll verwendet, so ist der Unterschied zwischen den Betriebsarten „Auslassen von möglichst wenig MIXen“ und „Auslassen von möglichst vielen MIXen“ gering. Jeder zum Mixen einer Nachricht aufgeforderte MIX muß das Koordinations-Protokoll für jeden MIX, den er auszulassen gedenkt, separat, d. h. zeitlich

nacheinander, ausführen: zunächst sendet MIX_i die Nachricht N_i an alle anderen MIXe und wartet auf eine Bestätigung, daß sie sie noch nicht gemixt haben und auch nicht mixen werden. Danach sendet MIX_i die Nachricht N_{i+1} an alle MIXe, usw. bis er schließlich $N_{i+ü}$ an alle MIXe sendet. Werden nur Bilder der Nachrichten unter einer *Einwegfunktion* (vgl. Abschnitt 5.3.2.3.1) statt ganzer Nachrichten oder statt Nachrichten unter einer *Hash-Funktion* (die im Gegensatz zu einer Einwegfunktion möglicherweise mit vertretbarem Aufwand invertiert werden kann, vgl. Abschnitt 2.5.2.6) an die anderen MIX gesendet, so kann dies für alle Nachrichten N_i bis $N_{i+ü}$ parallel, d. h. gleichzeitig, geschehen. Dies reduziert verglichen mit dem Senden ganzer Nachrichten nicht nur den Übertragungsaufwand (bzw. steigert in etwas verglichen mit dem Senden der Nachrichten unter einer Hash-Funktion), sondern es vermindert vor allem die zusätzliche Verzögerungszeit um den Faktor $ü$+1. Der Unterschied entsteht dadurch, daß wenn dann der Angreifer bei Verwendung einer Einwegfunktion dieselbe Nachricht an zwei von ihm nicht kontrollierten MIXe schickt, er zwar sehen kann, daß der von *beiden* ausgegebene Funktionswert dieser doppelt weitergegebenen Nachricht entspricht. Wenn er aber nie das Urbild dieser Einwegfunktion sehen wird, nützt ihm dies nichts. Folglich darf in diesem Fall keiner der MIXe die Nachricht mixen.

Wie bei der Betriebsart „Auslassen von möglichst wenig MIXen“ kann auch bei der Betriebsart „Auslassen von möglichst vielen MIXen“ der für die Koordinierung nötige Aufwand erheblich reduziert werden, wenn die Teilnehmer nicht alle MIXe potentiell zum Auslassen aller anderen befähigen: Jeder MIX sendet seine Eingabe-Informationseinheiten nur den MIXen, die von Teilnehmern potentiell zu seinem Auslassen befähigt werden. Nur diese MIXe (und natürlich er selbst) werden bei der Bestimmung einer absoluten Mehrheit berücksichtigt.

Um das Datenschutz-Kriterium von Abschnitt 5.3.2.3.2 für die Betriebsart „Auslassen von möglichst wenig MIXen“ zu begründen, wurde nicht benötigt, daß alle $ü$+1 vom Angreifer nicht kontrollierten, bezüglich der Verschlüsselungsstruktur aneinandergrenzenden MIXe von der Nachricht auch tatsächlich durchlaufen werden, sofern sie nicht ausgefallen sind. Damit stellt die in Abschnitt 5.3.2.3.3 gegebene Begründung zusammen mit dem oben beschriebenen Möglichkeiten einer effizienten Koordinierung eine Begründung für die Gültigkeit des Datenschutz-Kriterium auch für die Betriebsart „Auslassen von möglichst vielen MIXen“ dar.

5.3.2.4 Verschlüsselung zwischen MIXen zur Verringerung der nötigen Koordinierung

Wie die bisherigen Unterabschnitte des Abschnitts 5.3.2 „Ersetzen von MIXen“ zeigten, verursachen auch die effizienten Koordinations-Protokolle insbesondere bei „Auslassen von MIXen“ einen beträchtlichen Aufwand. Außerdem haben die effizienten Koordinations-Protokolle den Nachteil, daß bei geschickten und massiven aktiven physischen Angriffen manche MIXe bezüglich des Schutzes der Kommunikationsbeziehung überbrückt werden können.

Es stellt sich deshalb die Frage, ob der zur Koordinierung nötige Aufwand vermieden oder aber zumindest gesenkt werden kann, indem zwischen MIXen zusätzlich verschlüsselt wird (MIX-zu-MIX-Verschlüsselung). Das Ziel dieser zusätzlichen Verschlüsselung ist, daß, obwohl auch bei dynamisch aktivierter Redundanz manche Nachrichten mehrfach gemixt oder bei

statisch aktivierter Redundanz in verschiedenen Schüben gemixt werden, dies einem Angreifer, der nicht alle MIXe kontrolliert, wohl aber alle Leitungen abhört, nicht das Überbrücken einer längeren MIX-Folge bezüglich des Schutzes der Kommunikationsbeziehung erlaubt.

Bei **MIXen mit Reserve-MIXen** kann diese Frage für den Fall *dynamisch aktivierter* Redundanz sehr einfach und generell mit „nein“ beantwortet werden. Einerseits ist der zur Koordinierung nötige Aufwand beim effizienten Koordinations-Protokoll vergleichsweise sehr gering. Andererseits gibt es immer die Möglichkeit, daß sich eine zwei Mitgliedern des ersten Teams zum Mixen gesendete Nachricht innerhalb der vom Angreifer nicht kontrollierten Teamfolge zufällig nicht kreuzt und deshalb auch am Ausgang der Teamfolge zweifach erscheint.

Bei *statisch aktivierter* Redundanz liegt bei MIXen mit Reserve-MIXen der schon in den Abschnitten 5.3 und 5.3.2 diskutierte uninteressante Fall einer verteilten, intern fehlertoleranten Implementierung eines MIXes vor.

Bei **Auslassen von MIXen** kann obige Frage für den Fall *dynamisch aktivierter* Redundanz ebenfalls sehr einfach und generell mit „nein“ beantwortet werden. Sendet ein Angreifer eine Nachricht an zwei verschiedene, durch seinen MIX direkt erreichbare nachfolgende MIXe, so werden sich die zwei Exemplare der Nachricht, sofern keine MIXe ausgefallen sind, bei beiden Betriebsarten nicht kreuzen und deshalb auch am Ausgang der Teamfolge zweifach erscheinen.

Für *statisch aktivierte* Redundanz wurden bisher die folgenden beiden Teilantworten gefunden. Beide beziehen sich auf die Verwendung eines Verschlüsselungsschemas, das das Auslassen von $\ddot{u}$ MIXen in Folge ermöglicht.

Völlig unkoordinierte MIXe: Statt mindestens $\ddot{u}+1$ MIXe – wie beschrieben – zu koordinieren, kann man jeden MIX jede Nachricht MIX-zu-MIX-verschlüsselt an alle von ihm direkt erreichbaren nächsten MIXe schicken lassen. Wie in Abschnitt 2.5.2 beschrieben bearbeitet jeder MIX jede MIX-zu-MIX-entschlüsselte Nachricht nur einmal. Leitgedanke dieses Verfahrens ist, daß am Ende einer genügend langen vom Angreifer nicht kontrollierten MIX-Folge eine Nachricht – egal was der Angreifer tut – entweder gar nicht oder aber, sofern von den letzten $\ddot{u}+1$ MIXen i intakt sind, i mal erscheint.

Beh. Kann der Angreifer MIXe beliebig an- und abschalten (inkl. der Verhinderung der Zustellung von dem unterliegenden Kommunikationsnetz schon vor der Abschaltung übergebenen Nachrichten an einen gerade abgeschalteten, später aber möglicherweise wieder angeschalteten MIX), so kann er mit viel Ausprobieren $3\ddot{u}+1$ unkontrollierte MIXe und mit viel Glück auch mehr als $3\ddot{u}+1$ unkontrollierte MIXe überbrücken.

Bew. Seien die $3\ddot{u}+1$ MIXe MIX_i, MIX_{i+1} bis $MIX_{i+3\ddot{u}}$ (und nur diese) vom Angreifer nicht kontrolliert. Da der Angreifer $\ddot{u}$ MIXe auslassen kann, kennt er die nächsten $\ddot{u}+1$ MIXe, d. h. MIX_i, MIX_{i+1} bis $MIX_{i+\ddot{u}}$.
Der Angreifer schaltet von den ihm bekannten nächsten $\ddot{u}+1$ MIXen zunächst MIX_i, MIX_{i+1} bis $MIX_{i+\ddot{u}-2}$ und $MIX_{i+\ddot{u}}$ ab und sendet die Nachricht $N_{i+\ddot{u}-1}$ an $MIX_{i+\ddot{u}-1}$. Um herauszufinden, wer $MIX_{i+2\ddot{u}}$ ist, schaltet er nacheinander alle anderen, d. h. von ihm nicht kontrollierten MIXe aus bis auf jeweils einen. Den gesuchten MIX $MIX_{i+2\ddot{u}}$

erkennt er daran, daß am von ihm beobachteten Ausgang „etwas“ passiert, nämlich die gemixte Nachricht $N_{i+3\ddot{u}+1}$ das erste mal ankommt. Zu beachten ist, daß von den nachfolgenden MIXen nur $MIX_{i+\ddot{u}-1}$ und $MIX_{i+2\ddot{u}+1}$, sowie möglicherweise $MIX_{i+\ddot{u}+1}$ bis $MIX_{i+2\ddot{u}-1}$ die Nachricht mixten, aber alle anderen dazu noch bereit sind. Dann schaltet der Angreifer $MIX_{i+\ddot{u}-1}$ aus und dafür $MIX_{i+\ddot{u}}$ an. Danach sucht er analog $MIX_{i+2\ddot{u}+1}$ in der Reihe der nachfolgenden, und erkennt dies daran, daß er sowohl $N_{i+3\ddot{u}+1}$ als auch $N_{i+3\ddot{u}+2}$ erhält. Durch Vergleich der erhaltenen Nachrichten kann er wie üblich die $3\ddot{u}+1$ MIXe bezüglich einer Nachricht überbrücken.
Bei mehr als $3\ddot{u}+1$ unkontrollierten MIXen kann ein analoger Angriff existieren. Ob dies so ist, ist unbekannt. Auf jeden Fall kann der Angreifer mit viel Glück zwei verschiedene Wege durch die unkontrollierten MIXe anschalten. Ein deterministischer Schutz ist also ohne Koordinierung nicht möglich. ♦

Schwach koordinierte MIXe: Wie bei den völlig unkoordinierten MIXen schickt jeder MIX jede Nachricht an die $\ddot{u}+1$ nächsten MIXe. Der Angreifer kann jeden MIX in dem Sinne isolieren, daß ein isolierter MIX keine Nachrichten mehr erfolgreich senden und/oder empfangen kann, aber einmal isolierte MIXe dies bemerken und für eine vorgegebene Zeitdauer t am Mixen nur passiv teilnehmen, d.h. nur empfangen, aber nicht senden (und auch nicht umcodieren). Nach dieser Zeit vergleichen sie die aktuell empfangenen Nachrichten mit den während der passiven Phase empfangenen Nachrichten um sie ggf. nicht noch einmal, in diesem Falle verspätet, zu mixen. Alle Nachrichten werden vom ursprünglichen Sender mit einem Zeitstempel versehen und jeder MIX mixt nur Nachrichten, deren Zeitstempel weniger als t Einheiten alt ist. Ein ausgefallener MIX verhält sich nach seiner Reparatur genauso wie ein MIX, dessen Isolierung aufgehoben wurde.

Beh. 1 Verhalten sich MIXe schwach koordiniert, so kann ein Angreifer eine Folge von $2\ddot{u}$ von ihm nicht kontrollierten MIXen bezüglich des Schutzes der Kommunikationsbeziehung überbrücken.

Bew. Seien die $2\ddot{u}$ MIXe MIX_i, MIX_{i+1} bis $MIX_{i+2\ddot{u}-1}$ (und nur diese) vom Angreifer nicht kontrolliert. Da der Angreifer $\ddot{u}$ MIXe auslassen kann, kennt er die nächsten $\ddot{u}+1$ MIXe, d. h. MIX_i, MIX_{i+1} bis $MIX_{i+\ddot{u}}$.
Um die Folge überbrücken zu können, muß der Angreifer die Folge dazu bringen, dieselbe Nachricht in zwei vom Angreifer unterscheidbaren Zeitintervallen zu mixen.
Dies erreicht er, indem er zunächst $N_{i+\ddot{u}}$ an $MIX_{i+\ddot{u}}$ schickt, und später $N_{i+\ddot{u}-1}$ an $MIX_{i+\ddot{u}-1}$. Sind beide nicht ausgefallen, so erhält der Angreifer $N_{i+2\ddot{u}}$ von beiden in jeweils von ihm unterscheidbaren Zeitintervallen zugeschickt. ♦

Beh. 2 Verhalten sich MIXe schwach koordiniert, so kann ein Angreifer für keine Nachricht eine Folge von von ihm nicht kontrollierten $2\ddot{u}+1$ MIXen bezüglich des Schutzes der Kommunikationsbeziehung überbrücken.

Bew. Seien die $2\ddot{u}+1$ MIXe MIX_i, MIX_{i+1} bis $MIX_{i+2\ddot{u}}$ (und nur diese) vom Angreifer nicht kontrolliert. Da der Angreifer $\ddot{u}$ MIXe auslassen kann, kennt er die nächsten $\ddot{u}+1$ MIXe, d. h. MIX_i, MIX_{i+1} bis $MIX_{i+\ddot{u}}$.

Um die Folge überbrücken zu können, muß der Angreifer die Folge dazu bringen, dieselbe Nachricht in zwei vom Angreifer unterscheidbaren Zeitintervallen zu mixen.
Isoliert der Angreifer keinen der *hinteren ü*+1 MIXe $MIX_{i+ü}$ bis $MIX_{i+2ü}$, so gelingt ihm dies nicht: Sei $MIX_{i+ü+j}$ ($j \geq 0$) der erste nichtausgefallene der hinteren MIXe. Entweder erhält $MIX_{i+ü+j}$ die Nachricht nicht, dann geht sie verloren, oder aber $MIX_{i+ü+j}$ sendet sie an alle folgenden MIXe weiter.
Also muß der Angreifer wenigstens einen hinteren MIX der Folge isolieren. Nach der Definition, was schwache Koordinierung ist, bleibt dieser für die Zeitdauer *t* passiv. Da er bei den nicht isolierten MIXen bei dem Versuch, dieselbe Nachricht nochmal gemixt zu bekommen, kein Glück hat, muß er also die Isolierung von MIXen aufheben. Diese werden wiederum nur nach der Zeitdauer *t* aktiv, wonach sie aber die Nachricht, da inzwischen ihr Zeitstempel zu alt ist, auch nicht mixen. ♦

Zum Schluß sei noch ein Protokoll skizziert, das garantiert, daß ein isolierter MIX seine Isolierung rechtzeitig bemerkt:

Alle MIXe senden allen anderen MIXen für jeden Schub (vgl. Abschnitt 2.5.2) je ein Lebenssignal (wie in Abschnitt 5.3 eine Nachricht mit Datum und Zeit sowie Unterschrift, I'm alive message) und warten, bevor sie den Schub gemixt ausgeben, auf eine unterschriebene Empfangsbestätigung aller nicht ausgefallenen MIXe. Erhält ein MIX keine (oder nur wenige) Empfangsbestätigungen, so hält er sich für isoliert und nimmt für die Zeitdauer *t* nur noch passiv am Mixen teil. Er sendet aber weiterhin Lebenssignale und versendet für empfangene Lebenssignale unterschriebene Empfangsbestätigungen.

Je nach Angreifermodell sind erheblich effizientere Protokolle möglich. Kann ein Angreifer beispielweise nur physische Verbindungen unterbrechen, so kann im MIX-Netz eine Nachbarschaft als physische Nachbarschaft im Kommunikationsnetz definiert werden.

Dann braucht jeder MIX Lebenssignale und Empfangsbestätigungen nur an seine Nachbarn zu senden. Dies ist bei MIX-zu-MIX-Verschlüsselung mittels eines symmetrischen Kryptosystems fast ohne zusätzlichen Aufwand erreichbar: Aus den in Abschnitt 3.2.2 dargelegten Gründen ist es zweckmäßig, zwischen MIXen Kanäle zu schalten. Bestehen Kanäle in beiden Richtungen und wird vor der Verschlüsselung mit dem symmetrischen Kryptosystem nur einmal gültige Redundanz – etwa Datum und Uhrzeit – hinzugefügt und vom Empfänger nach der Entschlüsselung geprüft, so stellen diese Kanäle eine hinreichende „Empfangsbestätigung" dar.

Es sei hier schon darauf hingewiesen, daß die MIX-zu-MIX-Verschlüsselung eine Tolerierung aktiver Angriffe zur Verhinderung der Diensterbringung erschwert, wenn diese Tolerierung möglichst ohne vollständigen Verlust des Schutzes der Kommunikationsbeziehung erfolgen soll, vgl. Abschnitt 5.8.

5.3.3 Besonderheiten beim Schalten von Kanälen

Werden Kanäle geschaltet, können während des Schaltens oder Auflösens dieser Kanäle die bisher beschriebenen Fehlertoleranzverfahren verwendet werden.

Ist ein Kanal in Benutzung, so kann nur bei *statisch erzeugter* und *statisch aktivierter* Redundanz eine für die Benutzer des Kanals wahrnehmbare Unterbrechung bei Ausfall eines MIXes „im Kanal“ vermieden werden. Wie in den vorhergehenden Abschnitten diskutiert, ist statisch erzeugte, *statisch aktivierte* Redundanz aufwendig und läßt wenig Entwurfsspielraum. Werden Kanäle andererseits nicht permanent geschaltet („anonyme Standleitungen“ scheinen mir keinen Anwendungszweck zu haben), so ist der Ausfall eines MIXes „im Kanal“ pro Kanal relativ selten und die Kanalunterbrechung durch Vermeidung statisch aktivierter Redundanz kaum eine Benutzungsbeeinträchtigung. Deshalb scheint es günstiger zu sein, bei Ausfall eines MIXes „im Kanal“ den Kanal aufzugeben und geeignet aufzulösen sowie einen ganz neuen Kanal zu schalten. Hierzu müssen selbst Empfänger von Simplex-Kanälen Rückadressen erhalten. Diese können entweder für regelmäßige Empfangsbestätigungen oder für eine Fehlersignalisierung benutzt werden. Im letzteren Fall sollten für die Rückadressen geeignete Fehlertoleranzverfahren vorgesehen sein.

Dies Verfahren scheint sehr effizient zu sein und wirft keine Pobleme bezüglich des Schutzes der Kommunikationsbeziehung auf, sofern die Auflösung des durch Ausfall eines oder mehrerer MIXe unterbrochenen Kanals (genauer: seiner Teile) den in Abschnitt 3.2.2.1 hergeleiteten Regeln folgt. Selbstverständlich kann (aus Sicht des Schutzes der Kommunikationsbeziehung) ein neuer Kanal aufgebaut werden, bevor der unterbrochene aufgelöst ist.

Ist die zum Aufbau eines ganz neuen Kanals nötige Zeit zu lang, so können statt diesem Abschnitt 5.3.1 entsprechenden Verfahren solche hergeleitet werden, die den Abschnitten 5.3.2.2 oder 5.3.2.3 entsprechen. Die Anpassung (vielleicht sogar der Neuentwurf) entsprechender Koordinations-Protokolle erfordert besondere Sorgfalt.

5.3.4 Quantitative Bewertung

In diesem Abschnitt sollen die drei Fehlertoleranzverfahren „Verschiedene MIX-Folgen“, „MIXe mit Reserve-MIXen“ und „Auslassen von MIXen“ bezüglich ihrer Zuverlässigkeit (Verfügbarkeit der Nutzleistung) und ihres Schutzes der Kommunikationsbeziehung quantitativ bewertet werden, um einen Vergleich der Fehlertoleranzverfahren zu ermöglichen.

Wie zu Beginn von Kapitel 5 bei der Einführung der Begriffe Fehlermodell und Fehlervorgabe schon anklang, ist es schwierig, Fehlermodelle anzugeben, die sowohl realistisch als auch handhabbar sind. Entsprechendes muß auch für jede auf ihnen basierende quantitative Bewertung gelten – wegen den benötigten Verteilungen der Zufallsvariablen (*stochastisches Modell*) sogar in noch stärkerem Maße. Da die quantitative Bewertung hier nur zum Vergleich gedacht ist, werden sowohl das bisherige grobe *Fehler*- und *Sicherheitsmodell* (ein MIX ist ganz oder gar nicht ausgefallen bzw. vom Angreifer kontrolliert oder nicht, Fehler des unterliegenden Kommunikationsnetzes werden nicht betrachtet) als auch ein einfachstmögliches stochastisches Modell verwendet. Wie üblich wird gehofft, daß sich diese Grobheit bei allen drei Fehlertoleranzverfahren gleich auswirkt und die Aussage eines Vergleichs deshalb auch in der Realität Gültigkeit besitzt.

Sei *r* die Überlebenswahrscheinlichkeit (reliability) (oder Verfügbarkeit) und *s* die Sicherheit (security) eines MIXes. Die Überlebenswahrscheinlichkeit (oder Verfügbarkeit) ist wie üblich als die Wahrscheinlichkeit definiert, daß ein MIX nach einem festgelegten Zeitintervall (oder zu

einem zufälligen Zeitpunkt nach dem Einschwingen) nicht ausgefallen ist. Da im folgenden zwischen Überlebenswahrscheinlichkeit und Verfügbarkeit nicht unterschieden werden muß, wird Zuverlässigkeit als Oberbegriff verwendet. Die Sicherheit eines MIXes sei als die Wahrscheinlichkeit definiert, daß er nicht vom Angreifer kontrolliert wird. Um die Bewertung möglichst einfach zu halten, wird angenommen, daß alle MIXe dieselbe Zuverlässigkeit und Sicherheit besitzen und daß diese bei einzelnen MIXen und zwischen MIXen stochastisch unabhängig sind. Außerdem wird angenommen, daß kein MIX bezüglich einer Informationseinheit zweimal verwendet wird – nicht einmal als Reserve-MIX. Unter diesen Annahmen können die üblichen Formeln der Zuverlässigkeitstheorie verwendet werden.

Weiterhin wird angenommen, daß MIXe sicher wissen, welche anderen MIXe ausgefallen sind. Dann ist es nicht nötig, sich um Mehrheiten von MIXen zu kümmern, wie dies in den Koordinations-Protokollen der Abschnitte 5.3.2.1 bis 5.3.2.3 getan wurde. Anderenfalls würde nicht nur die Sicherheit, sondern auch die Zuverlässigkeit der Fehlertoleranzverfahren sinken. Aber zumindest die Zuverlässigkeit sinkt für vernünftige Werte von r, die in der Nähe von 1 liegen, nur wenig.

Außerdem wird angenommen, daß bei jedem Schub Informationseinheiten von so vielen verschiedenen Sendern gemixt werden, daß der in Abschnitt 2.5.2.1 beschriebene Angriff auf den Schutz der Kommunikationbeziehung mittels Zusammenarbeit aller Sender bis auf einen praktisch ausgeschlossen und deshalb bei der Berechnung der Sicherheit ignoriert werden kann.

Außerdem werden immer dort, wo dies einen Unterschied macht, bevorzugt Umcodierungsschemata für Empfängeranonymität berücksichtigt, da sie der allgemeine Fall sind und das Ersetzen von MIXen bei ihnen besonders nötig ist.

r und s sind also beliebige reelle Zahlen mit $0 \le r \le 1$ und $0 \le s \le 1$. Seien wie bisher $ü$ und m beliebige ganze Zahlen mit $ü \ge 0$ und $m \ge 1$.

Wie in Abschnitt 5.3.1 erwähnt, sind **Verschiedene MIX-Folgen** ein Parallel-Serien-System (Parallel-System aus Serien-Systemen) bezüglich Zuverlässigkeit und ein Serien-Parallel-System (Serien-System aus Parallel-Systemen) bezüglich Sicherheit.

Die Zuverlässigkeit $\mathbf{r}_{ü+1}(m)$ eines Systems aus $m \bullet (ü+1)$ MIXen, das von einer Nachricht derart durchlaufen werden muß, daß mindestens eine von $ü+1$ Folgen von jeweils m MIXen die Nachricht mixt, lautet

$$\mathbf{r}_{ü+1}(m) = 1 - (1 - r^m)^{ü+1},$$

und seine Sicherheit $\mathbf{s}_{ü+1}(m)$

$$\mathbf{s}_{ü+1}(m) = (1 - (1-s)^m)^{ü+1}.$$

Wie in Abschnitt 5.3.2.2 erwähnt, sind **MIXe mit Reserve-MIXen** ein Serien-Parallel-System (Serien-System aus Parallel-Systemen) bezüglich Zuverlässigkeit und ein Parallel-Serien-System (Parallel-System aus Serien-Systemen) bezüglich Sicherheit.

Die Zuverlässigkeit $\mathbf{r}_{ü+1}(m)$ eines Systems aus $m \bullet (ü+1)$ MIXen, das von einer Nachricht derart durchlaufen werden muß, daß m MIXe die Nachricht mixen und jeder MIX von $ü$ anderen ersetzt werden kann, lautet

$$\mathbf{r}_{ü+1}(m) = 1 - (1 - r^{ü+1})^m,$$

und seine Sicherheit $\mathbf{s}_{ü+1}(m)$

$$\mathbf{s}_{ü+1}(m) = (1 - (1-s)^{ü+1})^m.$$

Bei **Auslassen von MIXen** ist die Berechnung dieser Kennwerte nicht ganz so einfach, vgl. Abschnitt 5.3.2.3.

Die Zuverlässigkeit $\mathbf{r}_{\ddot{u}+1}(m)$ eines Systems aus m **koordinierten** MIXen, wobei jeder der m MIXe die nächsten $\ddot{u}$ MIXe auslassen kann, kann folgendermaßen rekursiv berechnet werden:

Sei $\mathbf{r}_{\ddot{u}+1}(i)$ die Zuverlässigkeit eines (Teil)Systems von i (bezüglich des Verschlüsselungsschemas) direkt aufeinanderfolgenden MIXen, d. h. die Wahrscheinlichkeit, daß es in dem (Teil)System eine Folge von nicht ausgefallenen MIXen gibt, mittels derer eine mit dem Verschlüsselungsschema verschlüsselte Nachricht von einem Sender direkt vor der Folge zu einem Empfänger direkt hinter der Folge richtig umcodiert übermittelt werden kann. Hierbei sei jeweils vorausgesetzt, daß der Sender direkt vor der Folge und der Empfänger direkt hinter der Folge nicht ausgefallen sind. Folglich ist für die Werte $i = 0,...,\ddot{u}$

$$\mathbf{r}_{\ddot{u}+1}(0) = \mathbf{r}_{\ddot{u}+1}(1) = ... = \mathbf{r}_{\ddot{u}+1}(\ddot{u}) = 1,$$

da der Sender direkt vor dem (Teil)Systems von i (bezüglich des Verschlüsselungsschemas) aufeinanderfolgenden MIXen bis zu $\ddot{u}$ MIXen auslassen kann. Für größere Werte von i kann die Zuverlässigkeit rekursiv berechnet werden durch

$$\mathbf{r}_{\ddot{u}+1}(i) = \sum_{j=0}^{\ddot{u}} (1 - r)^j \cdot r \cdot \mathbf{r}_{\ddot{u}+1}(i\text{-}j\text{-}1) \qquad \text{für } i \geq \ddot{u}+1.$$

Hierbei ist der j-te Term die Wahrscheinlichkeit, daß die ersten j der i MIXe ausgefallen sind, aber der j+1-te nicht ausgefallen ist, und es eine Folge von nicht ausgefallenen MIXen gibt, mittels derer die Nachricht durch die verbleibenden i-j-1 MIXe richtig umcodiert übermittelt werden kann. Wird hierbei angenommen, daß die Nachricht nach einem Umcodierungsschema für Empfängeranonymität gebildet ist, so gilt diese Formel nicht nur für MIXe, sondern auch für das gesamte System unter Einschluß des Verwenders der Rückadresse (sei es ein MIX oder ein „normaler“ Teilnehmer), da auch er nur $\ddot{u}$ MIXe auslassen kann. Wird kein Umcodierungsschema für Empfängeranonymität verwendet, so kann der Sender den ersten MIX beliebig wählen, so daß dessen Zuverlässigkeit (oder Vefügbarkeit) wohl als 1 angenommen werden müßte.

Dieselben Formeln können verwendet werden, um die Unsicherheit $\mathbf{u}_{\ddot{u}+1}(i)$ eines (Teil)Systems von i (bezüglich des Verschlüsselungsschemas) direkt aufeinanderfolgenden MIXen zu berechnen. $\mathbf{u}_{\ddot{u}+1}(i)$ ist die Wahrscheinlichkeit, daß der Angreifer eine Nachricht über das (Teil)System von einem unsicheren, daß heißt unter der Kontrolle des Angreifers stehenden Sender direkt vor dem (Teil)System zu einem unsicheren Empfänger direkt hinter dem (Teil)System verfolgen kann. Sei $u = 1 - s$ die Unsicherheit eines MIXes. Dann gilt

$$\mathbf{u}_{\ddot{u}+1}(0) = \mathbf{u}_{\ddot{u}+1}(1) = ... = \mathbf{u}_{\ddot{u}+1}(\ddot{u}) = 1,$$

da der Sender direkt vor dem (Teil)Systems von i (bezüglich des Verschlüsselungsschemas) aufeinanderfolgenden MIXen bis zu $\ddot{u}$ MIXen auslassen kann. Für größere Werte von i kann die Unsicherheit rekursiv berechnet werden durch

$$\mathbf{u}_{\ddot{u}+1}(i) = \sum_{j=0}^{\ddot{u}} (1 - u)^j \cdot u \cdot \mathbf{u}_{\ddot{u}+1}(i\text{-}j\text{-}1) \qquad \text{für } i \geq \ddot{u}+1.$$

Hierbei ist der *j*-te Term die Wahrscheinlichkeit, daß die ersten *j* der *i* MIXe nicht vom Angreifer kontrolliert sind, aber der *j*+1-te es ist, und es eine Folge von vom Angreifer kontrollierten MIXen gibt, mittels derer die Nachricht durch die verbleibenden *i*-*j*-1 MIXe verfolgt werden kann. $\mathbf{u}_{\ddot{u}+1}(m)$ ist nur für den Fall, daß ein Umcodierungsschema für Empfängeranonymität verwendet wurde und der Sender der Rückantwort vom Angreifer kontrolliert wird, die Unsicherheit des Gesamtsystems. Ist nämlich der Sender der Rückantwort nicht vom Angreifer kontrolliert, so wird er die Nachricht nicht dem ersten, vom Angreifer kontrollierten MIX zusenden, sondern dem ersten nicht ausgefallenen. Ist dieser nicht vom Angreifer kontrolliert, so schützt er bereits die Kommunikationsbeziehung. Für den Fall, daß der Sender der Rückantwort nicht vom Angreifer kontrolliert wird, ergibt sich die Unsicherheit $\mathbf{u}'_{\ddot{u}+1}(m)$ des Gesamtsystems als

$$\mathbf{u}'_{\ddot{u}+1}(m) \;=\; \sum_{j=0}^{\ddot{u}} (1 - r)^j \cdot r \cdot u \cdot \mathbf{u}_{\ddot{u}+1}(m-j-1).$$

Wird der Sender einer mit einem Umcodierungsschema für Senderanonymität gebildeten Nachricht vom Angreifer kontrolliert, gibt es natürlich überhaupt keinen Schutz der Kommunikationsbeziehung.

Deshalb ergibt sich für den wichtigsten Fall der Verwendung eines Verschlüsselungsschemas für Empfängeranonymität und eines vom Angreifer kontrollierten Senders der Rückantwort die Sicherheit eines (Teil)Systems von *i* (bezüglich des Verschlüsselungsschemas) aufeinanderfolgenden MIXen als

$$\mathbf{s}_{\ddot{u}+1}(0) \;=\; \mathbf{s}_{\ddot{u}+1}(1) \;=\; \ldots \;=\; \mathbf{s}_{\ddot{u}+1}(\ddot{u}) \;=\; 0 \qquad \text{und}$$

$$\mathbf{s}_{\ddot{u}+1}(i) \;=\; 1 - \sum_{j=0}^{\ddot{u}} s^j \cdot (1 - s) \cdot (1 - \mathbf{s}_{\ddot{u}+1}(i-j-1)) \qquad \text{für } i \geq \ddot{u}+1.$$

In den folgenden 9 Bildern sind jeweils die Werte $\mathbf{r}_{\ddot{u}+1}(m)$ und $\mathbf{s}_{\ddot{u}+1}(m)$ für „Verschiedene MIX-Folgen“, „MIXe mit Reserve-MIXen“ oder „Auslassen von MIXen“ für die drei Parameterkombinationen $r = 0{,}999$ und $s = 0{,}9$, $r = 0{,}99$ und $s = 0{,}9$ sowie $r = 0{,}99$ und $s = 0{,}1$ dargestellt. Auf der x-Achse ist für *m* in logarithmischem Maßstab der Wertebereich von 1 bis 100000 dargestellt, auf der y-Achse können die zugehörigen Werte der Zuverlässigkeit und Sicherheit abgelesen werden. Eingezeichnet sind jeweils die Werte von $\mathbf{r}_1(m)$, $\mathbf{r}_2(m)$, $\mathbf{r}_3(m)$, $\mathbf{r}_4(m)$, $\mathbf{r}_5(m)$ und $\mathbf{s}_1(m)$, $\mathbf{s}_2(m)$, $\mathbf{s}_3(m)$, $\mathbf{s}_4(m)$, $\mathbf{s}_5(m)$. Wegen der graphischen Lesbarkeit wurden diese mit den obigen Formeln nur für den Wertebereich der natürlichen Zahlen definierten Funktionen als kontinuierliche Funktionen gezeichnet, wobei die Funktionswerte jeweils durch gerade Linien verbunden wurden. Dies erklärt die im Bereich von $m \leq 10$ bei manchen „Kurven“ deutlich wahrnehmbaren Knicke. Um bei „Auslassen von MIXen“ trotz der durchgezogenen, aber nur an ganzzahligen Argumentwerten gültigen Funktionswert-„Kurven“ keinen falschen Eindruck für die Werte $m \leq \ddot{u}+1$ zu erzeugen, beginnen hier die „Kurven“ erst im Funktionswert $m = \ddot{u}+1$.

Um einen Vergleich der 3 Fehlertoleranzverfahren zu unterstützen, sind die Bilder aller 3 Fehlertoleranzverfahren für einen Parametersatz jeweils direkt hintereinander dargestellt.

Wie bereits in [Pfi1_85 Seite 92] begründet, ist es sinnvoll, m und nicht $m \bullet (\ddot{u}+1)$ als Kostenfunktion des MIX-Netzes anzunehmen und entsprechend MIX-Netze mit gleichem m zu vergleichen: m bestimmt die Verzögerungszeit, den Umschlüsselungs- und Übertragungsaufwand. Die die Produktions-Kosten der MIXe charakterisierende Zahl $m \bullet (\ddot{u}+1)$ ist für den Vergleich nicht wesentlich, da gemäß Abschnitt 3.2.2.4 jede Informationseinheit nur von wenigen MIXen gemixt werden kann und diese wenigen MIXe einen so geringen Teil aller MIXe darstellen dürften, daß in jedem Fall auch $m \bullet (\ddot{u}+1)$ MIXe vorhanden sind.

Zuverlässigkeit, Sicherheit

MIXanzahl m

Bild 61: Werte für „Verschiedene MIX-Folgen“ und die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$

Zuverlässigkeit, Sicherheit

MIXanzahl *m*

Bild 62: Werte für „MIXe mit Reserve-MIXen“ und die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$

Zuverlässigkeit, Sicherheit

MIXanzahl *m*

Bild 63: Werte für „Auslassen von MIXen“ und die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$

Der Gebrauch dieser Bilder sei an einem Beispiel beschrieben. Gesucht sei für jedes Fehlertoleranzverfahren und jede Parameterkombination das minimale m, so daß $\mathbf{r}_{\ddot{u}+1}(m) \geq 0{,}99999$ und $\mathbf{s}_{\ddot{u}+1}(m) \geq 0{,}99999$. Für die Parameterkombination $r = 0{,}999$ und $s = 0{,}9$ kann aus Bild 61 für „Verschiedene MIX-Folgen“ der Wert $m = 6$ (bei $\ddot{u} = 3$), aus Bild 62 für „MIXe mit Reserve-MIXen“ der Wert $m = 7$ (bei $\ddot{u} = 2$) und aus Bild 63 für „Auslassen von MIXen“ der Wert $m = 12$ (bei $\ddot{u} = 2$) abgelesen werden. Entsprechend kann für die Paramertkombination $r = 0{,}99$ und $s = 0{,}9$ aus Bild 64 für „Verschiedene MIX-Folgen“ der Wert $m = 6$ (bei $\ddot{u} = 4$), aus Bild 65 für „MIXe mit Reserve-MIXen“ der Wert $m = 9$ (bei $\ddot{u} = 3$) und aus Bild 66 für „Auslassen von MIXen“ der Wert $m \approx 30$ (bei $\ddot{u} = 4$) abgelesen werden. Aus den Bildern 67, 68 und 69 können die entsprechenden Werte nicht abgelesen werden, da bei „Verschiedenen MIX-Folgen“ hierfür die „Kurven“ für größere Werte von $\ddot{u}$ nötig wären und bei „MIXe mit Reserve-MIXen“ und „Auslassen von MIXen“ hierfür ein größerer Bereich von m und $\ddot{u}$ nötig wäre. Aus Gründen der graphischen Lesbarkeit und eines einheitlichen Maßstabes in allen 9 Bildern wurde darauf bewußt verzichtet.

Eine naive Interpretation dieser quantitativen Bewertungsergebnisse könnte nun lauten, daß „Verschiedene MIX-Folgen“ das beste Fehlertoleranzverfahren sind, da es bei vorgegebenen Parametern immer die kleinsten Werte von m ermöglicht und keinerlei Koordinations-Problem existiert. Deshalb sei noch einmal daran erinnert, daß Ende-zu-Ende-Fehlerbehebung statistische Angriffe über Sende- und Empfangsraten und -zeitpunkte ermöglicht, die Sicherheit von „Verschiedene MIX-Folgen“ von dem einfachen Bewertungsmodell also deutlich überschätzt wird.

Zuverlässigkeit, Sicherheit

MIXanzahl m

Bild 64: Werte für „Verschiedene MIX-Folgen“ und die Parameterkombination $r = 0{,}99$ und $s = 0{,}9$

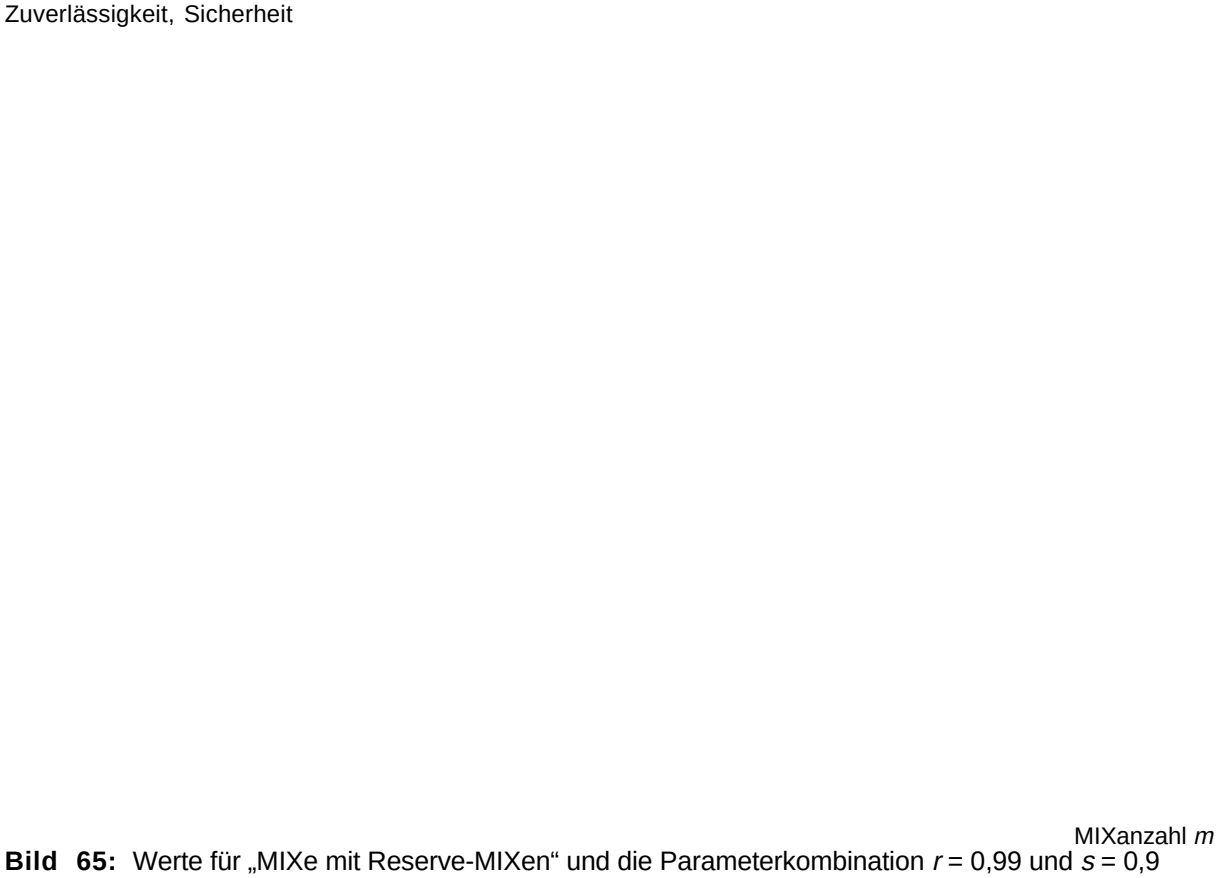

Bild 65: Werte für „MIXe mit Reserve-MIXen“ und die Parameterkombination $r = 0{,}99$ und $s = 0{,}9$

Bild 66: Werte für „Auslassen von MIXen“ und die Parameterkombination $r = 0{,}99$ und $s = 0{,}9$

Die Bewertungsergebnisse für „MIXe mit Reserve-MIXen“ und „Auslassen von MIXen“ sind vergleichbarer und ähnlicher. Ersteres schneidet für kleine Werte von *m* deutlich, für große Werte von *m* nur sehr geringfügig besser ab. Dies liegt daran, daß aus den geschilderten Gründen bei „Auslassen von MIXen“ die Sicherheit der ersten *ü* MIXe mit 0 angesetzt wird. Dies wirkt sich bei kleinem *m* deutlich, bei großem *m* so gut wie nicht aus. Da aber auch hier der genaue Aufwand und die genaue Nutzleistung (Verzögerungszeit, Durchsatz) vom unterliegenden Kommunikationsnetz, dem zu bedienenden Verkehr und den verwendeten Koordinations-Protokollen abhängt, kann letztlich nur eine quantitative Bewertung, die all diese Parameter berücksichtigt (und hoffentlich unter praktischen Randbedingungen einige fixieren kann) definitiv entscheiden.

Entsprechendes gilt, wenn auch schwach koordinierte MIXe bei „Auslassen von MIXen“ in den Vergleich einbezogen werden. Dies kann mittels obiger Formeln für „Auslassen von MIXen“ geschehen, indem unter Verwendung der Ergebnisse von Abschnitt 5.3.2.4 für die Berechnung von **r** und **s** nicht gleiche, sondern verschiedene Werte für *ü* verwendet werden. Die Werte können aus den Bildern 63, 66 und 69 direkt abgelesen werden, indem für die Situation, daß jeder MIX die nächsten *ü* MIXe auslassen kann, die „Kurven“ $\mathbf{r}_{\ddot{u}+1}$ und $\mathbf{s}_{2\ddot{u}+1}$ zum Ablesen verwendet werden.

Zuverlässigkeit, Sicherheit

MIXanzahl *m*

Bild 67: Werte für „Verschiedene MIX-Folgen“ und die Parameterkombination $r = 0{,}99$ und $s = 0{,}1$

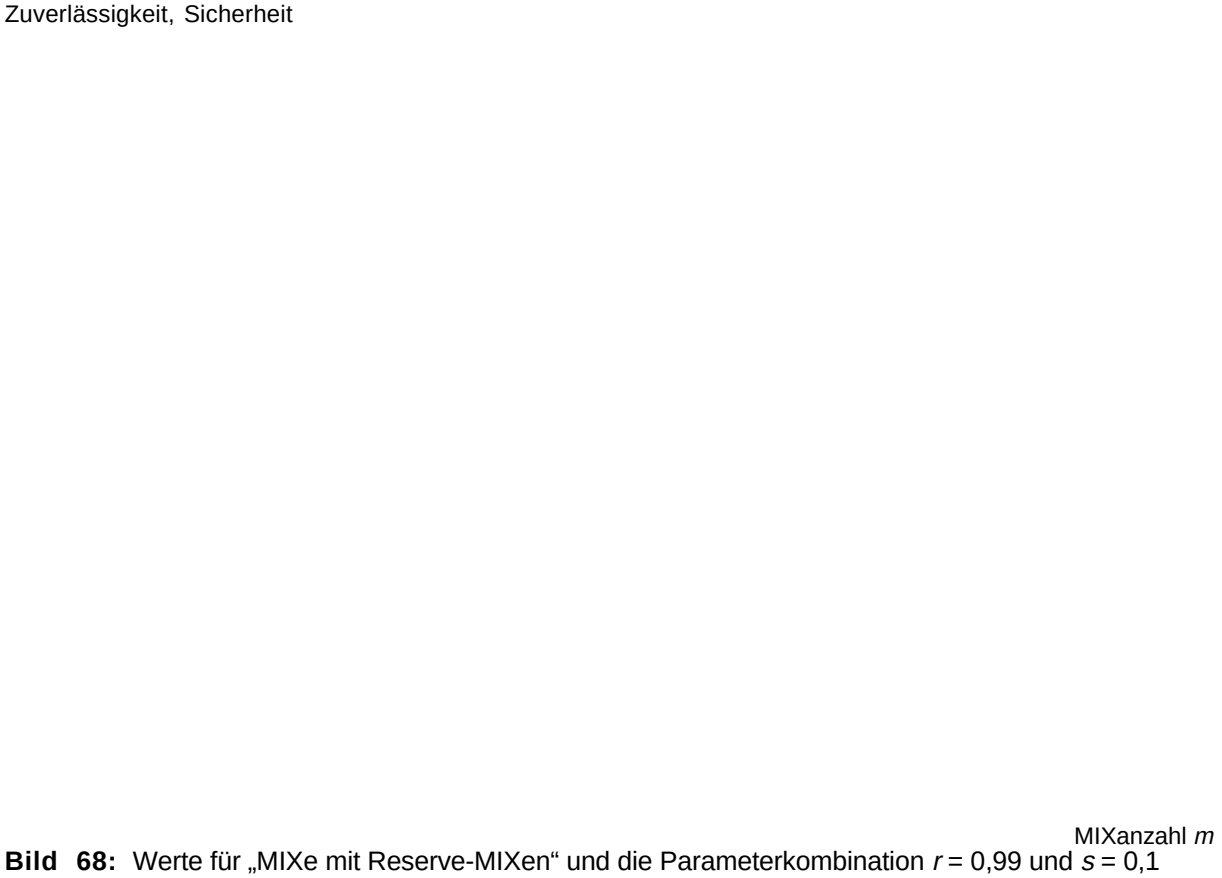

Bild 68: Werte für „MIXe mit Reserve-MIXen“ und die Parameterkombination $r = 0{,}99$ und $s = 0{,}1$

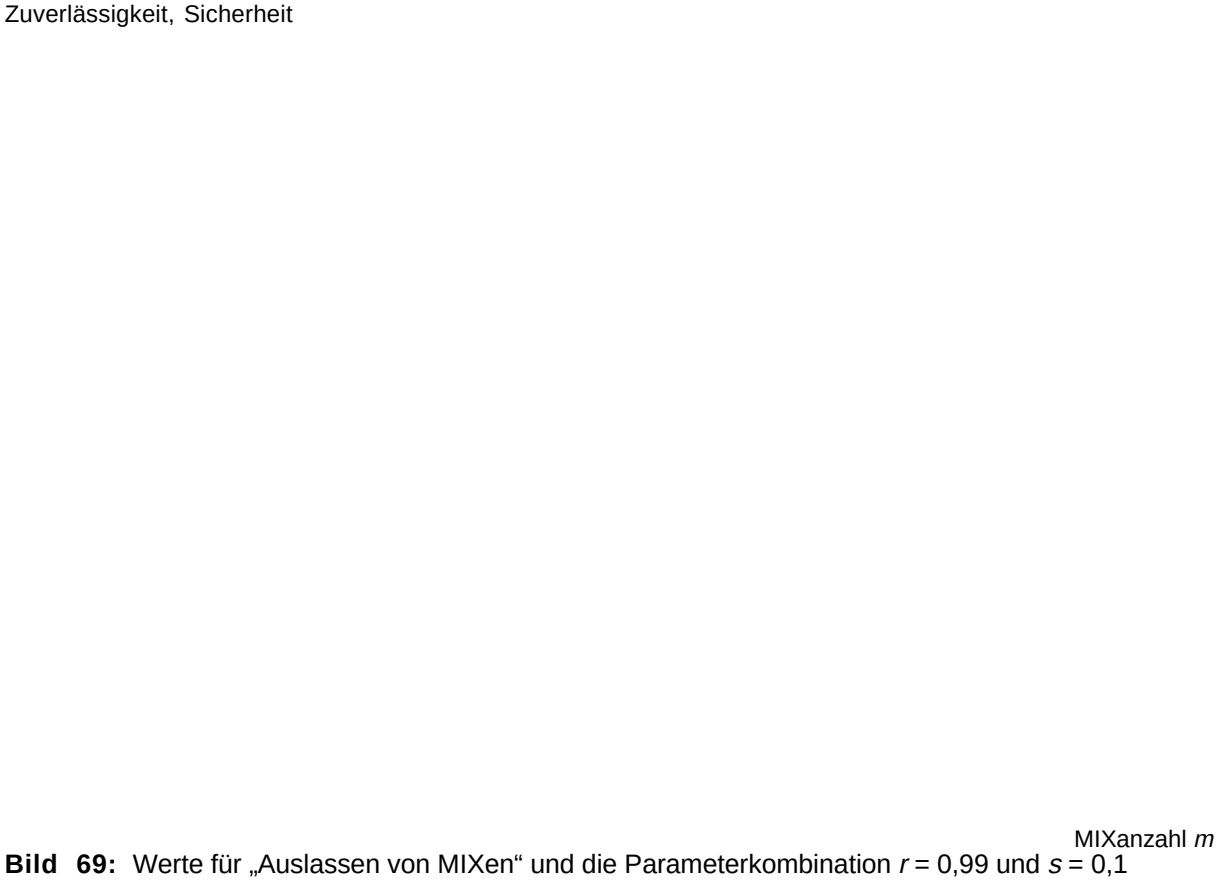

Bild 69: Werte für „Auslassen von MIXen“ und die Parameterkombination $r = 0{,}99$ und $s = 0{,}1$

5.4 DC-Netz

Entsprechend Abschnitt 2.6 und dem zu Beginn dieses Kapitels Gesagten ist beim DC-Netz ein beliebiges Bitübertragungsnetz, das die Schicht 0 und die tiefere Teilschicht der Schicht 1 des ISO OSI Referenzmodells umfaßt, mit konventionellen Fehlertoleranz-Maßnahmen ohne Rücksicht auf Anonymität, Unbeobachtbarkeit und Unverkettbarkeit möglich. Im folgenden werden deshalb vor allem die obere Teilschicht der Schicht 1 und die Schicht 2 behandelt.

Die zu Beginn des Kapitels 5 bereits angesprochene Serieneigenschaft des DC-Netzes besteht darin, daß alle Schlüssel fehlerfrei ausgetauscht worden sein müssen, alle Pseudozufallszahlengeneratoren (PZGs) und alle modulo-Addierer fehlerfrei arbeiten müssen und die Synchronisation erhalten bleiben muß.

Anders als beim MIX-Netz, bei dem Fehlertoleranz-Maßnahmen ständig im Hintergrund abgewickelt werden können, lassen sich beim DC-Netz zwei Phasen, später Modi genannt, klar voneinander trennen. Normalerweise übertragen alle Teilnehmerstationen anonym Informationseinheiten. Tritt ein permanenter Fehler im Verfahren zum anonymen Mehrfachzugriff oder im DC-Netz auf, so kann keine Teilnehmerstation Informationseinheiten übertragen, bis dieser Fehler durch Ausgliedern oder Reparatur der defekten Komponente(n) toleriert ist – es sei denn, es gibt mehrere voneinander unabhängige DC-Netze (*statisch erzeugte Parallel-Redundanz*, die wiederum *statisch* oder *dynamisch aktiviert* werden kann).

Die **Realisierung mehrerer unabhängiger DC-Netze** wird nicht vertieft betrachtet, da sie keine besonderen Entwurfs-Schwierigkeiten aufwirft.

Klaus Echtle wies darauf hin, daß es zweckmäßig sein dürfte, zwar jeder Station das Empfangen auf jedem der unabhängigen DC-Netze zu ermöglichen, das Senden jedoch nur auf relativ wenigen (*senderpartitioniertes DC-Netz*). Dadurch wird ein Fehler, der nur wenige Stationen betrifft, bzw. ein aktiver Angreifer, der nur wenige Stationen kontrolliert, daran gehindert, alle anderenfalls eben bezüglich des Fehlers bzw. aktiven Angreifers nicht unabhängigen DC-Netze zu stören. Die Bilder 70 und 71 zeigen ein für die Fehlervorgabe, beliebiges Fehlverhalten einer beliebigen Station zu tolerieren, konfiguriertes senderpartitioniertes DC-Netz für 10 Stationen. [Nied_87] enthält eine ausführliche und genaue Bewertung der Zuverlässigkeit, d. h. der Wahrscheinlichkeit, daß alle nicht fehlerhaften Stationen noch miteinander kommunizieren können, und Senderanonymität, d. h. unter wieviel Stationen ist ein Sender anonym, solcherart konfigurierter senderpartitionierten DC-Netze.

Wie schon am Beispiel ersichtlich, können auch von für die Fehlervorgabe eines beliebigen Einfachfehlers konfigurierten senderpartitionierten DC-Netzen in diesem Sinne manche Mehrfachfehler toleriert werden, beispielsweise beliebiges Fehlverhalten der Stationen 1, 2 und 5. In diesem Sinne nicht toleriert werden kann beispielsweise beliebiges Fehlverhalten der Stationen 1 und 8, da dann alle nicht an das DC-Netz 5 angeschlossenen Stationen, nämlich die Stationen 2, 3, 5, 6 und 8 nicht mehr ungestört senden können.

Das Konfigurierungsprinzip des Beispiels kann auf die Fehlervorgabe, beliebiges Fehlverhalten von f beliebigen Station zu tolerieren, erweitert werden. Eine notwendige und hinreichende Bedingung hierfür ist, daß die Sendemöglichkeiten keiner Menge von f Stationen die einer einzelnen anderen Station überdecken.

Der Aufwand dieser Fehlertoleranz-Maßnahme ist entgegen dem ersten Eindruck nicht groß, da mehrere, im Grenzfall alle DC-Netze mittels Zeitmultiplex auf einem unterliegenden Bitübertragungsnetz (was zumindest im Grenzfall seine eigenen Fehler tolerieren können muß) realisiert werden können. Nachteilig ist, daß auf jedem der DC-Netze die Senderanonymität deutlich geringer als auf einem alle Stationen umfassenden DC-Netz ist. Bei der Benutzung eines solchermaßen konfigurierten senderpartitionierten DC-Netzes müssen alle Teilnehmerstationen darauf achten, daß verkettbare Informationseinheiten nur auf demselben DC-Netz gesendet werden, was die Lastverteilung auf den DC-Netzen drastisch einschränkt. Anderenfalls ist bei für die Fehlervorgabe, einen beliebigen Fehler einer beliebigen Station zu tolerieren, konfigurierten senderpartitionierten DC-Netzen der Sender identifizierbar, und bei für eine umfassendere Fehlervorgabe konfigurierten senderpartitionierten DC-Netzen die Anonymität des Senders abermals drastisch eingeschränkt. Eine *statische Aktivierung* der Redundanz senderpartitionierter DC-Netze ist also trivialerweise nicht sinnvoll möglich.

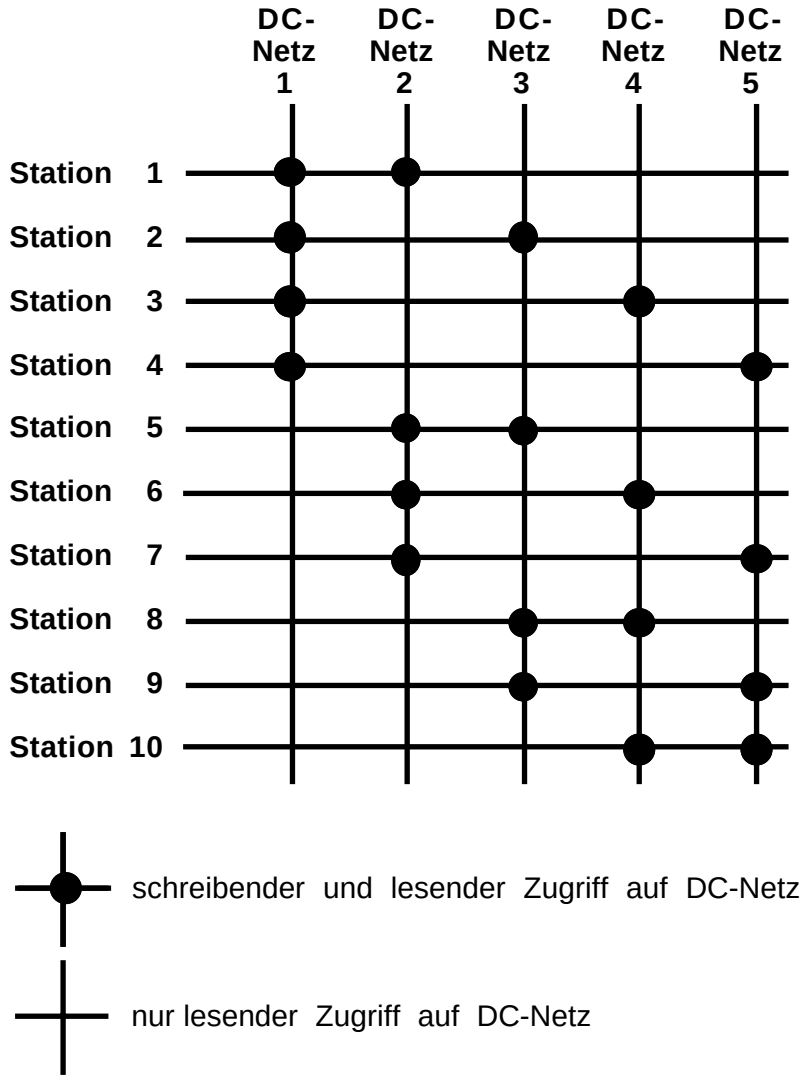

Bild 70: Für die Fehlervorgabe, beliebiges Fehlverhalten einer beliebigen Station ohne Fehlerdiagnose zu tolerieren, konfiguriertes senderpartitioniertes DC-Netz von 10 Stationen

Der Vorteil dieser Fehlertoleranz-Maßnahme ist, daß eine Fehlerdiagnose nicht oder zumindest nicht bei wenigen Fehlern nötig ist, und eine vollständige *Fehlerüberdeckung* erreicht wird, d. h. es gibt keine Fehler, die auf diese Weise nicht toleriert werden können.

Wird die Fehlervorgabe überschritten, kann selbstverständlich eine Fehlerdiagnose nötig werden, die mit den im folgenden beschriebenen Methoden durchgeführt werden kann, so daß dann beide Fehlertoleranzverfahren kombiniert werden.

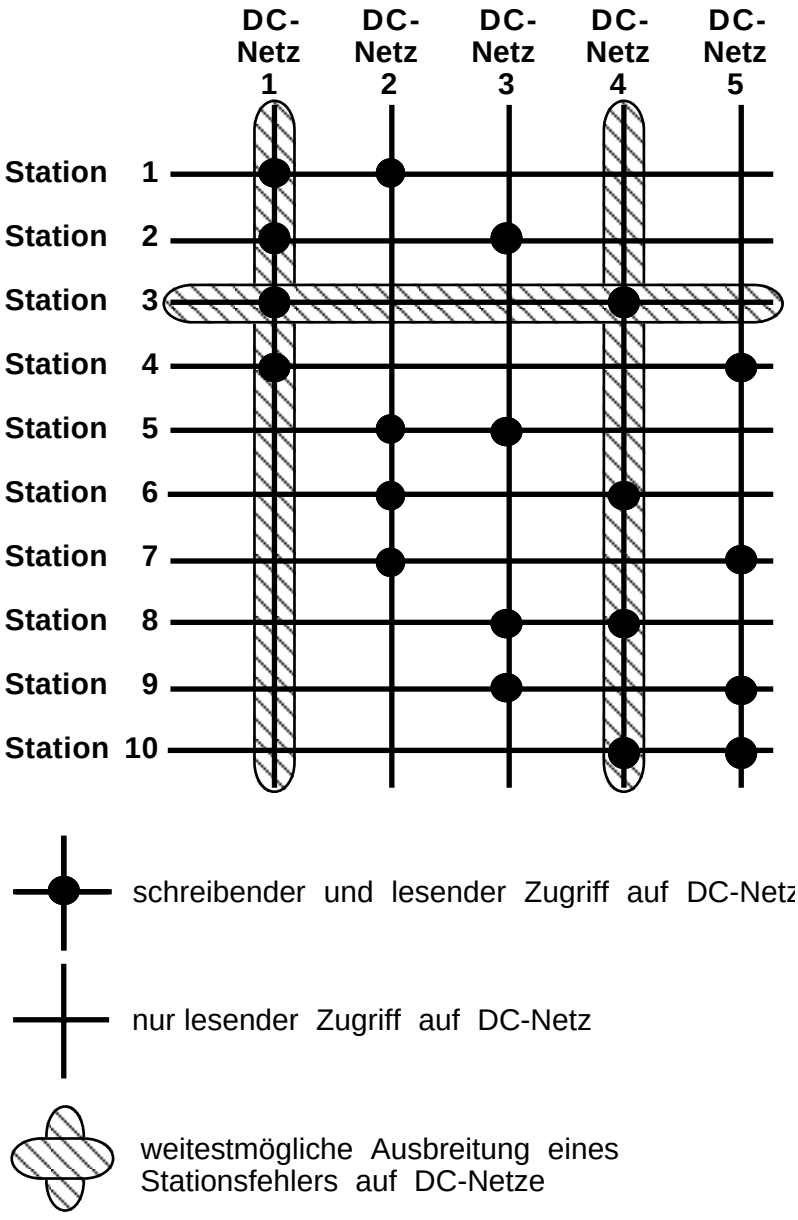

Bild 71: Weitestmögliche Ausbreitung eines Fehlers (bzw. aktiven Angriffs) der Station 3

Fehlererkennung, -lokalisierung und -behebung in einem DC-Netz: Transiente wie auch permanente Fehler im Bitübertragungsnetz können – wie erwähnt – durch gesonderte Fehlertoleranz-Maßnahmen in ihm selbst toleriert werden, oder führen andernfalls zu transien-

ten bzw. permanenten Fehlern im DC-Netz. Die transienten Fehler im DC-Netz werden durch Ende-zu-Ende-Protokolle (vgl. Beginn von Kapitel 5) toleriert. Es verbleiben somit die permanenten Fehler im DC-Netz (Ausfall von PZGs, von modulo-Addierern, Verlust der Konsistenz oder Synchronisation der Schlüssel usw.). Diese sind, wenn einmal erkannt und lokalisiert, leicht zu beheben. Die entsprechenden Schlüssel (von defekten PZGs) werden nicht mehr überlagert, Addierer werden ausgetauscht, Schlüssel werden neu verteilt oder sie werden neu synchronisiert. Das Hauptproblem liegt also in der *Fehlererkennung* und *-lokalisierung*.

Fehler der oberen Teilschicht der Schicht 1 lassen sich dadurch erkennen, daß jeder verschlüsselten Informationseinheit von ihrem Sender zusätzliche, allen Stationen zugängliche Redundanz zugefügt wird, z. B. ein linear gebildetes Prüfzeichen, z. B. CRC, am Ende der Informationseinheit. Dies kann immer geschehen, da die Redundanz nur einen Bruchteil der Länge der Informationseinheiten umfaßt, die nutzbare Übertragungsleistung also kaum sinkt. Wenn das Prüfzeichen linear gebildet ist, entsteht auch bei Überlagerungskollisionen ein gültiges Prüfzeichen. Entsteht ein ungültiges Prüfzeichen, so liegt ein Fehler bei der Überlagerung vor.

Die Erkennung von Fehlern des Mehrfachzugriffsverfahrens hängt vom verwendeten Verfahren ab, ist aber für alle in Abschnitt 3.1.2 empfohlenen Verfahren mit hoher Wahrscheinlichkeit möglich.

Wird beim Mehrfachzugriffsverfahren ein Fehler erkannt, so wird dieses neu initialisiert, um transiente Fehler des Bitübertragungsnetzes oder der oberen Teilschicht der Schicht 1 zu tolerieren. Schlägt dies fehl oder wird auf andere Weise ein andauernder Fehler der oberen Teilschicht der Schicht 1 erkannt, so wird aus dem die Anonymität garantierenden Anonymitäts-Modus (A-Modus) in den Fehlertoleranz-Modus (F-Modus), in dem Fehler lokalisiert und toleriert werden, geschaltet.

Alle Stationen führen folgendes **Fehlerlokalisierungs- und -behebungs-Protokoll** aus [Pfi1_85 Seite 123]:

> Jede Station sichert den momentanen Zustand ihrer paarweise ausgetauschten Schlüssel bzw. PZGs (in der Fachsprache: erstellt einen Rücksetzpunkt, recovery point [AnLe_81]) und führt anschließend folgende Selbstdiagnose durch: sie lädt paarweise zufällige Schlüssel in ihre Schlüsselspeicher bzw. PZGs und überlagert sie lokal mit einer ebenfalls zufälligen Informationseinheit.
>
> Ist das Ergebnis nicht die zufällige Informationseinheit, so ist die Station fehlerhaft und sendet eine dies signalisierende Nachricht über das DC-Netz. Alle anderen Stationen werfen mit dieser Station geteilte Schlüssel weg und wechseln (Einfehlerannahme) in den A-Modus zurück.
>
> Ist das Ergebnis die zufällige Informationseinheit, benutzt die Station den Rücksetzpunkt zur Herstellung des vorherigen Zustands ihrer paarweise ausgetauschten Schlüssel bzw. PZGs. An dieser Stelle des Protokolls gibt es drei wahrscheinliche Fehlertypen:
>
> 1. Eine Station ist so fehlerhaft, daß sie sich nicht selbst diagnostizieren und das Ergebnis den anderen mitteilen kann, oder
> 2. die Synchronisation der Schlüssel(erzeugung und -)überlagerung ging zumindest zwischen zwei Stationen verloren, oder
> 3. das unterliegende Kommunikationsnetz oder die globale Überlagerung ist fehlerhaft.

Um diese Fehlertypen zu unterscheiden und Fehler zu lokalisieren, wird die Zahl der überlagerten Schlüsselpaare sukzessive halbiert (der entsprechende Schlüsselaustauschgraph hat jeweils nur halb so viele Kanten) und beispielsweise 100 neue und nicht noch einmal verwendete Schlüsselzeichen überlagert.
Ist das globale Überlagerungsergebnis 100 mal das 0 entsprechende Zeichen, so ist der Fehler mit der Wahrscheinlichkeit $1 - g^{-100}$ in der anderen Hälfte (sofern ein 0-Haftfehler (stuck at zero fault) am letzten globalen Überlagerungsgerät ausgeschlossen werden kann. Dies kann dadurch getestet werden, daß alle Stationen vorher 100 zufällige Zeichen senden, was mit derselben Wahrscheinlichkeit ein Ergebnis $\neq 0$ ergibt, sofern dort kein Haftfehler vorliegt).
Ist das globale Überlagerungsergebnis nicht 100 mal das 0 entsprechende Zeichen, so gibt es mindestens einen Fehler bei der Speicherung oder Generierung der Schlüssel oder deren synchronisierter Überlagerung oder aber das unterliegende Kommunikationsnetz oder die globale Überlagerung ist fehlerhaft. Deshalb wird weiterhin halbiert.
Hat der Schlüsselaustauschgraph nur noch eine Kante und ist das globale Überlagerungsergebnis nicht 100 mal das 0 entsprechende Zeichen, tauschen beide Stationen einen neuen Schlüssel oder PZG-Startwert aus, um Schlüsselsynchronisationsfehler zu beheben. Danach wiederholen beide ihren Versuch.
Ist das globale Überlagerungsergebnis abermals nicht 100 mal das 0 entsprechende Zeichen, so werfen beide Stationen den gerade ausgetauschten Schlüssel bzw. PZG-Startwert weg und tauschen mit einer dritten und vierten Station einen Schlüssel oder PZG-Startwert aus. Beide neuen Stationenpaare überlagern nacheinander 100 Schlüsselzeichen.
Entsteht in beiden Fällen nicht 100 mal das 0 entsprechende Zeichen, so ist mit hoher Wahrscheinlichkeit das unterliegende Kommunikationsnetz oder die globale Überlagerung fehlerhaft. Beides weiter zu untersuchen sind übliche Probleme der Fehlertoleranz.
Entsteht nur in einem Fall nicht 100 mal das 0 entsprechende Zeichen, so wird die ursprünglich fehlerverdächtige Station dieses Paares als fehlerhaft angesehen und außer Betrieb genommen. Dies wird allen Stationen mitgeteilt, so daß sie mit dieser Station geteilte Schlüssel wegwerfen und (Einfehlerannahme) in den A-Modus zurückwechseln.

Mit dem Zurückschalten vom F-Modus in den A-Modus wird das Verfahren zum anonymen Mehrfachzugriff neu initialisiert, um Auswirkungen von Fehlern der Schicht 1 (physical) auf die Schicht 2 (data link) rückgängig zu machen. Alle gerade geschilderten Schritte sind in Bild 72 zusammengefaßt.

Natürlich gibt es hunderte von Variationen dieses Fehlerlokalisierungs- und -behebungsprotokolls, über deren Zweckmäßigkeit geurteilt werden kann, sobald die Wahrscheinlichkeiten von (Mehrfach-) Fehlern bekannt sind. Ist beispielsweise die Wahrscheinlichkeit von Mehrfachfehlern signifikant, so sollten Hälften des Schlüsselaustauschgraphen, die vom gerade beschriebenen Protokoll nicht getestet werden, auch getestet werden, was den Aufwand des Protokolls höchstens verdoppelt.

Da die Wahrscheinlichkeiten nicht bekannt sind, sind folglich nicht die Details von Fehlerlokalisierung und -behebung interessant, sondern daß sie mit logarithmischem Zeitaufwand (in der Zahl der Stationen) möglich sind.

Es ist beachtenswert, daß bei „Fehlererkennung, -lokalisierung und -behebung in einem DC-Netz“ die Anonymität trotz Fehlertoleranz nicht abgeschwächt wird, wenn entweder echt zufällig generierte Schlüssel oder kryptographisch starke PZGs (vgl. Abschnitte 2.2.2.2 und 3.2.3) verwendet werden. Durch das Einführen der zwei Modi und die Verwendung von Schlüsselzeichen entweder im einen oder aber im anderen Modus bleibt im A-Modus die Anonymität jederzeit in ihrem ursprünglichen Umfang garantiert.

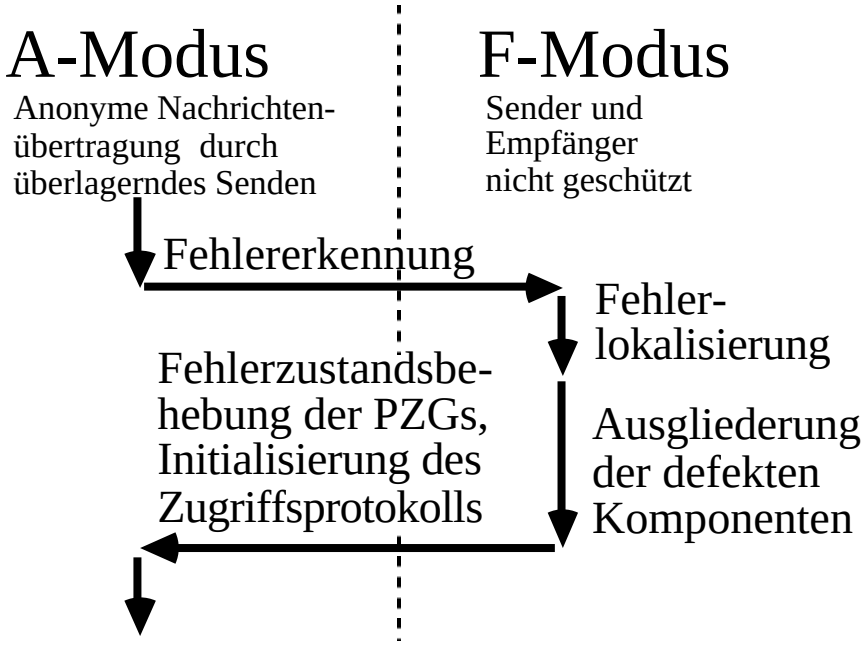

Bild 72: Fehlererkennung, -lokalisierung und -behebung beim DC-Netz

5.5 RING-Netz

Beim RING-Netz ist die Serieneigenschaft sofort ersichtlich: alle Leitungen und Stationen müssen funktionieren, damit Kommunikation zwischen zwei Stationen in beiden „Richtungen“ möglich ist.

Durch das in den Abschnitten 2.5.3.2, 3.1.4 und 3.2.4 beschriebene Zusammenspiel von ringförmiger Übertragungstopologie, digitaler Signalregenerierung und Verfahren zum anonymen Mehrfachzugriff, um innerhalb des Kommunikationsnetzes Anonymität und Unverkettbarkeit zu schaffen (vgl. Abschnitt 2.6), sind spezielle Fehlertoleranz-Maßnahmen erforderlich, die dieses Zusammenspiel nicht (zu sehr) stören.

Wie zu Beginn dieses Kapitels begründet, konzentriert sich das Folgende auf die Schichten 0, 1 und 2 des ISO OSI Referenzmodells, vgl. Bild 30 in Abschnitt 2.6.

Transiente Fehler des Zugriffsverfahrens (Schicht 2) können durch die bei Ringen mit umlaufenden Übertragungsrahmen oder umlaufendem Senderecht jeweils üblichen Verfahren zum Neustart des Zugriffsverfahrens toleriert werden.

Permanente Fehler des Zugriffsverfahrens (Schicht 2) implizieren, daß mindestens eine Station im RING-Netz fehlerhaft ist. Dies Station muß (und kann) mit den im folgenden geschilderten Verfahren solange ausgegliedert werden, bis sie repariert ist.

Transiente Fehler im Übertragungssystem des Rings (d. h. auf den Schichten 0 oder 1) betreffen entweder nur den Nutzinhalt übertragener Informationseinheiten oder auch das Zugriffsverfahren (Schicht 2). Ersterer Fehlertyp ist einfach und wird durch das Ende-zu-Ende-Protokoll (vgl. Beginn von Kapitel 5) erkannt und behoben. Schwierig sind diejenigen transienten Fehler, die das Zugriffsverfahren betreffen, z. B. bei einem Ring mit umlaufendem Senderecht das Senderechtszeichen zerstören. Dieser und ähnliche Fehler können bei Ringen mit umlaufenden Übertragungsrahmen oder umlaufendem Senderecht mit den jeweils üblichen Verfahren zum Neustart toleriert werden. Zwei zusätzliche Ideen sind bei der Fehlertoleranz des Zugriffsverfahrens (Schicht 2) wichtig:

1. Um transiente Fehler der zweiten Art auf den Schichten 0 oder 1 (siehe oben) tolerieren zu können, führt man bewußt Indeterminismus ein (*indeterministische Protokolle*, siehe [Mann_85 Seite 89ff]). Dadurch kann in dem deterministischen Angreifermodell (der Angreifer muß deterministisch schließen können, welche Station gesendet bzw. empfangen hat) kein Angreifer sichere Rückschlüsse ziehen. Da es bisher kein befriedigendes formales statistisches Angreifermodell gibt (darin gibt sich ein Angreifer zufrieden, wenn er den Sender bzw. Empfänger mit z. B. der Wahrscheinlichkeit 0,9 kennt, vgl. auch [Höck_85 Seite 60ff]), kann die Auswirkung des Indeterminismus nicht quantifiziert werden.
2. Eine andere Art der Fehlertoleranz basiert auf der Idee, einigen wenigen, ausgezeichneten Stationen keine Anonymität zu garantieren, etwa Protokollumsetzern in einem hierarchischen Kommunikationsnetz. Diese Stationen können nach anderen Protokollen arbeiten als die Stationen von Netzteilnehmern und dadurch gezielt Fehler tolerieren [Mann_85 Seite 99ff]. Daher spricht man von *asymmetrischen Protokollen*. Diese sind leichter zu implementieren und sehr viel leistungsfähiger, schwächen jedoch die Anonymität der Netzteilnehmer ab. Ist das einfache Zugriffsverfahren n-anonym, so sind die modifizierten asymmetrischen Protokolle häufig nur noch (n+1)- oder gar nur (n+2)-anonym.

Permanente Fehler im Übertragungssystem des Rings (d. h. auf den Schichten 0 oder 1) führen immer zu einer *Ringrekonfigurierung* mit Neustart (Synchronisation,...) des Verfahrens zum anonymen Mehrfachzugriff (Schicht 2). Da die zu tolerierenden Fehler auf den Schichten 0 (medium) und 1 (physical) angesiedelt ist, sind Fehler leicht zu erkennen und zu lokalisieren (Zeitschranken, Selbsttest sowie Fremdtest durch mehrere Instanzen, damit ein Angreifer, der wenige Stationen kontrolliert, nicht andere Stationen beliebig an- und abschalten kann, u. ä.). Problematisch ist die Fehlerbehebung, da für jede nachgewiesen werden muß, daß die Anonymität nicht verletzt wird. Ziel jeder Fehlerbehebung muß es sein, aus den fehlerfreien Stationen und Leitungen einen Ring (und nicht etwa eine „Acht“, d. h. zwei durch eine Station verbundene Ringe etc.) zu rekonfigurieren, der alle fehlerfreien Stationen umfaßt.

Die einfachste und am wenigsten aufwendige Art der Ringrekonfigurierung ist die Verwendung einer **By-Pass-Einrichtung** (bypass) an jeder Station. Diese By-Pass-Einrichtung schließt den Ring physisch, wenn die Station bemerkt, daß sie fehlerhaft ist, ausgeschaltet wird oder ihre Versorgungsspannung ausfällt. Allerdings kann mit diesem Verfahren natürlich der Ausfall einer Leitung genausowenig toleriert werden wie Fehler von Stationen, die diese nicht selbst diagnostizieren können. Kann nur die Station selbst ihre By-Pass-Einrichtung schließen, so hat deren Einrichtung keine tieferen problematischen Wechselwirkungen mit der Anonymität oder Unbeobachtbarkeit des RING-Netzes. Ein Angreifer kann natürlich insbesondere das Schließen der By-Pass-Einrichtung angrenzender, von ihm nicht kontrollierter Stationen beobachten, da sich dann analoge Charakteristika seines Eingangssignals ändern (vgl. das in Abschnitt 2.5.3.2 über digitale Signalregenerierung Gesagte). Dann weiß er, daß jetzt eine kleinere Gruppe von Teilnehmerstationen umzingelt ist, wodurch er entsprechend mehr Information über das Senden dieser Teilnehmer erhält. Kann ein Angreifer aber nur viele Teilnehmerstationen gleichzeitig umzingeln und sind an diesen Teilnehmerstationen jeweils nur wenige By-Pass-Einrichtungen geschlossen, so ist dies nicht schlimm.

Die Verwendung von *Ring-Verkabelungs-Konzentratoren*, d. h. von By-Pass-Einrichtungen, die nicht bei der Teilnehmerstation gelegen sind und auch nicht von ihr kontrolliert werden [BCKK_83, KeMM_83], ist mit den in Abschnitt 2.5.3.2.1 erläuterten Zielen des RING-Netzes unverträglich. Denn Ring-Verkabelungs-Konzentratoren wären ideale Beobachtungspunkte für einen Angreifer, da sie die vollständige Beobachtung aller angeschlossenen Stationen durch Beobachtung dieses einen Gerätes erlauben.

Eine ebenfalls einfache, aber bereits aufwendige Art der Ringrekonfigurierung ist die Verwendung **mehrerer paralleler Ringe** (statisch erzeugte Redundanz). Fällt eine Leitung eines Ringes aus, so wird ein anderer, noch intakter Ring verwendet (dynamisch aktivierte Redundanz). Dies erlaubt, solange noch mehr als ein Ring intakt ist, einen größeren Durchsatz als das Senden jeder Informationeinheit auf allen Ringen gleichzeitig (statisch aktivierte Redundanz). Allerdings muß dann, sofern kein Ring mehr als Ganzes intakt ist, entweder die Zuordnung von Leitungen zu Ringen gewechselt oder doch auf allen Ringen gleichzeitig gesendet werden. Allerdings kann natürlich auch mit diesem Verfahren ein Fehler einer Station, den diese nicht bemerkt, nicht toleriert werden.

Entsprechendes gilt für eine Kombination von By-Pass-Einrichtung und mehreren parallelen Ringen.

Um mindestens einen beliebigen permanente Einzelfehler im Übertragungssystem des Rings tolerieren zu können, wird ein **geflochtener Ring** (braided ring, siehe Bild 73) verwendet. Solange keine permanenten Fehler auftreten, werden die Leitungen, die benachbarte Stationen verbinden, als ein RING-Netz betrieben. Für ungerade Stationsanzahlen können die anderen Leitungen als ein zweites RING-Netz betrieben werden, was die nutzbare Übertragungskapazität verdoppelt.

Im geflochtenen Ring gibt es drei mögliche *Einzelfehler*, nämlich den Ausfall

- einer *Station i*: sie wird mit Leitung $L_{i\text{-}1 \rightarrow i+1}$ überbrückt (Bild 73, oben rechts).

- einer *inneren Leitung* $L_{i \rightarrow i+2}$: der äußerer Ring bleibt intakt und wird solange ausschließlich benutzt, bis der Ausfall der Leitung behoben ist.
- einer *äußeren Leitung* $L_{i \rightarrow i+1}$: Station S_{i-1} sendet an die Stationen S_i und S_{i+1} (kopiert den Datenstrom auf zwei Leitungen). Damit Station S_{i+2} die Station S_{i+1} nicht beobachten kann, sendet Station S_i die Hälfte aller Informationseinheiten (z. B. alle Übertragungsrahmen mit gerader Nummer, sofern i gerade) an Station S_{i+2}, entsprechend sendet Station S_{i+1} die andere Hälfte (z. B. alle Übertragungsrahmen mit ungerader Nummer, sofern i+1 ungerade) an Station S_{i+2}. S_{i+2} vereint die beiden (verzahnten) Datenströme wieder (Bild 73, unten rechts). Dies ist einer Rekonfigurierung des inneren Rings (Bild 73, unten links) vorzuziehen, da auf diese Weise ggf. noch Ausfälle von inneren Leitungen und Stationen toleriert werden können.

Basierend auf diesen drei Grundkonzepten zur Tolerierung des Ausfalls kann der geflochtene Ring (auch bei den meisten Mehrfachfehlern) mittels des folgenden, von jeder Station auszuführenden Protokolls so rekonfiguriert werden, daß jede fehlerfreie Station jederzeit in einem rekonfigurierten, fast alle fehlerfreien Stationen umfassenden Ring liegt, d. h. auf der ein- und der auslaufenden Leitung werden Informationseinheiten von fast allen nichtfehlerhaften Stationen übertragen.

> **Rekonfigurationsprotokoll für den geflochtenen Ring**:
> Bemerkt eine Station S_{i+1} einen permanenten Signalausfall auf einer ihrer Eingangsleitungen, so signalisiert sie das mittels einer an alle anderen Stationen adressierten Nachricht auf ihren beiden Ausgangsleitungen. Solange der Signalausfall nicht behoben ist, ignoriert S_{i+1} diese Eingangsleitung.
> Sendet die auf dieser Leitung sendende Station nicht auf ihrer anderen Leitungen, daß sie in Ordnung ist, so wird ihr Ausfall unterstellt und sie wird mit der entsprechenden inneren Leitung überbrückt. Anderenfalls wird ein Leitungsausfall unterstellt und entsprechend rekonfiguriert.

Da beim Ausfall einer Station oder einer inneren Leitung ein vollständiger Ring aller fehlerfreien Stationen entsteht, lassen sich in beiden Fällen die Beweise für die Anonymität aus dem fehlerfreien Fall direkt übernehmen. Beim Ausfall einer äußeren Leitung entstehen bezüglich der Anonymität des Senders zwei RING-Netze mit je der halben Bandbreite. In Bild 73 führt eines der RING-Netze halber Bandbreite durch S_{i-1} und das andere durch S_i. Daß in beiden RING-Netzen halber Bandbreite jeweils noch eine Station (nur) empfangen kann, ist irrelevant, da der Empfänger in den normalen Ringzugriffsverfahren an den empfangenen Informationseinheiten nichts ändert. Wird aber – wie in Abschnitt 3.1.4.3 beschrieben – ein Übertragungsrahmen von einer anderen Station als Duplex-Kanal mit einer der Stationen S_{i-1} oder S_i verwendet, so kann die gerufene Station in diesem Übertragungsrahmen nur mit der Wahrscheinlichkeit 0,5 senden. Die Situation, daß eine nur in einem RING-Netz halber Bandbreite liegende Station von einer anderen in einem Übertragungsrahmen zum Senden aufgefordert wird, in dem sie nicht senden kann, mag ein seltenes Ereignis sein, kann aber die Anonymität gegenüber der rufenden Partei aufheben. Aber dies ist nur ein spezieller Fall des generellen Problems, daß ein Empfänger identifiziert werden kann, wenn er wegen des Ausfalls seiner Teilnehmerstation nicht antworten

kann und seine Teilnehmerstation die einzige ausgefallene ist und der Sender dies weiß (vgl. den in Abschnitt 2.6 beschriebenen, und in den Abschnitten 3 und 5 erwähnten aktiven Verkettungsangriff über Betriebsmittelknappheit).

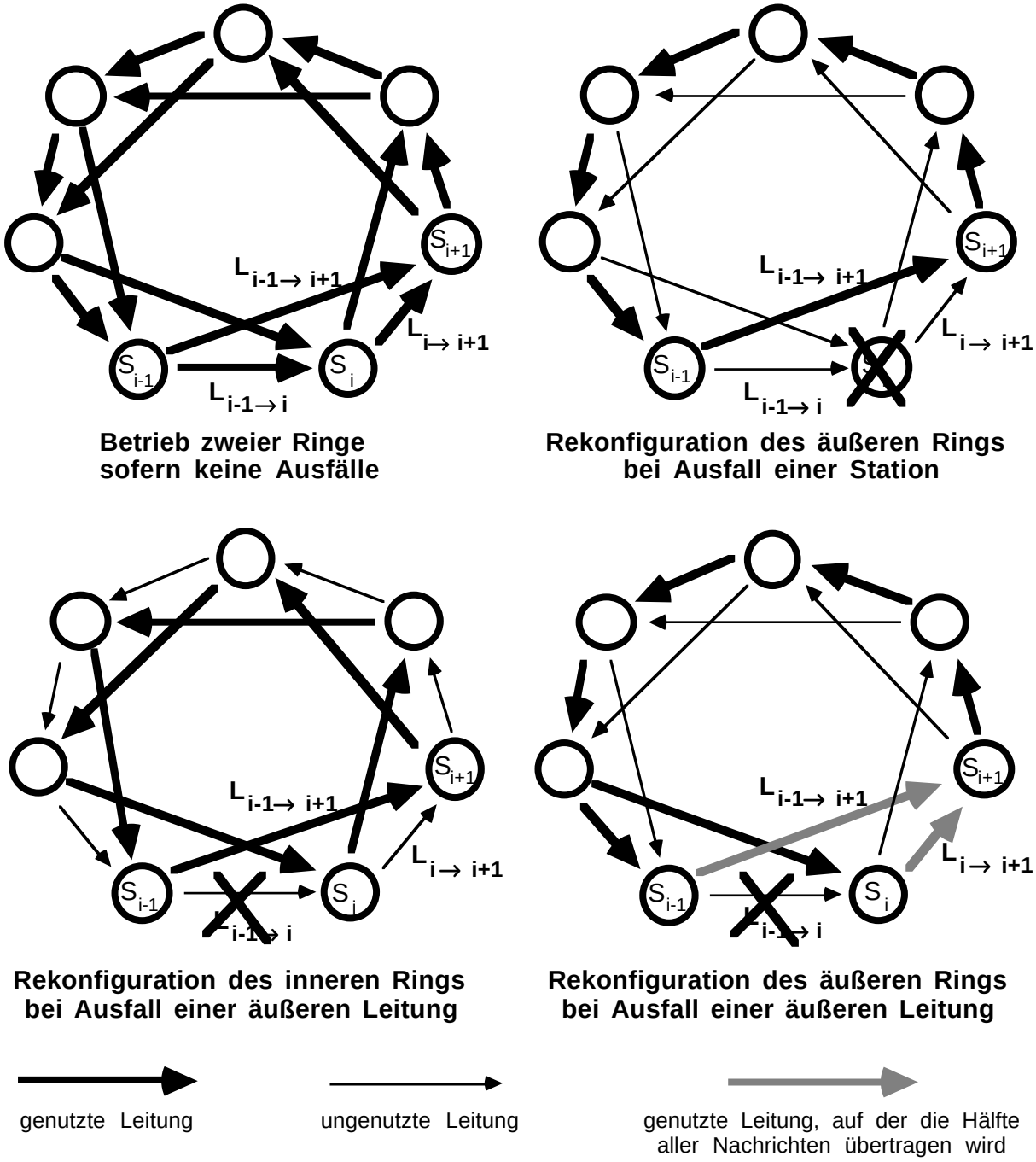

Bild 73: Geflochtener Ring kann bei Ausfällen von Stationen oder Leitungen so rekonfiguriert werden, daß die Anonymität der Netzbenutzer gewahrt bleibt.

Außerdem ist (wie beim Verfahren der By-Pass-Einrichtung) zu beachten, daß aus einem zulässigen Angreifer im nicht fehlertoleranten Fall im fehlertoleranten Fall ein unzulässiger Angreifer (gemäß Angreifermodell) wird. Kontrolliert der Angreifer die Stationen S_1 und S_4 (vgl. Bild 73 mit i=2), so kann er den Ausfall der Leitung $L_{3\rightarrow4}$ vortäuschen oder abwarten. In beiden Fällen sendet Station S_2 sowohl an Station S_3 als auch an S_4. Damit ist Station S_2 durch den Angreifer eingekreist und daher beobachtbar. Es sei angemerkt, daß bei manchen Ausfällen sogar eine Station allein eine andere beobachten kann. Fällt S_1 so aus, daß sie auf ihren beiden Ausgangsleitungen dasselbe sendet, so kann die Station S_3 die Station S_2 allein beobachten.

Eine genaue Beschreibung von Fehlertoleranz im RING-Netz, sowie viele Beispiele und Protokolle sind in [Mann_85] zu finden. Ebenfalls dort wurde eine genaue Analyse der Zuverlässigkeitsverbesserung durch die beschriebenen Fehlertoleranzverfahren vorgenommen. Die Ergebnisse sind äußerst positiv.

Neuere Formeln zur Berechnung der Zuverlässigkeit sind in [Papa_86] zu finden.

Es ist bemerkenswert, daß sowohl überlagerndes Senden als auch das RING-2-f-Netz auf dem geflochtenen Ring so implementiert werden können, daß ein auch nach einem beliebigen Einzelfehler mit der ganzen Bandbreite der einzelnen Leitungen arbeitendes DC- bzw. RING-2-f-Netz entsteht: die in Bild 28 bzw. 47 gezeigten „hellen“ Umläufe werden auf einen vollständig rekonfigurierten Ring gelegt. Der überflüssige Übertragungsabschnitt der „dunklen“ Umläufe wird so gelegt, daß er entweder mit der ausgefallene Leitung zusammenfällt oder nach der ausgefallenen Station beginnt.

Eine Kombination von By-Pass-Einrichtung und geflochtenem Ring ist möglich und zweckmäßig.

5.6 BAUM-Netz

Durch das in den Abschnitten 2.5.3.2, 3.1.3 und 3.2.5 beschriebene Zusammenspiel von baumförmiger Übertragungstopologie, digitaler Signalregenerierung und Verfahren zum anonymen Mehrfachzugriff, um innerhalb des Kommunikationsnetzes Anonymität und Unverkettbarkeit zu schaffen (vgl. Abschnitt 2.6), sind spezielle Fehlertoleranz-Maßnahmen erforderlich, die dieses Zusammenspiel nicht (zu sehr) stören.

Wie zu Beginn dieses Kapitels begründet, konzentriert sich das Folgende auf die Schichten 0, 1 und 2 des ISO OSI Referenzmodells, vgl. Bild 30 in Abschnitt 2.6.

Abgesehen davon, daß beim BAUM-Netz Übertragungsfehler das Mehrfachzugriffsverfahren nicht durcheinanderbringen können, sind die Fehlertoleranzverfahren beim BAUM-Netz denen des RING-Netzes sehr ähnlich (wie vermutlich überhaupt alle Fehlertoleranzverfahren für Kommuniktionsnetze nach dem Grundverfahren „Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung“ sehr ähnlich sein dürften). Bild 74 zeigt eine geeignet redundante Übertragungstopologie, deren Benutzung nach dem in Abschnitt 5.5 Gesagtem selbsterklärend sein dürfte.

Eine Alternative zu der in Bild 74 gezeigten redundanten Übertragungstopologie ist in [MaYa_86] beschrieben und bezüglich Zuverlässigkeit und Nutzleistung analysiert.

Beim BAUM-Netz ist Fehlertoleranz nicht ganz so dringend wie beim RING-Netz, da nur der Ausfall der Station an der Wurzel des Baumes oder eine permanent sendende Station einen vollständigen Nutzbarkeitsausfall des BAUM-Netzes bewirken können. Da zusätzlich das BAUM-Netz deshalb (und nur deshalb) eingeführt wurde, da es eine existierende Leitungsstruktur nutzt (vgl. Abschnitte 2.5.3.2.2 und 3.2.5) und eine zu Bild 74 oder geeigneten Alternativen passende Leitungsstruktur – soweit mir bekannt – noch nirgends in größerem Umfang existiert, wird diese redundante Übertragungstopologie nicht zum Zwecke der Realisierung, sondern zum Zwecke der Vollständigkeit der Fehlertoleranzverfahren angegeben.

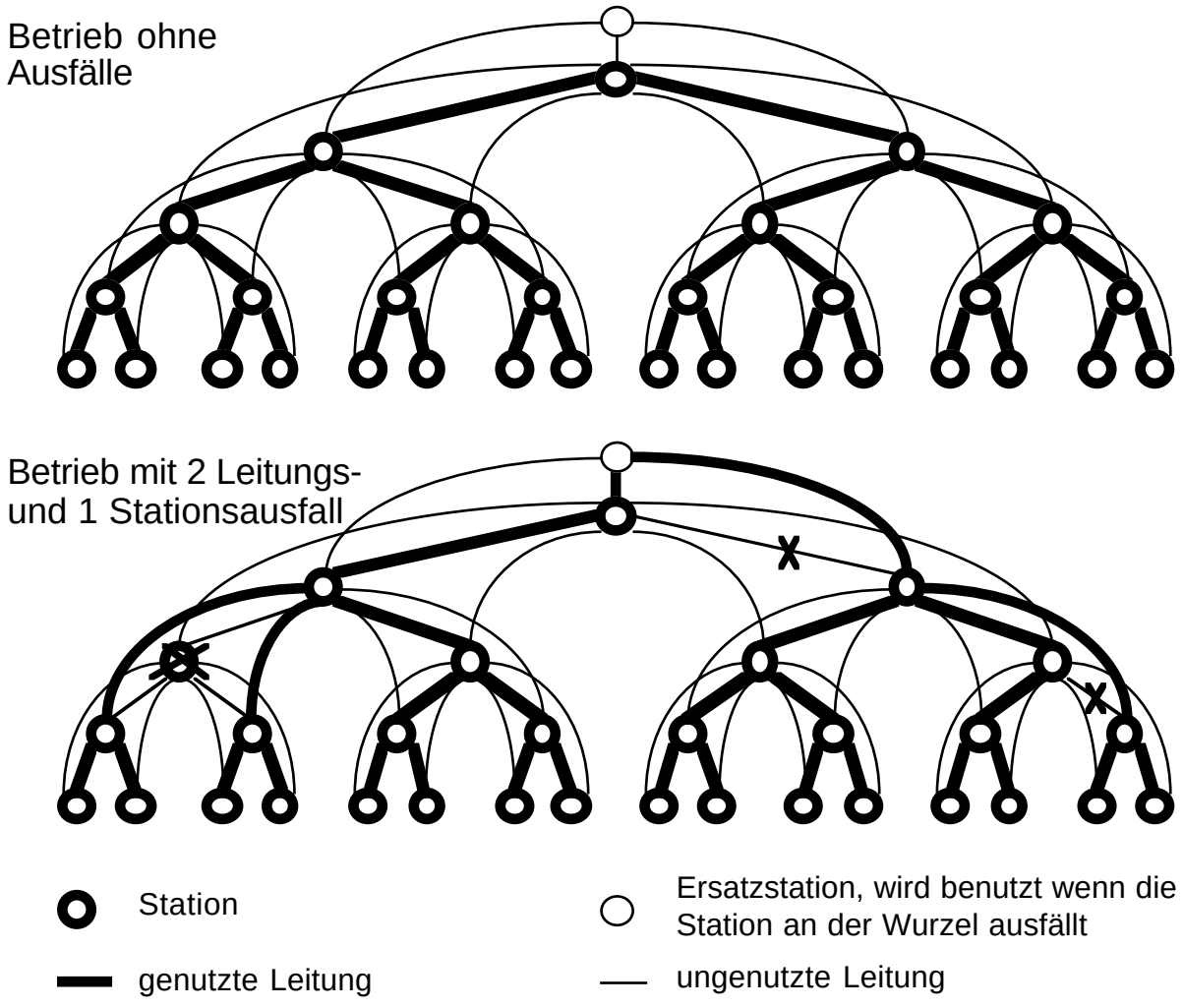

Bild 74: Geflochtener Baum kann bei Ausfällen von Stationen oder Leitungen so rekonfiguriert werden, daß die Anonymität der Netzbenutzer gewahrt bleibt

5.7 Hierarchische Netze

Hierarchische Kommunikationsnetze können fehlertolerant gemacht werden, indem die entsprechenden Fehlertoleranzverfahren in ihren Teilnetzen realisiert und jeweils mehrere Protokollumsetzer (gateways) verwendet werden, um auch den Netzübergang zwischen Teilnetzen fehlertolerant zu machen. (Anderenfalls träte am Netzübergang eine Redundanzverengung auf, die einen Zuverlässigkeitsengpaß bilden würde.)

Bild 75 zeigt dies am Beispiel des Vermittlungs-/Verteilnetzes. Da in ihm das Senden der Protokollumsetzer nicht geschützt zu werden braucht, können zwischen Protokollumsetzern beliebige Protokolle verwendet werden, um die Fehlertoleranz zu unterstützen, insbesondere die Redundanz zu verwalten, oder die Nutzleistung zu steigern.

Dies (und anderes) diskutiert Andreas Mann für das Vermittlungs-/Verteilnetz mit RING-Netzen im Teilnehmeranschlußbereich in großer Tiefe in [Mann_85].

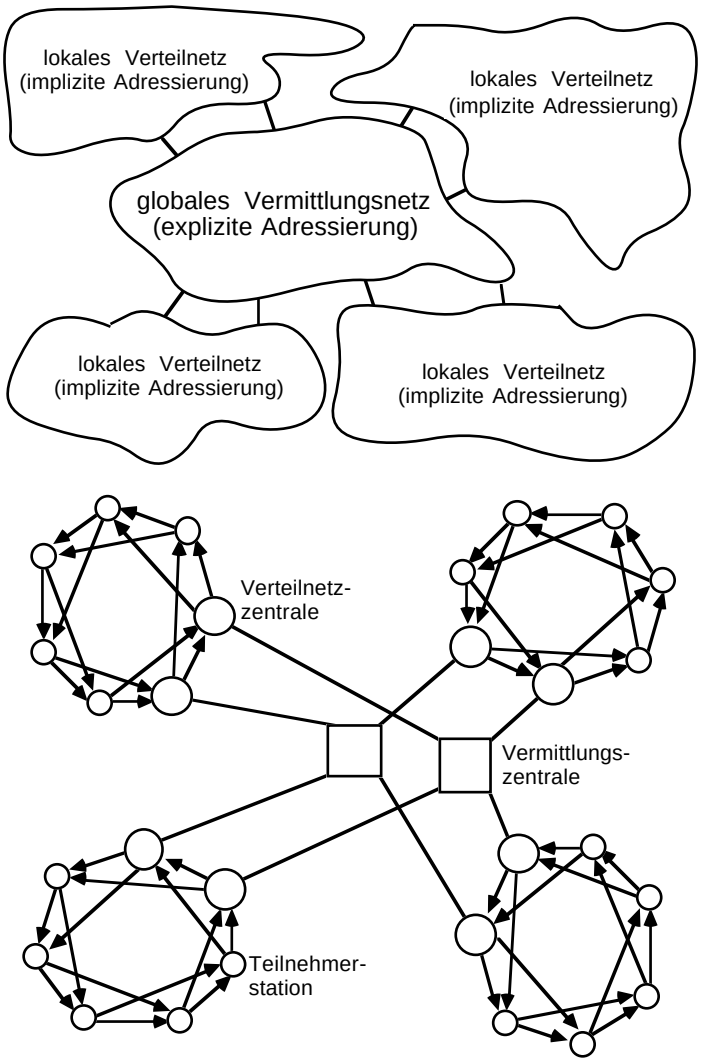

Bild 75: Allgemeine physikalische Struktur eines für die Fehlervorgabe eines beliebigen Fehlers in jedem Teilnetz gestalteten Vermittlungs-/Verteilnetzes (oben) und eine günstige Topologie (unten)

5.8 Tolerierung aktiver Angriffe

In einem Kommunikationsnetz kann jeder Fehler als aktiver Angriff angesehen werden. Fehler „aus Versehen“ bilden eine Untermenge aller möglichen (physischen, logischen) aktiven Angriffe. Trotzdem wurden Fehler bisher so behandelt, daß unter allen Umständen die Anonymität gewahrt blieb. Ein Angreifer kann jetzt soweit gehen, daß er ständig Fehler erzeugt, d. h. Nachrichten falsch umschlüsselt, fälschlicherweise nicht weiterüberträgt, eigene sendet, wenn er es gemäß des Protokolls zum anonymen Mehrfachzugriff nicht darf, oder Schlüssel falsch überlagert, um jede Diensterbringung zu unterbinden (*denial of service*). Dieses Problem kann auf zwei Arten gelöst werden [MaPf_87 Seite 403f].

Zum einen wird nach jedem Fehler untersucht, ob eventuell ein aktiver Angriff und, wenn ja, durch wen vorliegt. Da die erforderlichen Maßnahmen sehr aufwendig sind und darüber hinaus u. U. den Sender bzw. Empfänger einer Nachricht identifizieren, ist es besser, erst auf Verdacht (anormale Fehlerrate u. ä.) die entsprechenden Maßnahmen einzuleiten. Um aktive Angriffe erkennen zu können, muß bei allen Grundverfahren *jede Station ihre Aktivitäten aufdecken*:

- Beim MIX-Netz muß jeder MIX alle ein- und auslaufenden Informationseinheiten ab einem festgelegten Zeitpunkt offenlegen. Dann kann jeder prüfen, ob eine von ihm gesendete Informationseinheit von diesem MIX falsch ent- oder verschlüsselt oder gar ganz unterschlagen wurde. Um dies einer dritten Partei zu beweisen, müssen die Zusammenhänge der betroffenen Informationseinheiten aufgedeckt werden. Es ist jedoch nicht erforderlich, die Zusammenhänge aller Informationseinheiten zu offenbaren, so daß diese Maßnahme zwar hohen Aufwand verursacht, nicht aber die Anonymität unversehrt übertragener Informationseinheiten gefährdet [Chau_81 Seite 85].
  Bei MIX-zu-MIX-Verschlüsselung (vgl. Abschnitt 5.3.2.4) ist dies leider nicht der Fall.

- Beim DC-Netz muß jede Station alle Schlüsselzeichen (nicht aber den Startwert des PZG, sofern einer verwendet wurde) und ihr gesendetes Zeichen für die Zeichen aufdecken, bei denen ein aktiver Angriff vermutet wird [Cha3_85, Chau_88].

- Beim RING- und BAUM-Netz muß jede Station ihre gesendeten Zeichen für die Zeichen aufdecken, bei denen ein aktiver Angriff vermutet wird.

Sowohl beim DC- als auch beim RING- und BAUM-Netz ist es die Aufgabe eines global vereinbarten **Aufdeckverfahrens**, dafür zu sorgen, daß

A) einerseits *alle Zeichen potentiell aufgedeckt werden können*, denn anderenfalls könnte zumindest bei manchen Zeichen ohne Aufdeckrisiko gestört werden, und daß
B) andererseits *keine Zeichen aufgedeckt werden, die die Senderanonymität* von entweder selbst sensitiven oder mit solchen auch nur indirekt verkettbaren Nachrichten *untergraben*.

Letzteres erfordert anscheinend die Verwendung eines Reservierungsverfahrens als Mehrfachzugriffsverfahren.

In [Cha3_85, Chau_88] ist (nur) das folgende kombinierte Reservierungs- und **Aufdeckverfahren für das DC-Netz** enthalten:

- Alle Teilnehmerstationen reservieren in jeder Runde genau einen Übertragungsrahmen. Werden bei der Reservierung nicht genausoviel Übertragungsrahmen reserviert wie Teilnehmerstationen am DC-Netz teilnehmen, werden alle Reservierungsbits aufgedeckt und geprüft, ob jede Station genau ein Reservierungsbit gesendet hat. Da alle Teilnehmerstationen in jeder Runde genau einen Übertragungsrahmen reservieren, ergibt dies Aufdecken keinerlei Information über die Stationen, die sich an das Reservierungsschema gehalten haben.
- Bereits vor der Reservierung sendet jede Teilnehmerstation eine ihr zuordenbare, mögliche *Aufdeckforderung*, nämlich die Bitposition ihrer Reservierung und die zu sendende Nachricht – beides zusammen mit einer Blockchiffre verschlüsselt. Wird die Teilnehmerstation beim Senden gestört und möchte, daß die Störung aufgedeckt wird, so veröffentlicht sie (in ihr zuordenbarer Weise) den Schlüssel, mit dem ihre mögliche Aufdeckforderung verschlüsselt ist, wodurch aus der möglichen eine tatsächliche Aufdeckforderung wird. Da dies die Senderanonymität ihrer Nachricht untergräbt, wird eine Teilnehmerstation dies nur dann tun, wenn sie nichts zu senden hatte und ihre Nachricht also eine bedeutungslose Nachricht, in diesem Zusammenhang eine bedeutungsvolle Falle (trap) für Störer ist.
  ([Cha3_85, Chau_88 Seite 72] ist nicht zu entnehmen, ob Teilnehmerstationen auch für sinnvolle Nachrichten mögliche Aufdeckforderungen senden und ob diese möglichen, aber nie tatsächlichen Aufdeckforderungen auch die richtige Bitpositionen und Nachrichten enthalten. Wie gleich ersichtlich wird, ist zumindest ersteres sinnvoll. Außerdem vereinfacht beides die Beschreibung.)

David Chaums Aufdeckverfahren leistet B) überhaupt nicht und – je nach vom Leser unterstelltem Teilnehmerstationenverhalten – A) höchstens im *komplexitätstheoretischen* Sinne:

- Der Angreifer kann durch das Veröffentlichen möglicher Aufdeckforderungen, die sich gar nicht auf seine Nachricht beziehen, ein Aufdecken für beliebige, von ihm *vorher* gewählte (und zumindest hin und wieder von anderen benutzte) Zeichen erreichen. Werden die Reservierungsbits mit aufgedeckt (worüber David Chaum nichts sagt), so entlarvt dies den aktiven Angreifer allerdings.
- Kann ein Angreifer die für diese Aufdeckverfahren verwendete (von David Chaum nicht charakterisierte) Blockchiffre brechen, so kann er je nach (von David Chaum nicht definiertem) Verhalten der reservierenden Teilnehmerstationen und der verwendeten Blockchiffre möglicherweise
  a) ohne Aufdeckrisiko stören und
  b) sogar *nach* dem Senden gewählte Zeichen aufdecken lassen.

a) gilt, falls die Teilnehmerstationen nicht immer eine mögliche Aufdeckforderung senden oder bei sinnvollen Nachrichten falsche Bitpositionen verwenden und die verwendete Blockchiffre, wie z. B. DES, manche Abbildungen von Klar- auf Schlüsseltext ausschließt. Letzteres ist für $(2^{\text{Blocklänge}})! > 2^{\text{Schlüssellänge}}$ immer der Fall, vgl. Abschnitt 2.2.2.2.

b) gilt selbst *nach* dem Senden der Aufdeckforderung des Angreifers, falls die Blockchiffre alle möglichen Abbildungen von Klar- auf Schlüsseltext zuläßt. Anderenfalls kann der Angreifer nur vorher das bzw. die Zeichen beliebig wählen, das bzw. die er aufgedeckt haben will.

Bei ungünstiger Wahl von Teilnehmerverhalten und Blockchiffre gilt also sogar a) sowie b) mit nachträglicher Wahl des Angreifers.

Nach dem Gesagten ist klar, daß a) durch Ausführung des kombinierten Reservierungs- und Aufdeckverfahrens, wie es oben von mir beschrieben wurde, vermieden wird, sofern der Angreifer sinnvolle und bedeutungslose Nachrichten nicht unterscheiden kann. In [WaPf_89, WaPf1_89] werden Aufdeckverfahren beschrieben, die auch die Schwäche b) nicht haben. Die Forderungen A) und B) sind sogar in in der informationstheoretischen Modellwelt beweisbarer Form erfüllbar, wobei versucht werden sollte, diese Resultate auf weitere Klassen von Mehrfachzugriffsverfahren auszudehnen oder einen Beweis zu erbringen, daß dies nicht möglich ist.

Aufdeckverfahren für das DC-Netz können in kanonischer Weise auf RING- und BAUM-Netz übertragen werden.

Es sei darauf hingewiesen, daß, um ein Aufdecken zu ermöglichen, beim DC- und insbesondere beim RING- und BAUM-Netz – auch falls keine „Fehler“ auftreten – erheblicher zusätzlicher Aufwand zur Speicherung von Informationseinheiten nötig ist.

Im Rest dieses Abschnitts bleibt nun noch zu beschreiben, wie auf Dispute beim Aufdecken so reagiert werden kann, daß zumindest langfristig der „Schuldige“ bestraft wird.

Sind aus verläßlicher Quelle die *Übertragungen auf allen Leitungen bekannt* (z. B. bei ausschließlicher Verwendung eines physischen Broadcast-Mediums – im Gegensatz zu mit Hilfe von Protokollen realisierten Verteilnetzen, beispielsweise Ringen mit Punkt-zu-Punkt-Leitungen), so kann der aktive Angreifer beim MIX-Netz sicher entdeckt werden. (Beim RING- und BAUM-Netz natürlich auch, aber hier besteht der Witz der Verfahren gerade darin, daß niemand die Übertragungen auf allen Leitungen kennt.) Anders ist dies beim DC-Netz, da hier auch die von einer Station verwendeten Schlüssel bekannt sein müssen, um zu entscheiden, ob sie gesendet hat. Sind nicht alle Übertragungen auf Leitungen öffentlich bekannt, so kann derselbe Effekt dadurch erreicht werden, daß jede Station jede von ihr auf der Leitung gesendete Informationseinheit unterschreibt. Das Unterschreiben und Speichern von Unterschriften verursacht zwar einen erheblichen zusätzlichen Aufwand, erlaubt es aber, hinterher sicher festzustellen, was genau auf der Leitung übertragen wurde. (Ein Sonderfall liegt vor, wenn beide Stationen an einer Leitung Angreifer sind und gemeinsam lügen. Dann kann natürlich nicht festgestellt werden, was auf der Leitung übertragen wurde.)

Sind *nicht alle Übertragungen auf Leitungen bekannt und wird nicht jede Informationseinheit unterschrieben*, so können im MIX-, RING- und BAUM-Netz sowie im DC-Netz (dort über strittige gesendete Nachrichten oder strittige Schlüssel) drei Gruppen von Stationen identifiziert werden, wovon die erste Gruppe weder beschuldigt wird noch beschuldigt, während zumindest eins von beiden bei der zweiten und dritten Gruppe der Fall ist. Eine von ihnen ist der aktive Angreifer. Die andere ist unschuldig, wird aber vom Angreifer beschuldigt. Dabei wird davon ausgegangen, daß sich nur ein Angreifer im Kommunikationsnetz befindet, der aber mehrere Stationen besitzen oder unterwandert haben kann, und Widersprüche nur in der Umgebung des Angreifers vorkommen. Der Angreifer hat nur dann eine Chance, nicht

sofort ermittelt zu werden, wenn er wenige andere Stationen beschuldigt. Ansonsten spräche eine Mehrheit von zu Unrecht beschuldigten „ehrlichen“ Stationen gegen ihn. In diesem nicht entscheidbaren Fall jeweils weniger sich gegenseitig beschuldigender Stationen wird man normal weiterarbeiten, aber vorher so rekonfigurieren, daß sich im Wiederholungsfall diese wenigen Stationen nicht mehr gegenseitig beschuldigen können. Dies wird beispielsweise dadurch erreicht, daß

- beim MIX-Netz andere Wege (Adressen) verwendet werden, d. h. jeder Sender bildet Adressen nur noch so, daß keine Nachricht diese beiden MIXe direkt hintereinander passiert (dies geht auch bei MIX-zu-MIX-Verschlüsselung, vgl. Abschnitt 5.3.2.4).

- beim DC-Netz keine Schlüssel zwischen den beiden betroffenen Stationen mehr ausgetauscht werden (die vorhandenen Schlüssel werden entfernt). Eine Alternative wäre, daß jeweils beide Partner ihren gemeinsamen Schlüssel vor seiner Verwendung digital unterschreiben, so daß jeder Partner die Unterschrift des anderen hat. Dann kann bei gegenseitiger Beschuldigung von einem Dritten nach Vorlage der Unterschriften entschieden werden, welche Station im Unrecht ist [Cha3_85].
  An dem direkten Unterschreiben des gemeinsamen Schlüssels ist nachteilhaft, daß jeder der beiden einzeln – und damit möglicherweise ohne Wissen seines Partners – dann einem Dritten den Wert des gemeinsamen Schlüssels nicht nur mitteilen, sondern auch nachweisen kann, indem er die Unterschrift des anderen vorweist (seine eigene nützt nichts, da er selbst natürlich auch einen anderen, falschen Schlüssel unterschreiben könnte). Deshalb wird in [Chau_88 Seite 73f] vorgeschlagen, daß nicht der gemeinsame Schlüssel, sondern zwei Teile, deren Summe den Schlüssel ergibt und deren einer Teil zufällig gewählt ist, jeweils von einem der Partner unterschrieben werden. Um den Wert des gemeinsamen Schlüssels einem Dritten nachzuweisen, bedarf es nun – wie im Fall ohne Unterschriften – der Mitwirkung beider, da die Unterschrift jeweils von dem Partner angefordert werden muß, der sie nicht geleistet hat.

- beim RING- bzw. BAUM-Netz wird der Ring bzw. Baum rekonfiguriert. Dies ist bei einer Realisierung als virtueller Ring bzw. Baum, d. h. auf einem beliebigen Kommunikationsnetz wird ein logischer Ring bzw. Baum durch Verbindungs-Verschlüsselung zur Simulation der Unbeobachtbarkeit der Ring- bzw. Baum-Leitungen realisiert (was auf eine eigene Datenschutz-Schicht führt), sehr leicht möglich. Bei einer physischen Realisierung ist die Rekonfigurierung sehr aufwendig und daher kostenintensiv.

Ist ein Netzteilnehmer mehrfach in einer Gruppe, die eine andere beschuldigt oder von ihr beschuldigt wird, so wird er als der aktive Angreifer angesehen und aus dem Kommunikationsnetz ausgeschlossen. Dieses Verfahren ist nur dann praktikabel, wenn relativ wenige Netzteilnehmer aktive Angreifer sind. Ansonsten könnten die aktiven Angreifer zusammenarbeiten und die korrekt kommunizierenden Stationen aus dem Kommunikationsnetz ausschließen, wobei sie dann natürlich immer weniger Stationen zum Beobachten hätten.

5.9 Konzepte zur Realisierung von Fehlertoleranz und Anonymität

Zum Schluß dieses Kapitels sei noch auf die interessante Frage nach einer *Abwägung zwischen Fehlertoleranz* einerseits und *Anonymität* andererseits hingewiesen. Hier scheinen zwei grundlegend verschiedene Konzepte möglich zu sein.

Zum einen wird eine gesonderte Phase zur Fehlertoleranz eingeführt. Dadurch wird eine globale Sicht des Gesamtsystems erreicht, die die Fehlertoleranz erleichtert (vgl. die einleitende Bemerkung zu Beginn dieses Kapitels). In der Regel ist eine solche Realisierung jedoch wegen abrupter Unterbrechung der Nutzleistung unerwünscht. In der Phase zur Fehlertoleranz verwendete Schlüssel und Informationseinheiten können mit den während dem Nutzbetrieb verwendeten unverkettbar sein, so daß dann keine Abschwächung der Anonymität auftritt. Nicht diagnostizierbar und tolerierbar sind auf diese Weise Fehler (oder aktive Angriffe), die sich nur während des Nutzbetriebes ereignen.

Zum anderen kann die Fehlertoleranz aus Sicht des Netzbenutzers im Hintergrund, parallel zur anonymen Datenübertragung, ablaufen. Dies ist immer dann möglich, wenn Fehler ausgehend von einer lokalen Sicht des Gesamtsystems toleriert werden können. Solche die Anonymität abschwächende Maßnahmen wurden für das MIX-Netz (MIXe mit Reserve-MIXen sowie fehlertolerante Verschlüsselungsstruktur – nur der Zustand des benachbarten MIXes muß bekannt sein), das DC-Netz (senderpartitioniertes DC-Netz) sowie das RING- und BAUM-Netz (lokale Ring-bzw. Baumrekonfigurierung und indeterministische bzw. asymmetrische Protokolle) diskutiert und für hierarchische Netze angedeutet.